XXIII Congresso Ibero-americano de Direito e Informática 2019

Memórias

fiadi
FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES DE DERECHO E INFORMÁTICA

nic.br Núcleo de Informação e Coordenação do Ponto BR

cgi.br Comitê Gestor da Internet no Brasil

VISITE SÃO PAULO
HERE YOU FIND EVERYTHING YOU NEED

AASP Associação dos Advogados

IBDI INSTITUTO BRASILEIRO DE DIREITO DA INFORMÁTICA

UNIVERSIDADE DE SÃO PAULO FACULDADE DE DIREITO

Memórias do XXIII Congresso Ibero-Americano de Direito e Informática

Memorias del XXIII Congreso Ibero-Americano de Derecho e Informática

São Paulo

2019

FIADI A.C. y Luiz Fernando Martins Castro.

Creative Commons Atribución-NoComercial 4.0 Internacional (CC BY-NC 4.0)

https://creativecommons.org/licenses/by-nc/4.0/deed.es

Todos os direitos reservados.

Nenhuma parte deste livro pode ser utilizada ou reproduzida, em qualquer meio existente, sem autorização expressa do autor ou editora.

A editora não se responsabiliza por eventuais danos causados pelo mau uso das informações contidas neste livro.

Editora: Cia do eBook
Projeto editorial: Equipe Cia do eBook
ISBN: 978-85-5585-239-8

DADOS INTERNACIONAIS DE CATALOGAÇÃO NA PUBLICAÇÃO (CIP)

FIADI A.C. y Castro, Luiz Fernando Martins (organizador)
Memórias do XXIII Congresso Ibero-Americano de Direito e Informática / FIADI y Luiz Fernando Martins Castro (organizador). – Timburi, SP: Editora Cia do eBook, 2019.

Memorias del XXIII Congreso Ibero-Americano de Derecho e Informática / FIADI y Luiz Fernando Martins Castro (organizador). – Timburi, SP: Editora Cia do eBook, 2019. 737 p.

ISBN 978-85-5585-239-8

CDD 340

FIADI

Junta Diretiva período 2018-2021

Presidente: MARCELO BAUZÁ REILLY
Secretária: MARILIANA RICO CARRILO
Vice-Presidente de Relações Institucionais, Recursos Econômicos e Transparência: ERNESTO IBARRA SÁNCHEZ
Vice-Presidente de Formação e Desenvolvimento de Capital Humano: FEDERICO BUENO DE MATA
Vice-Presidente de Pesquisa e Inovação: BIBIANA LUZ CLARA

fiadi

FEDERACIÓN IBEROAMERICANA
DE ASOCIACIONES DE DERECHO
E INFORMÁTICA

IBDI

DIRETORIA EXECUTIVA
Presidente: ALYNE ANDRADE DE OLIVEIRA BEZERRA
Vice-Presidente: PAULO HENRIQUE ARAÚJO SANTIAGO REIS
Diretor-Geral: PAULO ROBERTO DE CARVALHO MACIEL
Diretor de Relações Internacionais: MANUEL DAVID MASSENO
Diretor Acadêmico: EDÉSIO CORDEIRO PONTES
Diretor Cultural: BRUNO JOSÉ COELHO TRIGUEIRO
Diretor de Internet: BRUNO PIRES MALAQUIAS
Diretor de Relações Institucionais: ANDRÉ HENRIQUE FONSECA

CONSELHO DE ADMINISTRAÇÃO
DURVAL JORGE PACHECO ALBERT
EDÉSIO CORDEIRO PONTES
FLÁVIO CLAUDEVAN DE GOUVEIA AMÂNCIO
GLADSTONE VALADARES VIEIRA RAMOS REINALDO
INALDO FERREIRA

CONSELHO CONSULTIVO
SERGIO PALOMARES
EURÍPEDES BRITO CUNHA JR.
LUIZ FERNANDO MARTINS CASTRO

INSTITUTO BRASILEIRO DE
DIREITO DA INFORMÁTICA

AASP – Associação dos Advogados de São Paulo

CONSELHEIROS
Dr. Antonio Carlos de Almeida Amendola
Dr. Antonio Carlos de Oliveira Freitas
Dr.ª Elaine Cristina Beltran Camargo
Dr.ª Flávia Hellmeister Clito Fornaciari Dórea
Dr. José Alberto Clemente Junior
Dr.ª Juliana Vieira dos Santos
Dr.ª Luciana Pereira de Souza
Dr.ª Paula Lima Hyppolito dos Santos Oliveira
Dr.ª Renata Mariz de Oliveira
Dr. Ricardo de Carvalho Aprigliano
Dr. Ricardo Pereira de Freitas Guimarães
Dr. Rodrigo Cesar Nabuco de Araujo
Dr. Ruy Pereira Camilo Junior

DIRETORES
Dr. Renato José Cury
Dr.ª Viviane Girardi
Dr.ª Fátima Cristina Bonassa Bucker
Dr. Mário Luiz Oliveira da Costa
Dr. Eduardo Foz Mange
Dr. Rogério de Menezes Corigliano
Dr. André Almeida Garcia
Dr.ª Silvia Rodrigues Pereira Pachikoski

AASP
Associação dos Advogados

FADUSP – Faculdade de Direito – Universidade de São Paulo

Estrutura administrativa – Faculdade de Direito do Largo São Francisco 2019 (USP)
Diretor: Prof. Titular Floriano de Azevedo Marques Neto
Vice-Diretor: Prof. Titular Celso Fernandes Campilongo

Chefes de Departamento
Direito Civil: Profa. Titular Silmara Juny de Abreu Chinellato
Direito Comercial: Prof. Associado Erasmo Valladão Azevedo e Novaes França
Direito do Trabalho e da Seguridade Social: Prof. Associado Jorge Luiz Souto Maior
Direito do Estado: Prof. Titular Virgilio Afonso da Silva
Direito Penal, Medicina Forense e Criminologia: Prof. Titular Renato de Mello Jorge Silveira
Direito Processual: Prof. Titular Flávio Luiz Yarshell
Direito Econômico, Financeiro e Tributário: Prof. Titular Luis Eduardo Schoueri
Direito Internacional e Comparado: Prof. Associado José Augusto Fontoura Costa
Teoria e Filosofia do Direito: rof. Titular. José Reinaldo de Lima Lopes

Presidentes de Comissões
Comissão de Graduação: Profa. Associada Maria Paula Dallari Bucci
Comissão de Pós-Graduação: Prof. Titular Fernando Facury Scaff
Comissão de Pesquisa: Profa. Assoc. Nina Beatriz Stocco Ranieri
Comissão de Cultura e Extensão Universitária: Profa. Associada Cláudia Perrone Moisés

Professores
Alamiro Velludo Salvador Netto
Alberto do Amaral Junior
Alessandro Serafin Octaviani Lui
Alexandre de Moraes
Alysson Leandro Barbate Mascaro
Ana Elisa Liberatore Silva Bechara
Ana Maria de Oliveira Nusdeo
André de Carvalho Ramos
Andre Ramos Tavares
Antonio Carlos Marcato

Antonio Carlos Morato
Antonio Claudio da Costa Machado
Antonio Rodrigues de Freitas Junior
Ari Marcelo Solon
Balmes Vega Garcia
Bernardo Bissoto Queiroz de Moraes
Calixto Salomão Filho
Camila Villard Duran
Carlos Alberto Carmona
Carlos Alberto Dabus Maluf
Carlos Alberto de Salles
Carlos Bastide Horbach
Carlos Pagano Botana Portugal Gouvêa
Celso Fernandes Campilongo
Claudia Perrone Moises
Claudio Luiz Bueno de Godoy
Conrado Hubner Mendes
Cristiano de Sousa Zanetti
Darcio Roberto Martins Rodrigues
David Teixeira de Azevedo
Diogo Rosenthal Coutinho
Eduardo Carlos Bianca Bittar
Eduardo Cesar Silveira Vita Marchi
Eduardo Secchi Munhoz
Eduardo Tomasevicius Filho
Elival da Silva Ramos
Elizabeth de Almeida Meirelles
Elza Antonia Pereira Cunha Boiteux
Eneas de Oliveira Matos
Enoque Ribeiro dos Santos
Enrique Ricardo Lewandowski
Erasmo Valladao Azevedo e Novaes Franca
Estevao Horvath
Estevao Mallet
Eunice Aparecida de Jesus Prudente
Fernando Campos Scaff
Fernando Dias Menezes de Almeida
Fernando Facury Scaff
Flávio Luiz Yarshell
Flávio Roberto Batista
Floriano Peixoto de Azevedo Marques Neto
Francisco Paulo De Crescenzo Marino
Francisco Satiro de Souza Junior
Geraldo Miniuci Ferreira Junior
Gilberto Bercovici
Giselda Maria Fernandes Novaes Hironaka
Guilherme Assis de Almeida
Guilherme Guimarães Feliciano
Gustavo Ferraz de Campos Monaco
Gustavo Henrique Justino de Oliveira
Gustavo Henrique Righi Ivahy Badaró
Heitor Vitor Mendonça Fralino Sica
Helcio Maciel França Madeira
Helena Regina Lobo da Costa
Heleno Taveira Torres
Homero Batista Mateus da Silva
Humberto Bergmann Ávila
Ignacio Maria Poveda Velasco
Janaina Conceição Paschoal
Jean Paul Cabral Veiga da Rocha
Joao Alberto Schutzer Del Nero
Jorge Luiz Souto Maior
José Augusto Fontoura Costa
José Carlos Baptista Puoli
Jose Eduardo Campos de Oliveira Faria
José Fernando Simão
José Levi Mello do Amaral Júnior
Jose Luiz Gaviao de Almeida
José Marcelo Martins Proença
José Maria Arruda de Andrade
José Mauricio Conti
José Raul Gavião de Almeida
Jose Reinaldo de Lima Lopes
Jose Roberto dos Santos Bedaque
Jose Tadeu de Chiara
Juliana Krueger Pela
Juliano Souza de Albuquerque Maranhão
Luciano Anderson de Souza

Luis Eduardo Schoueri
Luís Fernando Massonetto
Luís Virgílio Afonso da Silva
Manoel de Queiroz Pereira Calças
Mara Regina de Oliveira
Marcelo José Magalhães Bonizzi
Marcelo Vieira von Adamek
Marco Fabio Morsello
Marcos Alexandre Coelho Zilli
Marcos Augusto Perez
Marcos Paulo Verissimo
Marcus Orione Goncalves Correia
Maria Cristina da Silva Carmignani
Maria Paula Dallari Bucci
Maria Thereza Rocha de Assis Moura
Mariângela Gama de Magalhães Gomes
Maristela Basso
Marta Cristina Cury Saad Gimenes
Masato Ninomiya
Mauricio Stegemann Dieter
Maurício Zanoide de Moraes
Monica Herman Salem Caggiano
Nelson Mannrich
Nestor Duarte
Newton de Lucca
Nina Beatriz Stocco Ranieri
Oreste Nestor de Souza Laspro
Orlando Villas Bôas Filho
Otavio Luiz Rodrigues Junior
Otavio Pinto e Silva
Patricia Faga Iglecias Lemos
Paula Andrea Forgioni
Paulo Ayres Barreto
Paulo Borba Casella
Paulo Eduardo Vieira de Oliveira
Paulo Fernando Campos Salles de Toledo
Paulo Henrique dos Santos Lucon
Pierpaolo Cruz Bottini
Priscila Maria Pereira Correa da Fonseca
Rafael Diniz Pucci
Rafael Mafei Rabelo Queiroz
Renato de Mello Jorge Silveira
Ricardo de Barros Leonel
Roberto Augusto Castellanos Pfeiffe
Roberto Augusto de Carvalho Campos
Roberto Quiroga Mosquera
Rodrigo Octávio Broglia Mendes
Rodrigo Pagani de Souza
Roger Stiefelmann Leal
Ronaldo Lima dos Santos
Ronaldo Porto Macedo Júnior
Samuel Rodrigues Barbosa
Sebastiao Botto de Barros Tojal
Sergio Pinto Martins
Sergio Salomão Shecaira
Sheila Christina Neder Cerezetti
Silmara Juny de Abreu Chinellato
Susana Henriques da Costa
Vinicius Marques de Carvalho
Vitor Rhein Schirato
Wagner Luiz Menezes Lino

CGI-NIC

CONSELHEIROS (AS)

01.- Maximiliano Salvadori Martinhão/MCTIC
02.- Luiz Fernando Martins Castro/MCTIC
03.- Antonio José Barreto de Araújo Júnior/Casa Civil
04.- Rafael Henrique Rodrigues Moreira/MDIC
05.- Luis Felipe Salin Monteiro/MPDG
06.- Franselmo Araújo Costa/MD
07.- Leonardo Euler de Moraes-Suplente/ANATEL
08.- Thiago Camargo Lopes/CNPq
09.- Claudio Benedito Silva Furtado/CONSECTI
10.- Demi Getschko
11.- Eduardo Fumes Parajo
12.- Eduardo Levy Cardoso Moreira
13.- Henrique Faulhaber Barbosa
14.- Nivaldo Cleto
15.- Thiago Tavares Nunes de Oliveira
16.- Percival Henriques de Souza Neto
17.- Flávia Lefèvre Guimarães
18.- Tanara Lauschner
19.- Sérgio Amadeu da Silveira
20.- Marcos Dantas Loureiro
21.- José Luiz Ribeiro Filho

Observador MRE

Achilles Emilio Zaluar Neto

Diretores NIC.br

Hartmut Richard Glaser
Frederico A.C. Neves
Milton Kaoru Kawashikura
Ricardo Narchi

nic.br
Núcleo de Informação e Coordenação do Ponto BR

cgi.br
Comitê Gestor da Internet no Brasil

ABERTURA

O XXIII Congresso Iberoamericano de Direito e Informática, tradicional certame científico promovido pela FIADI – Federação Iberoamericana das Associações de Direito e Informática (www.fiadi.or) foi realizado pela primeira vez em território brasileiro, na Cidade de São Paulo - SP, entre os dias 01 e 04/10/2019.

O Congresso teve por local de realização a tradicional Faculdade de Direito do Largo de São Francisco (FADUSP), e a moderna e bem equipada sede da AASP – Associação dos Advogados de São Paulo.

Realizados desde 1984, os Congressos da FIADI têm assumido especial interesse, dada a crescente importância dos temas jurídicos ligados à tecnologia, direito digital e ao uso global da internet, e seus impactos na sociedade.

Tendo atraído centenas de profissionais de todo o Brasil, bem como de vários países ibero-americanos, de diferentes especialidades, o Congresso abordou temas ligados relacionados a:

- Desafios legais da sociedade em rede,
- Governança da Internet,
- Cibersegurança e Confiança na Economia Digital
- Inteligência Artificial,
- Impactos das tecnologias disruptivas: Indústria 4.0, IoT e Smart Cities, Relações de Trabalho,
- Startups, Fintechs, Legal Techs, E-commerce,
- Direitos Humanos, Educação e Democracia na rede,
- Direitos Intelectuais na era Digital, Aplicativos e Softwares,
- Nova Lei Brasileira de Proteção de Dados Pessoais (LGPD) e GDPR,
- Processo Eletrônico e Prova Digital,
- Jurimetria e Justiça Preditiva.

O rigor acadêmico dos trabalhos apresentados por dezenas de pesquisadores e estudiosos, colecionados nestas Atas, foi assegurado pelo criterioso processo seletivo dos artigos acadêmicos, com o apoio de renomados professores brasileiros e estrangeiros.

De especial importância foi o apoio dado ao Congresso, e aos seus eventos preparatórios, pelo CGI.br – Comitê Gestor da Internet no Brasil (www.cgi.br), órgão multisetorial responsável pelos nomes de domínio sob o ponto BR (.br), e pela governança da internet no país.

Este Congresso ficará registrado positivamente na memória de todos que dele participaram, tendo sido uma oportunidade preciosa, e mesmo única, para que profissionais e especialistas da área pudessem trocar experiências e aprofundar o conhecimento acerca de matéria tão atual e relevante.

Comitê Organizador do Congresso:
Luiz Fernando Martins Castro (Presidente)
Andrea Campos de Almeida de Castro Monteiro (Secretária-Geral)
André Almeida Garcia
Carlos Medina Guerrero
Federico Bueno de Mata
Maria Pérez Pereira
Mariliana Rico
Yoselin Vos

Comitê Científico do Congresso:
Otávio Luiz Rodrigues Jr. (Presidente)
Bibiana Beatriz Luz Clara (Secretária-Geral)
María Pérez Pereira
Yarina Amoroso Fernández
Miguel Arrieta Zinguer
Marcelo Bauza Reilly
Eurípedes Brito Cunha Jr.
Tania Cristina D'Agostini Bueno
Federico Bueno de Mata
Lorenzo Cotino Hueso
Hallrison Souza Dantas
Horacio Fernández Delpech
Myrna García Barrera
José Caldas Góis Jr.
Ernesto Ibarra Sanchez
Têmis Limberger
Laura Nahabetian Brunet
Inácio Maria Poveda Velasco
Patricia Reyes Olmedo
Mariliana Rico Carrillo
José Luis Romo Santana
Vilma Sánchez del Castillo

APERTURA

El XXIII Congreso Iberoamericano de Derecho e Informática, tradicional evento científico promovido por la FIADI – Federación Iberoamericana de Asociaciones de Derecho e Informática (www.fiadi.org) fue llevado a cabo por primera vez en territorio brasileño, en la Ciudad de San Pablo – SP, entre los días 01 y 04/10/2019.

El Congreso tuvo como sedes la tradicional Facultad de Derecho de Largo de San Francisco (FADUSP), y la moderna y bien equipada sede de la AASP – Asociación de Abogados de San Pablo.

Realizados desde 1984, los Congresos de la FIADI concitan especial interés, dada la creciente importancia de los temas jurídicos ligados a tecnología, derecho digital y el uso global de la internet, y sus impactos en la sociedad.

Atrayendo centenas de profesionales de todo el Brasil, así como de varios países ibero-americanos, de diferentes especialidades, el Congreso abordó temas relacionados a:

- Desafíos legales de la sociedad en red,
- Gobernanza de la internet,
- Ciberseguridad y Confianza en la Economía Digital,
- Inteligencia Artificial,
- Impactos de las tecnologías disruptivas: Industria 4.0, IoT y Smart Cities, Relaciones de Trabajo,
- Startups, Fintechs, Legal Techs, E-commerce,
- Derechos Humanos, Educación y Democracia en la red,
- Derechos Intelectuales en la era Digital, Aplicativos y Softwares,
- Nueva Ley Brasileña de Protección de Datos Personales (LGPD) y GDPR,
- Proceso Electrónico y Prueba Digital,
- Jurimetría y Justicia Predictiva.

El rigor académico de los trabajos presentados por decenas de investigadores y estudiosos, presentados en estas Actas, fue asegurado por el criterioso proceso selectivo de los artículos académicos, con el apoyo de renombrados profesores brasileños y extranjeros.

De especial importancia fue el apoyo dado al Congreso, y a sus eventos preparatorios, por el CGI.br – Comité Gestor de Internet de Brasil (www.cgi.br), órgano multisectorial responsable para los nombres de dominio sobre el punto BR (.br), y para la gobernanza de internet en el país.

Este Congreso quedará registrado positivamente en la memoria de todos sus participantes, habiendo sido una oportunidad preciosa e incluso única, para que profesionales y especialistas del área pudiesen intercambiar experiencias y profundizar el conocimiento de materia tan actual y relevante.

Comité Organizador del Congreso:
Andrea Campos de Almeida de Castro Monteiro (Secretaria-General)
André Almeida Garcia
Carlos Medina Guerrero
Federico Bueno de Mata
Maria Pérez Pereira
Mariliana Rico
Yoselin Vos

Comité Científico del Congreso:
Otávio Luiz Rodrigues Jr. (Presidente)
Bibiana Beatriz Luz Clara (Secretaría-General)
Yarina Amoroso Fernández
Miguel Arrieta Zinguer
Marcelo Bauza Reilly
Eurípedes Brito Cunha Jr.
Tania Cristina D'Agostini Bueno
Federico Bueno de Mata
Lorenzo Cotino Hueso
Hallrison Souza Dantas
Horacio Fernández Delpech
Myrna García Barrera
José Caldas Góis Jr.
Ernesto Ibarra Sánchez
Têmis Limberger
Laura Nahabetián Brunet
Inácio Maria Poveda Velasco
Patricia Reyes Olmedo
Mariliana Rico Carrillo
José Luis Romo Santana
Vilma Sánchez del Castillo

ÍNDICE

DESAFIOS LEGAIS DA SOCIEDADE EM REDE
..... 23

Alexis German Antoniucci Luz Clara
"PROTECCION DE LOS DATOS EN LAS REDES SOCIALES"
axe_antoniucci@hotmail.com
País de Origem: Argentina
..... 24

Mariel Alejandra Suárez
"LA INFLUENCIA DIGITAL"
masuarez@juschubut.gov.ar
País de Origem: Argentina
..... 31

Oscar Rodrigo Paredes Fernández
"REGULACIÓN DE LA "ECONOMÍA NARANJA" O "ECONOMÍA CREATIVA" LA LEY NARANJA COLOMBIANA"
oscarparedes@upb.edu
País de Origem: Colombia
..... 45

Jacqueline Guerrero Carrera; Diómedes E. Palacios
"UNA COMUNIDAD GLOBAL PARA LA CIUDADANÍA DIGITAL"
jacqueline.guerrero@udla.edu.ec
País de Origem: Ecuador
..... 59

Rodrigo Alejandro Gómez Torre
"LA CAPACIDAD PROGRESIVA DE LOS MENORES DE EDAD FRENTE A LA UTILIZACIÓN NO CONSENTIDA DE SU IMAGEN EN REDES SOCIALES"
rgomeztorre@usal.es
País de Origem: Espanha
..... 70

Glenda Gonçalvez Gondim; Emanuella Regina Leal da Silva
"DESAFIOS DA APLICABILIDADE DO DEVER DE ESQUECIMENTO AOS PROVEDORES DE BUSCA"
glendagondim@hotmail.com
País de Origem: Brasil
..... 80

Jânia Saldanha; Lucas Silva de Souza
"O DISCURSO ODIOSO NA SOCIEDADE EM REDE: DO ABUSO DA LIBERDADE DE EXPRESSÃO À IDENTIDADE REFÚGIO"
Adv.lucassouza@gmail.com
País de Origem: Brasil
..... 91

Sonia Patricia Cortés Zambrano
"EL ESTADO Y SU ROL EN LA REVOLUCIÓN 4.0 Y EL CAPITALISMO DE DATOS"
País de Origem: Chile
..... 103

GOVERNANÇA DA INTERNET
..... 116

Luiz Fernando Martins Castro
"A GOVERNANÇA DA INTERNET NO BRASIL"
lf@mcma.com.br
País de Origem: Brasil
..... 117

Cynthia Raquel Rudas Murga
"ANÁLISIS JURÍDICO-POLÍTICO DE LA GOBERNANZA DE INTERNET Y LA EFICACIA DE LOS DERECHOS HUMANOS EN PERÚ"
work_crrm@hotmail.com ; dra.crrm@outlook.com
País de Origem: Perú
..... 130

CIBERSEGURANÇA
..... 142

Gustavo Adolfo Amoni Reverón
"INTERCEPACIÓN Y DIFUSIÓN NO AUTORIZADAS DE LAS AUDIENCIAS TELEMÁTICAS ANTE LA SALA DE CASACIÓN PENAL VENEZOLANA"
gustavoamoni@hotmail.com
País de Origem: Venezuela
..... 143

José Luis Romo Santana; Jonathan Marcelo Ramos Mera
"CIBERDELINCUENCIA EN LA LEGISLACIÓN PENAL ECUATORIANA A LA LUZ DEL CÓDIGO ORGÁNICO INTEGRAL PENAL (2014)"
josepepers@hotmail.com
País de Origem: Ecuador
..... 155

Katty Pérez Ordóñez
"CIBERSEGURIDAD VS CIBERDELINCUENCIA"
katty.perez.30@hotmail.com
País de Origem: Perú
..... 179

Humberto Martín Ruani
"LOS ESTADOS, LAS CRIPTOMONEDAS Y LA CIBERSEGURIDAD"
hruani@hotmail.com
País de Origem: Argentina
..... 192

Federico Bueno de Mata
"USO DE DRONES POR POLICÍA Y JUECES PARA LA INVESTIGACIÓN DE DELITOS"
febuma@usal.es
País de Origem: España
..... 203

INTELIGENCIA ARTIFICIAL, E LEGAL TECHS
..... 215

José Heriberto García Peña
"PYME O STARTUP: ¿LA FORMA ES FONDO? BASES LEGALES EN SU ORGANIZACIÓN ACTUAL"
jhgarcia@tec.mx; jhgarcia@itesm.mx
País de Origem: Cuba-México
..... 216

Alberto Enrique Nava Garcés; Juliette Núñez Ruiz
"LAS OPERACIONES CON RECURSOS DE PROCEDENCIA ILÍCITA Y LAS FINTECH " (RESPONSABILIDAD PENAL DE LAS PERSONAS MORALES)"
iusnava@yahoo.com.mx
País de Origem: México
..... 239

Manuel Leonardo Prada Rodríguez
"VALORACIÓN CRÍTICA DE PROMETEA, A LA LUZ DE LA FILOSOFÍA DE LA MENTE DE JOHN SEARLE"
manuelprada@usantotomas.edu.co
País de Origem: Colombia
..... 256

Lucana María Estévez Mendoza
"REGULACIÓN DE LA INTELIGENCIA ARTIFICIAL Y LA PROTECCIÓN DE LOS DERECHOS FUNDAMENTALES EN LA CUARTA REVOLUCIÓN INDUSTRIAL"
lucana@ceu.es
País de Origem: España
..... 266

Graciela Cami Soria
"LOS NUEVOS MODELOS DE NEGOCIOS Y LA APLICACIÓN DEL PRINCIPIO DE PRE-VENCION DE OPERACIONES ILICITAS DESAFIOS Y RESPONSABILIDADES"
escribaniacami@gmail.com
País de Origem: Uruguay
..... 279

Olivia Andrea Mendoza Enríquez
"DIGNIDAD HUMANA, DERECHOS HUMANOS Y TECNOLOGÍA: NUEVOS DESAFÍOS A PARTIR DEL DESARROLLO Y USO DE ALGORITMOS"
olivia.mendoza@infotec.mx
País de Origem: México
..... 290

Sebastián Carlos Chumbita
"INTELIGENCIA ARTIFICIAL APLICADA AL SISTEMA DE REVISIÓN JUDICIAL. EL CASO DE LA SUPREMA CORTE DE JUSTICIA DE LA PROVINCIA DE BUENOS AIRES COMO MODELO DE IMPLEMENTACIÓN"
schumbita@hotmail.com
País de Origem: Argentina
..... 303

Angie Verónica Rubio Velásquez
"IA EN CONTACTO CON EL DERECHO"
angie.rubio@usantotomas.edu.co
País de Origem: Colombia
..... 314

Julio Núñez Ponce
"CROWDFUNDING EN EL DERECHO DE LAS NUEVAS TECNOLOGIAS EN EL PERU: IMPLICANCIAS JURIDICAS DEL FINANCIAMIENTO PARTICIPATIVO FINANCIERO POR INTERNET"
julionunezponce@gmail.com
País de Origem: Perú
..... 323

Ana Karin Chávez Valdivia
"IMPLICANCIAS JURIDICAS DE LA NUEVA GENERACION DE SISTEMAS ROBOTICOS INTELIGENTES: ROBOTS SOCIALES Y ESTEREOTIPOS CULTURALES"
achavez@ulasalle.edu.pe
País de Origem: Perú
..... 345

Rodrigo Cortés Borrero; Paola Consuelo Ramos Martínez
"DISCRIMINACIÓN 4.0: LA INTELIGENCIA ARTIFICIAL COMO UN DESAFÍO DE GÉNERO
rodrigocortes@usantomas.edu.co; paolaramosmartinez@hotmail.com
País de Origem: Colombia
..... 359

Manuel Martín Pino Estrada
"INTELIGÊNCIA ARTIFICIAL E DESEMPREGO"
martinpino@yahoo.com
País de Origem: Brasil
..... 375

Antonio Martino
"INTELIGENCIA ARTIFICIAL Y DERECHO"
aamartino@gmail.com
País de Origem: Argentina
..... 386

Ernesto Ibarra Sánchez
"INTELIGENCIA ARTIFICIAL Y INNOVACIÓN JURÍDICA"
País de Origem: Mexico
..... 406

Laura Nahabetián Brunet
"TIEMPO DE ALGORITMOS: ALGOCRACIA Y DERECHOS CIVILES Y POLÍTICOS"
lnahabetian@gmail.com
País de Origem: Uruguay
..... 426

INDUSTRIA 4.0, CIDADES INTELIGENTES E IoT
..... 444

Nayibe Chacón Gómez
"LAS TECNOLOGÍAS DISRUPTIVAS: LOS RETOS A LA PROTECCIÓN DE DATOS"
nayibechacon@yahoo.es
País de Origem: Venezuela
..... 445

Felipe Miguel Carrasco Fernández
"EL TRABAJO EN LA INDUSTRIA 4.0., RETOS JURÍDICO-LABORALES"
felipemiguel.carrasco@upaep.mx
País de Origem: México
..... 456

Têmis Limberger; Gustavo da Silva Santanna
"INTERNET DAS COISAS E A OBSERVÂNCIA AO DIREITO À PRIVACIDADE DO CIDADÃO"
temis@mprs.mp.br
País de Origem: Brasil
..... 466

TELETRABALHO
..... 477

Danny Alejandra Cuevas López
"LOS ELEMENTOS ESENCIALES DEL CONTRATO DE TRABAJO EN LAS NUEVAS FORMAS LABORALES EN UN MUNDO GLOBALIZADO - CALL CENTERS, AIRBNB Y UBER"
dannycuevas111@gmail.com
País de Origem: Colombia
..... 478

Oscar Rodrigo Paredes Fernández
"DESARROLLADORES DE APLICACIONES, LA "FUERZA LABORAL" DE GOOGLE".
oscarparedes@upb.edu
País de Origem: Colombia
..... 489

Sulmer Paola Ramírez
"ANÁLISIS DEL TELETRABAJO COMO FORMA DE PRESTACIÓN DE SERVICIO"
sulmerp@yahoo.com
País de Origem: Venezuela
..... 504

E-COMMERCE
..... 518

Antonio Faúndez-Ugalde; María Teresa Blanco Lobos; Mario Pino Moya
"ESTADOS UNIDOS VERSUS CHINA FRENTE A LOS DESAFÍOS FISCALES DE LA OCDE Y EL G-20 EN EL E-COMMERCE"
Antonio.faundez@pucv.cl
País de Origem: Chile
..... 519

Edda Karen Céspedes Babilón
"EL IMPACTO DEL DINERO ELECTRÓNICO EN LA INCLUSIÓN FINANCIERA – REALIDAD PERUANA"
kcespedes@infonegocio.net.pe
País de Origem: Perú
..... 531

DIREITOS INTELECTUAIS NA ERA DIGITAL, APLICATIVOS E SOFTWARES
..... 543

Diego Adrián Moreno Carrasco
"RESGUARDO DE LA PROPIEDAD INTELECTUAL Y LA INFORMACIÓN EN ACTIVIDADES DE I+D Y LEY DE ACCESO A LA INFORMACIÓN PÚBLICA EN CHILE: ANÁLISIS DE CASOS"
damorenoc@gmail.com
País de Origem: Chile
..... 544

Julia Rugno; Rafael Stefanini Auilo
"OS MÉTODOS ONLINE DE RESOLUÇÃO DE DISPUTAS COMO INSTRUMENTOS DE ACESSO À ORDEM JURÍDICA JUSTA: EXPERIÊNCIA E DESAFIOS."
juliarugno02@gmail.com; Rafael.Stefanini@lefosse.com
País de Origem: Brasil
..... 556

Horacio Fernandez Delpech
"RETRIBUCION DE LOS AUTORES POR LA REPRODUCCION DIGITAL DE SUS OBRAS EN INTERNET"
hofede@hotmail.com
País de Origem: Argentina
..... 569

NOVA LEI DE PROTEÇÃO DE DADOS PESSOAIS E GDPR
..... 581

Antonio Carlos Efing; Eduarda Alencar Maluf Kiam
"UMA ANÁLISE DO DIREITO AO ESQUECIMENTO NO DIREITO BRASILEIRO"
ace@eradv.com.br; Eduarda_kiame@hotmail.com
País de Origem: Brasil
..... 582

Taynara Arceno; Fernada Cantali
"GERAÇÕES DE LEIS DE PROTEÇÃO DE DADOS: UM PANORAMA"
País de Origem: Brasil
..... 595

Nicolas Addor; Cinthia Obladen de Almendra Freitas; Miriam Olivia Knopik Ferraz
"A GDPR E SUA INFLUÊNCIA NO ORDENAMENTO JURÍDICO BRASILEIRO"
nicolasaddor@gmail.com; cinthia@ppgia.pucpr.br
País de Origem: Brasil
..... 607

Mártin M. Szinvelski
"AS GARANTIAS DE INDEPENDÊNCIA DAS AUTORIDADES DE PROTEÇÃO DE DADOS: VISÃO COMPARADA ENTRE O REGULAMENTO DA UNIÃO EUROPEIA E A LGPD"
martin_ms@live.com.
País de Origem: Brasil
..... 619

Pedro Bastos Lobo Martins
"CATEGORIZANDO DADOS EM UM CONTEXTO DE BIG DATA: EM DEFESA DE UMA ABORDAGEM FUNCIONAL"
pedroblmartins@gmail.com
País de Origem: Brasil
..... 633

PROCESSO ELETRONICO E PROVA DIGITAL
..... 644

José Francisco Vega Sacasa
"EL DERECHO CRIPTOGRÁFICO"
jfvega@j-vega.com
País de Origem: Panamá
..... 645

João Felipe Fernandes de Souza
"O SISTEMA JUDICIAL ELETRÔNICO E OS BENEFÍCIOS QUE O USO DO INSTRUMENTO DO BLOCK CHAIN PODERIA OCASIONAR NA INSTRUMENTALIZAÇÃO DOS PROCESSO E CONTRATOS"
Joao.souza94@hotmail.com
País de Origem: Brasil
..... 656

Marcos da Costa
"IMPACTO DA TECNOLOGIA SOBRE A JUSTIÇA"
País de Origem: Brasil
..... 664

Sabrina Rodrigues Santos
"COOPERAÇÃO JURÍDICA INTERNACIONAL NA PRODUÇÃO DE PROVA DIGITAL – CASO MERCOSUL"
Sabrinars13@uol.com.br
País de Origem: Brasil
..... 673

Bibiana Luz Clara
"EL PROCESO ELECTRÓNICO EN ARGENTINA"
luzbibianaclara@gmail.com
País de Origem: Argentina
..... 686

JURIMETRIA E JUSTIÇA PREDITIVA
..... 692

María Paula Castellanos Peña
"PROMETEA: JUSTICIA DIGITAL AL SERVICIO DE LA COMUNIDAD"
mariacastellanosp@usantotomas.edu.co
País de Origem: Colombia
..... 693

Audilio Gonzalez; Ana María Sanabria Clavijo
"LA JUSTICIA PREDICTIVA: ENTRE MITO Y REALIDAD"
audilio.gonzales@gmail.com
País de Origem: França
..... 703

Yarina Amoroso Fernández; Eliober Cleger Despaigne; Ayrat Faridovich Hasyanov; Carlos Rafael Rodríguez
"ONTOLOGÍAS JURÍDICAS: TECNOLOGÍAS PARA LA REUTILIZACIÓN Y LA INTEROPERABILIDAD ENTRE FUENTES HETEROGÉNEAS DE CONOCIMIENTO DEL ÁMBITO JURÍDICO"
yarina@uci.cu
País de Origem: Cuba
..... 725

DESAFIOS LEGAIS DA SOCIEDADE EM REDE

PROTECCION DE LOS DATOS EN LAS REDES SOCIALES

Eje Temático: Desafíos legales y éticos de la Sociedad Digital en Red

Autor:
Alexis German Antoniucci Luz Clara
Licenciado Procurador Ufasta, Mar del Plata, Buenos Aires Argentina. Ayudante de Trabajos Prácticos en las Materias de Derecho y Aspectos profesionales Ucaece Mar del Plata, Buenos Aires Argentina.

PALABRAS CLAVE:
Redes, Sociales, Protección, Datos, Usuarios, Privacidad, Plataformas

RESUMEN
Si bien hoy en día se toma como algo habitual el hecho de que nuestra información esté en las redes, estamos expuestos a los riesgos que el entorno electrónico nos ofrece. Se tiene la idea de que todo aquello que encontramos en las redes sobre nosotros fue subido por nosotros y es bueno, pero, ¿y si no fuese así? ¿Tenemos pleno control sobre nuestros datos en las redes?

ABSTRACT
Although nowadays it is taken as usual the fact that our information is on the networks. We are exposed to the risks that the electronic environment offers us. We have the idea that everything that we find in the networks about us was uploaded by us and it is good, but, and if it were not so. Do we have full control over our data in the networks?

1.1: INTRODUCCION

La masividad con que las redes sociales se dan en la sociedad es cada vez más abrumadora, esto lleva intrínseco que las personas se expongan de forma más violenta a la naturalización de tener que volcar información personal tanto pública como privada en favor de lograr una mejor experiencia plataforma – usuario.

La sobre exposición hace que nos veamos muy propensos a la posibilidad de caer en una desprotección de los derechos, y hablando en el caso concreto, sobre todo aquellos que traen aparejados el uso, almacenamiento, y recolección de datos.

En un entorno jurídico donde las leyes buscan reparar los daños causados (forma reparadora), y no se conciben junto con la tecnología para evitar que se produzcan daños (forma preventiva).

Se da el peligroso hecho de la auto determinación y reglamentación de forma totalmente discrecional del uso y tratamiento de los datos de los usuarios de estas redes. Esto, choca con las distintas leyes que se sancionan haciendo inevitable la modificación y ajuste de las modalidades empleadas a la adecuación de la nueva norma vigente.

2.: DATOS Y PAUTAS

2.1: Instancias de Proteccion de los Datos

En todo aquel momento, en que a los usuarios se les solicita por parte de la red proporcionar datos personales, se los ponen en una posición muy vulnerable. Se analizan estos estadios desde el punto de vista de la relación usuario-empresa. Pudiendo entonces desprender tres etapas clave y diferenciadas que se asimilan a las etapas contractuales (precontractual, contractual y post contractual).

Una primera aproximación, se da al momento de crear la cuenta donde al usuario se le exige para poder hacerse de su respectivo perfil, sin los cuales no se le permite operar. La única alternativa seria no crear en dicha red un perfil, y así resguardar los datos solicitados. Dentro de este "contrato" se tiene que determinar muy bien el uso, finalidad, alcance entre otras cualidades, de la manipulación de los datos que se están brindando. Por lo general se lo realiza en una ventana donde nos muestra todas las condiciones y políticas de privacidad la cual sólo se necesita aceptar.

Claro está, en este punto, que son escasas las personas que se detienen realmente a tomar conciencia de la modalidad, alcance y dimensiones que sus datos van a adquirir.

Luego, que el usuario realizó con éxito la creación de su perfil, se puede diferenciar otra instancia. En este caso, ya no se le solicita de manera necesaria al usuario la información, sino que éste mismo, de manera desinteresada quien comparte información tanto propia como de terceros en la plataforma utilizando las herramientas que se le proveen. Por otro lado, también el empleo e instalación de cookies[1], proporciona información sin que, en la mayoría de los casos, los usuarios se den cuenta, y en consecuencia, sin brindar su consentimiento.

En esta segunda instancia de constante interacción con la red, se pueden dar otros riesgos que conllevan los datos, como la utilización de la información para bases de correos comerciales o (SPAM), y se podría también llegar al hecho de utilizar la información del usuario para una posible suplantación de identidad.

La última fase que se desprende del hecho de la interacción de los usuarios con las plataformas de redes sociales, es obviamente, el dejar de ser usuario y pretender dar de baja la cuenta creada a tal fin. Los problemas que se generan en esta etapa son la imposibilidad en algunos casos, de concretar la baja efectiva de todos los datos y de la cuenta. En el caso de poder lograr la baja efectiva queda aún pendiente el control sobre la conservación de los datos que mantiene el servicio y con ello el cumplimiento

1 Una cookie es un archivo creado por un sitio web que contiene pequeñas cantidades de datos y que se envían entre un emisor y un receptor. En el caso de Internet el emisor sería el servidor donde está alojada la página web y el receptor es el navegador que usas para visitar cualquier página web.

de la calidad del tratamiento. Aquellos datos que se mantengan una vez dada de baja la cuenta, pasarían a ser conservados sin el consentimiento del usuario, ya que, al darse de baja como usuario, expone una inequívoca intención de cesar con la relación contractual.

La vulneración de este derecho de protección de datos en el ámbito de las redes sociales trae aparejado una responsabilidad civil objetiva. Esta exigencia no va a excluir ni dejar sin efecto la posibilidad del titular de pedir el acceso, rectificación y cancelación de estos datos frente al titular de la base de datos que tiene que está debidamente registrada para poder operar.

Estos afectados o interesados de forma legítima sobre los datos en conflicto, se encuentran facultados para conocer y acceder a las informaciones que les pudieran afectar, archivadas en bancos de datos, y controlar su calidad, permitiendo que puedan ser corregidos o cancelen los datos inexactos o indebidamente procesados, y la disposición sobre su transmisión.

2.2: Las Pautas Básicas del RGPD en las Distintas Plataformas

Se obliga a las páginas a que cumplan con los siguientes requerimientos en forma general:

- El registro de operaciones de tratamiento y uso de datos de los usuarios.
- Consentimiento expreso de los usuarios sobre el uso de la información que se va a almacenar y difundir sobre ellos.
- Información transparente y clara sobre todo aquello que sea necesario conocer, para la correcta utilización de la plataforma, de la forma más segura posible.
- Gestión de formularios de usuarios o de bases de datos con adecuación a todos los preceptos del Reglamento General de Protección de Datos de la Unión Europea.

El Reglamento de la UE obligó a que las principales redes sociales (Facebook, Whatsapp, Instagram) todas propietarias de la primera, tomaran medidas para adecuarse a las nuevas disposiciones y requerimientos que se les exigen a las entidades que manipulen datos.

3.: MODIFICACIONES DE ADECUACION

3.1: Principales Modificaciones que Sufrio Facebook

- Poder acceder y descargar de forma más fácil la información que se comparte

de uno mismo.
- Mejoras en los datos que se comparten desde los dispositivos móviles.
- Adecuación de la plataforma para el uso de los usuarios más jóvenes.
- Cambio en la visualización de los anuncios publicitarios que realiza la plataforma.

3.2: Principales Modificaciones de Instagram y WhatsApp

- Comunicar y obtener el consentimiento expreso de cada usuario sobre el uso de los datos en la plataforma y su uso en otras.
- Facilitar la descarga de las publicaciones tanto de fotos como videos.
- Elevación de la edad mínima para utilizar la plataforma WhatsApp (16 años).

3.3: Modificación Principal en Twitter

- Poder descargar de forma directa del historial del usuario, el grado de protección de los posts y la información que se comparte de modo público.

3.4: Modificación Principal en LinkedIn

- Posibilidad de negar la visualización de los datos de los usuarios fuera de la plataforma.

3.5: Caso de Google

En el caso de Google, se creó un servicio dentro de la misma plataforma que ofrece la posibilidad de conocer todos los datos, que la base de la empresa tiene almacenados sobre nosotros de forma fácil y rápida. Este método lo llamaron MY ACTIVITY. Abarca no sólo, el empleo del buscador, sino que va más allá, brindando todos los datos que se vinculan como el uso de YouTube, el correo de Gmail, la navegación en Chrome y la gestión de las aplicaciones móviles. Se le ofrece al usuario la posibilidad de poder borrar la información que este considere comprometedora.

En la Unión Europea, desde el 25 de mayo del 2018 entró en vigencia el Reglamento sobre la protección de los datos, obligando a todas las empresas que operen dentro de la Unión, a que adecuen sus políticas de protección para continuar operando, independientemente del lugar geográfico donde su sede se sitúa.

En la Argentina, la Dirección Nacional de Protección de Datos Personales que es la encargada de efectivizar esta protección que se ve reconocida en la ley 25326 sancionada en el año 2001. Es también la encargada la registración de las distintas bases de datos que en el país es menester que se inscriban para poder operar de forma legal.

En Brasil en el año 2019 se realizó la aprobación por parte del congreso de la puesta en marcha a partir del año 2020 de la Autoridad Nacional de Protección de Datos. Los principales pilares para el desarrollo de la nueva adecuación y modificación de la LGDP[3] son: Gobernanza de los datos, Seguridad de la información, Atención a los titulares de los Datos.

Esta modificación va a traer aparejada la posibilidad de que las empresas brasileñas puedan dar un salto y evolucionar en llevar a la práctica transparencia, seguridad y eficiencia. La ley no solo abarcará aquellas prestadoras de servicios con sede en el país, sino que es extensible a todas las empresas que sin importar el lugar donde se asienten, presten servicios u ofrezcan productos en este territorio.

La ley estipula sanciones para aquellas empresas que se rehúsen a realizar las modificaciones pertinentes para estar en consonancia con la misma, pudiendo ser estas sanciones: advertencia, publicidad de la infracción, multas con un tope de R$50 millones de reales.

4.1: CONCLUSIÓN

El primer punto a tener en cuenta dentro de la protección de los datos siempre es, claro está, la concientización de las personas, potenciales usuarios de la red, de los riesgos que conlleva y de las consecuencias a las que se pueden ver expuestas en las redes, si no se tiene un particular cuidado al momento de informar al usuario todos los pormenores a los que se va a ver expuesto en estas etapas donde se interactúa con las redes.

¿Es posible que muchas personas dejen de contratar con estas prestadoras de servicios sabiendo de forma fehaciente todos los por menores que conlleva?

Sí es más que probable, que de los usuarios a los que se les interiorice sobre cómo se ven expuestos sus datos y del poco control efectivo, que una vez ingresados pueden tener. Parte de la transparencia consiste en que se de a los usuarios, pleno conocimiento, no solo de los datos que se van recolectando a lo largo de su interacción, sino también de qué tratamiento se les va a brindar.

3 Lei Geral de Proteçao de dados pessoais

Pero es aún más importante, que estos titulares de los datos puedan comprender de forma sencilla todos los riesgos, y una vez comprendidos decidan libremente enfrentarse o no estas posibles consecuencias.

Las normas van creciendo y haciéndose cada vez más específicas en la materia. La mayoría de los estados tratan de dar un entorno de seguridad jurídica exigiéndoles a las empresas ajustarse a las nuevas normativas. Sin embargo, siempre van a encontrarse con la barrera más grande que es, en definitiva, el propio titular, que de forma desinteresada e ignorando los riesgos, se dan a conocer, vuelcan su información pública, privada, y también sensible.

Las políticas de protección de datos no sólo tienen que mirar con recelo a las empresas, tienen que poner sus esfuerzos también en los usuarios. Se ve a las leyes de protección de datos desde un punto reparador dejando de lado que la norma también puede ser preventiva.

Dejando claro que desde una edad temprana se tiene que tomar conciencia de todos aquellos pormenores. La sociedad se vuelve cada vez más cibernética pero no por ello más capacitada para transitar o interactuar en este espacio. Al contrario, pasa a darse casi una constante de no comprender realmente que ocurre o que procesos conllevan determinadas acciones (subir una foto, hacer un comentario, compartir un video, etc).

La vida gira en torno a la informática, pero la educación lejos está de dar las herramientas necesarias.

BIBLIOGRAFIA

https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_es

https://www.argentina.gob.ar/aaip/datospersonales

https://www.efe.com/efe/america/tecnologia/brasil-ya-tiene-su-ley-de-proteccion-datos-mas-vale-tarde-que-nunca/20000036-3989178#

https://www.blog.andaluciaesdigital.es/my-activity-como-borrar-lo-que-google-sabe-de-ti/

https://twitter.com/es/privacy#update

https://www.facebook.com/help/1735443093393986?helpref=hc_global_nav

https://es-la.facebook.com/help/instagram/155833707900388

https://www.blog.andaluciaesdigital.es/proteccion-de-datos-y-redes-sociales/

https://letslaw.es/ley-de-proteccion-de-datos-brasil/

LA INFLUENCIA DIGITAL

Eje temático: Desafíos Legales y Éticos de la Sociedad Digital en la Red

Autor:
Mariel Alejandra Suárez
Abogada (UBA 2001), Experta en Derecho Digital (CEUPE 2019), especialista en Derecho Penal (UBA 2009), Juez Penal de la Provincia del Chubut, Argentina (2009 hasta la Fecha), Especialista en Derecho Tributario (ECAE 2014).

RESUMEN

La Sociedad desde siempre fue atraída por la imagen que se generaba desde el espectáculo. Desde las luchas en el coliseo romano, la quema de brujas en la época de la inquisición, los teatros de Revistas en Argentina, los carabareth en Cuba, los *realitty show* mundialmente famosos en la actualidad, las noticias criminales en los diarios o las noticias de la realeza en las revistas.

El espectáculo, aquello pensado como una acumulación de imágenes conectadas entre sí, es lo que vislumbró y despierta la atención a la sociedad en general.

En la era digital, el espectáculo es la exhibición de la vida privada a través de *facebook,* la emisión de opiniones a través de *Twitwer,* exhibiciones de imágenes en *Instagram,* y el fomento y sostenimiento de las relaciones sociales y familiares en el *Whats app,* entre otras formas de comunicación telemática y multimedia.

Pasamos del uso masivo de la televisión, las revistas, los diarios en papel y las radios, a las computadoras, las que son cada vez más pequeñas y más veloces, hoy interconectadas entre sí a través del *internet,* el que es aún de pago, y cada vez más rápido como más costoso cuanto más velocidad y tiempo de uso se prefiera.

La tecnología forma parte del proceso de modernización actual, siendo los medios telemáticos, los de comunicación por excelencia. Por ello, algunos oficios deben aggiornarse para subsistir.

La privacidad, es uno de los bienes en juego con el uso masivo de las redes sociales, el que indudablemente esta dotado de valor, no sólo moral, sino que económico.

Nuestra privacidad es el conjunto de datos que nosotros podemos proporcionar o no a los particulares, al gobierno y a las empresas; a través de esos datos pueden conocer nuestros intereses, nuestras necesidades para crear en nosotros una necesidad.

Podemos elegir si lo hacemos o no, si lo hacemos falsamente, si lo hacemos falsamente para vernos más felices o si lo hacemos falsamente para provocar un daño. Si ese daño es delito, si ese delito ésta tipificado o no, si necesita ser tipificado. Si

necesitamos educación o no para manejarnos y entender el riesgo del uso inadecuado de las redes sociales o, si la regulación es la solución a todos los conflictos digitales.

Los ataques en la web nos afectan directamente, causando muchas veces un daño irreparable, ya que extraen nuestra información y la utilizan en forma negativa.

El objetivo del presente trabajo es observar el panorama actual de la utilización de las redes sociales, evaluar las acciones humanas, sus riesgos, las posibles consecuencias, las soluciones, para finalmente concluir que una de las más trascendentales podría ser la educación, la que ubico en primer lugar para luego pensar en la regulación moderada no excesiva, siempre pensando en la participación de la sociedad para solucionar el conflicto.

También pretendo, dejar en claro cuál es el impacto y el grado de manipulación que pueden ejercer las redes sociales, hoy como un medio central de comunicación, que por supuesto proporciona el espectáculo actual.

LA NECESIDAD DE LA IMAGEN

Decía Guy Debord en 1967, que el espectáculo no sólo es un conjunto de imágenes sino una relación social entre personas mediatizadas por las imágenes.[4]

Sin duda, esta definici n sigue siendo de actualidad. Observen sino, la red social *facebook,* la que acumula espectáculos de la vida privada o gustos de las personas, siendo además una fuente de opiniones particulares de los usuarios.

No pretendo juzgar las bondades o maldades de la existencia del espectáculo, sino ponderar la medida de su incidencia en la vida de las personas que lo contemplan como aquellas que participan e interactuan y, determinar si el espectáculo, hoy traspolado a lo digital, puede manipular las voluntades de las personas.

El ser humano no sólo necesita ver, sino mostrarse, lo que a veces implica mentir sobre algunos aspectos, para mostrarse más feliz, algo que no parece causar daño alguno.

Aquí comienza el punto en cuestión. Si se trata de un simple *photoshop* en una fotografía, no le hace daño a nadie; pero si se trata de una *fake news,* debemos evaluar si es una noticia falsa que perjudica o no a alguien, con lo cual si afectamos aspectos de la privacidad de esa persona y por ende si incurrimos en delito o no y en su caso qué tipo de delito se nos podría atribuir.

4 Guy Debord, "la Sociedad del Espectáculo", Rosario, Santa Fé, Argentina (2007) escrito originalmente en Paris, Francia en 1964 y publicada por primera vez en 1967.

También, los invito a pensar si esa *fake news* nos lleva a tomar decisiones diferentes a las que tomaríamos si no la hubiéramos leído, para conocer si podemos ser manipulados falsamente o si podemos manipular o influir en la decisión de otros.

Por lo tanto, podemos afirmar sin lugar a dudas, que el uso de la red social, proporciona felicidad por mostrarse habiendo cumplido objetivos, y felicidad de mostrar emociones como la solidaridad, la bondad, el carisma.

En las redes sociales somos diferentes, no sólo somos más felices sino más sencibles, a parte de tener una mejr apariencia.

LA SOCIEDAD DORMIDA

No puede siquiera cuestionarse los múltiples beneficios de los avances tecnológicos, máxime cuando la tecnología se vincula a internet y se interconecta en tiempo real.

A modo de ejemplo se puede mencionar, que surgen oportunidades laborales a través de la *web*, proyectos educativos de diferentes niveles presenciales y a distancia tanto para el ciudadano común como para aquel que se encuentra cumpliendo una condena, adquisición y pago de bienes y servicios, realización de trámites públicos y privados, entretenimiento, información, cultura, economía.

Sin duda, una gran repercusión en el tiempo que insume cada evento y en el modo de su realización.

A través de la web, se hacen valer los derechos, como aquellos vinculados al acceso a la justicia, ya que los poderes judiciales en el mundo se actualizan, crean aplicaciones, expedientes digitales, la validación de la utilización de la comunicación electrónica , usan inteligencia artificia [5], todo con el fin de garantizar la tutela judicial efectiva de las personas que requieren el acceso a la justicia a fines de que sus conflictos sean atendidos.

Todos los aspectos de la vida actual del hombre han sido transformados por la red y la tecnologia.

Pero, es imprescindible acotar que hay numerosos aspectos negativos los que quizas no pudieron preeverse o no se estan controlando debidamente. Veamos.

En relacion a los Derechos Digitales: los que son considerados como la cuarta generación de derechos humanos[6], algunos países han avanzado en el proceso de aprobacion de la carta de derechos digitales. Este el caso de España en la Union

5 https://www.lanacion.com.ar/tecnologia/prometea-una-inteligencia-artificial-para-ayuda -a--la-justicia-portena-nid2084991 consultada el 04/06/2019

6 http://www.corteidh.or.cr/tablas/r33897.pdf consultada el 04/06/2019

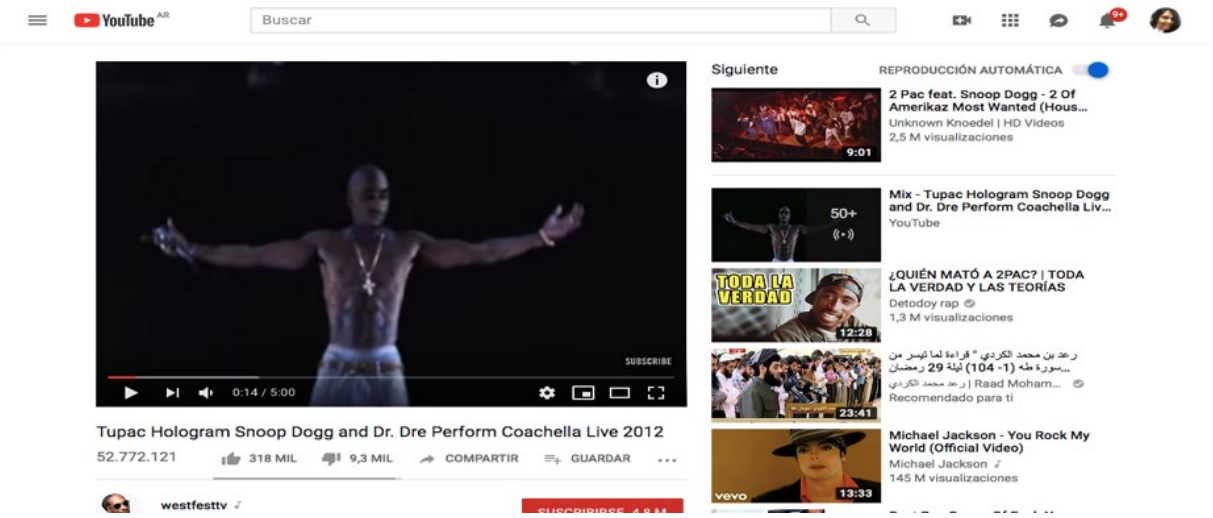
Europea (en adelante UE) en el que es pionera en ello, con un proyecto aprobado al que solo le restaba ser publicado en el Boletin oficial para su entrada en vigo [7].

Proyecto que garantiza al igual que el Reglamento Europeo la seguridad jurídica de los ciudadanos en cuanto a la protección de sus datos personales, le impone a las empresas requisitos más severos para garantizar la privacidad personal, como disponer del consentimiento claro y expreso del afectado por el uso de sus datos, la desconexion laboral, el testamento digital.

La crítica fundamental a éste instrumento, es que no se expresa sobre el uso de los datos por parte de partidos politicos o sobre los costos de internet, porque para hacer efectivos aquellos derechos que he referenciado, los costos deben ser revisados y minimizados al máximo posible para garantir el acceso.

Otra cuestión para analizar en éste proceso de modernización que vislumbra a la sociedad, son las *Deepfake*.

Si bien el espectáculo sirve para entretenernos e incluso para revivir momentos y emocionarnos, como es el caso del cantante de rap estadounidense Tupac, quien falleció de modo violento en el año 1996[8]:



Más tarde en el año 2012, en un recital apareció sorpresivamente en el escenario, el primer holograma en el que se proyectó de forma tan real, la imagen del cantante fallecido[9]:

Lo mismo ocurrió, luego de la muerte del famoso cantante de *rock Michael Jackson*, lo que provocó una gran emoción a miles de admiradores.

También, se puede hacer un mal uso de este mismo sistema de proyección de imagen humana mediante la utilización de un computador, podría provocar, dependiendo de quién sea la persona que se proyecte, conflictos políticos nacionales e internacionales, haciéndole decir al holograma cosas que la persona no diría.

Esto puede ocurrir en cualquier momento y en forma masiva como el diluvio de las *fake news*.

Un ejemplo de ello, el ya famoso video de Obama hablando mal de Trump, en donde un actor muestra como aprende gestos del ex - presidente, y mediante un software le implantan la imagen y la voz de Obama.

A continuación, exhibiré una foto captura de pantalla del video de referencia[10]:

El derecho a la información, sin duda se ve fomentado por el uso de las redes sociales, pero éste se ve francamente afectado por las *fakes news* a las que ya me había referido.

Diluvio de noticias falsas, incluso publicadas y difundidas por medios periodísticos digitales, que deben controlar con varias fuentes aquella información, ello impuesto como una regla ético profesional.

10 https://www.youtube.com/watch?v=cQ54GDm1eL0 consultado el 25/05/2019

Por ese motivo, algunos países se tratan de controlar lo que se dice en las redes[11], pretendiendo hacerlo mediante regulaciones limitadoras de aquella actividad.

En el caso resulta necesario que luchemos por la libre circulación de la información, como derecho fundamental que nos mantiene a los ciudadanos actualizados, para la toma de decisiones y nos dota claramente de herramientas para poder elaborar ideas propias.

La desinformacion es una herramienta util para aquellos que quieren generar discordia entre ciudadanos o paises, con el proposito de obtener beneficios que en circunstancias comunes no recabaría.

Las noticias falsamente creadas con un fin específico, han logrado conseguir en algunos casos una manipulacion masiva de la sociedad, para que emita opinion o vote en un determinado sentido.

Por ejemplo el famoso caso del *Brexit*, ocurrido durante el plebiscito en Gran Bretaña, en el que los ciudadanos debian decidir si seguian o no en la UE.

Es sabido que un diario digital, uno de los más leidos en aquel país, logro torcer la voluntad del pueblo ingles para conseguir la salida de UE, mediante el la creacion y difusion de noticias falsas, las que consistian en desinformar sobre una realidad especifica, en el caso los inmigrantes y refugiados europeos que supuestamente migraban a Londres, generando no solo miedo sino xenofobia[12].

11 https://www.dw.com/es/venezuela-refuerza-control-sobre-redes-e-internet/a-41401089 consultada el 07/05/2019

12 https://eu-rope.ideasoneurope.eu/2017/11/05/brexit-impact-report-published-parliament/ consultada el 24/05/2019

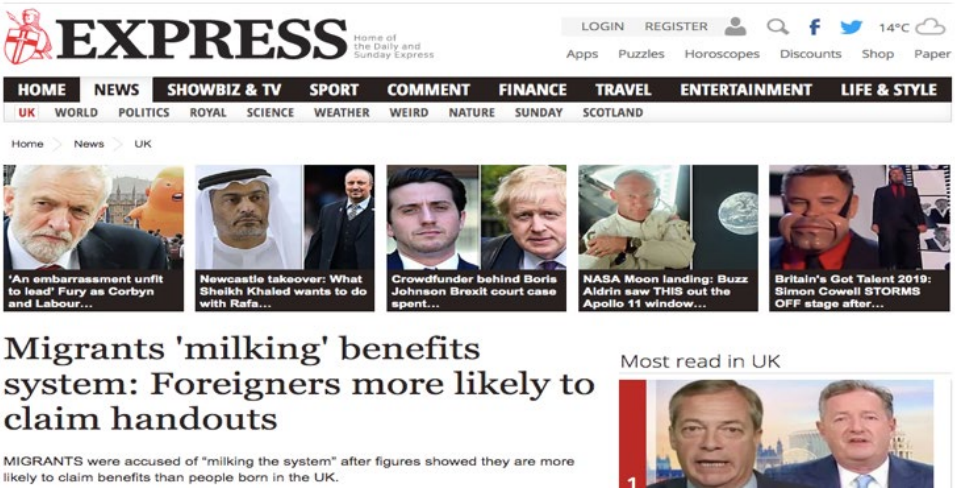
THE SCANDAL OF OPEN-DOOR BRITAIN

How immigrants milk the system

Big crime survey reveals that illegals and criminals head for the UK to rake in benefits cash

Daily Mail [13]

Noticias que finalmente fueron receptadas en forma masiva, por otros medios de comunicación, que sabiendo o no de que se trataba de una noticia falsa, no verificaron fuentes distintas y contribuyeron con la intencion inicial, demostrando la velocidad a la que se mueve la informacion internet y el poder de manipulacion de la misma.



Esas noticias generalmente referían a inmigramtes y refugiados. Los ciudadanos comenzaron a creer en la cantidad de inmigrantes que iban a llegar a su tierra, pensaron

13 Noticia publicada en Daily Mail diario de gran circulacion en UK (Reino Unido) tomada de una investigación de Jon Danzig https://neweuropeans.net/article/603/jon-danzig-speaks-out--about-mistreatment-migrants-media consultada el 04/06/2019

en el impacto en el sistema de salud, en la economia, en la vivienda, el transporte y la mano de obra, y decididamente votaron por salir de la U.E., lo que vale como un claro ejemplo del poder de manipulacion de los medios digitales.

Este tipo de acciones son las que se utilizan finalmente como un justificativo para promover mecanismos de control a veces innecesarios.

La pregunta es si es necesario implementar un marco regulatorio para evitar las noticias falsas.

En Argentina, surgio recientemente un proyecto entre medios de comunicación, dirigentes politicos y plataformas digitales, llamado compromiso ético, con el que se pretende poner en marcha un sistema activo de control y verificación de las *fake news*.

Dicho sistema, originado a raíz de las elecciones que este año se realizaran en el país[14], podria ser uno de los caminos posibles a adoptar como forma de controlar este problema, el que ha llegado a preocupar hasta los Ministros de la Corte Suprema de Justicia[15].

En España, se dio origen a un novedoso protocolo de seguridad de Interior para las elecciones recoge medidas para prevenir y contrarrestar ataques informáticos al recuento de votos y las *fake news* en el 28 A[16]

En Brasil, existe un gran problema en torno a éste tópico. Incluso se ha dicho que el presidente de aquel país, ha contribuido a difundir una noticia falsa a sabiendas de que lo era.

Por ello, resulta trascendente tener en claro, que no deben usarse las falsas noticias como un disparador para controlar internet y, que pueden haber mecanismos menos limitadores para evitar su propagación, contribuyendo a la libre circulación de la información.

También se ha instalado una discusión en torno a la nueva legislacion europea sobre *copyrigth* o derechos de autor.

Como un medio de "combatir" las falsas noticias, nacieron sitios en la red, que se encargan de desmentir la información falsa.

Es criticada la nueva ley Europea de derechos de autor, porque obliga a las plataformas a tener sistemas automatizados de censura previa para evitar que se publique contenidos que originalmente hayan sido publicados en otro sitio.

Ello conllevaría que no pueda reproducirse el contenido originalmente publicado, y que complique la forma de desmentir noticias por ejemplo.

---

14 https://www.clarin.com/politica/firman-compromiso-etico-digital-combatir-fake--news-campana_0_vk6prxs-s.html consultada el 06/06/2019.

15 https://www.infobae.com/politica/2018/06/29/ricardo-lorenzetti-pidio-regular-la-difusion-de-noticias-falsas-a-traves-de-las-redes-sociales/ consultada el 02/02/2019 y el 06/06/2019

16 https://elpais.com/politica/2019/03/14/actualidad/1552571931_168409.html consultada el 09/06/2019

La intención del presente trabajo no es analizar exhaustivamente la ley mencionada, sino plantear el tema, sus críticas y posibles soluciones. Sin duda cualquier forma de censura previa, debe ser cuestionada.

Se ha habla también, del "derecho a la rectificaci n" sin control judicial, en donde se obligaría tanto a medios, plataformas como a las personas a incluir la opinión de un tercero que pueda sentirse afectado por la información. Quizás este no se un aspecto negativo considerando que no se encuentra legislada una acción judicial expedita como en Argentina, considerando además que los tiempos judiciales no son los mismos que se los órganos administrativos.

Pareciera que frente a este problema la única solución que se ofrece, es desde el punto de vista legislativo y censurando los contenidos.

Por ello, no el individuo no debe distraerse frente al espectáculo que se presenta atractivo y satisfactorio frente a sus ojos. No se debe dejar espacio al Estado que como única solución nos ofrece el mecanismo regulatorio de control con consecuencias directas sobre derechos fundamentales, como justificativo de las acciones perjudiciales que provoca el uso indebido de la tecnología interconectada[17].

DE LOS ATAQUES Y DE LOS DELITOS CIBERNÉTICOS

Otro aspecto vinculado al uso negativo de los medios tecnológicos, son los ataques cibernéticos los que pueden ocurrir con o sin conexión a la red.

La forma de introducir virus y gusanos en los ordenadores parece ir modificándose y perfeccionándose a diario.

Aunque parezca sorprendente, uno los primeros ataques cibernéticos han sido en el año 1999, cuando un joven de tan sólo 15 años de edad quebró la seguridad de la NASA y accedió a 13 ordenadores de donde robó software e información con un valor de 1,7 millones de dólares, lo que provocó que la agencia tuviera que apagar sus sistemas por 21 días, una acción que les costaría 41.000 dólares en reparaciones y pérdidas[18]. Otro gran ataque, el que fue sin conexión a la red se registró en el 2010 en una planta nuclear que producía Uranio en Irán[19], el que ha podido detener toda la maquinaria allí utilizada, volviendo a aquella infraestructura en un estado crítico. A ese virus de lo llamo Stuxnet[20].

---

17 https://elpais.com/internacional/2019/04/16/actualidad/1555427376_009178.html consultada el 09/06/2019

18 https://www.xataka.com/historia-tecnologica/jonathan-james-el-joven-que-con-solo--15-anos-hackeo-y-puso-de-cabeza-a-la-nasa-y-al-pentagono; consultada el 09/06/2019

19 https://www.welivesecurity.com/la-es/2017/06/20/sistemas-industriales-en-la-mira/ consultada el 07/05/2019

20 https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet consultada el 07/06/2019

Los últimos ataques registrados en marzo de éste año el acceso a las direcciones de correo de Microsoft[21][22], el secuestro virtual de datos del ayuntamiento de Baltimore en mayo de éste año[23], el ataque a google[24], la campaña presidencial de Hilary Clinton[25].

El Centro Nacional de Inteligencia (CNI) español, detectó en 2018, 38.000 incidentes de *cyber* seguridad, lo que representa un crecimiento del 43% respecto a 2017. Aunque la mayoría fueron neutralizados fueron 102 los que se consideraron críticos[26].

Según los expertos en *Cybertech*, los ataques van ya por la quinta generación y son cada vez más sofisticad s. De los virus de los noventa se pasó a la interferencia de las redes, a la intromisión en las aplicaciones, a los robos de datos y, en los últimos años, a los grandes ataques globales señalados.

Serán más fuertes, más rápidos y con mayor sofisticación. Los *crackers* aprovecharan la conexión y la desconexión, desde las nubes de información, los coches o las redes sociales hasta subtítulos, juegos, drones o elementos aparentemente inofensivos como los juegos o electrodomésticos robotizados o computarizados (heladeras, equipos de música, aspiradoras robotizadas)[27]. No hay lugar para la distracción.

Las legislaciones penales para combatir los delitos cibernéticos, deben ser actualizadas o entendidas y aplicadas dentro de la realidad que ofrece el contexto actual, en cuanto al avance tecnológico.

Algunas legislaciones han podido aggiornarse a las nuevas herramientas delictivas y otras han quedado atrás, pero no por ello inutilizadas.

Mientras que el código penal español fue modificado y actualizado en el 2015 previendo específicamente delitos cometidos con el uso de medios tecnológicos y mediante la conexión a internet, otras legislaciones deberán adecuar sus figuras ya existentes a estas nuevas formas comisivas.

Quien no tiene legislado por ejemplo el hurto o el robo o la estafa o las amenazas en sus legislaciones penales, pues bien ahora esos delitos pueden ser cometidos con la utilización de la tecnología y de la tecnología interconectada.

---

21 https://elpais.com/tecnologia/2019/04/16/actualidad/1555396697_102102.html, consultada el 09/06/2019

22 https://elpais.com/internacional/2019/02/20/actualidad/1550647379_548195.html consultado el 09/06/2019

23 https://elpais.com/tecnologia/2019/05/23/actualidad/1558646983_883457.html, consultada el 09/06/2019

24 https://elpais.com/diario/2010/01/24/domingo/1264308754_850215.html, consultada el 06/09/2019

25 https://elpais.com/internacional/2015/09/06/actualidad/1441500389_514632.html, consultada el 06/09/2019

26 https://elpais.com/politica/2019/02/14/actualidad/1550170544_939859.html, consultada el 06/06/2019

27 https://elpais.com/tecnologia/2019/01/30/actualidad/1548871131_125689.html, consultada el 09/06/2019

La protección de datos personales también debe ser un objetivo de los gobiernos y un interés de los ciudadanos.

Algunas legislaciones han contemplado minuciosamente la protección de los datos, concebido como aquella información de los ciudadanos que puede ser de utilidad para la mercadotecnia, para los gobiernos y para otros ciudadanos, implementando legislaciones estrictas y órganos de contralor con facultades administrativas de imposición de severas sanciones económicas en el caso de violaciones al mismo, como ocurre con el Reglamento de la UE legislado en 2016, el que entro en vigor en 2018.

Algunos países acercándose a la estricta concepción de la necesidad de proteger el dato personal desde el valor económico y respetuoso de los derechos fundamentales siguiendo la línea europea, sancionaron leyes acordes a esa visión, como el caso de Panamá con la ley 81, la que entrará en vigor en 2 años.

Argentina con una ley desde el año 2000, sin seguir la filosofía del Reglamento Europeo y con grandes modificaciones a evaluar, ha diseñado un sistema de protección con una acción judicial expedita, el habeas data.

Brasil, en camino de sancionar su ley de protección de datos personales, en miras al Reglamento Europeo.

Siendo este un panorama actual de la influenc a de lo digital en la vida de las personas, intentando resaltar sin duda el benefi io que implica la tecnología para las sociedades, pero, advirtiendo sus peligros y las herramientas adoptadas por parte de los interesados, el Estado y las empresas, restando al ciudadano abrir sus ojos para colaborar con la lucha para una red protectoria de los derechos fundamentales.

CONCLUSIONES

Internet no tiene fronteras, por ello generó una nueva forma de comunicación dinámica, efectiva y en tiempo real, donde la nacionalidad no importa, lo que importa es estar conectados e intercambiar información.

Las finalidades de la interconectividad entre las personas son multiples, información, educación, comunicación, fortalecimiento de lazos familiares o afectivos, y miles más.

Lo importante es entender que actualmente si bien no hay fronteras, existen barreras de acceso, de uso, de credibilidad, que deben combatirse con una efeiciente conducta generada en los ciudadanos a traves de la informacion y la educación, y una regulacion que medianamente defina lo que esta bien y lo que está mal, sin limitar actividades de los usuarios, respetando los derechos digitales y la privacidad de los datos que se erigen como los grandes derechos fundamentales de cuarta generacion.

A través de políticas que concreten el acceso universal a la red, en equilibrio con el derecho a la información real, efectiva, actualizada y su libre circulación.

La solución no es la regulacion indiscriminada y solo con el objeto de controlar lo que se vierte en la red para censurarlo, o desinformar, se puede interpretar la legislación actual.

Nuevas formas de investigación, capacitación de los operadores, inversión del estado y mantener la premisa de un servicio de internet universal como pilar fundamental del respeto por los nuevos derechos fundamentales del hombre.

Se deben identificar las vulnerabilidades y garantizar la seguridad en la red a través de prevención y de la solución efectiva a los conflictos actuales.

Tomar conciencia que no sólo es responsabilidad de los gobiernos o de las empresas, sino que además una de las patas de esta mesa, debe ser integrada por el usuario quien debe asumir su responsabilidad y conocer acabadamente sus derechos, porque nadie se encuentra exento de las consecuencias negativas del mal uso de la red.

La sociedad no puede seguir siendo una mera espectadora del espectáculo, deber ser un actor importante en el desarrollo del mundo digital.

BIBLIOGRAFIA

Leyes:

Constitución de la Nación Argentina;

Constitución Española;

Convenciones Internacionales;

RGPD de la UE redactado y promulgado en el año 2016, entrada en vigor año 2018;

Ley Argentina de Protección de Datos Personales N° 25326

Ley Panameña de Protección de Datos personales N° 81 promulgada en 2018, entrada en vigor en 2020

Código Penal Argentino;

Código Penal Español;

Libros:

Guy Debord, “la Sociedad del Espectáculo”, Rosario, Santa Fé, Argentina (2007) escrito originalmente en Paris, Francia en 1964 y publicada por primera vez en 1967;

Páginas web:

https://www.lanacion.com.ar/tecnologia/prometea-una-inteligencia-artificial-para-ayudar-a-la-justicia-portena-nid2084991 consultada el 04/06/2019;

http://www.corteidh.or.cr/tablas/r33897.pdf consultada el 04/06/2019;

https://innovadores.larazon.es/es/not/espana-ya-tiene-su-carta-de-derechos-digitales-como-el-olvido-en-internet-o-el-testamento-virtual consultada el 29/05/2019;

https://www.nytimes.com/1996/09/14/arts/tupac-shakur-25-rap-performer-who-personified-violence-dies.html consultada el 03/06/2019

https://www.youtube.com/watch?v=TGbrFmPBV0Y consultado el 02/06/2019;

https://www.youtube.com/watch?v=cQ54GDm1eL0 consultado el 25/05/2019;

https://www.dw.com/es/venezuela-refuerza-control-sobre-redes-e-internet/a-41401089 consultada el /07/05/2019;

https://eu-rope.ideasoneurope.eu/2017/11/05/brexit-impact-report-published-parliament/ consultada el 24/05/2019;

https://neweuropeans.net/article/603/jon-danzig-speaks-out-about-mistreatment-migrants-media consultada el 04/06/2019;

https://www.clarin.com/politica/firman-compromis -etico-digital-combatir-fake-news-campana_0_vk6prxs-s.html consultada el 06/06/2019;

https://www.infobae.com/politica/2018/06/29/ricardo-lorenzetti-pidio-regular-la-difusion-de-noticias-falsas-a-traves-de-las-redes-sociales/ consultada el 02/02/2019 y el 06/06/2019;

https://www.welivesecurity.com/la-es/2017/06/20/sistemas-industriales-en-la-mira/ consultada el 07/05/2019;

https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet consultada el 07/06/2019;

https://www.xataka.com/historia-tecnologica/jonathan-james-el-joven-que-con-solo-15-anos-hackeo-y-puso-de-cabeza-a-la-nasa-y-al-pentagono, consultada el 09/06/2019;

https://elpais.com/tecnologia/2019/04/16/actualidad/1555396697_102102.html, consultada el 09/06/2019

https://elpais.com/internacional/2019/02/20/actualidad/1550647379_548195.html consultado el 09/06/2019

https://elpais.com/internacional/2019/04/16/actualidad/1555427376_009178.html, consultada el 09/06/2019;

https://elpais.com/politica/2019/02/14/actualidad/1550170544_939859.html, consultada el 06/06/2019;

https://elpais.com/tecnologia/2019/01/30/actualidad/1548871131_125689.html, consultada el 09/06/2019;

https://elpais.com/diario/2010/01/24/domingo/1264308754_850215.html, consultada el 06/09/2019;

https://elpais.com/internacional/2015/09/06/actualidad/1441500389_514632.html, consultada el 06/09/2019;

https://elpais.com/politica/2019/03/14/actualidad/1552571931_168409.html consultada el 09/06/2019;

REGULACIÓN DE LA "ECONOMÍA NARANJA" O "ECONOMÍA CREATIVA"
LA LEY NARANJA COLOMBIANA

Eje temático: Desafíos legales y éticos de la Sociedad Digital en Red

Autor:
Oscar Rodrigo Paredes Fernández
Lic. En Ciencias Jurídicas y Políticas[28]
Docente de planta
Universidad Privada Boliviana
Facultad de Ciencias Empresariales y Derecho
Carrera de Derecho

ABSTRACT
Las transformaciones operadas en la mayor parte de las sociedades, luego de la crisis financiera global, ha permitido que se comiencen a visibilizar nuevos escenarios, con nuevos actores, servicios y productos, fruto de la denominada economía colaborativa o si gustan economía naranja. Ámbitos como la cultura, las artes escénicas, cine y teatro, la música, las actividades socioculturales y medioambientales se terminan posicionando frente a sectores tradicionales de la economía, mostrando que bajo un soporte creativo y colaborativo pueden traer consigo una serie de ventajas y beneficios para la sociedad. El reconocimiento de emprendimientos disruptivos, que nos muestran otra forma de hacer negocios (Uber, BlaBlaCar, Couch Surfing y otros) así como de encarar las diversas formas de generación de bienestar y la satisfacción de necesidades individuales y colectivas, trae consigo también la imperiosa necesidad de abordar una regulación acorde a empresas colaborativas y creativas, procurando con ello que se las fomente en ves de generar cuellos de botella o barreras burocráticas excesivas. Bajo esa línea, en nuestra región es loable destacar la posición Colombiana con la promulgación de la Ley Naranja, una disposición legal de carácter sustantivo que plantea un escenario de fomento y construcción de las condiciones para los exponentes de esta forma de economía, pensada en la población y con un horizonte prometedor, como las cifras lo evidencian en los diferentes sectores en los que se inserta. Una postura digna de imitarse y fomentarse al interior de los países que integramos la región, puesto que, al romper con los viejos paradigmas de la economía tradicional, el surgimiento de empresas creativas, locales, regionales, e incluso continentales, nos permiten ser parte de movimientos económicos bastante dinámicos, fundados en la creatividad y la cooperación.
Bajo el precepto del fomento y difusión de las industrias creativas, surge la normativa planteada por la República de Colombia como una norma sustantiva que sirva y acompañe a una política estatal "naranja", presentando una mirada fresca y actual de las necesidades del sector en términos de incentivos y regulación, una faceta digna de emularse en los diferentes países de la región, lo que a la postre permitirá obtener los beneficios de una "industria" en constante desarrollo, transformación y crecimiento.

28 Con Maestría en Administración de empresas mención recursos humanos, programa concluido, en elaboración de la tesis para defensa. Con Maestría en Seguridad, Defensa y Desarrollo, elaborando el trabajo final de grado. Diplomado en Altos Estudios Nacionales, Diplomado en Docencia Universitaria. Educador Google Nivel 1 Certificado y próximo a certificar nivel 2

ANTECEDENTES

En nuestra región, resulta muy poco lo que se ha conversado, desde el enfoque del Derecho, sobre economía naranja u economía "creativa". Si bien en otros ámbitos (administración de empresas, economía, régimen comercial y otros) se identificaron los pormenores y los beneficios que otorga el advenimiento y reconocimiento de una economía naranja, para la ciencia jurídica termina siendo un concepto poco explorado y desarrollado, por ello la motivación de abordar su estudio y comprensión, en procura de sistematizar las necesidades de una norma que regule, sin asfixia , los emprendimientos "naranja".

Al iniciar la investigación de la economía naranja o disruptiva surge la necesidad de comprenderla y definirla, ya que resulta poco práctico el regular algo que no se entiende, pero proponer una regulación efectiva. En ese sentido es importante determinar qué entendemos por economía naranja. Para tal propósito podemos recurrir a las definiciones dadas por la UNCTAD, UNESCO, WIPO y otras entidades, las que desde sus diferentes enfoques pretenden visualizar a la economía naranja (creativa o disruptiva).

Según la UNESCO, en el año 2005 en la Convención sobre protección y promoción de la diversidad de las expresiones culturales, en su artículo 4, define a las "industrias culturales" como aquellas que producen y distribuyen bienes o servicios culturales. (Es importante resaltar que la UNESCO, de manera deliberada, emplea el término cultural en vez de creativo basado en el siguiente razonamiento, expuesto por Kazuko Goto: "Muchos países utilizan el término creativo para describir estas industrias, pero muchas de ellas, sin el carácter creativo, no llegan a serlo. La definición y medida de la creatividad en si misma es sujeta a mucho debate. Las industrias creativas usualmente cubren un mayor alcance que los dominios artísticos tradicionales, con la inclusión de todas las industrias de Tecnologías de Información y Comunicación, o investigación y desarrollo. El marco aborda este tema permitiendo la inclusión de algunas industrias creativas específicas (diseño y publicidad) como un dominio separado." (Goto, 2017)

La Convención de la UNESCO definió los bienes y servicios culturales como "aquellos que, en el momento en que se consideran como un atributo, uso o propósito específico, incorporan o transmiten expresiones culturales, independientemente del valor comercial que puedan tener. Las actividades culturales pueden ser un fin en sí mismas o pueden contribuir a la producción de bienes y servicios culturales." (UNESCO, 2005)

Ya desde 1986, la UNESCO planteó un marco de referencia para la identificación de las categorías culturales a ser empleadas con fines estadísticos, dichas categorías eran las siguientes:

1.- Patrimonio cultural

2.- Material impreso y literatura
3.- Música
4.- Artes visuales
5.- El cine y la fotografía
6.- Radio y televisión
7.- Actividades socioculturales
8.- Deportes y juegos
9.- Medioambiente y naturaleza

Como podemos apreciar, en gran medida, el desarrollo de emprendimientos económicos colaborativos o creativos ha estado enmarcado en las áreas identificadas por la UNESCO. Sin embargo, en el 2009, se propuso un nuevo marco, el que contempla un modelo jerárquico compuesto por dominios culturales y relacionados (UNESCO, 2009) de acuerdo con el siguiente detalle:

1.- Patrimonio cultural y natural
2.- Rendimiento y celebración
3.- Artes visuales y manualidades
4.- Libros y prensa
5.- Medios audiovisuales e interactivos
6.- Diseño y servicios creativos
7.- Turismo (dominio relacionado)
8.- Deportes y recreación (dominio relacionado)

Además, en el nuevo marco se hace alusión a los dominios considerados transversales (Herencia cultural intangible, educación y entrenamiento, archivo y conservación y equipos y materiales de apoyo), debido a que estos pueden ser aplicados a todos los dominios culturales afines.

De la misma manera vemos que, con la actualización planteada al marco de referencia, la UNESCO posiciona los ámbitos en los que actualmente se evidencian los emprendimientos emergentes de la denominada economía creativa o economía naranja.

En la misma línea, ya en el año 1997, la Oficina Europea de Estadísticas (EUROSTAT) introdujo estadísticas culturales a ser aplicadas de forma común en la zona euro, dentro de las cuales definía diferentes categorías de bienes culturales para poder estimar su importación y exportación. En el año 2016 se termina definiendo a los bienes culturales como: "los productos de la creatividad artística que transmiten valores artísticos, simbólicos y estéticos; los ejemplos son antigüedades, obras de arte, libros, periódicos, fotos, películas y música. La categoría incluye CDs, DVDs y videojuegos y consolas, como medios de comunicación, permitiendo el acceso a contenidos culturales. También incluye instrumentos musicales, que no son bienes culturales en sí mismos, sino que representan medios de expresión artística. Los

"bienes culturales" excluyen los productos de fabricación a gran escala, incluso si facilitan el acceso al contenido cultural". (EUROSTAT, 2016)

Los mencionados "bienes culturales" son los que actualmente movilizan a la denominada economía naranja, identificándose rendimientos que la permitirían posicionarse como la cuarta economía del mundo, como describiremos más adelante.

Por su parte, el Reino Unido, a través del Departamento de Cultura, medios, "digital" y deportes (DCMS), nos plantea que la economía naranja alberga aquellas actividades que tienen su origen en la creatividad, la habilidad y el talento individual, y que tienen el potencial de crear empleos y riqueza a través de la generación y la explotación de la propiedad intelectual. Esta definición enfatiza la importancia de los aspectos culturales (creatividad individual, habilidad y talento) y los aspectos económicos (propiedad intelectual y crecimiento económico). A partir de las definiciones y estadísticas planteadas por el DCMS, se pueden caracterizar las siguientes industrias creativas: publicidad, arquitectura, mercado de arte y antigüedades, artesanía, diseño, moda de diseñadores, cine y video, software de ocio interactivo, música, artes escénicas, publicaciones, software y servicios informáticos, televisión y radio. Áreas que se enmarcan en el desarrollo de la denominada economía colaborativa, disruptiva o economía naranja, que con el paso de los años se van posicionando como emprendimientos generadores de empleo, desarrollo y crecimiento fundamentados en la creatividad.

Otro de los pilares que puede ser fácilmente ubicado en el desarrollo de la economía naranja es el relacionado a la propiedad intelectual, razón por la que termina concitando la atención de la Organización Mundial de la Propiedad Intelectual (OMPI) ya que, junto a los derechos de autor, se posiciona entre los aspectos más relevantes al interior de las industrias creativas. Bajo el lineamiento establecido por el DCMS del Reino Unido, se pudo apreciar la importancia de la propiedad intelectual como fuente de crecimiento económico y generación de empleo, lo que derivó en el 2003 a que la OMPI publique la Guía sobre el estudio de la contribución económica del Derecho de Autor en las industrias. En el año 2015, el organismo terminó definiendo a las industrias de derechos de autor como aquellas que desarrollan sus funciones bajo la esfera de protección de la propiedad intelectual y sus derechos conexos (OMPI, 2015). De acuerdo con lo señalado por la OMPI, el término industrias creativas implica un significado mucho más amplio ya que abarca, más allá de los derechos de autor e industrias culturales, toda producción artística o cultural en sus diferentes géneros y soportes. Ahora bien, inicialmente puede resultar contradictorio el que señalemos que la propiedad intelectual se constituye en un valor dentro de la economía colaborativa, porque comúnmente, cuando ligamos la protección de derechos de autor, se entiende que ésta bloquea a cualquier "uso no consentido" de las ideas o lo generado por ellas, sin embargo, gracias a la evolución del concepto de propiedad al de "creative

commons" o creatividad común, que alienta el desarrollo colaborativo de las ideas, reforzando el hecho de las ventajas de la conformación de plataformas, donde varios favorecen al desarrollo de productos, servicios y el propio conocimiento.

Si recurrimos a lo planteado en el seno de la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD por sus siglas en inglés), se tiene a la economía creativa como un concepto en constante evolución, donde los activos creativos generan crecimiento y desarrollo económico por medio de la creación de empleos, la incidencia en las exportaciones y su efecto positivo respecto a la inclusión de diversos actores de, fuera de promover la diversidad cultural y el desarrollo de la sociedad. La interacción entre la tecnología, la inteligencia, el turismo y la propiedad intelectual, basados en el conocimiento, que permite fomentar el desarrollo de emprendimientos innovadores, que acompañados de las políticas apropiadas impulsarán un crecimiento adecuado de las industrias creativas. Es por ello que la UNCTAD termina definiendo a la economía creativa como aquella resultante de "los ciclos de creación, producción y distribución de bienes y servicios que usan la creatividad y el capital intelectual como insumos primarios" donde se visibilizan productos tangibles e intangibles con contenido artístico o intelectual, que inciden en el dinamismo de la economía y comercio actual. (UNCTAD, 2010)

Ya en una lógica más cercana a nuestra región (Sud américa) dentro del esquema de integración del MERCOSUR se procuró medir el flujo de bienes denominados culturales, estableciéndose tres categorías: 1.- Bienes característicos: Bienes y servicios típicos dentro del campo de la manifestación cultural, relacionados a la creación, expresión, interpretación, conservación y transmisión cultural de contenido simbólico. 2.- Productos relacionados: Aquellos que sirvan tanto como insumos, así como capital para la producción de productos característicos. 3.- Bienes auxiliares: Relacionados con el mercadeo, distribución y productos que permitan a los usuarios el poder consumir bienes y servicios culturales. La interacción y relación entre estos tres tipos de bienes terminaron combinándose en una matriz de las industrias culturales: Grabaciones fonográficas, publicaciones y la industria audiovisual. (UNC AD, 2010)

Ahora bien, desde un punto de vista teórico, podemos recurrir a lo planteado por Kazuko Goto, mismo que nos entrega una definición basada en tres aspectos característicos:

- Los aspectos culturales y económicos relacionados a las políticas de desarrollo, así como las políticas económicas.
- La combinación del arte y el comercio (en un sentido general).
- La presencia de entidades sin fines y con fines de lucro.

En esa misma línea, Towse señala que "las industrias creativas combinan las artes creativas y escénicas con las industrias culturales, que incluyen publicidad, arquitectura, arte y mercado de antigüedades, artesanías, diseño, moda, cine, juegos,

servicios de patrimonio, museos, bibliotecas, Internet, publicaciones, software, televisión, radio y video." (Towse, 2011)

Por su parte, Howkins, al definir a la economía creativa, manifiesta que "esta comprende a los sectores en los que el valor de sus bienes y servicios se fundamenta en la propiedad intelectual:

> - Arquitectura, artes visuales y escénicas, artesanías, cine, diseño, editorial, investigación y desarrollo, juegos y juguetes, moda, música, publicidad, software, TV y radio, y videojuegos" (Buitrago Restrepo & Duque Márquez, 2013)

En opinión de Alejandra Luzardo, especialista senior del Banco Interamericano de Desarrollo y líder estratega de economías creativas, innovación y emprendimiento, "la creatividad como motor de innovación puede contribuir a la diversificación como herramienta necesaria para contar con una economía competitiva a nivel mundial basada en el conocimiento. Una de estas áreas de desarrollo es la denominada economía naranja, es decir el conjunto de actividades que de manera encadenada permiten que las ideas se transformen en bienes y servicios, y cuyo valor puede estar basado en la propiedad intelectual, según la definición del Banco Interamericano de Desarrollo. (Banco Interamericano de Desarrollo, 2018)

Pero, al fin y al cabo, ¿Qué es la economía naranja o economía creativa?, para resolver esa duda, luego de todas las anteriores definiciones y siguiendo lo señalado por Restrepo y Duque, podemos terminar afirmando que se trata del conjunto de actividades que permiten que las ideas se transformes en bienes y servicios, donde su valor se encuentra determinado por su contenido, el que además está protegido por la propiedad intelectual.

¿POR QUÉ DEBIERA IMPORTRNOS LA ECONOMÍA NARANJA O DISRUPTIVA?

Procurando dar respuesta a la pregunta enunciada, varios autores e instituciones se han pronunciado al respecto, de entre ellas destacamos la postura asumida por el Informe del Banco Interamericano de Desarrollo, manifestada a través de la publicación titulada *"Retos y posibilidades de la economía colaborativa en América Latina y el Caribe"* en el que ponen de manifiesto que: "El concepto de colaboración es inherente a la civilización misma. Desde la Revolución Industrial hasta nuestros días, el progreso económico ha estado anclado en la idea de que la colaboración social agrega valor productivo. Esa misma idea se refleja en el desarrollo de plataformas colaborativas digitales, que han impuesto en la última década un nuevo modelo de colaboración,

mucho más extendido y eficiente, dando lugar a una verdadera revolución digital." (Buenadicha, Cañigueral Bagó, & De León, 2017)

Cabe resaltar, como se enuncia en el informe preparado por Buenadicha y otros, manifestado en la publicación del BID, "según un informe de Yaraghi y Ravi, del Instituto Brookings, dentro de 10 años, cinco de los sectores más importantes de la economía colaborativa (préstamos P2P , empleadores en línea, alojamiento P2P, transporte compartido, y vídeo y música en línea), generarán más del 50% del total de los ingresos mundiales (en la actualidad, representan 5%)." (Buenadicha, Cañigueral Bagó, & De León, 2017) Esto nos marca una tendencia que acrecienta en diferentes latitudes y que no resulta ajeno al desarrollo de economías latinoamericanas, como la Brasileña, la Mexicana, la Argentina y Colombiana, sin dejar de lado al resto de los países latinos, los que bajo el influjo de lo que significó la crisis del 2008, tendieron la mirada hacia sectores no tradicionales para el desarrollo de emprendimientos, a través de formas novedosas de producción y consumo, bajo un enfoque colaborativo y disruptivo, para hacer frente al desempleo y la caída de las grandes economías, orillando a los diversos actores a un mercado colaborativo con una fuerte dosis de innovación que poco a poco ha permitido visualizar a las plataformas de economía colaborativa, las que frente a modelos tradicionales, generan mayor valor, beneficios, ganancias y confianza, además de permitir un manejo a pequeña escala con la inclusión de actores diversos que desde lo local y regional permiten una expansión de servicios e intercambios colaborativos, algo que podemos apreciar con ejemplos de emprendimientos disruptivos como Airbnb: Según los datos del BID/FOMIN (2016), Rio de Janeiro es hoy la cuarta ciudad del mundo en ofrecer plazas a través del servicio de hospedaje, con 33.000 propiedades, frente a otros destinos tradicionales en el ámbito turístico como es el caso de París, Londres y Nueva York:

Fuente: Airbnb Data & Analytics.
Nota: Los anuncios se refieren a apartamentos enteros, habitaciones privadas y habitaciones compartidas.

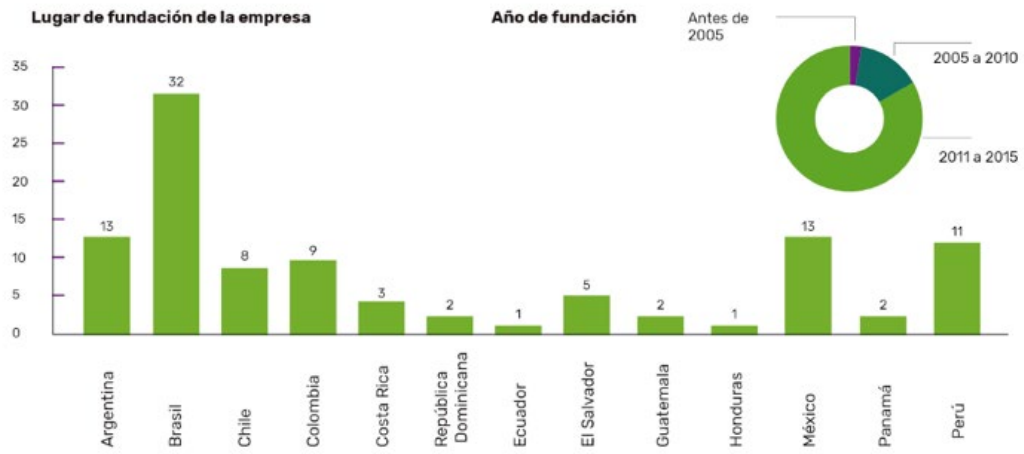
Gráfico extraído del Reporte del BID sobre Retos y posibilidades de la economía colaborativa en América Latina y el Caribe.

Si bien Airbnb en su momento fue un detonante de la economía disruptiva, también termina incidiendo en la necesidad de replantear los horizontes de negocios tradicionales poniendo en jaque a las empresas hoteleras, las que se ven en la necesidad de salir de su zona de confort en procura de mantenerse vigentes dentro de un mercado que poco a poco visibiliza emprendimientos cada vez "más creativos" como es el caso del "couchsurfing", paralelo al hecho de la diversificación de servicios de hospedaje, desde los temáticos, los que combinan arte y hospedaje o los exclusivos. Sin duda un cambio con beneficios particulares para los viajeros.

Así también tenemos ejemplos de emprendimientos colaborativos que poco a poco se van posicionando entre los más representativos, como es el caso de BlaBlaCar, que sobre todo en Europa, nos muestra la forma en la que una idea básica puede ser explotada en múltiples propósitos, además de los beneficios, en términos de ahorro, reducción de gases contaminantes y de efecto invernadero, así como la propia esencia colaborativa de un viaje compartido (carpooling) que de forma paulatina se va popularizando, sobre todo en el viejo continente, ya que por ahora no se tiene una presencia efectiva en América Latina, más allá de México. Pero la apertura de la región en torno a emprendimientos colaborativos permitiría que pronto se pueda contar con dicho servicio u otro de orden similar.

La región, poco a poco, se va abriendo a un mercado en franco crecimiento, como se puede evidenciar en el siguiente gráfico, el que demuestra el predominio de Brasil, Argentina, México, Perú y Colombia, concentrando el 80% de los emprendimientos de la región:

Proyectos de economía colaborativa en América Latina



Fuente: FOMIN (2016).

Gráfico extraído del Reporte del BID sobre Retos y posibilidades de la economía colaborativa en América Latina y el Caribe.

Situación que no resulta del todo extraña en Bolivia, donde poco a poco las industrias culturales también se van posicionando, pasando de los disruptivo a los emprendimientos creativos, tal el caso de los mentados "Cholets", descritos como escenarios emergentes con un alto potencial turístico:

> *"La arquitectura en la ciudad del El Alto se constituye en un espacio complejo en el que se articulan actividades, significados, actores, capitales, tanto económicos como culturales. Esto permite que se produzca una arquitectura innovadora que, aunque no sea reconocida por la academia, se sigue y seguirá produciendo, reivindicando silenciosamente la identidad de sus propietarios"* (Cárdenas, Mamani, & Sejas, 2010)

Lo anterior nos permite evidenciar que América Latina va manifestando un interés creciente y sostenible respecto a los emprendimientos colaborativos de la economía naranja, los que, más allá del efecto disruptivo de servicios como Uber o Airbnb, comienzan a afianzar desarrollos de orden local en los ámbitos educativos, manufacturados, medioambientales, agrícolas, de desarrollo de software y aplicaciones, los que ponen de manifiesto mayores posibilidades de crecimiento, siempre y cuando las políticas y la regulación acompañen su puesta en marcha, recordando que "las grandes oportunidades de negocio y transformación son para quienes se atreven a encarar la innovación y la adopción temprana" (Buitrago Restrepo & Duque Márquez, 2013), lo que repercute (o debiera repercutir) en la regulación que cada región y Estado asume en términos política, normativa e incentivos.

INTENTOS DE REGULACIÓN DE LA ECONOMÍA NARANJA

"Política Naranja" en Colombia, la ley 1834 de 23 de mayo de 2017

Fue una grata sorpresa el poder ubicar una norma jurídica de fomento de la economía naranja en Sudamérica. Se trata de la ley 1834 de 23 de mayo de 2017, promulgada en Colombia, como mecanismo de incentivo a las industrias creativas. Si bien la ley 1834, resulta ser una norma de carácter sustantivo, que requiere de una norma adjetiva que la desarrolle, no le quita el mérito de ser una que promueve el reconocimiento, así como el soporte, para el fortalecimiento de la economía naranja como motor de desarrollo del país y de la región. En el caso concreto de la mencionada ley, ésta determina lo siguiente respecto a su objeto:

> *"Artículo 1°. Objeto. La presente ley tiene como objeto desarrollar, fomentar, incentivar y proteger las industrias creativas. Estas serán entendidas como aquellas industrias que*

generan valor en razón de sus bienes y servicios, los cuales se fundamentan en la propiedad intelectual" (Republica de Colombia, 2017).

Con ello, Colombia se posiciona en el primer país de la región en procurar el establecimiento de una línea normativa, con un enfoque de fomento antes que de fiscalización y regulación, destacando el hecho de la protección de las industrias creativas, valorando su aporte respecto a la dinamización de la economía, algo que se acredita en el artículo tercero que destaca la importancia de la economía naranja:

> *"Artículo 3°. Importancia. El Gobierno nacional tomará las medidas necesarias para que las industrias creativas nacionales sean exaltadas, promocionadas, incentivadas, protegidas y reconocidas.*
> *Para ello coordinará articuladamente sus esfuerzos, con miras a visibilizar este sector de la economía promoviendo su crecimiento e identificándolo como un*
> *sector generador de empleo de calidad, motor de desarrollo, y que fomenta el tejido social y humano, así como la identidad y equidad."* (Republica de Colombia, 2017)

Bajo el razonamiento indicado, se esgrime una política integral que viabilice la identificación de los sectores creativos para poder desarrollarlos, fortalecerlos, posicionarlos, protegerlos y acompañarlos (Artículo 4 de la ley), es así que termina planteando una estrategia denominada de las 7i:

LAS 7i. EESTRATEGIA PARA LA GESTIÓN PÚBLICA

Fuente: Elaboración propia en base a la ley Naranja Nro.1834 (Colombia)

La Información se constituye en la base de la estrategia planteada en la norma, procurando que pueda fluir de forma apropiada, tanto en las instituciones vinculadas al fomento y desarrollo de los emprendimientos creativos, como también la posibilidad de integrar a los diversos sectores (público, privado, mixto, no gubernamental) que permita articular los postulados *"naranja"* al interior de las industrias creativas identificadas, procurando que la infraestructura (física y virtual) acompañe la

integración e inclusión de todos los actores y que ello sirva de aliciente e inspiración a nuevos emprendimientos, los que se van visibilizando día a día.

En el plano institucional se conforma el Consejo Nacional de la Economía Creativa, cuyas atribuciones fueron desarrolladas mediante el Decreto 1935 de 18 de Octubre de 2018, perfilando al mismo como un organismo asesor y consultivo del Gobierno Nacional, encargado de impulsar las estrategias, políticas y modelos, así como de coordinar las acciones interinstitucionales necesarias para la promoción, defensa, divulgación y desarrollo de la economía creativa, se pretende darle un impulso y consolidar el desarrollo de la Ley 1834 de 2017. (Portal Iberoamericano de Derecho de la Cultura, 2019) Para ello se determina, a través del Decreto 1935, que las entidades que componen el Consejo "deban brindar el apoyo necesario para el fortalecimiento del mismo, por lo cual deberán disponer y entregar al Consejo toda la información relacionada con las políticas, programas, proyectos y acciones que desde su entidad se adelanten en materia de Economía Creativa". (República de Colombia, 2018)

Otro de los puntos llamativos de la denominada Ley Naranja es el relacionado a los incentivos, indicados en el artículo 8:

> "Artículo 8°. Incentivos. El Gobierno nacional identificará acciones e incentivos para el desarrollo y crecimiento de las industrias creativas y culturales, incluyendo facilitación de procesos de importación y exportación de bienes y servicios vinculados a actividades creativas y culturales, facilitación migratoria, promoción de agremiaciones dentro del sector, administración adecuada de las sociedades de gestión colectiva y el establecimiento de incentivos estratégicos sectoriales, entre otras acciones. Las entidades territoriales velarán para que los permisos, autorizaciones y demás requerimientos necesarios a nivel local para el desarrollo de actividades creativas y culturales sean fácilmente previsibles, transparentes y expeditos.
>
> *Parágrafo. Para el otorgamiento de los beneficios de los que trata este artículo, se deberá contar con el aval previo del Consejo Nacional de la Economía Naranja."* (Republica de Colombia, 2017)

Así mismo, se determina que el Gobierno Nacional, a través de Findeter (Financiera de Desarrollo Territorial), *"pueda crear líneas de crédito y cooperación técnica para el impulso a la construcción de infraestructura cultural y creativa en los entes territoriales"* labor que permita también la construcción de agendas de "municipios, ciudades y regiones creativas", en procura de brindar un impulso tanto de la cultura como del desarrollo de la economía creativa, que se sume a las líneas de ciencia y tecnología en las iniciativas que se implementen en coordinación con los Órganos colegiados de Administración y Decisión (OCAD). (Republica de Colombia, 2017)

Otro de los ámbitos en los que se concentra la ley es el referido a la educación, donde lo más representativo aborda la necesidad de incluir en la política educativa

componentes de las Tecnologías de Información y Comunicación como herramientas de desarrollo e innovación, así como la inclusión de estos preceptos en la currícula educativa. Con ello se pretende que la formación escolar y universitaria pueda visibilizar la importancia de los emprendimientos creativos, situación que, sumada a los trabajos de financiac ón, el fomento a la exportación de productos y servicios resultantes de la economía creativa posibilitará que se extiendan los beneficios de esta en términos sociales y productivos.

La puesta en marcha de todo lo indicado permitirá posicionar a los emprendimientos creativos y disruptivos en Colombia, además de brindar un panorama de colaboración y fomento tanto desde el sector público como privado, donde el rol que se asuma por parte del Estado vaya más allá de las regulaciones tradicionales en la región, las que se caracterizaron por estar enmarcadas en un criterio más restrictivo e impositivo, como se adelanta en el caso Boliviano.

CONCLUSIÓN

Es evidente que las ventajas y oportunidades que presenta la economía naranja en la región se han puesto de manifiesto, como lo demuestran los datos estadísticos, gracias a los innumerables trabajos relacionados a la economía creativa, disruptiva y naranja, sobre todo aquellos desarrollados por el Banco Interamericano de Desarrollo y por otras entidades que permitieron que el término se popularice y que las ventajas y beneficios se visibilicen, ingresando en el desarrollo de nuevos emprendimientos dentro de un contexto en constante cambio y desarrollo.

Poco a poco, los emprendimientos creativos en la región se van posicionando como actividades rentables y estables que disputan presencia frente a negocios tradicionales, todo esto a pesar de las crisis financieras evidenciadas en los últimos años, que más allá de sus efectos negativos, trajo consigo la necesidad de innovar y ser más creativo. De ahí es que surgen grandes exponentes disruptivos como Uber, Airbnb, Spotify, Netflix y otros, dando lugar ahora a los pequeños emprendimientos creativos de orden local, los que como se menciona en el trabajo del BID, su origen desconocido por muchos se concentra en Latinoamérica, lo que nos muestra el alto potencial de la región.

El desarrollo de los emprendimientos creativos que caracterizan a la economía naranja ha permitido también identificar el rol de todos los actores, entre ellos el propio Estado, además de los organismos y actores internacionales, ya que sin un soporte político, o normativo como en el caso Colombiano, dichos emprendimientos se insertarían (como actualmente ocurre en muchas regiones) en un plano de informalidad, como identifican los estudios del BID, y que corresponde a los gobiernos

locales el brindar los escenarios y oportunidades para un crecimiento estable, sostenible y sustentable, sin ahogar los emprendimientos con regulaciones o acciones poco meditadas, que posterguen la formalidad de los exponentes locales de la economía naranja.

Bajo el precepto del fomento y difusión de las industrias creativas, surge la normativa planteada por la República de Colombia como una norma sustantiva que sirva y acompañe a una política estatal "naranja", presentando una mirada fresca y actual de las necesidades del sector en términos de incentivos y regulación, una faceta digna de emularse en los diferentes países de la región, lo que a la postre permitirá obtener los beneficios de una "industria" en constante desarrollo, transformación y crecimiento.

BIBLIOGRAFIA

Banco Interamericano de Desarrollo. (2018). *Economía Naranja. Innovaciones que no sabias que eran de America Latina.*

Buenadicha, C., Cañigueral Bagó, A., & De León, I. L. (2017). *Retos y posibilidades de la economía colaborativa en América Latina y el Caribe.* BID.

Buitrago Restrepo, F., & Duque Márquez, I. (2013). *Economía Naranja - Una oportunidad infinita.*

Cárdenas, R., Mamani, E., & Sejas, S. B. (2010). *Arquitecturas Emergentes en el Alto.*

EUROSTAT. (2016). *Estadísticas Culturales.* Luxemburgo.

Goto, K. (2017). Defini g Creative Industries. En S. H. Goto, *Tax Incentive to the Creative Industries* (págs. 11-17).

OMPI. (2015). *Guide on Surveying the Economic Contribution of The Copyrigth Industries.*

Portal Iberoamericano de Derecho de la Cultura. (05 de mayo de 2019). Obtenido de https://derechodelacultura.org/novedades/con-la-creacion-del-consejo-nacional-de-la-economia-naranja-se-refuerza-y-se-le-da-un-nuevo-impulso-a-la-ley-1834-de-2017/

Republica de Colombia. (23 de mayo de 2017). Ley Naranja. *Ley Nro. 1834*. Colombia.

República de Colombia. (18 de Octubre de 2018). Decreto 1935. Colombia.

Towse, R. (2011). *Creative industries. In: Towse R (ed) A handbook of cultural economics.*

UNCTAD. (2010). *Creative Economy Report 2010.*

UNESCO. (21 de Octubre de 2005). Convención sobre protección y promoción de la diversidad de las expresiones culturales. Paris.

UNESCO. (2009). Marco de estadísticas culturales (MEC) de la UNESCO 2009. *Marco de estadísticas culturales*. Montreal, Canadá.

UNA COMUNIDAD GLOBAL PARA LA CIUDADANÍA DIGITAL

Eje temático: Desafíos legales y éticos de la Sociedad Digital en Red

Autores:
Jacqueline Guerrero Carrera
Docente titular de tiempo completo. Magíster en Derecho. Doctora en Jurisprudencia.
Universidad Internacional del Ecuador

Diómedes E. Palacios
Máster en Ciencia Política. Profesor, investigador y consultor.
Casa de la Cultura Ecuatoriana

RESUMEN
La presente investigación busca explicar el aporte de las comunidades virtuales al constructo de la ciudadanía digital. Para ello, el análisis se realiza desde la perspectiva de los componentes estructurales de esta nueva forma de ciudadanía que emerge en la Sociedad Red. La pregunta conductora de la investigación está relacionada con la configuración de una comunidad global, la que permite reconocer el componente estructural colectivo de la ciudadanía digital, del que se desprende, además, el atributo del sentido de pertenencia de esta forma de ciudadanía. La investigación aborda el caso específico de *Facebook* que, además de ser considerada la red social más grande del mundo, es el espacio para la construcción de una infraestructura social, que permite la formación de una comunidad global. El hallazgo de la investigación indica que la Sociedad Red advierte una nueva forma de ciudadanía, que precisa como atributo el sentido de pertenencia de los individuos a una comunidad virtual. Desde la perspectiva de la infraestructura social y tecnológica específica requerida para este fin, es posible proyectar la construcción de una comunidad virtual de alcance global.

PALABRAS CLAVE: ciudadanía, ciudadanía digital, comunidades virtuales, redes sociales, Sociedad Red.

I. INTRODUCCIÓN

La ciudadanía digital es una nueva forma de ciudadanía que emerge en el contexto de la Sociedad Red, entendida como aquella que depende de las TIC y de la infraestructura en red, pues las redes son parte de todas las esferas de la sociedad y conectan todos los niveles de la misma (Amoroso et al, 2019; Castells, 2006; Dijk, 2012). Este nuevo paradigma refleja las tensiones que existen entre las TIC y la ciudadanía, debido a los cambios que han operado en los ciudadanos y las formas de participación. Estos procesos son resultado del acceso a las TIC, así como de la movilización política que se realiza a través de ellas. El ciudadano digital se ha convertido, por tanto, en un ciudadano activo, informado y comprometido con los asuntos públicos y sociales, entre otros campos, de la comunidad local, nacional, regional y global, a la que pertenece y se desenvuelve en los espacios físicos y virtuales.

La conceptualización de la ciudadanía digital considera como un atributo de esta forma de ciudadanía el sentido de pertenencia de los individuos a las comunidades virtuales. Éste atributo, como una condición para la configuración de la ciudadanía digital, constituye un reto en un mundo global pero local, móvil pero estático, virtual pero material (Dumbrava, 2017). Entonces, es pertinente preguntarse si es posible reconocer la existencia de una comunidad virtual de alcance global que otorgue sentido de pertenencia a los individuos que la conforman, mismo que es definido como atributo de la ciudadanía digital. Existen importantes esfuerzos académicos, desde diferentes campos del saber, los que han generado aportes sustanciales para dar criterio a esta pregunta. No obstante, el debate actual continúa y es pertinente a las necesidades estaduales e internacionales para garantizar los derechos del ciudadano, considerando que la idea de una comunidad global que opera en el espacio virtual requiere de una construcción teórica pero esencialmente de una evidencia práctica.

II. METODOLOGÍA

La metodología empleada para la investigación es de tipo cualitativa, mediante una inferencia descriptiva y análisis bibliográfico documental. Este tipo de investigación es teórica, con componentes sociológicos y filos ficos, por lo que requiere hechos que visibilicen los fundamentos del análisis. Por tanto, se pone a discusión el tema a través de la propuesta conceptual de comunidad virtual global de la red social más grande del mundo: *Facebook*. Del proceso de sistematización de la información, que se construye a través de una tabla de doble entrada, en la que se contrastan las referencias, conceptos, aportes y observaciones obtenidas de las fuentes empleadas, se identificaron los ejes para la elaboración del documento: comunidades virtuales, participación y ciudadanía.

III. DE LAS REDES SOCIALES A LA COMUNIDAD GLOBAL

a. Aspectos básicos de las comunidades virtuales

El término comunidad virtual fue introducido por Rheingold en 1993, al incluirlo como título de su obra publicada *The Virtual Community*. El término fue empleado para identificar a los sujetos que participaban en dichas comunidades, determinando la presencia de elementos de empatía y solidaridad. Actualmente, la frase se asocia con los distintos grupos sociales que interactúan a través de Internet. Hay diferentes tipos de comunidades virtuales con características, funcionalidades y grados de desarrollo particulares. Por el factor de composición, existen sub comunidades, comunidades virtuales de menor alcance y potencialmente comunidades de alcance global. Entre los

tipos de comunidades virtuales se identifican los foros virtuales, con o sin moderación, abiertos o cerrados; las redes sociales; los chats; los mundos virtuales o dimensiones de usuario múltiple; los gestores de contenido; los grupos de correo electrónico; los sistemas *peer to peer*; las comunidades de creación en línea, cuyo objetivo común es la construcción de archivos integrados que se convierten en un bien público de libre acceso, entre otros.

A decir de Fuster (2012), las comunidades de creación en línea (OCC) constituyen el ejemplo de comunidades virtuales que han redefinido un elemento trascendente de la ciudadanía, como es la participación ciudadana. Esto sucede puesto que, por tratarse de un tipo de comunidad virtual "de hacer" o "de construir", la participación deja de ser un acto individual aislado y supera el factor de la deliberación. El resultado de este proceso son actitudes dinámicas de participación activa, que da un nuevo sentido de pertenencia a la acción colectiva. Por esta razón, en las OCC se desarrolla el concepto de participación eco-sistémica, que se caracteriza por la interacción y la sinergia, así como la codependencia y la adaptación de los sujetos y los sistemas en los que se desarrollan.

Los principios organizativos fundamentales de la participación en las comunidades virtuales OCC (Ibídem) permiten aproximar esta nueva forma de participación. El principio esencial es la apertura a la participación, que se materializa en los múltiples canales que se ofrecen para la participación, los que van desde comentarios, carga virtual de materiales, edición digital, entre otros. En las OCC, la participación es posible en múltiples formas y diversos grados, aunque no todos los interventores que participan aportan en el mismo grado ni calidad, siendo una minoría responsable del mayor grado de contribución. Esto refleja el nivel de compromiso con la comunidad, que es factor crítico para la participación.

Por otro lado, en las OCC la participación en su mayor parte es asíncrona y en línea, debido a razones como la zona horaria y la ubicación geográfica, lo que dificulta que los colaboradores se reúnan al mismo tiempo en la plataforma y lo hagan, básicamente, en línea. El diseño de las plataformas permite una participación descentralizada y en diferentes grados, por lo que cada participante puede decidir acerca de su nivel de participación, su contribución y aporte. Esto favorece a la descentralización de la participación, la que tiene su origen en la voluntad del individuo. Como efecto, la participación se torna fl xible, espontánea y libre; aunque se reconocen factores de limitación más allá de la voluntad, como los recursos de los que dispongan los colaboradores. Por esta causa, la participación se vuelve autónoma y voluntaria, lo que implica, además, que el participante asuma el costo-beneficio de la participación. En el mismo sentido, el diseño de la plataforma determina el nivel de inclusión, proporción y fluj de información, así como la facilidad de uso, la accesibilidad técnica, la apertura a la participación y las posibilidades de comunicación. Este diseño, en gran medida,

está predeterminado por el proveedor, el cual incide en la gobernanza del entorno e, inclusive, en las interacciones que se generan entre los miembros de la comunidad (Fuster, 2012).

Por su parte, las redes sociales son el tipo de comunidades virtuales de mayor convocatoria para cualquier clase de miembros, entendidos como individuos parte de las sociedades. El concepto de las redes sociales, como tecnologías precedidas de las redes sociales como conexiones humanas, surge conjuntamente con *Linkedin,* en el 2002. Luego, dos años más tarde aparecen *Facebook* y *Flickr* y, seguido, en el 2006 se crea *Twitter.*

Las redes sociales son parte de la revolución tecnológica que, esencialmente, en términos de Barrico (2019), es una revolución mental que ha cambiado a los individuos y las sociedades, permitiendo postular la idea de una nueva humanidad. Así, las redes sociales redefine el concepto de la identidad, puesto que los usuarios colocan en el espacio virtual una copia digital de sí mismos, permitiendo la conexión del mundo analógico con el ciberespacio. Ambos mundos forman parte de un único sistema de realidad, en el que se combinan las experiencias individuales con las colectivas. Las redes sociales permiten, además, la colonización de la web, a partir de un éxodo al mundo virtual sin distinción de fronteras geográficas o limitaciones de similar tipo (Ibídem). Esto es lo que hace posible que, en la actualidad, se pueda entablar comunicación en una comunidad virtual de alcance global.

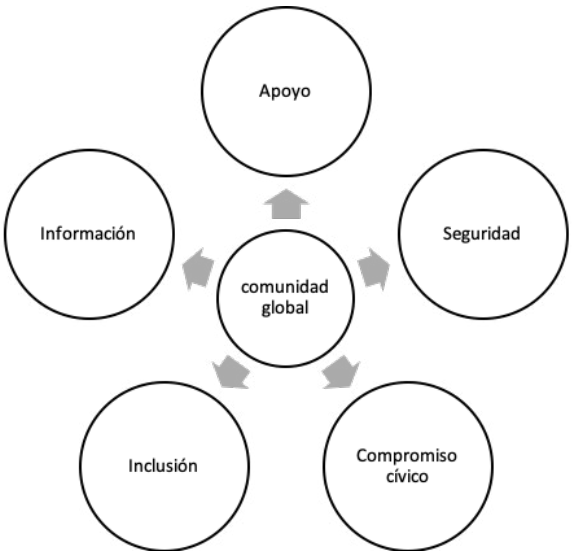
Las redes sociales son, también, el mejor ejemplo de redes distribuidas, que permiten la acción colectiva, establecida en términos de suma de acciones de individuos que, manteniendo su individualidad, forman parte de lo colectivo. Las redes sociales digitales constituyen la representación de las actividades en la Red y el medio para la construcción de la identidad *on line.* En términos de participación, las redes sociales digitales han potenciado las posibilidades de participación ciudadana a partir de sus recursos de comunicación horizontal como un *link*, un *tweet* o un mensaje enviado a través de cualquier aplicación digital desde un dispositivo fijo o móvil. En el caso de la interacción móvil, ésta segura aún más la simultaneidad de la comunicación puesto que el individuo está siempre conectado 24/7 al espacio virtual. Además, estos recursos tienen un efecto multiplicador que dinamiza la acción colectiva, tal como se evidencia en experiencias como las del 15M, la primavera árabe, los Indignados, entre otros.

b. Transición hacia una comunidad virtual de alcance global

Desde finales de la primera década del siglo XXI, el debate sobre la composición y alcance de las comunidades virtuales ha girado en torno a la pregunta sobre si es

posible construir una comunidad virtual de alcance global. Ésta encontró una posible respuesta en la carta que Mark Zuckerberg (2017), la que dirigió a la comunidad de *Facebook*, titulada "Construyendo una Comunidad Global". Zuckerberg manifestó que *Facebook* ha cambiado los paradigmas sociales y los procesos de interacción entre las personas, puesto que la plataforma tiene, sin duda, una trascendencia que rompe barreras locales y se orienta a una libertad e interconexión mundial. Esto gracias a que es una comunidad que reúne a más de dos mil millones de personas de todo el planeta y está disponible en más de cien idiomas. Conforme a dicha propuesta, la construcción de una verdadera comunidad global sería posible mediante cinco pilares, los que servirán, además, de ejes para el diseño de la infraestructura social de la comunidad de *Facebook*.

Ilustración 1 . Ejes para el diseño de la infraestructura social de la comunidad de *Facebook*



Elaborado por los autores

Estos pilares se traducen en cinco medidas, que permitirían a *Facebook* aportar en la construcción de la infraestructura social para una comunidad global:

1- Construir **comunidades de apoyo**, que fortalezcan las instituciones tradicionales y se asienten en las millones de comunidades más pequeñas, que operan en capas, que van desde las estructuras sociales íntimas hasta llegar al relacionamiento con el Estado. Esto refleja el tejido social que, en las últimas décadas, ha sido profundamente afectado en cuanto al sentido de pertenencia a las comunidades locales. En este contexto, las comunidades en línea tienen la potencialidad de fortalecer las comunidades existentes, tal es el caso de la sociedad estadounidense y sus medios; diseminar y extender las características y peculiaridades de su sociedad a otras; y permitir la creación de

nuevas comunidades en línea, uniendo a las personas en una experiencia que trasciende la ubicación física. *Facebook* puede ayudar a conectar a mil millones de personas con comunidades significativas, fortaleciendo el tejido social. Para esto se requiere mejorar las herramientas de la red social para la formación y administración de grupos, incluyendo lo relativo a las sub comunidades.

2- Construir una **comunidad segura** que prevenga daños, ayude durante las crisis y luego se reconstruya. La infraestructura debe corresponderse con las amenazas que, cada vez, son más globales y requieren una respuesta desde una perspectiva global. Así, por ejemplo, ningún país puede enfrentar un virus sólo o hacer frente a la contaminación. Es posible construir una infraestructura de seguridad global que permita a los usuarios ser parte de acciones colectivas. En este planteamiento, *Facebook* se propone emplear, intensivamente, la inteligencia artificial, lo que permitirá, inclusive, la prevención de actividades terroristas. No obstante, la seguridad de la comunidad tiene como punto de partida la seguridad y la libertad individual, sin comprometer la privacidad de las personas.

3- Construir una **comunidad informada** que facilite la exposición a nuevas ideas para lograr un entendimiento común, evitando la fragmentación de la comprensión de la realidad. Esto supone evitar las noticias falsas o las burbujas, para que los usuarios estén bien informados con base en diversas perspectivas. En este punto, la libertad de expresión es trascendente, pues todo miembro debe tener la oportunidad de expresar su opinión, en cualquier momento y sin limitaciones. Para ello, se requiere el acceso de todos a Internet, ya que de esto depende la formación de la comunidad.

4- Construir una **comunidad cívicamente comprometida**. Esto implica dos tipos distintos de infraestructura social. La primera fomenta la participación en los procesos políticos que ya existen. La segunda busca que todos los ciudadanos del mundo tengan parte en la toma de decisiones colectivas. En la primera, el aporte de *Facebook* se traduce en la ayuda para que los votantes se registren y ejerzan su derecho político. En relación con la inclusión de las personas en la toma de decisiones, *Facebook* permite que los votantes estén en contacto con sus representantes electos y la aspiración futura es el diseño de herramientas que fomenten un compromiso cívico refl xivo. Para esto es necesario que las personas estén conectadas con los asuntos que son de su interés y establezcan un diálogo directo con los representantes. *Facebook* ha desarrollado herramientas matemáticas, como los algoritmos, que orientan a cada usuario a conectarse con otras personas y contenidos en función de sus preferencias y registros de búsqueda.

5- Construir una **comunidad inclusiva** que refleje los valores colectivos, desde

los niveles locales hasta los globales, abarcando culturas, naciones y regiones. Es necesario que los ciudadanos de todo el mundo participen en el gobierno de la comunidad, a través de la toma de decisiones colectivas. Para esto se requieren estándares comunitarios, los cuales deben considerar la diversidad cultural de todos los usuarios. Por esta razón, una alternativa son los sistemas de control personal de las experiencias. La construcción de los estándares comunitarios requerirá la participación de todos los usuarios para lograr mínimos colectivos y tener la oportunidad de personalizarlos.

La posibilidad de reconocer en *Facebook* una comunidad virtual de alcance global es más real que nunca. Pero en la misma experiencia de esta red social, el desafío actual gira en torno a la garantía de los derechos de sus partícipes. Por esta razón, el tema de la ciudadanía digital es trascendente y necesario para proyectar el desarrollo futuro de las comunidades globales.

IV. APORTES AL CONSTRUCTO DE LA CIUDADANÍA DIGITAL

La idea de la ciudadanía digital, entendida como una nueva forma de ciudadanía que se corresponde con la Sociedad Red, parte de la existencia de una sociedad civil transnacional. Tal premisa determina que la ciudadanía se constituya en una experiencia no tradicional de vida que sobrepasa los límites del Estado en el mundo físico. Esta construcción presenta una nueva noción de sentido comunitario, diferente del tradicional, debido a que los individuos de diferentes espacios geográficos se empiezan a agrupar en espacios virtuales, donde sus interacciones se determinan por intereses correlacionales y en base a su experiencia (Molina Quiroga, E.; Altmark D.). Esta correlación es simultánea y tiene como principio la evolución del vínculo Estado-territorio. Una de las razones para tal modificación es la existencia misma del ciberespacio, puesto que los ciudadanos pueden ser parte de colectivos trasnacionales, en los que sus miembros están geo localizados en diferentes partes del mundo (Parada, 2009).

Por tanto, pensar en una ciudadanía digital implica la aspiración de que todo hombre sea conciudadano de una misma comunidad, una comunidad virtual complementaria del plano individual, en la que la ciudadanía digital debe integrar la experiencia de ser y sentirse ciudadano. Tal aspiración se entiende debido a que, en la época actual, es posible sentir y vivir a/en las comunidades virtuales, conformadas por ciudadanos digitales interesados en asuntos públicos, cada vez más globales. Un claro ejemplo de ello es el fenómeno denominado *hacktivismo*, que ha permitido la construcción de comunidades virtuales que buscan crear, mediante la acción colectiva,

nuevos espacios democráticos que resultan complementarios de los espacios físicos tradicionales.

Entonces, uno de los elementos clave en la construcción de la ciudadanía es la pertenencia de un individuo a un colectivo, lo que condiciona su participación en los asuntos de dicha comunidad. En el concepto tradicional de ciudadanía, el sentido de pertenencia es atribuido al individuo, que por su estatus de ciudadano adquiere un conjunto de derechos y obligaciones frente a la comunidad. En la dinámica de la sociedad moderna, el ser humano relaciona sus acciones individuales con las colectivas, toda vez que, como individuo, es parte de una comunidad y se siente parte de ella. Por tanto, sus acciones dentro y con la sociedad parten de su voluntad y en función de su interés frente a lo colectivo como opción de sobrevivencia. Nada haría el individuo sin que el desee hacerlo y lo haga. Esto, en términos políticos-jurídicos, lo convierte en un ciudadano por su voluntad de adherencia hacia dicha sociedad.

Otro de los elementos importantes en la construcción de la ciudadanía digital es la participación ciudadana, que para muchos es, además, un elemento constitutivo de la democracia. Este aspecto ha sido redimensionado en una sociedad contemporánea cada vez más compleja y caracterizada por ser activa, multitudinaria, multinivel y tecnificada. Ello implica que los ciudadanos contribuyen, cada vez más, de manera significativa a su entorno, a fin de confrontar múltiples problemas locales, nacionales y globales. Parafraseando a Bobbio (1986), la evolución de la democratización del Estado a la democratización de la sociedad está marcada por la participación de los ciudadanos activos.

La participación es un término polisémico y ambivalente, que puede ser abordado desde diferentes acepciones y campos. El término participación explica "la incidencia de los individuos y grupos sociales en las diferentes etapas en que se resuelven asuntos de interés público, [tales como…] la consulta, discusiones, planteo de propuestas y todo tipo de actividades en las cuales se interrelacionan el Estado y los ciudadanos, para el progreso de la comunidad" (Guillen, A.; Sáenz, K.; Badii, M.; Castillo, J, 2009, pág. 179). La participación ciudadana es un concepto histórico que, clásicamente, ha involucrado una relación indefinida entre el Estado y la sociedad civil. Sin embargo, las nuevas dinámicas de la Sociedad Red permiten extender esta relación a un espacio en el que no hay la presencia estatal, como sucede en las comunidades virtuales globales.

Acertadamente, Arnstein estableció que la participación ciudadana es la etiqueta que representa el poder ciudadano, lo que permite la inclusión de los ciudadanos excluidos del poder político. Ésta *es el medio* por el cual los ciudadanos pueden inducir una reforma social significativa, que les permite compartir los beneficios de la sociedad. Por tanto, se trata de un *poder real* que, necesariamente, debe implicar una redistribución del poder (Arnstein, 1969, pág. 216). La participación ciudadana se traduce en el conjunto de mecanismos que permite a los ciudadanos y a la sociedad influir en

la toma de decisiones. Esto sucede cuando es posible demostrar que la ciudadanía ha influido en la toma de decisiones y no solo ha participado en la deliberación. La participación que realizan los ciudadanos, como un fin en sí mismos o un medio para alcanzar determinados objetivos, implica la posibilidad de incidir o influencia , de manera real y plausible, en la toma de las decisiones públicas. En esencia, no se trata de decidir, sino de influir en la decisión. Aquello es posible si existen al menos los siguientes elementos: i) la voluntad individual y colectiva de participar; ii) la existencia de espacios y mecanismos que permitan la participación de los individuos y grupos de la sociedad; y, finalmen e, iii) la implementación de instrumentos y procedimientos que viabilicen la participación. Cumplidos estos tres elementos esenciales para que pueda existir participación, ésta opera a través de diversos mecanismos.

Facebook es una red social y por tanto una comunidad virtual, que por el número de individuos de todo el mundo que la componen es cuantitativamente una comunidad global. Sin embargo, *Facebook* también permite ejemplificar una especie de gobernanza comunitaria que funciona fuera de la lógica del Estado-nación. En términos de participación y de ciudadanía, esta red afronta los desafíos propios de nuevos procesos cívicos y el de la garantía de los derechos, respectivamente. Respecto de los derechos, el tema no es de reconocimiento sino de garantía de los mismos; pues, adhiriendo a la propuesta de Rodotá (2014), el individuo es portador de sus derechos, que, además, constituyen su patrimonio y no le están atribuidos como una concesión. La garantía de los derechos es un tema que aún no tiene una respuesta clara.

V. CONCLUSIÓN

Las TIC son una herramienta trascendente para el desarrollo de las sociedades, así como de sus procesos de integración, interacción y sistematización. Esto sucede gracias a que se incorporan, desde su diseño, los mecanismos con los que las sociedades se articulan en la actualidad y con los que se proyecta la humanidad al futuro. La relación del mundo físico con el ciberespacio en la actualidad se entiende como un sistema de realidad único, en el que se proyecta la vida de los individuos, en su plano individual y colectivo.

La ciudadanía digital, como nueva forma de ciudadanía que emerge en el contexto de la Sociedad Red, se configura por el sentido de pertenencia de los individuos a las comunidades virtuales que no reconocen restricciones de fronteras o límites geográficos. Se aproxima, entonces, la idea de una comunidad virtual de alcance global a la que se adhieren ciudadanos de todo el mundo, en cuyo escenario deviene una condición de desarrollo de la ciudadanía como lo es la participación ciudadana. Para

esto, es necesaria la garantía efectiva de los derechos, cuyo portador es cada individuo como parte de su patrimonio.

La idea de la comunidad virtual global deja de ser una utopía a partir del 2017 con base en la propuesta de *Facebook*, para construir la infraestructura que permita el desarrollo de una verdadera comunidad global para los más de dos mil millones de individuos de todo el mundo que participan en esta red social. Dos años después hay avances de la infraestructura invisible propuesta, como el botón Safety Check o algunas campañas de recaudación colectiva de fondos para obras solidarias. Sin embargo, desde la perspectiva de la ciudadanía digital el tema en el que hay que reparar en este escenario es la intimidad, la privacidad y la protección de los datos de los usuarios. Cada día las personas nos volvemos más visibles, en cuanto a nuestro comportamiento, especialmente en estos nuevos espacios colectivos globales. Por tanto, el desafío es la garantía de los derechos en estos espacios.

BIBLIOGRAFÍA

Aguirre, J. (2013). Nuevos alcances de la participación ciudadana a través de redes sociales. *Culturales, 1*(2). Obtenido de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-11912013000200004

Amoroso, Y; Chacón, N; García, M; Guerrero, J; Reyes, P. (2019). *Gobierno de la Información. Realidades contemporáneas.* Quito: UDLA Ediciones. Obtenido de https://www.udla.edu.ec/wp-content/uploads/2019/01/Gobiernodelainfor_issuu-1.pdf

Arnstein, S. (1969). A Ladder Of Citizen Participation. *Journal of the American Planning*, págs. 216-224. doi:10.1080/01944366908977225

Baricco, A. (2019). *The Game.* Anagrama.

Bobbio, N. (1986). *El futuro de la democracia.* (J. F. Santillán, Trad.) México: Fondo de Cultura Económica.

Castells, M. (2006). *La Sociedad Red: una visión global.* Madrid: Alianza.

Dahl, R. (1989). Democratización y oposición pública. En R. Dahl, *La Poliarquía* (págs. 13-25). Madrid: Tecnos.

Dijk, J. v. (2012). *The Network Society* (Tercera ed.). Londres: SAGE.

Dumbrava, C. (2017). Citizenship and technology. *The Oxford Handbook of Citizenship*.

doi:DOI: 10.1093/oxfordhb/9780198805854.013.33

Fuster, M. (2012). Concepción de la participación en entornos en línea: lecciones y retos para las experiencias de democracia digital. En I. R. (Coord), *Ciudadanía en 3D: Democracia Digital Deliberativa. Un análisis exploratorio.* Madrid: Edhasa.

Guillen, Amalia; Karla Sáenz; Mohammad Badii; Jorge Castillo. (2009). Origen, espacio y niveles de participación ciudadana. *Daena: International Journal of Good Conscience*, 179-193.

Held, D. (2007). *Modelos de Democracia.* Madrid: Alianza.

Molina Quiroga, Eduado; Altmark Daniel Ricardo. (s.f.). *Justicia Santa Fé.* Recuperado el 02/02/2019, de Derecho Informático e Infomática Jurídica : www.justiciasantafe.gov.ar/ckfinder/userfiles/files/institucional/cen -de-capacitacion-judicial-3067.pdf

Parada, C. (2009). Hacia un nuevo concepto de ciudadanía global. *VIA IURIS* (7), 98-111. Obtenido de https://dialnet.unirioja.es/descarga/articulo/3293442.pdf

Zuckerberg, M. (16 de Febrero de 2017). *Building Global Community.* Obtenido de https://www.facebook.com/notes/mark-zuckerberg/building-global-community/10154544292806634/

"LA CAPACIDAD PROGRESIVA DE LOS MENORES DE EDAD FRENTE A LA UTILIZACIÓN NO CONSENTIDA DE SU IMAGEN EN REDES SOCIALES"

Eje Temático: Desafíos legales y éticos de la sociedad digital en la red

Autor:
Abogado Magíster Rodrigo Alejandro Gómez Torre
Universidad de pertinencia: Docente de la Universidad Nacional de Cuyo
Maestrando Facultad Latinoamericana de Ciencias Sociales (FLACSO) sede Buenos Aires
Doctorando Universidad de Salamanca

ABSTRACT
El presente trabajo, que se enmarca en los desafíos legales y éticos de la sociedad digital, surge como producto de las experiencias de un abogado que se especializa en Derecho y Nuevas Tecnologías, que ejerce su profesión en una provincia del interior de la República Argentina, tanto a nivel profesional como a nivel académico y que complementa su formación en diferentes instituciones de Iberoamérica. Observando la carencia doctrinaria para abordar un tema de consulta diaria en el despacho particular, como así también del alumnado en general y de los medios de comunicación cuando acaecen hechos trágicos, se propone contrastar los derechos en juego al momento de decidir los pasos legales a seguir cuando la imagen de un menor de edad se viraliza en redes sociales y los progenitores del mismo desean iniciar un proceso legal en contraposición a la voluntad expresa o tácita del menor de edad.
¿Cuáles son los límites de la responsabilidad parental para el caso concreto? ¿Cuáles son los derechos de los menores? En la colisión de intereses ¿Cuál ha de primar? En el rol de operario de la justicia, siendo indiferente la posición que a este le toque desempeñar ¿Cómo debería actuarse? ¿Debería volcarse por uno o por otro? ¿Existe normativa legal que desentrañe el asunto?
Frente a estos interrogantes se comienza por determinar el objeto de estudio y se diferencia diversos supuestos dejando de lado el tratamiento del grooming o el tráfico e pornografía infantil, para centrarse en el fenómeno social del sexting y las consecuencias indeseables más comunes, es decir la difusión no consentida de las imágenes de contenido erótico o sexual.
Se realiza un análisis fenomenológico de los bienes jurídicos protegidos y su preponderancia en las sociedades al momento de dictar las normas que protegen dichos bienes para ver si siguen en vigencia con la misma intensidad en la sociedad actual. Se analizan las normas jurídicas que están implicadas en el caso de investigación y se termina confirmando a hipótesis de la primacía del derecho del menor de edad frente a los derechos parentales. Al mismo tiempo se aportan conclusiones de índole académicas y educativas que contribuyen al análisis exclusivamente jurídico.

1.- INTRODUCCIÓN Y ABORDAJE DEL OBJETO DEL ESTUDIO

Cada tanto los medios de comunicación informan con grandes titulares: ***"Una joven de XX años se suicidó tras aparecer en "packs" publicados en Facebook y Twitter"***[29]. Este titular, citado a pie de página, es simplemente un ejemplo de tantos que seguramente el lector/asistente puede recordar mientras se hace mención de él. Es en esos momentos cuando los diferentes medios, algunos nacionales, otros regionales y también los locales, que replican las noticias, comienzan a contactar a diferentes especialistas para que al aire de sus programas expliquen a los mayores, quienes teóricamente no entienden como funciona el sexting, de los peligros y de las fórmulas para evitar estas situaciones. En el tiempo que dure la noticia en los medios, dependerá de cuan cercana a la comunidad de uno sea la trágica noticia, quienes nos dedicamos al Derecho y su interconexión con las "Nuevas Tecnologías", nos convertimos en oráculos que deben ir respondiendo las dudas existenciales no sólo de los periodistas sino también de los adultos que nos rodean, también debemos dar respuestas a los miedos de las personas de mediana edad que se acercan a preguntar los pormenores legales y finalmente nos convertirnos en los señores serios y sabiondos que deben alertar y reprimir a cuanto menor de edad nos acerquen para que los concienciemos sobre el tema.

Ciertamente quienes tenemos por objeto de estudio, así como fuente de trabajo, a ésta temática sabemos que es una situación que se da a diario y que no siempre termina en situaciones tan trágicas, es más, en algunas oportunidades ni terminan siendo trágicas sino mas bien placenteras o fructíferas, claro está dependiendo del concepto que le dé el sujeto tanto a su honor como a su intimidad. El presente trabajo pretende abordar situaciones comunes que en el día a día me consultan en torno a las actividades de los menores de edad en internet o redes sociales y en particular a las actividades que desarrollan relativas a sus imágenes en la red y la utilización que se realiza de estas imágenes por terceros.

En la presente etapa de la humanidad, la que podríamos denominar como Capitalismo Informacional (Castells, 2006) o Sociedad del Conocimiento (OCDE, 1996) o Período Posindustrial (Bell, 1973) o porque no Modernidad Líquida (Zygmund Bauman, 1999), la comunicación y por consecuente su contenido, la información, ha crecido con una virulencia notable en los más diversos terrenos, generando una puerta que como sociedad estamos atravesando para nutrirnos tanto de vivencias positivas como de negativas y es ahí donde la tecnología atraviesa nuestra sociedad para mostrarnos tanto su cara risueña así como la cara triste al igual que el dios Jano, aquel dios romano que con sus dos caras miraba hacia el futuro y hacia el pasado, una sonriente y otra triste.

29 https://www.infobae.com/america/mexico/2019/02/27/una-joven-de-19-anos-se-suicido-tras-aparecer-en-packs-publicados-en-facebook-y-twitter/ [Fecha de consulta: 27 de febrero de 2019].

Para delimitar mejor el objeto de estudio indicaré que estas líneas pretenden abordar una situación más concreta inclusive que la que se describió en los párrafos anteriores. La situación a analizar es aquella en que los representantes legales de los menores pretenden ejercer una acción legal (de índole penal o civil) contra un tercero o grupo de terceros por el uso no autorizado de la imagen o video de un menor, el cual está a su cargo y ejercen los derechos parentales sobre el mismo. Sin embargo, pretendo reducir el presente trabajo a una situación fáctica aún más particular, la que he podido observar en reiteradas ocasiones y que complica más, aún, el hecho.

La situación que deseo exponer y analizar es aquella en que el menor de edad, titular del derecho vulnerado, se niega (o se muestra reticente) a atravesar un proceso judicial, sea cual fuere, en el cual se debe ventilar la vulneración de su imagen, su honor e intimidad. ¿Cómo deberíamos proceder frente a este hecho? ¿Existe una regulación legal concreta para el conflicto?

Entiendo que los derechos en juego son por un lado los conferidos a los progenitores en el Código Civil y Comercial bajo el Título VII y por otro los derechos del menor que se han vulnerado y que desde ya son la imagen del mismo y dependiendo del material compartido (fotografía, voz, video) se puede sumar la vulneración de la intimidad, y el honor de este.

2.- MARCO LEGAL CORRESPONDIENTE

En lo que refiere al marco legal correspondiente, depende mucho de cada caso concreto, ya que no es lo mismo los casos en que la imagen fue tomada por el menor y compartida a un destinatario (quien luego la distribuye) a que el tercero la haya tomado sin el consentimiento de éste. También se modifica conforme a las cualidades subjetivas tanto del menor fotografiado como del receptor de la imagen, que puede ser un mayor que procura ser un par del menor de edad, para acceder a su círculo de confianza y desde allí vulnerar su imagen, honor e intimidad. Si la persona que sufre esta vulneración lo sobrelleva como un mal momento que le toca vivir o llega al punto de atentar contra su vida también entraran en juego otras normas[30].

Dejando de lado esos supuesto nos adentraremos cuando la situación consultada viene por parte de progenitores, quienes preocupados por la intimidad de sus hijos (menores de edad) y en la idea de ejercer su responsabilidad parental (art. 638 C.CyCom y consecuentes) frente a una situación que se escapa de sus manos, ven como una posible solución al conflicto acudir a la justicia para solucionar el "desliz de su hijo/a" que envía documentos de contenido erótico o sexual por diferentes

30 Tiziana Cantone, quien el 14 de setiembre del 2016 decidió suicidarse luego de que se filtrara un video suyo de carácter sexual. https://www.antena3.com/temas/tiziana_cantone-1 [Fecha de consulta: 27 junio de 2019]

redes sociales. Quiero destacar que desde mi experiencia profesional puedo afirmar que existen por igual casos de personas mayores de edad, es decir que el tono de las presentes líneas escapan a un análisis de carácter moral sobre la sexualidad de las nuevas generaciones, ya que, tanto las generaciones viejas como las nuevas han visto sus vidas atravesadas por las nuevas tecnologías, y entre las esferas atravesadas de su vida está la intimidad, el honor y hasta la sexualidad. Sin embargo al no ser objeto del trabajo omitiré cualquier referencia a los casos de mayores de edad pretendiendo centrarme en la dicotomía jurídica que plantea para el operario jurídico que debe analizar el proceder frente a la viralización de una imagen de una persona menor de edad, la pretensión de quien ejerce su responsabilidad parental de iniciar un proceso judicial en pos de una indemnización y la negativa (expresa o tácita) de ese menor de edad.

La Corte Suprema de Justicia de la Nación, al pronunciarse en el famoso caso Ponzetti de Balbin estima que es procedente la demanda de daños y perjuicios promovida contra una editorial propietaria de una revista *por la esposa e hijo de una persona fallecida*, por haber publicado en su tapa una fotografía de ésta cuando se encontraba internada en la sala de terapia intensiva de una clínica, la que ampliada con otras en el interior de la revista, *provocó el sufrimiento y mortificación de los actores*[31]. (El subrayado y la cursiva me pertenece).

Entonces la duda que surge es la siguiente, ¿Los progenitores pueden aducir que la divulgación de la imagen de su hijo/a provoca su sufrimiento y mortificación? Probablemente para una acción de daños y perjuicios pueda aducirse el daño en cabeza propia, sin embargo quienes acuden a la justicia en estos casos, no lo hacen tanto en procura de una compensación dineraria sino por sentir vulnerados los derechos de honor e intimidad del menor, procurando el cese de la circulación de la imagen y alguna pena para el sujeto activo del delito. Así mismo, muchas veces no consiguen discernir que ventilar este problema con un abogado y luego en las diferentes instancias legales puede aparejar una revictimización del sujeto pasivo de la conducta reprochada.

Dejando de lado por un momento lo casuídico, lo cierto es que como bien afirma Umberto Eco **cabe preguntarse: En la sociedad contemporánea ¿Realmente preocupa mucho la privacidad? O mejor dicho, en los usos y costumbres de la sociedad actual, los bienes jurídicos honor e intimidad, ¿Tienen el mismo valor e interpretación que tenían en antaño para la sociedad? ¿Las nuevas generaciones se sienten como pudieron sentirse la viuda e hijo de Balbín?** Ya que si se compara con aquella época, en que la mayor amenaza a la privacidad de una persona era el chisme, y en donde la gente temía que su ropa sucia fuera ventilada en público ya que eso podría dañar su reputación, en la actualidad, muchos temen más a la disminución de su visibilidad que a la vulneración de su privacidad. Así es que este prestigioso

31 "Ponzetti de Balbín, Indalia c. Editorial Atlántida S.A."- C.S.J.N. – 11/12/1984

filósofo afirma que ***"En nuestra sociedad híperconectada, muchos de nosotros solo queremos que nos vean[32]".***

Eco, cita como ejemplo, una mujer que se prostituye (cuando, en los viejos tiempos, hubiera intentando ocultar su oficio tanto a la familia como a vecinos), y se promueve como una "acompañante", adoptando un papel público, quizá apareciendo incluso en televisión. Por citar un caso similar, de tantos que acontecen a diario, en la República Argentina tomó estado público recientemente las vivencias de Sonia Pellizzari[33]. Eco continúa en su artículo ejemplificando como se puede observar a parejas que en otra época pudieran haber mantenido en privado las dificultades de su relación, cómo ahora se presentan en vulgares programas de TV, revelándose como adúlteros o cornudos, y son recibidos con aplausos, aún más son los casos en que se ventilan tales situaciones por medio de las diferentes redes sociales.

El sociólogo Zygmunt Bauman en su obra *La República* desarrolla la temática del poder de Facebook y otras redes sociales para hacer que la gente se sienta interconectada. **Bauman destaca que, a final de cuentas, ese tipo de violaciones a la privacidad son posibles gracias a la entusiasta participación de la misma gente cuya privacidad está siendo violada.** Él argumenta que "vivimos en una sociedad confesional, promoviendo la propia exposición en público del orden de la principal y más fácil disponible, así como discutiblemente la más potente y la única prueba en verdad apta de existencia social".

Simplificando el razonamiento podríamos decir que nos encontramos en una época donde la persona promedio extrae satisfacción de rendir su privacidad a cambio de sentir que otros lo están "viendo" y le manifiestan su atención por medio de la cantidad de "likes, retweets o me gusta".

De la mano de este cambio de paradigma encontramos que se ha instalado una nueva forma de relacionarse sexualmente, comúnmente llamada sexting (envío de contenidos de tipo sexual, principalmente fotografías y/o vídeos, producidos generalmente por el propio remitente, a otras personas por medio de teléfonos móviles u ordenadores). Este "nuevo" hecho social que se conoce como sexting, por la unión de la palabra sexo en ingles (sex) y la palabra mensajeando en el mismo idioma (texting). Según una encuesta de la Asociación Civil Chicos.net y dos organizaciones extranjeras, se constata que nueve de cada 10 adolescentes tiene celular y que el 36% admitió que envía fotos suyas en poses provocativas[34].

---

32 http://espresso.repubblica.it/opinioni/la-bustina-di-minerva/2014/06/11/news/la-perdita-della-privatezza-1.168822?refresh_ce [Fecha de acceso: 13 junio de 2014]

33 https://www.clarin.com/sociedad/polemica-plata-empleada-municipal-dice--echaron-videos-hot_0_kEx7P56QD.html [Fecha de acceso: 2 de mayo de 2019]

34 https://www.clarin.com/ultimo-momento/sexting-crece-pesar-peligros_0_rJebPAFRptg.html [Fecha de acceso: 10 de mayo 2019]

Volviendo al ámbito jurídico y al caso de los menores de edad, debemos analizar la evolución de los derechos del niño, la cual en palabras de la Dra. Graciela Medina, la regulación de los derechos de los menores ha sido lenta, compleja y recién a partir del siglo XIX los Estados comenzaron a preocuparse por sus niños.

Fue así que en los orígenes de las normas los niños, niñas y adolescentes comenzaron por ser «objeto» de protección y de allí que ellos debieran ser representados/sustituidos por parte de los adultos -familia y Estado-, por considerarlos como «incapaces», conformándose la doctrina que conocemos como de «situación irregular», que focalizaba en los aspectos negativos, en las ideas de carencias o lo que les faltaba para ser una persona completa y en uso de todas sus facultades, es decir, los denominados como adultos.

Con el advenimiento de la Convención sobre los Derechos del Niño en el seno de Naciones Unidas en 1989, la legislación específica a nivel nacional en la República Argentina, Ley 26.061 del año 2005, y finalme te la aprobación del Código Civil y Comercial de la Nación en agosto del año 2015, se superó esa etapa, colocándolos a los menores en el lugar de sujetos activos de sus derechos y dejando de lado aquella concepción en la que simplemente son objetos de derecho.

Así, la prestigiosa jurista afirma con toda razón que "Este reconocimiento no se satisface en sí mismo, sino que es menester llevar adelante todos los mecanismos que resulten necesarios para que sus titulares puedan ejercer esos derechos. Es en este punto, cuando surge con toda claridad la necesidad de analizar la capacidad progresiva de los niños, niñas y adolescentes".

Si analizamos la legislación vigente argentina, podemos decir que conforme al artículo 53 del Código Civil y Comercial de la Nación la imagen es un Derecho Personalísimo, por lo tanto se restringe la posibilidad de su ejercicio mediante representación. El artículo mencionado precedentemente se complementa con artículo 55 del mismo cuerpo legal, en donde se afirma que para la captación de la imagen o voz de una persona es necesario su consentimiento, el cual, dejando de lado las excepciones normadas en el mismo artículo, no se presume, no puede ser prestado cuando sea contrario a la ley, la moral o las buenas costumbres y siempre será interpretado en forma restrictiva pudiendo ser revocado libremente en cualquier momento.

Si a las normas anteriores le agregamos lo que establece el artículo 646 del Código Civil y Comercial de la Argentina en su apartado c) y lo normado en el artículo 677 y 678 del mismo cuerpo, este último entendido a "*contrario sensu*", no caben mayores dudas que en la pugna de derechos debe prevalecer la opinión del menor. Cabe resaltar que siempre se debe analizar el caso concreto en cuanto a la capacidad progresiva del menor y las particularidades del caso ya que difiere absolutamente el caso analizado si agregamos aditamentos relativos a la edad de la persona vulnerada en su intimidad,

ya que, no es lo mismo hablar de imágenes de un menor de 6 años de otro de 16 años, si estos menores prestaron o no el consentimiento para tomar y luego divulgar su foto, si el sujeto que es destinatario de la fotografía es otro menor de edad que luego la reproduce o caso contrario es una persona mayor de edad que se hace pasar por un par para lograr vulnerar la privacidad, honor e intimidad del menor, si hay o no participación de los sujetos en redes de pornografía infantil y otros supuestos que no son objeto de estudio en las presentes líneas.

3.- CONCLUSIONES Y PROPUESTAS

Ubicándome entre los estudiosos del Derecho y las Nuevas tecnologías y no entre aquellos que han optado por dedicar su tiempo de estudio al derecho de familia, puedo afirmar que, si bien existe mucha doctrina en el ámbito que refiere al cuidado del propio cuerpo por parte de los menores y su capacidad progresiva para decidir sobre el mismo, se torna un poco más difícil encontrar doctrina y jurisprudencia sobre el objeto de estudio desarrollado en la actual monografía, ya que, muchas veces los damnifi ados terminan optando por silenciar el problema o bien procurando una solución autogestiva en las mismas redes sociales, es decir, "escrachando" o exponiendo a la persona que hizo publicas las imágenes. (en la gran mayoría de los casos, personas de sexo masculino). Para abordar las conclusiones hago propias las palabras de la Dra. Kemelmajer de Carlucci cuando trata la capacidad progresiva de los menores para tomar decisiones relativas al cuidado de su cuerpo pero las refiero a la intimidad y la capacidad para delimitarla en las redes sociales.

La prestigiosa jurista afirma que *"la mayoría médica anticipada se funda en la idea de que la conciencia del propio cuerpo viene a cada ser humano mucho antes de su mayoría de edad.* Y así es como se afirma que s*e trata de proteger al niño de informaciones que puedan perturbarlo o producirle temor, olvidando que existe una relación inversa entre el temor y la comprensión. Solo en la medida que un niño pueda comprender la información sobre su salud estará en condiciones de ejercer el derecho a expresar su opinión o deseo al respecto".* Así, quien redacta estas líneas entiende que la regla es aplicable de lleno a la situación de las imágenes del menor, siempre y cuando en el caso concreto se pueda analizar que el menor actúo en pleno uso de sus capacidades, y, analizando al mismo tiempo, quien fue el destinatario de esas imágenes.

A la afirmación del párrafo anterior la completa las cavilaciones que ya hiciera el Dr. Bidart Campos, cuando afirmaba que esta autonomía progresiva no impide a los padres ejercer respecto de sus hijos su responsabilidad educadora y orientadora primaria, y acá es donde se vuelve fundamental el conocimiento de la realidad tecnológica tanto para los mayores (para poder ejercer su responsabilidad parental)

como para menores (quienes conforme a la presunción del artículo 26 del Código Civil y Comercial a partir de los 13 años los niños y niñas tienen aptitud para decidir por sí respecto de aquellos tratamientos que no resultan invasivos, ni comprometen su estado de salud o provocan un riesgo grave en su vida o integridad física, así como luego de los 16 años el adolescente es considerado como un adulto para las decisiones atinentes al cuidado de su propio cuerpo).

Apoyándome en la legislación citada y con el apotegma *"qui potest plus, potest minus"* considero que el menor de edad puede claramente decidir, y se le debe dar prioridad a esta decisión, si pretende o no pasar por un proceso legal en el que se deberá peritar su celular entre otras medidas procesales en las cuales deberá quedar expuesta, nuevamente, su intimidad.

Al mismo tiempo, luego de la experiencia vivida como patrocinante de algunas mujeres mayores de edad que decidieron judicializar su conflicto, y reconociendo los avances legislativos relativos a la protección integral de la mujer, se resalta que no se debe olvidar que debe tenerse especial consideración a la realidad del Poder Judicial, que no siempre nos ubica en un contexto apropiado para materializar el objetivo de justicia, por ello debemos evitar la creación de falsas expectativas que no se compadecen con un correcto sistema de administración de justicia.

Con observar las estadísticas se demuestra que llevar un proceso penal hasta una sentencia es una aventura que necesita extrema templanza. No me refiero a la que precisan el juez, el fiscal o los abogados, todos ellos son parte del estamento administrador y, pase lo que pase con el asunto en el que intervienen, no se verán afectados directamente por la decisión o consecuencia del pleito.

Todo lo contrario sucede con la víctima del delito que debe enfrentarse a una serie de situaciones que no solamente le resultan totalmente oscuras, sino que -la propia experiencia lo señala- pueden llevar a confusas explicaciones de vericuetos ininteligibles para neófitos del sistema de administración de justicia; la desorientación, la incertidumbre y el temor que produce un proceso, de cualquier índole, en un primerizo que debe enfrentarse al sistema es, poniéndonos en los zapatos del otro, francamente horrible.

Ahora bien, si para colmo de males el legislador desde lo formal instituye situaciones que pueden llevar a una clara, lógica y palmaria confusión a un abogado, a un fiscal, a un juez o incluso a un analista jurídico con especiales conocimientos en un área específica del derecho, debe concluirse que antes de pensar en la aplicación de las normas precedentemente citadas debe tenerse en cuenta la situación que ha vivido y vive la víctima del delito.

Concluyendo con estas líneas, podemos afirmar que contamos con una buena cantidad de herramientas jurídicas para tratar de hacer frente a estos fenómenos sociales ellas son de carácter civil, penal, constitucional y supranacional, sin embargo,

es fundamental tomar conciencia y conocimiento de la realidad en la que vivimos y a ello no se llega más que por medio de la educación de toda la sociedad, ya que una vez viralizado el archivo, no puede ser retirado de internet por completo, y partiendo desde la base donde un 90% de los casos, las consultas vienen desde la posición de la mujer (mayor o menor de edad) que es tratada como objeto de consumo sexual para ser vendida por cualquier medio de comunicación, podemos afirmar que la ley formal nos garantiza la libertad de expresión, el derecho de los menores a ser oídos, sus capacidades progresivas para aplicar en el caso concreto, la responsabilidad parental de los progenitores y las acciones civiles y penales que procuran combatir este tipo de delitos, pero cuando no se toma cabal conocimiento de la realidad, que no sólo abarca a la física sino también a la virtual, nos encontramos en la misma posición social del pobre que cuenta con el a derecho a dormir en el Sheraton, o del lobotomizado que cuenta con el derecho a pensar, es que al fin y al cabo, y más aún en la ubicación geográfica donde nos encontramos desarrollando estas jornadas, cabe resaltar que sigue totalmente vigente aquella afirmación que rezaba, *"la educación no cambia el mundo, pero si a las personas que lo van a cambiar"*.

4.- BIBLIOGRAFIA

Bell, Daniel (1976). "The Coming Of Post-Industrial Society". Basic Books Editorial.

Bauman, Zygmunt (2000). "Liquid Modernity". Polity Press and Blackwell Publishers Editorial.

Castells, Manuel (2006). "La era de la información (Vol. 1): Economía, Sociedad y Cultura". Alianza Editorial.

MONOGRAFÍAS.

Barbieri, Pablo Carlos (2014). "Derecho a la imagen personal en el nuevo Código Civil y Comercial: un paso adelante". 2 de octubre de 2014. Infojus Id SAIJ: DACF140721.

Famá, María Victoria. "Capacidad progresiva de niñas, niños y adolescentes en el Código Civil y Comercial", La Ley (20/10/2015).

Kemelmajer de Carlucci, Aída, Herrera, Marisa, Lamm, Eleonora, Fernández, Silvia. "El principio de autonomía progresiva en el Código Civil y Comercial. Algunas reglas para su aplicación», 18 de Agosto de 2015, cita online SAIJ: DACF150461.

Lamm, Eleonora (2015). "Derecho a la imagen".

Verbauwhede, Lien (2015). "Problemas jurídicos que plantea tomar o utilizar fotografías de marcas, personas y material protegido por derecho de autor".

OCDE. (1976) informe de 1996 accesible en **http://www.oecd.org/education/innovation-education/33664172.pdf**

ENLACES WEB

https://www.clarin.com/ultimo-momento/sexting-crece-pesar-peligros_0_rJebPAFRptg.html [Fecha de acceso: 10 de mayo 2019]

https://www.infobae.com/america/mexico/2019/02/27/una-joven-de-19-anos-se-suicido-tras-aparecer-en-packs-publicados-en-facebook-y-twitter/ [Fecha de consulta: 27 de febrero de 2019].

http://espresso.repubblica.it/opinioni/la-bustina-di-minerva/2014/06/11/news/la-perdita-della-privatezza-1.168822?refresh_ce [Fecha de acceso: 13 junio de 2014]

https://www.clarin.com/sociedad/polemica-plata-empleada-municipal-dice-echaron-videos-hot_0_kEx7P56QD.html [Fecha de acceso: 2 de mayo de 2019]

SENTENCIAS

Corte Suprema de Justicia de la Nación Argentina 11/12/1984. "Ponzetti de Balbín, Indalia c. Editorial Atlántida S.A."

DESAFIOS DA APLICABILIDADE DO DEVER DE ESQUECIMENTO AOS PROVEDORES DE BUSCA

Eixo temático: Desafios legais e éticos da sociedade digital na rede

Autores:
Glenda Gonçalvez Gondim
Professora de Direito da Universidade Positivo. Doutora e Mestre em Direito das Relações Sociais pela Universidade Federal do Paraná.

Emanuella Regina Leal da Silva
Graduanda do último ano do curso de Direito da Universidade Positivo

RESUMO
A natureza humana determina como mecanismo saudável que a pessoa tenha um passado que, aos poucos, vai sendo fragmentado e esquecido. Contudo, a evolução tecnológica, representada, sobretudo, pela criação da Internet, estreita a perspectiva do passado, determinando que os fatos ocorridos estejam sempre presentes ao alcance de um simples clique, independente de barreiras temporais e espaciais. Esse simples clique, na maioria das vezes, se realiza através de um provedor de busca, tal como o *Google Search*, o *Bing* e o *Yahoo!*. A partir deles, as informações e os dados pessoais inseridos na *web* podem ser encontradas de modo muito mais célere e fácil, mas, por outro lado, são lembrados por muito mais tempo. À dista disso, é de se refletir sobre a possibilidade de se imputar aos provedores de busca o dever de esquecimento de determinado conteúdo ou dado que diz respeito a vida privada do indivíduo.
Palavras-chave: Provedor de busca. Direito ao esquecimento. Ambiente digital. Internet.

1. INTRODUÇÃO

Virtualmente, cada pessoa no mundo é um polo de criação e transmissão de informações, o que causa um fenômeno importantíssimo: o aumento da densidade de informação no tempo presente. Com isso, enquanto no passado as possibilidades de se obter informações estavam limitadas a um número determinado de fontes, hoje, a todo momento, o volume de informações geradas em tempo real por um número incontável de origens inunda o presente.

Todas essas informações podem ser obtidas mais facilmente através da utilização de um provedor de busca, também denominado provedor de pesquisa. Diariamente, milhares de pessoas recorrem ao *Google Search*, por exemplo, para encontrar informações que estão na Internet com maior rapidez e facilidade por desconhecerem a página específica em que estão inseridas.

No entanto, em conjunto, essas informações constituem um correlato digital do indivíduo, o qual é constituído de dados particulares, hábitos, preferências, e, não raras vezes, de conteúdos de sua esfera íntima. Assim, a fim de proteger as garantias naturais da vida privada, é imprescindível refletir sobre a necessidade de se estabelecer limites à capacidade que os provedores de busca possuem de recordar tudo.

Opostamente à ideia de recordar, está a de esquecer. Permitir que o indivíduo possa autodeterminar a utilização e a disponibilização de suas informações, principalmente aquelas relativas a aspectos personalíssimos de sua vida privada. Esse constitui o escopo do direito ao esquecimento, originalmente denominado *"derecho al olvido"*, em espanhol, ou, *"right to be forgotten"*, em inglês.

O debate acerca dos desafios da aplicabilidade do dever de esquecimento aos provedores de busca é atual e de extrema relevância, dada a importância assumida por esses mecanismos – haja vista a impossibilidade de se conhecer todo o diversificado conteúdo das páginas que formam a *web* –, a facilidade e rapidez com que as informações se propagam neste ambiente – o que torna mais célere, também, a difusão dos danos – e, ainda, o expressivo número de demandas judiciais existentes no cenário jurídico brasileiro que visam o esquecimento de conteúdo encontrado a partir da realização de uma busca por meio dos provedores de pesquisa existentes.

No presente estudo, pretende-se analisar este desafio, à luz da doutrina e jurisprudência atuais, bem como a legislação pertinente.

2. AS INFORMAÇÕES E OS PROVEDORES DE BUSCA

Inserido no ambiente da Internet[35], o provedor de busca proporciona uma enorme facilidade: possibilita o encontro de informações mais rapidamente e independente de barreiras físicas.

A Ministra Nancy Andrighi (2012, p. 66), ao discorrer sobre a responsabilidade civil dos provedores de pesquisa via Internet (também denominados provedores de busca), afirmou que eles integram o gênero mais abrangente chamado "provedor de conteúdo". Esse último, segundo Marcel Leonardi, corresponde a:

> toda pessoa natural ou jurídica que disponibiliza na Internet as informações criadas ou desenvolvidas pelos provedores de informação, utilizando para armazená-las servidores próprios ou os serviços de um provedor de hospedagem. Dessa forma, o provedor de conteúdo pode ou não ser o próprio provedor de informação, conforme seja ou não o autor daquilo que disponibiliza (2005, p. 30).

35 A Internet é defin da por Marcel Leonardi como um sistema de comunicação em escala global, que possibilita a troca de informações de toda natureza, lícita ou ilícita, em escala nacional e internacional (2012, p. 69).

Mas, segundo a Ministra, as duas modalidades de provedores não se confundem, porquanto os provedores de busca:

> não incluem, hospedam, organizam ou de qualquer outra forma gerenciam as páginas virtuais indicadas nos resultados disponibilizados, se limitando a indicar *links* em que podem ser encontrados os termos ou expressões de busca fornecidos pelo próprio usuário (ANDRIGHI, 2012, p. 66).

Acerca da sua atuação, explica:

> (i) uma espécie de robô navega pela web identificando páginas; (ii) uma vez identificada, a página passa por uma indexação, que cataloga e mapeia cada palavra existente, compondo a base de dados para as pesquisas; e (iii) realizada uma busca pelo usuário, um processador compara os critérios da pesquisa com as informações indexadas e inseridas na base de dados do provedor, determinando quais páginas são relevantes e apresentando o resultado. Evidentemente, esse mecanismo funciona ininterruptamente, tendo em vista que, além de inúmeras páginas serem criadas a cada dia, a maioria das milhões de páginas existentes na web sofrem atualização regularmente, por vezes em intervalos inferiores a uma hora, sendo que em qualquer desses momentos pode haver a inserção de informação com conteúdo ilícito (ANDRIGHI, 2012, p. 70).

Compreende-se, portanto, que os provedores de conteúdo se subdividem em (i) provedor de conteúdo em sentido estrito e (ii) provedor de busca, de modo que aquele disponibiliza as páginas eletrônicas ou *web sites*, em regra, exercendo controle editorial prévio sobre todas as informações disponíveis. Dentre os exemplos estão os *blogs* e os portais de notícias. O último, por outro lado, não exerce controle ou gerencia as páginas eletrônicas, ele apenas fornece ao usuário da Internet os *links* das páginas em que a informação por ele requerida pode ser localizada (ANDRIGHI, 2012). Dentre eles, o Google *Search*, o *Yahoo!*, o *Bing* e o *JusBrasil*.

Através do Projeto Estatísticas em Tempo Real, desenvolvido por uma equipe internacional de pesquisadores, analistas e desenvolvedores, criou-se o *Internet Live Stats*[36], um site que fornece dados sobre a utilização da Internet e de outros meios de tecnologia, tais como o *Twitter*, o *Youtube* e o *Instagram*.

Segundo estatística do ano de 2012[37], o *Google Search* processou mais de 40 mil pesquisas a cada segundo, o que significa mais de 3,5 bilhões de buscas por dia em todo o mundo. Esse número, porém, é irrisório perto dos resultados atuais, que demonstram um aumento de 30 mil buscas por segundo no mês de abril de 2019,

36 Acesso ao site em: https://www.internetlivestats.com. Estatística de realização de pesquisas através do *Google Search* disponível em: https://www.internetlivestats.com/one-second/#google-band.

37 Íntegra da estatística correspondente ao ano de 2012 disponível em: https://www.internetlivestats.com/google-search-statistics/

totalizando, aproximadamente, 70 mil buscas por segundo. Esse é um número bem expressivo. Se essa média permanecer, ao final do dia serão mais de 10 bilhões de buscas por dia em todo o mundo no ano de 2019 (INTERNET LIVE STATS).

Esses dados revelam que a sociedade vivencia uma revolução dos provedores de busca, "uma guerra onde todos os buscadores passaram a otimizar seus sistemas para garimpar informações relevantes em tempo real" (GABRIEL, 2013, p. 56). A grande preocupação é que o incremento da capacidade de armazenamento e comunicação de informações otimiza a variedade de maneiras pelas quais a informação pode ser organizada – e, portanto, utilizada e mesmo apropriada (DONEDA, 2006, p. 153).

3. O DIREITO AO ESQUECIMENTO NO AMBIENTE DIGITAL

Exercer controle sobre as informações no ambiente digital, implica ter domínio sobre o espaço pelo qual irão desenvolver-se as potencialidades humanas.

As informações do usuário encontradas quando da realização de uma busca por meio do provedor podem ser consideradas fragmentos do seu "eu". Juntos, esses fragmentos dão origem a um correlato digital, um corpo eletrônico que se contrapõe a própria realidade do indivíduo. Ele é constituído de uma síntese de seus hábitos, preferências e outros registros relativos à sua vida (DONEDA, 2006), tais como seu nome, e-mail, cidade, profissão, círculo de amizades e, principalmente, seus gostos.

Os dados coletados são muito valiosos economicamente porque definem tendências políticas, religiosas, comportamentais e de consumo, podendo servir para que empresas e políticos direcionem suas estratégias de acordo com essas informações. Assim, a partir do momento em que uma pessoa faz uma conta no *Facebook*, no *Instagram* ou qualquer outra rede social, bem como realiza um cadastro em determinado *site*, as empresas responsáveis passam a coletar dados pessoais a ela relacionados. O mesmo ocorre ao realizar uma pesquisa através de um provedor de busca, tal como o *Google Search*, o *Bing* e o *Yahoo!*[38].

Esses provedores fornecem *links* com as páginas em que se encontram informações conforme os critérios de busca estabelecidos. Ou seja, ao pesquisar o nome de determinada pessoa, por exemplo, surgirão conteúdos que eventualmente

38 Nesse sentido, veja-se, por exemplo, a política de privacidade da Google do Brasil acerca da coleta e armazenamento de dados: "Coletamos informações para fornecer serviços melhores a todos os nossos usuários, o que inclui descobrir coisas básicas, como o idioma que você fala, até coisas mais complexas, como anúncios que você pode considerar mais úteis, as pessoas on-line que são mais importantes para você ou os vídeos do YouTube de que você poderá gostar. Quando você não está conectado a uma Conta do Google, armazenamos as informações que coletamos com identificadores exclusivos vinculados ao navegador, aplicativo ou dispositivo que você está usando. Isso nos ajuda a manter as preferências de idioma em todas as sessões de navegação, por exemplo. Quando você está conectado, também coletamos informações que armazenamos com sua Conta do Google e que tratamos como informações pessoais (GOOGLE, 2019, p. 2).

indicarão se ela é sócia de alguma empresa, se está envolvida em algum fato, qual a sua conta em dada rede social, qual seu trajeto profissional, entre outros.

Portanto, não raras vezes, esse correlato digital, que também pode surgir de uma busca, guarda informações íntimas e sensíveis atinentes ao passado e ao presente do indivíduo, compondo-se de aspectos personalíssimos de sua vida privada. À vista disso, a ele deve ser assegurado o direito à autodeterminação informativa, ou seja, a faculdade de "determinar e controlar a utilização dos seus dados pessoais" (CANOTILHO, 2003, p. 515).

Para Joaquim Sousa Ribeiro, o direito à autodeterminação informativa "impede que o 'eu' seja objeto de apropriação pelos outros, como matéria de comunicação na esfera pública." (2012, p. 853). Atua, portanto, criando regulamentos para a defesa das informações relativas a vida privada.

Porém, associado às mudanças da sociedade, à atuação dos provedores de busca – a qual facilitou o acesso e a difusão das informações de maneira inimaginável, como visto anteriormente –, e o valor econômico das informações obtidas pelo meio digital, é de se considerar que "o conceito de vida privada como algo precioso, parece estar sofrendo uma deformação progressiva em muitas camadas da população" (COSTA JÚNIOR, 2007, p. 16), o que dificulta ainda mais o controle sobre as informações pessoais e viabiliza, crescentemente, a concretização de violações. Quando da violação, surge, como mecanismo de proteção, o direito ao esquecimento.

O direito ao esquecimento nasceu no campo das condenações criminais. Possui sua origem vinculada, principalmente, à precedentes do continente Europeu[39] e dos Estados Unidos[40].

No ordenamento jurídico brasileiro ele decorre (i) dos direitos à privacidade e à intimidade, previstos no artigo 5º, inciso X, da Constituição da República Federativa do Brasil de 1988 e (ii) dos direitos da personalidade, regulados de maneira não exaustiva no capítulo II do Código Civil de 2002[41].

Historicamente, o direito ao esquecimento ampara o indivíduo que pretende ver esquecido determinado fato pretérito ocorrido em sua vida, não permitindo que o

---

39 No âmbito europeu, o debate sobre seu reconhecimento e alcance está relacionado ao caso Lebach (1973) e, mais recentemente, ao caso de Mario Costeja Gonzalez (2010).

40 Nos Estados Unidos está vinculado ao precedente Melvin *versus* Reid (1931).

41 O direito ao esquecimento foi incluído dentre os direitos da personalidade através da ampliação da interpretação dada ao artigo 11 do Código Civil de 2002. Esse alargamento de percepção ocorreu através do enunciado nº 531, pronunciado em março de 2013, na VI Jornada de Direito Civil, realizada pelo Centro de Estudos do Judiciário do Conselho da Justiça Federal (CJE/CJF), *in verbis*: ENUNCIADO 531 - A tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento. Artigo: 11 do Código Civil. Justifi ativa: Os danos provocados pelas novas tecnologias da informação vêm-se acumulando nos dias atuais. O direito ao esquecimento tem sua origem histórica no campo das condenações criminais. Surge como parcela importante do direito do ex-detento à ressocialização. Não atribui a ninguém o direito de apagar fatos ou reescrever a própria história, mas apenas assegura a possibilidade de discutir o uso que é dado aos fatos pretéritos, mais especificamente o modo e a finalidade com que são lembrados

acontecimento e as pessoas nele envolvidas sejam retratados indefinidamente no tempo. Na prática, seu reconhecimento era visto como um corretivo – tardio, mas possível – das vicissitudes do passado, seja de inquéritos policiais ou processos judiciais, seja da exploração populista da mídia ou de pessoas irrespeitosas. Precedentes do Tribunal Superior, como o caso Chacina da Candelária (Resp n. 1.334.097/RJ) e caso Aída Curí (Resp n. 1.335.153/RJ)[42], retratam essa visão clássica do direito ao esquecimento, que pretende impedir que fatos passados que não mais possuem – ou nunca possuíram – interesse público e histórico sejam eternizados no tempo.

Essa visão clássica, limitada aos meios tecnológicos cada vez menos utilizados, não mais atende as necessidades atuais. O direito ao esquecimento não pode se limitar ao direito de cada um de ser "deixado só" ou de impedir a intromissão alheia na sua vida íntima e particular. Deve ser reconhecida, também, sua aplicabilidade ao ambiente digital. Anderson Schreiber, atento as mudanças da sociedade, assevera:

> [o direito ao esquecimento] transcende essa esfera doméstica para alcançar qualquer ambiente onde circulem dados pessoais do seu titular, aí incluídos suas características físicas, código genético, estado de saúde, crença religiosa e qualquer outra informação pertinente à pessoa (2013, p. 130)

Com efeito, não é o outro o entendimento sufragado pelos tribunais brasileiros, os quais têm reconhecido a aplicabilidade do direito ao esquecimento em casos envolvendo violações neste ambiente[43]. O Poder Legislativo, igualmente alerta as transformações, buscou integrar o Brasil – não sem um certo atraso – ao grupo de países que possuem legislação específica para proteção de dados pessoais. Criou, então, a Lei 13.709/2018, mais conhecida como Lei Geral de Proteção de Dados ou simplesmente LGPD, promulgada em 14 de agosto de 2018.

Para Ronaldo Lemos (2018), diversas foram as razões para a criação da lei. O autor afirma que:

> com o aumento exponencial de processamento de dados, inteligência artificial e compartilhamento de informações, estava claro que a privacidade e a intimidade das pessoas estava morrendo aos poucos, vítima de inúmeros mecanismos do mundo moderno, especialmente redes sociais, bancos de dados públicos, migração da informação que antes estava registrada em papel, agora disponível na Internet e outros meios, livre para garimpagem e enriquecimento de bancos de dados de todos os tipos, entre outros. O tratamento de dados era "uma terra sem lei" no Brasil (LEMOS, 2018, p. 82).

42 Em apertada síntese, em ambos os casos discutia-se a (des)necessidade de que crimes ocorridos no passado fossem retratados pelo programa Linha Direta Justiça, exibido pela emissora Rede Globo, o qual tinha como característica a teledramatização de crimes que chocaram o país.

43 Veja-se, por exemplo: REsp n. 1.660.168/RJ, Terceira Turma, julgado em 08/05/2018, DJe 05/06/2018; HC n. 256.210/SP, Sexta Turma, julgado em 03/12/2013, DJe 13/12/2013; REsp n. 1.335.153/RJ, Quarta Turma, julgado em 28/05/2013, DJe 10/09/2013; e REsp 1334097/RJ, Quarta Turma, julgado em 28/05/2013, DJe 10/09/2013.

Contudo, sustenta que o cenário de fundo é econômico, uma vez que a promulgação da Lei foi essencial para a melhora da reputação do Brasil no cenário internacional, já que ela tende a facilitar o fluxo internacional de dados entre o Brasil e demais países que possuem leis semelhantes (LEMOS, 2018), tais como Portugal, Espanha e Alemanha.

Logo de início, a Lei n. 13.709/18 estabelece em seu art. 1°, que o objetivo é proteger os "direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (BRASIL, 2018).

Por direito à liberdade, entende-se não somente os direitos de liberdade específicos, como é o caso das liberdades de expressão, liberdades de reunião e manifestação, mas também um direito geral de liberdade, que atua como uma espécie de cláusula de abertura constitucional para liberdades fundamentais especiais não nominadas. Ou seja, "funciona como um princípio geral de interpretação e integração das liberdades em espécie e de identificação de liberdades implícitas na ordem constitucional" (SARLET; MARINONI; MITIDIERO, 2015, p. 496)[44].

Ademais da proteção implícita que se extrai do artigo 1º da lei, constata-se que ele também está amparado no artigo 18, inciso VI, porquanto concede ao titular dos dados pessoais[45] os quais, nos termos da legislação, foram coletados, produzidos, receptados, classificados, utilizados, acessados, reproduzidos, transmitidos, distribuídos, processados, arquivados, armazenados, eliminados, avaliados ou controlados, o direito a eliminação do conteúdo tratado, ainda que tenha consentido com o seu tratamento.

Em outras palavras, quando o ato de tratamento venha a ferir a autodeterminação do titular sobre seus dados pessoais, seja pelo tratamento de um dado não autorizado – sem consentimento, portanto –, seja pela inobservância das diretrizes de tratamento

---

44 Em verdade, o direito geral de liberdade pode ser interpretado em conjunto com o § 2º do artigo 5º da Constituição Federal (1988) ("Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] § 2º Os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte".), o qual concebe um sistema aberto de direitos e garantias fundamentais, autorizando o reconhecimento de outros direitos não explícitos no texto constitucional. Nesse sentido, para Ingo Sarlet, Luiz Guilherme Marinoni e Daniel Mitidiero: O direito geral de liberdade (ou liberdade geral) também está aberto à integração com outras liberdades previstas nas declarações de direitos no plano internacional, além de guardar sintonia com a ideia de liberdades implícitas. Apenas para ilustrar a afirmação, é possível relacionar, por exemplo, a liberdade de utilização da informática, o livre e igual acesso à rede de comunicação, a livre disposição dos dados pessoais (para os alemães, o direito à autodeterminação informativa), entre outros que poderiam ser nominados e que não encontram previsão direta e expressa no texto constitucional (2015, p. 495).

45 O dado é a informação relacionada a pessoa natural identificada ou identificável, nos moldes do artigo 5º, I, da LGPD (2018). A depender de sua importância, o dado pode se subdividir em dado pessoal sensível, compreendido como aqueles que refletem a origem racial ou étnica, a convicção religiosa, a opinião política, a filiação a sindicato ou a organização de caráter religioso, filosófic ou político ou, ainda, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos de uma pessoa natural (art. 5º, II, LGPD).

com ele acordadas quando da concessão de sua autorização, poderá requerer que estes dados sejam esquecidos, ou, nos termos da legislação, eliminados.

4. DESAFIOS DA APLICABILIDADE DO DEVER DE ESQUECIMENTO AOS PROVEDORES DE BUSCA

A fim de obstar ou pelo menos inibir a disseminação de conteúdos ofensivos ou de dados atinentes a vida íntima e particular do indivíduo, tem se tornando comum o requerimento de adoção de medidas judiciais tendentes a impedir que os provedores exibam resultados para determinados critérios de pesquisa, tais como notícias que vinculem o nome do indivíduo ao cometimento de crimes ou a fatos desabonadores de sua vida, decisões judiciais de processos em que seja parte, *links* que levam à fotos de cunho sexual, entre outros.

No entanto, a despeito de o direito ao esquecimento decorrer do direito à intimidade e à privacidade, o Superior Tribunal de Justiça, por exemplo, tem entendimento reiterado no sentido de afastar a responsabilidade dos provedores de busca pelos resultados apresentados.

Tal entendimento se funda em duas grandes razões. A primeira, vinculada a própria atuação dos provedores de busca. Como visto antes, ao contrário dos provedores de conteúdo, eles não exercem gerência sobre as informações. Atuam tão somente no fornecimento de ferramentas que, através de algoritmos e de indexação, auxiliam o usuário a encontrar *sites* ou outros recursos conforme os argumentos de pesquisa inseridos na busca.

A segunda, é que a filtragem das informações não constituí atividade intrínseca dos provedores de pesquisa, de modo que a eles compete apenas garantir o sigilo, a segurança e a inviolabilidade dos dados cadastrais de seus usuários e das buscas por eles realizadas, bem como o bom funcionamento e manutenção do sistema (STJ, 2018).

Em síntese, então, afasta-se o dever de esquecimento dos provedores de busca, o qual deve ser direcionado contra os provedores de conteúdo, responsáveis pela disponibilização na Internet, sob pena de admitir que eles se tornem verdadeiros "censores digitais" (STJ, 2018, p. 12).

Nesse sentido, se manifestou a Corte Superior:

> No particular, não haverá nenhum interesse em demandar contra o provedor de pesquisa, pois, munida do URL da página onde inserido o conteúdo dito ofensivo (indispensável para o exercício da ação), poderá a vítima acionar diretamente o autor do ato ilícito, com o que, julgado procedente o pedido e retirada da Internet a página, o respectivo conteúdo será automaticamente excluído do resultado das buscas realizadas junto a qualquer provedor de pesquisa (STJ, 2012, p. 19).

Contudo, esse entendimento que visa excluir a responsabilidade dos provedores de busca não se mostra o mais adequado. Ele pressupõe que o titular dos dados pessoais ou das informações encontradas por meio da busca conhece o provedor que abriga o conteúdo. Ocorre que, não raras vezes, em um piscar de olhos, o conteúdo é difundido por diversos provedores, revelando que, ao titular, se tornaria extremamente custoso e moroso dirigir sua pretensão a cada um deles.

CONCLUSÃO

Não obstante a importância do esquecimento de determinada informação ou dado, o maior desafio encontrado perante os provedores de busca está relacionado a definição de sua atividade. Entende-se que eles não podem atuar como censores digitais, ou seja, que não podem selecionar qual conteúdo possui ou não natureza violadora e deixar de mostrá-los. Sustenta-se, também, que a seleção de informações não constitui atividade intrínseca dos provedores. Em síntese, diante da função que exercem, entende-se que não caberia a eles a exclusão do conteúdo.

Contudo, com o advento da Lei Geral de Proteção de Dados, a qual, em breve, entrará em vigor no país[46], esse entendimento deverá ser repensado à luz das hipóteses de tratamento definidas pela legislação.

REFERÊNCIAS BIBLIOGRÁFICAS

ANDRIGHI, Fátima Nancy. A responsabilidade civil dos provedores de pesquisa via Internet. n. 3. **Rev. TST**. vol. 78. São Paulo, 2012. Disponível em: <https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/34301/003_andrighi.pdf?sequence=1&isAllowed=y>. Acesso em: 15 de junho de 2019.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. **Código Civil**. Diário Oficial da União, Brasília, DF, 11 de jan. de 2002.

CANOTILHO, José Joaquim Gomes. **Direito Constitucional e Teoria da Constituição**. 7ª ed. Coimbra: Almedina, 2003.

CANOTILHO, José Joaquim Gomes. MOREIRA, Vital. **Constituição da República**

46 A Medida Provisória n. 869/18 **adiou a vigência da LGPD para agosto de 2020**, antes determinada para fevereiro de 2020.

Portuguesa Anotada. 4ª ed. Coimbra Editora, 2007.

COSTA JÚNIOR, Paulo José da. (2007). **O direito de estar só**: tutela penal da intimidade. São Paulo: Revista dos Tribunais.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

GABRIEL, Martha. **Educ@r**: A (r)evolução digital na educação. São Paulo: Saraiva, 2013.

GOOGLE. **Política de Privacidade do Google**. Disponível em: <https://www.gstatic.com/policies/privacy/pdf/20190122/f3294e95/google_privacy_policy_pt-BR.pdf>. Acesso em: 12 de jun. de 2019.

INTERNET LIVE STATS. Disponível em: <https://www.internetlivestats.com>. Acesso em: 28 de abril de 2019.

LEONARDI, Marcel. **Responsabilidade Civil dos Provedores de Serviços de Internet**. São Paulo: Juarez de Oliveira, 2005.

LEONARDI, Marcel. **Responsabilidade Civil Na Internet e nos Demais Meios de Comunicação**. 2º ed. São Paulo: Saraiva, 2012.

NASCIMENTO, Fábio Calheiros do. **Do Direito à Identidade ao Direito ao Esquecimento**: uma breve comparação entre a posição do Tribunal de Justiça da União Europeia e do Superior Tribunal de Justiça. Revista Forense, Rio de Janeiro, v. 422, mar. 2016.

SCHREIBER, Anderson. **Direito e mídia**. São Paulo: Atlas, 2013.

SCHREIBER, Anderson. **Direitos da Personalidade**. 2. ed. São Paulo: Atlas, 2013.

SOUSA RIBEIRO, Joaquim. A tutela de bens da personalidade na Constituição e na jurisprudência constitucional portuguesas. In **Estudos de Homenagem ao Prof. Doutor José Joaquim Gomes Canotilho**, vol. III. Boletim da Faculdade de Direito. Universidade de Coimbra.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Recurso Especial n. 1.660.168/RJ** (2014/0291777-1. Relatora Ministra Nancy Andrighi. Relator para o acórdão Ministro Marco Aurélio Belizze. Terceira Turma. Julgado em 08/05/2018, DJe

05/06/2018. Disponível em: <https://ww2.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ITA?seq=1628798&tipo=0&nreg=201402917771&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20180605&formato=PDF&salvar=false>. Acesso em: 01 de jun. de 2019.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Recurso Especial n. 1.316.921/RJ** (2011/0307909-6). Relatora Ministra Nancy Andrighi. Terceira Turma. Julgado em 26/06/2012, DJe 29/06/2012. Disponível em: <https://ww2.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ITA?seq=1161904&tipo=0&nreg=201103079096&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20120629&formato=PDF&salvar=false>. Acesso em: 01 de jun. de 2019.

O DISCURSO ODIOSO NA SOCIEDADE EM REDE: DO ABUSO DA LIBERDADE DE EXPRESSÃO À IDENTIDADE REFÚGIO [47]

Eixo temático: Desafios legais e éticos da sociedade digital na rede

Autores:
Jânia Saldanha
É professora do PPG em Direito e do Curso de Direito da Escola de Direito da UNISINOS, realizou estágio Sênior no IHEJ – Institut des Hautes **Études** sur la Justice, em Paris (2014-2015), onde é pesquisadora associada. Doutora em Direito público

Lucas Silva de Souza
Mestrando do programa de pós-graduação em Direito da Universidade Federal de Santa Maria (UFSM)

RESUMO
Na sociedade em rede, o fim das distâncias geográficas revelou a extensão das distâncias socioeconômicas e culturais. Realidade que, muitas vezes, ao invés de aproximar, acelerou divergências e segregação. Isso ocorre, devido à grande visibilidade das diferenças e desigualdades que demandam um enorme esforço de compreensão em um mundo onde o desenvolvimento social não acompanhou o econômico. Contexto do qual exsurgem questionamentos quanto ao que se vê e espera para o horizonte que se desacortina e desafia a navegar em meio às turbulentas águas da sociedade em rede. Portanto, indubitavelmente, a tão sonhada ideia de "aldeia global" é real, mas limita-se ao plano técnico e econômico, não alcançando o cultural, o político e o social. Abismo aprofundado pelo fato de o ciberespaço ter se tornado um ambiente profícuo não somente para a liberdade de expressão, mas também para a propagação do discurso de ódio. A presente pesquisa visa analisar esse cenário de exclusão advindo do embate entre discursos de ódio/liberdade de expressão. Para tanto, de início, será proposta uma análise refl xiva desse complexo panorama visando verificar se o ideário de autoregulação na rede efetiva direitos ou, em sentido contrário, os viola. Posteriormente será abordado o tratamento dado ao tema na Alemanha, Brasil, Estados Unidos e França. Quanto a metodologia, optou-se pela abordagem dialética, porque a partir da análise das contradições internas da temática talvez seja possível delinear alguns parâmetros que possibilitariam solucionar a aparente colisão da liberdade de expressão com outros direitos. Conclui-se que de um lado o dinamismo do mundo virtual exige, sim, uma margem para autoregulação, mas do outro, deve-se assegurar a atuação do sistema de justiça para que sejam garantidos o respeito e a efetivação dos direitos fundamentais. Torna-se claro, portanto, ser imperiosa a busca de novas orientações para refundar o direito tendo como base o questionamento de qual é o seu papel no contexto atual. Assim como promovida uma profícua refl xão sobre as implicações das relações humanas com o ambiente virtual. Contudo, para isso, é necessário reposicionar a bússola e redirecionar a navegação.
Palavras-chave: democracia, discursos de ódio, filtragem de dados, liberdade de expressão; sociedade em rede.

"- Et l'horizon? Rien à l'horizon

47 O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001"

- Mais que veux-tu qu'il y ait à l'horizon? »
- Fin de partie. Becket"

INTRODUÇÃO

Na sociedade em rede, o fim das distâncias geográficas revelou a extensão das distâncias socioeconômicas e culturais. Realidade que, muitas vezes, ao invés de aproximar, acelerou divergências e segregação. Isso ocorre, devido à grande visibilidade das diferenças e das desigualdades que demandam um enorme esforço de compreensão em um mundo onde o desenvolvimento social não acompanhou o econômico. Contexto do qual exsurgem questionamentos quanto ao que se vê e espera para o horizonte que se desacortina e desafia a navegar em meio às turbulentas águas da sociedade em rede.

Portanto, indubitavelmente, a tão sonhada ideia de "aldeia global[48]" é real, mas se limita ao plano técnico e econômico, não alcançando o cultural, o político e o social. Abismo aprofundado pelo fato de o ciberespaço ter se tornado um ambiente profícuo não somente para a liberdade de expressão, mas também para a propagação do discurso de ódio que ocorre quando o uso abusivo desse direito cerceia o diálogo e a construção do conhecimento se tornando um instrumento segregatório que obsta o exercício de outros direitos fundamentais daquele que o discurso vitima.

A presente pesquisa visa analisar esse cenário de exclusão advindo do embate entre discursos de ódio/liberdade de expressão. Para tanto, de início será proposta uma análise refl xiva acerca desse complexo panorama e posteriormente o tratamento dado ao tema na Alemanha, Brasil, Estados Unidos e França. Quanto a metodologia, optou-se pela abordagem dialética, porque a partir da análise das contradições internas da temática talvez seja possível delinear alguns parâmetros que possibilitariam solucionar a aparente colisão da liberdade de expressão com outros direitos.

1. DA ALDEIA GLOBAL À IDENTIDADE REFÚGIO: TENSÕES ENTRE INFORMAÇÃO E COMUNICAÇÃO

Durante as últimas duas décadas, a internet modificou significativamente vários aspectos da vida cotidiana além de se revelar, em vertiginosa velocidade, um potente vetor de interação em mátéria de liberdade de expressão e de produção de dissensos.

48 "*Global village*" ou "Aldeia Global" é um termo apresentado pelo filósof Herbert Marshall MacLuhan, antes mesmo da criação da rede mundial de computadores, primeiramente em sua obra *"The Gutemberg Galaxy"*, 1962, e posteriormente em "*Understanding Media - The Extension of Man"*, 1964, para preconizar que a interdependência eletrônica tende a encurtar distâncias e o progresso tecnológico recria o mundo à imagem de uma aldeia global. Ambas as obras indicam que a evolução tecnológica deixaria de ocupar um papel secundário na vida social e passaria a ser parte complementar dela, delineando uma nova forma de organização da sociedade.

Mudança paradigmática oriunda do fato de que as pessoas, outrora, assumiam somente a posição de receptoras das informações dispersas pelas mídias, situação que se configurava em uma comunicação um-todos, haja vista que a propagação dos informes era dependente de um centro emissor. Cenário alterado pela rede global que possibilitou não somente uma horizontalização da propagação da informação, mas também, um modo de interação todos-todos, o qual viabilizou que qualquer pessoa seja produtora e receptora de ideias e posições. (LEAL DA SILVA; BOLSON DALLA FAVERA, 2017, p. 275).

Com essa expansão das possibilidades de comunicação por meio de espaços mais inclusivos e acessíveis, cuja principal característica é a atemporalidade que incessantemente aniquila o tempo e nega a sua sequenciação, a cultura global da atualidade se tornou a da comunicação por meio de uma rede aberta de significados culturais que podem não só coexistir, mas também interagir e se modificar mutuamente a nível global. (CASTELLS, 2006, p.84-85).

Dissolução do tempo e do espaço que fez com que as pessoas se agarrem a espaços físicos, recorrendo à memória histórica, pois, conforme descreve Wolton (2004, p. 134), o outro, enquanto estava longe, não se constituía em ameaça. Agora ele está perto demais, no metrô, na loja da esquina, na escola de seu filho Isso faz com que, para o referido autor, a atual etapa da mundialização não seja apenas política e econômica, mas cultural. Disso resulta como grande desafio do século XXI a assunção de uma postura política que possibilite uma outra mundialização, que viabilize a convivência cultural pacífica.

Trata-se de um desafio quase intransponível em um contexto onde impera a arte de fabricar o ódio que, nas palavras de Sen (2015, p. 13-14), assume a forma de uma invocação do poder mágico de uma identidade supostamente predominante que afoga outras filiaç es e, de uma forma belicosa, pode também subjugar qualquer simpatia humana ou bondade natural que possamos normalmente ter.

A despeito desse ódio latente, as diversas identidades que integram as sociedades multiculturais devem ter voz e, sem sombra de dúvida, a vida em rede é caracterizada pela ampla expressão das suas mais diversas opiniões. Trata-se de algo fundamental ao convívio em sociedade e ao crescimento humano, pois é por meio do intercâmbio de informações que se realiza a construção do saber.

Isto posto, torna-se claro que a liberdade de se expressar consiste em um dos pilares que sustentam a democracia. Necessário por em relevo, contudo, que esse direito pode se tornar também uma das razões para a sua ruína, haja vista que, muitas vezes, o radicalismo identitário gera a crença falaciosa de classificações singulares com base na religião ou cultura. Desse modo, tal como exposto por Sen (2015), a liberdade de expressão é usada abusivamente para chancelar o discurso de ódio e acaba por ferir outros direitos e princípios fundamentais, como a dignidade humana.

Esse é o caráter dual da informação que por um lado significa emancipação e progresso e do outro incompreensão e ódio. Dualidade que, por vezes, obsta a comunicação e possui o potencial de incitar até mesmo o seu oposto. Para que haja efetivamente comunicação, deve haver receptividade de ideias em um mundo finito, cuja diversidade de pontos de vista é infinita. Destarte, a comunicação se tornou um dos maiores desafios na sociedade atual, onde os avanços tecnológicos tornaram mais próximas e visíveis as diferenças; gerando, por conseguinte, um esforço descomunal de compreensão (WOLTON, 2004, p. 12).

Após a euforia, oriunda de uma visão "cor de rosa" e monofocal de que a internet se tratava de uma rede "global de comunicação" símbolo da mobilidade e da transposição das identidades culturais coletivas, verificou-se ser ela uma das principais ferramentas para a propagação de afirmações de superioridade identitária e do ódio. Situação muito perigosa, pois, segundo Castells (2017, p.32), qualquer coisa que se coloque na internet, independentemente da intenção do autor, converte-se numa garrafa lançada ao oceano da comunicação global, uma mensagem susceptível de ser recebida e processada de formas imprevistas.

Panorama onde, segundo Wolton (2004, p. 24 e 185), surge um triângulo explosivo composto pelas relações entre identidade, cultura e comunicação. Para que essa "bomba" se mantenha inativa, o autor defende que se deve promover a passagem da informação (a mensagem) para a comunicação (a relação), tarefa que é desafiada pela cultura e exige um grande exercício de alteridade em um contexto onde a "aldeia global" se limita ao plano técnico e econômico, não alcançando o social, cultural e político.

Visando uma real coexistência intercultural, deverá ser cunhado um conceito democrático capaz de ordenar a diversidade de culturas aos moldes do que era, inicialmente, a grande aposta política da "aldeia global". Esse desafio consiste em aceitar a heterogeneidade social e construir uma identidade cultural coletiva. Em outras palavras, uma coexistência de identidades que leve em conta as dimensões sociais e coloque a cultura não "do lado" dos Direitos do Homem, mas no centro deles. (WOLTON, 2004, p. 83, 89 e 91).

Segundo Wolton (2008, p. 199), a reivindicação de identidade cultural nem sempre é sinônimo de um comunitarismo[49] obscuro. Do mesmo modo, nenhuma comunicação generalizada sem retorno significa revalorização da identidade. Premissas que evidenciam uma necessária análise acerca das identidades culturais sob perspectivas distintas: a cultural-relacional e a cultural-refúgio.

---

49 O comunitarismo apresenta-se, historicamente, como teoria da vida social em torno da defesa do bem comum e de sujeitos arraigados na comunidade dentro da qual eles e socializaram. Esta teoria se opunha à Teoria da Justiça desenvolvida por J. Rawls, no início dos anos 1970, que justificava o modo como o liberalismo se desenvolvia (POULAIN, 2001).

Pensar o papel das identidades culturais face à internacionalização da comunicação é examinar uma questão política atrelada a um futuro em que as diferenças sinalizam ser mais relevantes que as semelhanças. Desse modo, a identidade, que por muito tempo foi o obstáculo à comunicação, é, atualmente, pré-condição para que ela exista. Isto posto, a construção de uma identidade cultural-relacional que pugne pelo respeito à universalidade como contraposição a uma identidade cultural-refúgio, muitas vezes agressiva e excludente, torna-se um imperativo categórico (WOLTON, 2004, p. 69).

Neste diapasão, a identidade cultural relacional inscreve a defesa da identidade cultural no âmbito da comunidade internacional, sem abandonar suas reivindicações de identidade. O aspecto relacional se volta à promoção do respeito pelas diferentes identidades culturais. Nesse sentido, pressupõe-se a existência de um projeto político que transcenda as distintas problemáticas culturais e identitárias. Para tanto, ele deve reconhecer a alteridade, confrontá-la e tentar encontrar os meios necessários para, além de reconhecer as identidades mútuas, transcender às diferenças de forma harmônica e universal.

Em sentido contrário, a identidade cultural refúgio visa se contrapor à abertura e a perda de referências e pode levar a uma identidade cultural agressiva, tanto no plano religioso, quanto no comportamental e legislativo. (WOLTON, 2008). Essa identidade cultural é, ao mesmo tempo, a mais perigosa e a mais compreensível manifestação identitária coletiva, uma vez que é nela que se abrigam todos os que se sentem excluídos no que diz respeito ao plano cultural econômico e social. Ela é geralmente hostil aos outros e alimenta exclusões, populismo e até mesmo racismo.

A desestabilização oriunda da globalização reforça essa identidade cultural refúgio, a qual apresenta como uma de suas faces o discurso de ódio que, para Leal da Silva e Bolson Dalla Favera (2017, p.286), consiste na exteriorização do pensamento preconceituoso que incita a discriminação racial, social, ou religiosa em relação a determinados grupos minoritários com o fito de desqualificar pessoas consideradas inferiores. Logo, todos os que partilham de características distintas ou comungam de posições divergentes ao emitente do discurso de ódio são inferiorizados e apontados como inimigos.

Isto posto, trata-se de uma manifestação segregacionista, devido ao seu caráter discriminatório, mas que apenas passa a existir e gerar seus efeitos quando é conhecida por outra pessoa além do próprio autor. É também uma exteriorização odiosa permeada de preconceito na qual não há "espaço para o outro, não há diálogo capaz de gerar conhecimento e consenso, há apenas a necessidade furiosa de estabelecer no outro, distante de si, a fonte da própria indignidade". (ALVES; MISSI, 2016, p.154). Assim, se estabelece uma lógica binária entre o bom e o ruim, isto é, aquele que profere o discurso e a sua vítima.

Nesse viés, Meyer-Plfug (2009, p. 101-104) explana que no discurso de ódio o preconceito pode ser individual, caso em que a pessoa expressa sua posição religiosa ou política como verdadeiros dogmas, ou pode refle ir a intolerância e o preconceito social quando um grupo de pessoas ataca outro. Esse preconceito traz à tona a intolerância e a dificuldade de conviver e respeitar ideias contrapostas. Ou seja, extrapolando os limites da liberdade de expressão, o discurso de ódio se torna um óbice ao exercício de outros direitos fundamentais daquele que o discurso vítima.

Obstaculiza-se, portanto, o diálogo, a construção do conhecimento e se ceifa a liberdade do outro. Desse modo, a liberdade de expressão, ainda que seja um valor importante na sociedade democrática, apresenta-se por vezes como uma cabeça dupla de Janus, cuja face positiva expressa um direito e a outra, negativa, traduz-se como um instrumento de violação da dignidade da pessoa humana.

2. O TRATAMENTO JURÍDICO DADO AO APARENTE EMBATE ENTRE DISCURSOS DE ÓDIO E LIBERDADE DE EXPRESSÃO

O embate entre valores juridicamente tutelados é sempre uma situação bastante delicada e, por vezes, subjetiva, não sendo diferente quando ocorre a ponderação entre a liberdade de expressão e outros direitos. Realidade refletida na visão equivocada e imperante na sociedade atual de que a liberdade de expressão é um direito irrestrito a ponto de se proteger inclusive o discurso odioso.

Tal pensamento, conforme Wolton (2004, p. 38), advém da concepção ocidental de que a liberdade de informação é ligada à luta política pela democracia de tal modo que qualquer ideia de regulação nesse setor ainda é considerada um ataque à liberdade. No entanto, o controle não se traduz necessariamente em uma posição liberticida, podendo ser, muitas vezes um sinal da vontade de proteger a liberdade de comunicação, por meio do não silenciamento de diversas vozes que seriam excluídas do diálogo democrático.

Um exemplo que elucida a incoerência na ponderação entre a liberdade de expressão e outros valores foi o caso nº 13-7017, *Klayman v. Zuckemberg*, julgado pela *Court of Appeals for the District of Columbia Circuit*, em junho de 2014, nos Estados Unidos. De acordo com o relator do caso, a razão pela qual Klayman ingressou com ação contra o *Facebook, foi* a existência, na rede social, de uma página intitulada "*Third Palestinian Intifada*" ou "Terceira Intifada Palestina", na qual continham publicações que incentivavam os muçulmanos a exterminar o povo judeu. A despeito do *Facebook* ter removido o conteúdo, Klayman entendeu que a rede social demorou para indisponibilizar o conteúdo ilícito e, devido a isso, ajuizou ação requerendo indenização, sob o pretexto de que a morosidade na exclusão constituiu uma agressão

intencional e demonstrou negligência por parte do site. (UNITED STATES COURT OF APPEALS, 2014)

Cumpre destacar que no direito norte-americano, prevalece a visão do "mercado de ideias", a qual apregoa que o Estado deve se manter neutro e não coibir a expressão de qualquer pensamento, ainda que equivocado, ofensivo ou preconceituoso. Esse ideário exsurge da tese de que, para a construção do conhecimento, todas as ideias e opiniões devem ser expostas, só sendo cabível a intervenção estatal em caso de violência clara e iminente. (SARMENTO, 2007, p.5)

Com isso, na resolução do litígio em tela, o sistema de justiça norte-americano considerou de maior peso a liberdade de expressão consolidada na 1ª Emenda[50] de sua Constituição, tornando-a um direito absoluto. Trata-se de uma decisão, a qual não se coaduna com um direito que visa, segundo Cendejas Jáuregui (2007, p.60), promover um ambiente onde a exaltação dos direitos do indivíduo e a crença na comunidade entre seres humanos livres e iguais fomentará a realização mais plena de cada um, por meio da aceitação da tolerância visando a germinação das liberdades de consciência e pensamento.

Decisões como esta exarada pela *Court of Appeals for the District of Columbia Circuit* contrariam instrumentos internacionais, tais como o Pacto Internacional dos Direitos Civis e Políticos que prevê, em seu artigo 19, a legitimidade de restrições à liberdade de expressão em virtude deveres que acompanham o seu exercício e são baseados na necessidade de amparar outros direitos e interesses igualmente protegidos. Assim como a Convenção Interamericana de Direitos Humanos que, ao tratar da liberdade de expressão, dispôs expressamente no art. 13.5 que a "[...] lei deve proibir toda propaganda a favor da guerra, bem como toda apologia ao ódio nacional, racial ou religioso que constitua incitação à discriminação, à hostilidade, ao crime ou à violência." (ORGANIZAÇÃO DOS ESTADOS AMERICANOS, 1969).

Elas também desrespeitam o entendimento cristalizado no Parecer Consultivo 05/85, da Corte Interamericana de Direitos Humanos[51] que apregoa a existência de

50 A Primeira Emenda da Constituição dos Estados Unidos protege o direito à liberdade de religião e liberdade de expressão da interferência do governo. Proíbe quaisquer leis que estabeleçam uma religião nacional, impeçam o livre exercício da religião, **reduzam a liberdade de expressão**, infrinjam a liberdade de imprensa, interfiram no direito de se reunir pacificamente ou proíbam cidadãos de requererem uma reparação governamental diante de injustiças. Foi adotada por meio da *Bill of Rights,* em 1791. Esta Emenda foi interpretada pelo Supremo Tribunal Americano como aplicável a todos os órgãos daquele governo federal, apesar de ser expressamente aplicável ao Congresso Americano, no sentido de proibir que esse órgão legisle sobre a adoção de uma religião ou proíba seu livre exercício; ou abreviando a liberdade de expressão ou de imprensa [...], nos seguintes termos: *Amendment I - Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.* (ESTADOS UNIDOS, 1791).

51 A Corte Interamericana de Direitos Humanos foi instada pelo Governo da Costa Rica a se manifestar quanto à inserção da liberdade de expressão no Estado Democrático de Direito,em seu Parecer Consultivo nº. 05 de 1985, afirmando que ela apresenta duas dimensões, pois, "requer, por um lado, que ninguém seja arbitrariamente prejudicado ou impedido de manifestar seu próprio pensamen-

duas dimensões da liberdade de expressão: uma individual e a outra social. Em sua dimensão individual, a liberdade de expressão implica no respeito ao dever de não ceifar ou restringir arbitrariamente de ninguém o direito de manifestar suas opiniões e pensamentos. A dimensão social da liberdade de expressão, por seu turno, visa promover um meio de intercâmbio de ideias e informações para a comunicação massiva entre os seres humanos. (ALVES; MISSI, 2016, p. 158)

Sem sombra de dúvida, a tutela dos discursos de ódio inibe a proteção dessas duas dimensões da liberdade de expressão, pois, cala diversas vozes e, ao invés de promover a comunicação, gera uma real incomunicação. Insta destacar que, embora se verifique no ocidente uma preponderância da liberdade de expressão quando em choque com outros direitos, esse entendimento não é o único existente.

No direito alemão, por exemplo, a liberdade de expressão não é vista apenas como um direito individual daqueles que se exprimem, mas também como um valor objetivo da ordem jurídica democrática que exige, muitas vezes, ações estatais positivas. (SARMENTO, 2007, p. 12). Na França, o nível de proteção dado à liberdade de expressão é ainda inferior ao proporcionado na Alemanha, pois no direito francês se tende a priorizar a tutela de outros interesses, como a ordem pública, o direito à honra e à privacidade quando em choque com a liberdade de expressão. (SARMENTO, 2007, p. 17)

No Brasil, inexiste legislação que trate especificamente sobre os discursos de ódio. Contudo, ainda que o mundo do direito não tenha acompanhado o mundo dos fatos, a ponderação entre a liberdade de expressão e outros direitos recai nos tribunais pátrios. Devido a esse silêncio legal, o Supremo Tribunal Federal firmou o entendimento jurisprudencial de que a amplitude dessa liberdade não pode ser absoluta nem ilimitada. Exegese sedimentada na decisão do *leading case* Ellwanger[52], quando o tribunal expressou que deve prevalecer a proteção aos direitos da personalidade e a dignidade da pessoa humana quando esses colidirem com o direito à liberdade de expressão, diante de um excesso no seu exercício. (STF, 2003)

O Superior Tribunal de Justiça também decidiu inúmeros casos envolvendo discursos de ódio e liberdade de expressão. Dentre eles, se destaca a recente decisão do Recurso Especial nº 1.569.850-RN, onde a corte manteve a condenação do acusado pelo crime de racismo por ter afirmado, em sua página pessoal no *Facebook,* que os nordestinos seriam a "praga" responsável pela reeleição da presidente Dilma Rousseff e que deveriam ser olhados com carinho pelo ebola. (STJ, 2018)

---

to e representa, portanto, um direito de cada indivíduo; mas implica também, por outro lado, um direito coletivo a receber qualquer informação e a conhecer a expressão do pensamento alheio." (CORTE INTERAMERICANA DE DIREITOS HUMANOS, 1985, p. 7)

52 Na decisão do julgamento do Habeas Corpus (HC-82424) ajuizado pela defesa do editor Siegfried Ellwanger o Supremo Tribunal Federal manteve a condenação imposta a ele pelo Tribunal de Justiça do Rio Grande do Sul por crime de racismo contra o povo judeu.

Interessante consignar também que o Superior Tribunal de Justiça reconhece a responsabilidade civil dos provedores de aplicação[53], dentre eles redes sociais como o *Facebook*, por conteúdo gerado por terceiros. A responsabilização civil desses provedores sofreu modificações ao longo do tempo, atravessando da responsabilidade objetiva, fundada na teoria do risco da empresa; para a vicária, na qual o provedor somente responderia quando houvesse possibilidade de controle da informação e ele se omitisse em exercê-la até chegar; e, por fim, à responsabilidade subjetiva até então vigorante.

Essa responsabilidade subjetiva é solidária pelos danos gerados por terceiros, desde que, uma vez ciente da ofensa, o provedor não venha a tomar as providências necessárias para a sua remoção. Necessário destacar que, desde a vigência do Marco Civil da Internet, a ciência deve ser feita pela via judicial, com a indicação da URL *(Uniform Resource Locator)*, ou seja, do endereço da página na internet, onde se encontra a ofensa. (BRASIL, 2014)

A exceção a essa regra ocorre somente quando as publicações forem de caráter mais íntimo com a divulgação de imagens de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado. O termo inicial da ciência do provedor, para fins de responsabilização, será considerado a partir a notificação feita pelo próprio usuário ou por seu representante legal, a teor do artigo 21[54], da Lei n.º 12.965. (BRASIL, 2014). Logo, no contexto pátrio, ainda que haja maior proteção do internauta brasileiro pelo uso abusivo da liberdade de expressão comparado ao direito americano, recai sobre ele o ônus de utilizar-se do aparelho estatal para que a lesão seja obstada, salvo quando o ocorrido se enquadrar nos termos do art. 21 do MCI.

CONCLUSÃO

53 A atual jurisprudência do Superior Tribunal de Justiça, em conformidade com o Marco Civil da Internet, distinguiu duas espécies de provedores. A primeira é o provedor de conexão não responde, civilmente, por danos decorrentes de conteúdos gerados por terceiros, visto que, nesse serviço, apenas se viabiliza o acesso, dá-se a porta de entrada. Não se oferecem aplicações, tampouco há qualquer envolvimento com conteúdo. O segundo trata-se dos provedores de aplicação, há responsabilidade subjetiva e solidária pelos danos gerados por terceiros, na hipótese de uma vez ciente da ofensa, não venha a tomar providências necessárias para sua remoção

54 Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo. Parágrafo único. A notificação prevista no caput deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido. (BRASIL, 2014)

Vive-se ume verdadeira revolução informática, que "não apenas se espalha com uma velocidade fulgurante, mas que se sofistica no que diz respeito à desterritorialização e destemporalização das informações, comunicações e registro de dados" (SALDANHA, 2015). Nesse contexto, onde as fronteiras físicas são rompidas, o discurso odioso contamina a democracia ao excluir, estigmatizar e, consequentemente calar vozes. Dever que encontra óbice na defesa daqueles que entendem ser a Internet uma zona neutra, imune a qualquer tipo de regulação que não seja gerada dentro do próprio ciberespaço.

Será árdua a conquista do equilíbrio nesse domínio, pois, de um lado o dinamismo do mundo virtual exige, sim, uma margem para autoregulação, mas do outro, deve-se assegurar a atuação do sistema de justiça para que sejam garantidos o respeito e a efetivação dos direitos fundamentais. Torna-se claro, portanto, ser imperiosa a busca de novas orientações para refundar o direito tendo como base o questionamento de qual é o seu papel no contexto atual. Assim como uma profícua refl xão sobre as implicações das relações humanas com o ambiente virtual. Contudo, para que se siga em direção a um novo horizonte, é necessário reposicionar a bússola que guia o caminho a ser navegado em meio as turbulentas águas da sociedade em rede. (SALDANHA, 2015)

REFERÊNCIAS

ALVES, Ayala do Vale; MISSI, Márcia Costa. Da liberdade de expressão ao discurso de ódio: uma análise da adequação do entendimento jurisprudencial brasileiro à jurisprudência da Corte Interamericana de Direitos Humanos. In: **Revista da Faculdade de Direito da UFRGS**. Volume Especial nº 35, p. 149-170, vol. esp., dez. 2016. Disponível em:

<http://seer.ufrgs.br/index.php/revfacdir/article/view/69863>. Acesso em: 05 jun. 2019.

BRASIL. Lei nº 12965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.. . Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 19 jun. 2019.

BRASIL, Superior Tribunal de Justiça. **REsp: 1569850 RN 2015/0302695-0**. Recorrente: Ministério Público Federal recorrido: não indicado. Relator: Ministro Sebastião Reis Júnior. Brasília, 2018)

BRASIL, Supremo Tribunal Federal. **Habeas Corpus 82.424-2/RS**. Paciente: Siegfried Ellwanger. Impetrante: Werner Cantalício João Becker. Coator: Superior Tribunal de

Justiça. Relator: Ministro Moreira Alves. Brasília, 2003.

CASTELLS, Manuel. **O poder da comunicação.** 2 ed. Tradução de Isabela Machado de Oliveira Fraga. São Paulo: Paz e terra, 2017

CASTELLS, Manuel. **O poder da identidade.** A era da informação: economia, sociedade e cultura. v.2, 5ed. Tradução de Klaus Brandini Gerhardt. São Paulo: Paz e terra, 2006

CENDEJAS JÁUREGUI, Mariana. Evolución histórica del derecho a la información. **Revista Derecho comparado de la información**, Cidade do México, n. 10, jul-dez, 2007. Disponível em:< https://revistas-colaboracion.juridicas.unam.mx/index.php/decoin/article/view/33136>. Acesso em: 17 jun. 2019.

CORTE INTERAMERICANA DE DIREITOS HUMANOS. Parecer Consultivo nº. 05 de 1985. Disponível em: <http://www.cnj.jus.br/files/conteudo arquivo/2016/04/5a3794bc4994e81fd534219e2d57e3aa.pdf>. Acesso em: 29 agosto 2019.

ESTADOS UNIDOS. First amendment to the american constitutions. 1791. Disponível em:< https://www.senate.gov/civics/constitution_item/constitution.htm#amendments >. Acesso em: 19 jun. 2019.

LEAL DA SILVA, Rosane; BOLSON DALLA FAVERA, Rafaela. Estudo do caso Klayman v. Zuckerberg and facebook: da liberdade de expressão ao discurso do ódio/ Study of the case klayman v. zuckerberg and facebook: from freedom of speech to hate speech. **Revista Brasileira de Direito**, Passo Fundo, v. 13, n. 2, p. 273-292, ago. 2017. ISSN 2238-0604. Disponível em: <https://seer.imed.edu.br/index.php/revistadedireito/article/view/923/1221>. Acesso em: 2 jun. 2019. doi:https://doi.org/10.18256/2238-0604/revistadedireito.v13n2p273-293.

MEYER-PFLUG, Samantha Ribeiro. **Liberdade de expressão e discurso do ódio**. São Paulo: Editora Revista dos Tribunais, 2009.

RGANIZAÇÃO DOS ESTADOS AMERICANOS. **Convenção Americana de Direitos Humanos**, 22 nov.1969. Disponível em: < https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm >. Acesso em: 30 jun. 2019.

POULAIN, Jacques. **Comunitarismo.** Disponível em:<http://www.mondialisations.org/php/public/art.php?id=166&lan=PO >. Acesso em 30 de maio de 2019.

RAIMUNDO, João Pedro Sargaço Dias. **Uma nova frente da proteção de dados pessoais:** a (im)possibilidade de assegurar um eventual direito ao esquecimento. Dissertação de Mestrado em Direito. Faculdade de Direito. Universidade do Porto. Disponível em: <https://repositorio-aberto.up.pt/handle/10216/75966 >. Acesso em: 12 junho 2019.

SALDANHA, Jânia Maria Lopes. **Qual direito para os dados pessoais em tempos de Big data**. Justifica do, 16 mar. 2015. Disponível em: < http://justificando cartacapital.com.br/2015/03/16/qual-direito-para-os-dados-pessoais-em-tempos-de-big-data/> Acesso em: 18 jun. 2019.

SARMENTO, Daniel. **Liberdade de expressão, pluralismo e o papel promocional do Estado.** Revista Diálogo Jurídico, Salvador, nº. 16 maio-junho-julho-agosto, 2007. Disponível em: <http://www.direitopublico.com.br>. Acesso em: 27 de mai. 2019.

SEN, Amartya. **Identidade e violência:** a ilusão do destino. Traduzido por José Antônio Arantes. São Paulo: Iluminuras, Itaú Cultural, 2015.

UNITED STATES COURT OF APPEALS. Larry Elliot Klayman – Appellant v. Marc Zuckemberg and Facebook, Inc – Appellees. Appeal from de United States District Court for the District of Columbia, No. 1.11-cv-00874. Disponível em: <https://www.cadc.uscourts.gov/internet/opinions.nsf/254D33E032BAD82A85257CF60050AB5F/$file/13-7017-1497426.pdf> Acesso em: 02 jun. 2019

WOLTON, Dominique. **La otra mundialización:** los desafios de la cohabitación cultural global. Barcelona: Gedisa, 2004.

EL ESTADO Y SU ROL EN LA REVOLUCIÓN 4.0 Y EL CAPITALISMO DE DATOS

Eje temático: Desafíos legales de la sociedad en red

Autora:
Sonia Patricia Cortés Zambrano
Abogada Universidad Santo Tomás, Especialista en Derecho Constitucional y Derecho Parlamentario de las Universidades Externado de Colombia y Autónoma de Madrid España, Magister en Derecho Público de las Universidades Santo Tomás y Universidad de Konstanz Alemania, Doctora en Derecho de la Universidad Externado de Colombia, Docente Investigadora del Centro de Investigaciones jurídicas y políticas Francisco de Vitoria, Líder del Grupo de Investigación "Doctor Angélico: Iure et Realitas" Conjuez para la Magistratura del Tribunal Administrativo del Meta, Profesora asociada al Instituto Colombo-Alemán para la paz CAPAZ, Investigadora del Centro de Investigaciones y Altos Estudios Legislativos CAEL del Senado de la República. Decana Facultad de Derecho de la Universidad Santo Tomás Villavicencio. E-mail: soniacortes@usantotomas.edu.co

RESUMEN
La revolución del mundo digital y de los datos ha ahondado cada vez más en todos los aspectos de la economía, la sociedad y la política. Se generan grandes y trascendentales transformaciones que afectan al Estado Social de Derecho. Esta revolución ha cambiado no solo la producción industrial, sino también ha impactado la organización y el ejercicio de la política y la economía impactando las relaciones sociales, tales como la prestación de servicios sociales, los mecanismos de participación en el mercado laboral, la prestación de asistencia sanitaria y seguridad social, por mencionar solo algunos. Este documento relata las problemáticas derivadas de la asistencia pasiva del individuo y el Estado en éste gran revolución 4.0 y las demandas de la sociedad en términos de justicia, igualdad, solidaridad, bien común y dignidad humana.

SUMMARY
The revolution of the digital and data world has delved deeper and deeper into all aspects of the economy, society and politics. Large and transcendental transformations are generated that affect the Social State of Law. This revolution has changed not only industrial production, but has also impacted the organization and exercise of politics and economics impacting social relations, such as the provision of social services, mechanisms for participation in the labor market, the provision of health care and social security, to mention just a few. This document recounts the problems derived from the passive assistance of the individual and the State in this great revolution 4.0 and the demands of society in terms of justice, equality, solidarity, common good and human dignity.

Palabras Clave: Capitalismo de Datos, Estado Social, Internet, Regulación Jurídica, Revolución 4.0

Key Words: Data Capitalism, Social State, Internet, Legal Regulation, Revolution 4.0

¿Cómo será la sociedad del futuro? ¿Cuál será el papel del ser humano? ¿Qué función cumplirá el trabajo? ¿Cuál es el papel del Estado como regulador, controlador, vigilante y sancionador?

Nos encontramos en lo que parece ser un relevo de turno, las máquinas tienden a hacer todo lo que hace el hombre y a veces mejor, ¿qué sucederá cuando la inteligencia artificial sea más inteligente que la humana.

Hemos comenzado a vivir una revolución en silencio, sin resistencia, una revolución a la que tres profesores alemanes llamaron "Industria 4.0" y que tuvo lanzamiento en la Feria Industrial de Hanover. El fenómeno y su nombre ha sido altamente debatido en discusiones políticas y económicas, ya a la par se desarrolla el internet de las cosas y los servicios. (Wolfgang Wahlster, 2019) (Centro alemán de inteligencia artificial DFKI)

Hoy se han producido computadores y robots, en forma exitosa, con oídos, manos, pies y con algo de razón para impulsar el desarrollo de la fábrica del futuro. Grandes y eficaces sistemas robóticos superan al ser humano, incluso en el campo de percepción sensorial.

El concepto de industria 4.0, sin duda cuestiona la figura del hombre como factor de producción, producción en masa, eliminando millones de puestos de trabajo. Por primera vez las nuevas tecnologías destruirán más puestos de trabajo de los que podrían generar; para el mismo rendimiento económico se requieren menos trabajadores. Es predecible una crisis laboral a una escala sin precedentes, un cambio de gran impacto de larga escala sobre la economía y la sociedad, lo que genera sentimientos sin duda contrarios al optimismo y entusiasmo 4.0.

Como consecuencia de la digitalización en el mercado laboral, hay un 97% de probabilidades de desaparición de carreras profesionales, un 89% de actividades auxiliares, y un 98% de desaparición de tereas de gestión de almacenes, todo ello hay que ponerlo en perspectiva, los puestos de trabajo poco calificados, los no calificados y los técnicos, son los primeros en ser llamados a desaparecer y profesionales reemplazados por procedimientos sistematizados, las máquinas reemplazando al ser humano.

Las empresas están en la competencia acelerada de automatizar los procesos de producción, obteniendo el máximo de beneficio, es decir las máquinas podrían decidir cuándo aumentar o disminuir el nivel de producción según factores de costos.

Es prioridad regular la responsabilidad de las empresas y de los estados frente a los derechos de los trabajadores, en la medida en que se están creando nuevas modalidades de trabajo y de trabajadores, los virtuales, a quienes parece regir el modelo comercial de hacer dinero con la venta de información y datos. Los teletrabajadores y en general las nuevas tendencias de modelo de trabajo, están orientadas a eliminar la protección social y el salario mínimo. Se cuantifica lo que puede hacer el trabajador en una hora y su valor está estandarizado entre 8 y 12 euros y el mayor competidor es el avance tecnológico la competencia la determina el avance tecnológico que no se detiene.

Paul Jorion (2019), plantea como cuestión filosó ca, que es necesario entender si el ser humano está creando algo que estará y se mantendrá cuando haya desaparecido, o algo con lo que puede convivir en armonía. Hoy, por ejemplo, existen productos Software, que reemplazan a los analistas de una empresa, y este Software, actúa como un médico empresarial, automatizado, que revisa cuidadosamente la información completa de la compañía, y sobre ese informe elabora una muestra del perfil de la empresa, sus debilidades, sus fortalezas, y ayuda a la empresa en el proceso de toma de decisiones importantes como por ejemplo en que invertir tiempo y dinero.

Estamos frente a un cambio cultural importante, socioeconómico, que conduce a una pérdida masiva de empleos, causante de gran dolor, destructor de esperanzas de quienes piensan, que al tener un título universitario y están bien capacitados, tienen un trabajo seguro. Este cambio traerá muchas cosas buenas, pero también grandes perjuicios. Las computadoras ya no solo reemplazan trabajos de operarios fabriles, éstas son tan inteligentes que reemplazan a oficinistas, y a empleados administrativos.

Por ello hoy se requiere una formación totalmente diferente y una legislación que responda a las necesidades constitucionales vigentes, éste es el gran desafío, que tiende a que las consecuencias de esta revolución económica 4.0, no avasalle los principios del Estado Social.

Joe Shoendorf (2019), del Foro Económico Mundial, insiste en que esta revolución no solo hace innecesarios a millones de trabajadores, sino a muchos consorcios internacionales. Silicón Valley, funciona sin duda como un semillero de trabajadores de la economía digitalizada, y como producto hay personas tristes con rostros de melancolía servil, impulsando procesos que fortalecen la tendencia de cuantificarlo todo para poderlo controlar, manejarlo mejor, un régimen de perfeccionamiento continuo, productividad ya al extremo. Silicón Valley, pretende ser un generador de resolución de problemas de orden social, político y humano, el cual puede resolverlo todo si se aplica en forma eficiente y eficaz la tecnología.

Justamente debido a la automatización y a la revolución industrial 4.0, será más importante la creatividad, la intuición, la empatía, lo romántico. Si realmente el individuo debe someterse a competir en términos de rendimiento, de automatización, de inteligencia artificial, de robótica, y los únicos índices de su obra son la eficiencia y el incremento de la productividad, entonces está fuera de juego. (Leberecht, 2019)

Por tanto, el Estado debe generar espacios protegidos por la ley, para la creatividad, la intuición, la individualidad, el cual siempre irá acompañado de un margen de pérdida de control por parte de la empresa. Sin duda surge una transformación que pone en las artes y las humanidades un foco de luz con un nuevo significado.

LAS NUEVAS RELACIONES LABORALES Y LOS NUEVOS MERCADOS

El trabajador tiende a ser hoy un nómada, un migrante moderno que se gana la vida con ayuda de Internet y las posibilidades es digitales, son independientes y ejecutan sus propios proyectos.

Las relaciones laborales permanentes en el tiempo son cada vez más escasas, hoy las personas luchan con esa "cuestión de honor" de tener trabajo, no poder realizar un aporte al bien común en esta sociedad, significa no ser un miembro respetado por la sociedad y ello es justamente el origen de la presión enorme laboral a la que se someten las personas. La muerte por exceso de trabajo ocurre porque empleados por lealtad a sus empresas, miedo al despido pasan la mayor parte del día en el trabajo, no toman vacaciones u y trabajan aun estando enfermos, y pese a ello, los gobiernos insisten, por la forma de trabajo que fomenta la automatización, la revolución de los robots.

Los grandes problemas sin solución en todo el mundo, son la seguridad de los datos, la protección contra ataques cibernéticos y la manipulación de la información. El Estado a través de la regulación, debe generar acuerdos legislativos que sean la conexión o el puente entre los distintos actores sociales para la gestión de intereses en el marco de los principios de Justicia, igualdad, libertad, dignidad humana, bien común, y solidaridad. Es una cuestión de poder, el desarrollo tecnológico siempre tiene que ver con la dominación.

Cuando una persona ingresa a un motor de búsqueda, necesariamente visibiliza sus propósitos, intensiones y deseos, al hacer uso de la digitalización, se pone en manos de quienes tienen el poder, entrega sus datos y poseen la tecnología para ejercer influencia sobre ella, para que haga o no determinadas cosas.

Google, Facebook, Apel, Microsoft, Amazon, ¿qué es lo que estas empresas de internet hacen en nuestro mundo globalizado?

El cambio de la era industrial a la era de Datos es absolutamente trascendental, le asiste mayor relevancia, a la transición de la sociedad agrícola a la sociedad industrial, y en la era digital de los datos empresas que negocian con datos, lideran este cambio radical, que empezamos a sentir en la actualidad. Satariano A. (2019)

Si queremos entender la dinámica de estas empresas, en necesario salir y analizar las dinámicas del mercado Mesón M. (2019) ... En el mercado se reúnen vendedores y compradores y una cantidad increíble de productos y tal vez aquello que uno necesita. Analizando, cómo funcionan los mercados en línea, empresas gigantescas como como Amazon, con millones de productos diferentes, son sin duda acaparadoras del mercado, en los albores del internet, cuando muchas personas intentaron replicar el modelo de mercado digital , simplemente ofrecían muchos productos y no funcionó muy bien, solo Amazon tuvo éxito, y en que radicó el hecho de que ésta empresa controle casi la mitad del comercio en línea de Estados Unidos y de Alemania, ésta empresa vende

de todo y usa los datos para cargar de eficiencia y efectividad esta actividad económica en red global.

Si analizamos, en un mercado en línea, dejamos que nos interesen cosas que antes no nos interesarían en un mercado convencional, para comprenderlo, nos situamos en un mercado clásico, sería como si estuviésemos caminando por el mercado y como si detrás nuestro estuviese un vendedor observando lo que nos llama la atención, lo que probamos, los precios que comparamos, las calidades y preferencias que buscamos y el registra todo, para luego usar la información, para generar ofertas de productos que sin duda se ajustan a nuestras preferencias.

Pero que es lo que no está bien aquí, quienes se dedican al a protección de datos, advierten que el almacenamiento de los datos personales que realizan estas grandes compañías, cuando se realizan compras, o cuando solo se explora el mercado, necesitan de regulación.

En Europa, las empresas por disposición legal, se encuentra obligada a poner a disposición, los datos almacenados, y ellas se toman su tiempo. Estas empresas registran movimientos de cada año, 15 mil o más clics registrados y si se imprimiera el registro de datos obtenidos de una persona en un año, éste abarcaría cerca de 15 mil páginas. Por cada clic se completan y procesan hasta 50 columnas de información. El registro contiene no solo el segundo del tiempo en que se hizo el clic, que tipo de productos miraba, sino también la ubicación, el tipo de proveedor de telecomunicaciones utilizado, y que páginas lo direccionaban a la compra o a la empresa proveedora del servicio. Mesón M. (2019).

Estas empresas que almacenan datos saben cuándo la persona está de vacaciones, y hasta pueden establecer perfiles detallados de los usuarios. Estas empresas que capitalizan datos lo hacen de manera eficiente y muy completa, la frase. “mis datos me pertenecen”, no es una verdad.

Los expertos aseguran que es una batalla perdida, exigir el uso controlado de los datos, por estas empresas, las grandes compañías que almacenan y comercian con datos, observa la navegación de cualquiera, y evalúan su comportamiento según la búsqueda de información y lo que hacen con ella. Por ejemplo, compara que productos se compran a menudo, junto con otros productos de la gama, luego los ofrece y advierte quienes han comprado el producto, lo cual suele ser determinante para los consumidores, éste es el juego de la persuasión a través de los datos. Por eso no es de extrañar que el volumen 30% del negocio provenga de las recomendaciones y ello tiene que ver con lo predecibles que somos como consumidores.

El comercio en línea no consiste solo en encontrar el producto correcto, luego de compararlo en sus múltiples características, sino también en encontrar patrones y esto es algo que las máquinas pueden hacer mejor que los humanos y ello les permite reconocer preferencias que ni siquiera nosotros reconocíamos que teníamos.

El secreto está en el análisis de grandes cantidades de datos (BIG DATA), las máquinas de autoaprendizaje reconocen los patrones y es precisamente Amazon quien lidera el uso de ésta tecnología maneja el mercado de alimentos orgánicos más grande del mundo, su propia flota de aviones, seguros, productos farmacéuticos, administra editoriales, marcas de ropa, sistema de pagos y servicios en la nube, produce sus propias películas y programas de televisión en línea, crece en todas las áreas de nuestra vida y recopila datos en todas partes.

¿Cómo se percibe el futuro en el marco de esta realidad? Uno de cada tres empleados en los Estados Unidos depende de las tarjetas de racionamiento de los alimentos del gobierno. En los últimos diez años hubo una explosión en el número de personas sin hogar, gente que trabaja, pero cuyos salarios son muy bajos, mientras que el precio de los alquileres es cada vez más alto, esto es una combinación mortal, que cada día deja más personas sin donde vivir.

Los locales comerciales, las plazas de mercado tienden a desaparecer y estos grandes mercados en línea tienden a ser los únicos distribuidores. En países como Alemania y Estados Unidos la tasa de desocupación es del 40% y en aumento, con un importante número de negocios arruinados. Los métodos de éstas grandes empresas, garantizan una experiencia de compra lo más eficiente posible, pocos empleados, inmediatez de la transacción y entrega inmediata.

Estas empresas tienen tal poder que influencian los mercados, los precios, establecen términos y condiciones para los distribuidores y productores, tienden a ser ellos mismos productores de sus propios productos, acaparando el mercado, se reduce la variedad y esto se conoce como economía planificada.

En los procesos de formación hoy debe incluirse la ciencia de datos digital, para que las personas cuenten con las herramientas que faciliten con protección la toma de decisiones en el mundo digital. Y sin duda debe regularse la publicidad de los datos para el uso global de la información, para democratizar el mercado en tiempos de revolución industrial y globalización 4.0. J. Gamba, CEPAL (2010).

Estamos de cara a una nueva era, pero el hombre no está preparado para ella, no hay una sociedad nueva, la digitalización está trasformando todo lo que hasta ahora era natural al individuo social, la era digital no solo cambia la vida de las personas sino la relación entre ellas y la sociedad, la predicción lleva a intuir que la máquina se convertirá en persona.

La política, la economía y los sindicatos, debaten sobre la revolución 4.0 y los conflictos que de ella se derivan. Política y economía están de acuerdo en que las empresas deben obtener éxito económico, la política es responsable de las condiciones en que se desempeña el trabajador, sin que éste pueda decidir sobre estas condiciones, y por ello es necesario establecer diferentes alternativas de regulación necesarias para proteger derechos de los trabajadores. Deben concertarse condiciones justas y el salario

mínimo es una de ella junto con el establecimiento de las condiciones contractuales laborales, de tal forma que no se presten para prácticas abusivas.

El trabajo temporario y el prestamismo laboral no deben ser una práctica común para el individuo, pues con ello se atacan los derechos fundamentales y humanos de la persona trabajadora. La gran incertidumbre jurídica y política de cara a la implementación de las nuevas tecnologías en el marco de la sustitución de las personas por las máquinas es un temor generalizado. La responsabilidad es de la política, del Estado y sin duda divide la sociedad, ya está dividida en clases, pero sin duda el desarrollo tecnológico conduce a nuevas y profunda divisiones y conflictos sociales.

Sociedades representadas en instancias de decisión europeas, han propuesto el gravar con impuestos la riqueza obtenida por las máquinas que reemplazan al hombre, ya que el proceso tecnológico, constituye un progreso de la humanidad, por tanto, debe ser beneficiosa para el ser humano, por tano si un trabajador es sustituido debe ser indemnizado, pero la propuesta no goza de aceptación, ya que si hoy se pierde un empleo a causa de la robotización, ese dinero aumenta los dividendos de la compañía y las bonificaciones de los accionistas.

Estas grandes empresas de datos se creen al margen de la ley, al margen de los Estados, que no necesitan de éste o aún más que les son un obstáculo. En su actuar siempre hay una provocación, ellos redefinen el mundo y los Estados se desgastan debatiendo, ésta empresas cruzan la línea de los sagrado lo protegido por la ley, por el derecho, la dignidad humana y ello constituye el mayor reto legislativo de nuestro tiempo, la intervención del Estado que debe dirigirse a la universalización de los sistemas de seguridad social, un seguro para los ciudadanos, una renta básica universal a la que todos tengan derecho como base para las actividades económicas. Al parecer en un futuro próximo solo un tercio de la población mundial vivirá del trabajo remunerado.

LA REGULACIÓN DE INTERNET

En este apartado se enfocan algunas transformaciones, que están teniendo lugar sobre la relación entre las sociedades democráticas y el internet, partiendo de la determinación de algunos conflictos y como ellos se abordan en la actualidad a través de la legislación existente. Entonces ¿cómo entender la relación Estado – Internet? La idea es que Internet hoy puede entenderse como un sujeto político, y en cierta manera como un sistema jurídico: con sus jefes, su organización, su autorregulación: facebook, twiter, google, liked in, youtube, bebo, amazon etc. Internet es un estado y estas organizaciones que lo componen son sus territorios, si me permiten la comparación. Y para hablar de la realidad política de internet, es necesario comenzar por sus dirigentes,

el ICANN (Board of Directors), es un ajunta que decide quién puede ser titular de un nombre de dominio, es decir quién puede ocupar un territorio en la red y por tanto tiene poderes reales de gobierno de la ley, y así otros organismos de autogobierno, entre ellos está el World Wide Web Consortium, como un parlamento, si se pudiera pensar, donde se reúnen los principales actores de la red 450 miembros, entre ellos universidades, asociaciones sin fin de lucro, empresas, centros de investigación, regulan los idiomas informáticos, los estándares de los sitios web, las normas sobre propiedad intelectual en la red, y estos organismos son de naturaleza internacional.

Para poder entender la regulación de Internet, y partiendo de ésta realidad ya descrita, debe tenerse en cuenta que internet no es el objeto de regulación, pero existe una relación de fuerza horizontal con los Estados, es decir Internet es un sujeto con el que los Estados deben enfrentarse, y es a partir de allí donde surgen la dificultades más relevantes, sin embargo los Estados trabajan para regular esta relación vertical de control unilateral de la red, mientras que internet y sus organizaciones, responde como una fuerza contractual política.

El intento de los Estados por regular la Internet, han tenido variadas dificultades y conflictos diferente, en algunos casos el Estado ha dictado realmente leyes de regulación, aunque con dificultad, y en otros casos ha sucedido lo contrario, el Estado ha implementado reglas que nacieron en la ley, pasivamente. C. Ruiz Gallardo y J.C. Lara (2007). Particularmente las leyes que versan sobre la privacidad, el control de la publicidad de los espacios virtuales en donde se expresan las preferencias de las personas, instrumentos que tienden a ser muy invasivos. Así todos los sitios operativos, deben insertar una parte explicativa, que solicite autorización de la persona para ingresar al sitio, un consentimiento explícito a través de un link. Lo que prevalecía antes era el interés del sitio sobre la privacidad de la persona.

La regulación de internet ha sido estricta en establecer que la persona debe consentir antes de que estas organizaciones hagan uso de sus datos, lo que sucedió originariamente, fue que estas empresas de la web, usan los datos de la persona libremente hasta que ella se lo niegue expresamente. Y esto ha constituido una revolución sobre el ejercicio de la privacidad, ya que el éxito comercial y económico de estas grandes organizaciones, está en la cláusula de exclusión voluntaria, que manifiesta que en silencio pueden usar los datos de la persona.

En cuanto a la regulación de los nombres de dominio, por ejemplo, el internet quien dicta las normas, es decir corresponde al ICANN, determinar quién puede y como acceder a un dominio en la web, y el procedimiento parece adecuarse a unas reglas de procedimiento administrativo de internet, y pueden ser otorgados a personas de derecho privado y a personas de derecho público, y se siguen dos criterios para la adquisición de un dominio: el criterio del primer solicitante y el de quien ofrece más.

Otro tema regulado tiene que ver con la accesibilidad a la red, conjunto de reglas para que un sitio pueda tener acceso de cualquier persona, sin barreras excluyentes, es decir la obligación de establecer medidas que impidan la exclusión. Estas reglas han sido incorporadas a la regulación de internet de facto, y es así como una norma originada en internet ha sido implementada en ordenamientos jurídicos de los Estados. Incluso, el fenómeno de los datos abiertos, es decir compartir información, bases de datos, sin cobrar comisiones, (open data) nació espontáneamente en Internet y solo posteriormente fue adoptada por la agenda digital de los Estados.

Los Estados comienzan a ver a internet como realidad jurídica, se enfrenta con ella, intuyendo donde es necesario regular y donde implementar en la regulación buenas prácticas. De esta forma se puede crear entre la realidad de la web y los estados una nueva diplomacia informática.

AFECTACIÓN A LAS POLÍTICAS DEL ESTADO

La política laboral comprende la regulación de las medidas públicas, que planifican estrategias para garantizar y crear puestos de trabajo, aumentar las oportunidades para la ciudadanía en busca de empleo y mejorar las circunstancias laborales. (Buhr & otros, 2018). En Estados democráticos, las responsabilidades de gestión corresponden a los ministerios de trabajo y en Estados de bienestar moderados o conservadores, tales como Alemania, regulan sus mercados laborales en forma juiciosa, justa estricta, mientras que Estados liberales como el británico, otorgan más libertad al mercado. La política laboral cumple un papel clave en la generación de infraestructura y contribuye sin duda al desarrollo educativo de los pueblos.

Debido al auge de la digitalización y la automatización, se generan procesos de transformación en sistemas de producción y mano de obra y por ende su regulación. Es también importante poner en relieve, que las consecuencias no tienen la misma repercusión para los distintos actores y clases sociales, lo cual conduce a una polarización social. Es indudable que ante nuevos sistemas de producción existan, nuevas formas de conocimientos, nuevos conocimientos, nuevas profesiones, nuevas tecnologías lo que conduce a la polarización de la demanda laboral.

Entonces cuando hablamos de brecha digital, hablamos de precarización del empleo (Buhr & otros, 2018), por tanto, la consecuencia lógica es la necesidad de un cambio en la política de educación y la política del mercado laboral.

Sin duda alguna, la unión entre políticas industrial, estructural, de tecnología e investigación convergen en la gran política de innovación, de tal forma que la mayor parte de los esfuerzos institucionales de carácter público, han estado orientados al desarrollo tecnológico y la innovación.

La responsabilidad del Estado, debe estar dirigida a su rol fundamental: regulador, vigilante, controlador y sancionador y adicionalmente, es una necesidad en éstos tiempos la creación de una institución estatal, que promueva la agenda digital, estableciendo y garantizando principios de política digital, de los que se derivan oportunidades de desarrollo para ámbitos concretos de políticas (administración pública en el mundo digital, participación digital, educación, política digital, infraestructura digital).

Lo anterior conlleva al fomento de la capacidad de innovación en plena era digital, y ello exige que se repiensen lo fenómenos de aprendizaje en torno a la red, al internet, para poder generar innovación y se transformen las políticas laborales, de tal forma que mejoren la calidad de vida de todos los individuos, es decir fomentar el bienestar de todo el conglomerado social. Por tanto, el llamado a la evolución digital y tecnológica debe estar enfocado al progreso social. Ello implica sin dudas una importante inversión en infraestructura digital, que modernice la economía y el propio estado social.

LA LEGISLACIÓN DE INTERNET EN COLOMBIA

La Corte Constitucional considera que, en materia de controles institucionales tanto en medios de comunicación no virtuales, como virtuales, la libertad de expresión conlleva el mismo grado de responsabilidad. Para el caso la Corte Constitucional ordena, en un fallo inédito, a Google Estados Unidos, el motor de búsqueda en Internet más grande del mundo, el respeto a la legislación nacional en materia de protección de los usuarios y consumidores por ejercer sus actividades en el país.

La Corte establece, que, si bien Google Inc. ha manifestado estar amparado por la legislación estadounidense en materia de libertad de expresión, la protección de datos y contravenciones a los derechos de autor se ven limitados cuando se presentan casos de calumnia, injuria y difamación a través de plataformas que tiene bajo su autoridad.

La Corte Constitucional establece que *"Resulta necesario resaltar que la presencia territorial de Google en Colombia no comporta únicamente una representación comercial aislada, también implica responsabilidades legales y administrativas con las autoridades colombianas cuando se trata de garantizar los derechos de los usuarios de los servicios de telecomunicaciones e Internet que han sido amparados por sentencias de tribunales nacionales competentes"*. Sentencia T-73ª-2017.

Así mismo, la Corte establece que debe realizarse en el Ministerio de Tecnologías de la Información y las Comunicaciones, tal y como lo establece la Ley 1341 de 2009, un registro de todas las empresas proveedoras de servicios de telecomunicaciones e Internet en Colombia con el propósito de brindar mayores garantías en cuanto a la protección de los derechos de los usuarios y consumidores de servicios de telecomunicaciones e Internet en el país.

Algunas de las leyes aprobadas en el Congreso de la República, regulan temas como: Comercio Electrónico, Ley No 527 de 1999, la cual define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, Comercio electrónico.

Ya Colombia ha avanzado hacia la regulación de la actividad digital, y aunque no existen normas que regulen específicamente a las redes sociales, las normas que rigen son las que protegen la información de los datos y salvaguardan la utilización de tecnologías de información y las comunicaciones.

La constitución Política de Colombia en su artículo 15, establece el fundamento que protege a los ciudadanos el derecho a su intimidad personal y familiar y a su buen nombre. Este además les da "derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas".

Así, por ejemplo, se aprueba la Ley 1273 de 2009 modificó el Código Penal para incluir penas para delitos digitales como el acceso abusivo a sistemas informáticos, es así como, las redes sociales que están constituidas en Colombia deben respetar Leyes locales para el manejo de datos, en especial aquellas que brindan derecho a las personas para conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos.

De la misma forma la legislación, transforma a Colciencias en Departamento Administrativo, se fortalece el Sistema Nacional de Ciencia, Tecnología e Innovación en Colombia, el Decreto 1727 de 15 de mayo de 2009, del Ministerio de Hacienda y Crédito Público, que determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información. (Diario Oficial nº 47.350 de 15 de mayo de 2009). La ley 1341 de 2009, que establece los principios y conceptos sobre la Sociedad de la Información y la Organización de las Tecnologías de la Información y las Comunicaciones. La ley 1288 2009, que regula temas relacionados con TIC: Control de pornografía infantil en la Internet, la ley 1286 de 2009, que regula la Universalización de las TIC, Sistema Nacional de Ciencia y Tecnología, Colciencias, desarrollo productivo, la ley 679 de 2001, que regula la Explotación, la Pornografía y el Turismo Sexual con Niños, Niñas y Adolescentes, la Ley Estatutaria 1581 de 2012 que regula la protección de datos, la Ley 1065 de 2006, que define la administración de registros de nombres de dominio .co, el decreto 4540 de 2006, que regula los controles en aduana, para proteger la Propiedad Intelectual, la Ley 1221 de 2008, que regula la promoción del Teletrabajo y se dictan otras disposiciones.

Y la ley 1928 de 2018, que regula el "Convenio sobre la Ciberdelincuencia sobre la obligación de registro de bases de datos. Que son leyes expedidas según lineamientos adoptados internacionalmente.

Sin duda los temas que, de mayor relevancia para los legisladores en Colombia, son los que tienen que ver con actos discriminatorios y violencia en línea, la seguridad nacional, la pornografía infantil y protección de la minoridad en general. Sin duda en los últimos años, se aprecia un aumento paulatino del número de proyectos de ley, que proponen regular importantes aspectos de internet, cuya regulación sugiere tácitamente la misma Internet y las grandes empresas que lo componen.

BIBLIOGRAFIA

Buhr D, Christ C. Frankenberger R. &otros (2018). ¿Hacia el Bienestar 4.0? La digitalización del Estado de bienestar. Friedrich -Ebert -Stiftung. Oficina Madrid. En: http://fes-madrid.org/media/2017_FESpublicaciones/FES_Bienestar_4.0-p2.pdf

C. Ruiz Gallardo y J.C. Lara (2007). Responsabilidad de los proveedores de servicios de internet en relación con el ejercicio del derecho a la libertad de expresión en Latinoamérica, en CELE, Hacia una Internet libre de censura, 2013, p. 68, disponible en: https://bit.ly/1QFZMpg.

J. Gamba, CEPAL (2010). Panorama del derecho informático en América Latina y el Caribe, Disponible en https://bit.ly/2r12brF

Joe Shoendorf (2019), Las máquinas con grandes capacidades de aprendizaje son el próximo desafío de la tecnología. En: https://www.emol.com/noticias/Tecnologia/2015/12/22/765094/Las-maquinas-con-grandes-capacidades-de-aprendizaje--son-el-proximo-desafi -de-la-tecnologia.html

Meson M. (2019). El futuro de Internet se decide en Europa: la modificación de la normativa sobre propiedad intelectual, Recuperado en: https://hayderecho.expansion.com/2019/02/26/el-futuro-de-internet-se-decide-en-europa-la-modificacion-de-l -normativa-sobre-propiedad-intelectual/

Paul Jorion (2019). Des robots intelligents seront nos successeurs. Recuperado en: https://www.pauljorion.com/blog/2019/07/26/des-robots-intelligents-seront-nos--successeurs/

Satariano A. (2019). Europa limita a los gigantes tecnológicos y desata temores sobre libertad de expresión. En https://www.nytimes.com/es/2019/05/14/europa-tecnolo-

gia-activismo/

Tim Leberecht (2019). Amazone. Recuperado en: https://www.amazon.es/l/B00J-GBAUDQ?_encoding=UTF8&redirectedFromKindleDbs=true&rfkd=1&shopping-PortalEnabled=true

Wolfgang Wahlster, (2019). Industria 4.0. En: https://pro-archive.merckgroup.com/es/smart-data-es/llegan-los-motores-de-respuesta/

GOVERNANÇA DA INTERNET

A GOVERNANÇA DA INTERNET NO BRASIL

Eixo Temático: Governança da Internet

Autor:
Luiz Fernando Martins Castro
Conselheiro do CGI.br; Advogado em São Paulo – SP; Doutor em Informática e Direito pela Universidade de Montpellier – França; Diretor-Adjunto de Compliance da Assespro -SP

RESUMO
No presente trabalho é apresentado o tema da Governança da Internet, especialmente como tal temática adquiriu seus atuais contornos e interesse global. O trabalho ressalta a importância do tema, considerando a arquitetura da rede e as diversas implicações políticas, sociais e econômicas decorrentes da forma como se realiza a governança dos recursos e o próprio uso da rede, com especial atenção à garantia de direitos humanos, de acesso e de liberdade econômica e de expressão. Numa segunda parte do artigo é apresentada a forma como se organiza e se organiza a governança da internet no Brasil, através de modelo "multistakeholder" do CGI.Br – Comitê Gestor da Internet, e do seu braço executivo, o Nic.br, dos quais o autor faz parte como Conselheiro (2016/2019).

ABSTRACT
The present paper presents the theme of Internet governance, especially as this theme has acquired its current contours and global interest. The work emphasizes the importance of the theme, considering the architecture of the network and the various political, social and economic implications arising from the way the governance of resources and the use of the network itself, with special attention to the guarantee of Human Rights, access, economic freedom and speech freedom. In a second part of the article is presented the way in which Internet Governance is structured in Brazil, through the multistakeholder model of CGI. BR – Internet Steering Committee, and of its executive arm, the Nic. br, of which the author is part as Counselor (2016/2019).

a) Introdução

No presente trabalho, iremos apresentar a forma como se organiza e se estrutura a internet no Brasil, através do CGI.Br – Comitê Gestor da Internet, e do seu braço executivo, o Nic.br.

Antes de apresentarmos o modelo "multistakeholder" brasileiro de governança da internet, devemos entender o que seria essa governação e identificar qual seria o âmbito de atuação, e concordar com a sua importância para o país.

Mais do que apresentar um modelo conceitual e téorico para o enfrentamento do problema, e tentar então justifica-lo, pensamos que a melhor forma de apresentar o tema passa pelo entendimento do objeto dessa governança, e da relevância dos temas que a justificam.

Vinton Cerf[55], um dos pais da internet, sintetiza a questão de modo preciso ao pontuar que historicamente o sistema evoluiu de forma colaborativa e global, sendo razoável estimar que esta narrativa o continuará caracterizando. A Internet é composta por redes operadas de modo independente, por diferentes atores, submetidos a distintos modelos comerciais. Não existem regras estritas para a interconexão das redes, salvo decisões bilateriais de operadores de interconexão, em termos mutuamente aceitos. Aponta, também, a existência de competição entre diferentes provedores de banda larga, o que resulta em debates sobrea neutralidade da rede, quanto à provisão do acesso. Por fim, relata a existência de temas atuais que desafiam a internet nos dias de hoje, como: o acesso inclusivo, a proteção de dados pessoais, a segurança dos serviços on line, e os efeitos das tecnologias disruptivas que podem por fim a modelos tradicionais de negócios. Também lança luz sobre o evidente paradoxo verificado com o desenvolvimento da internet. Se uma das principais motivações de sua criação foi a eliminação de barreiras para o compartilhamento e acesso à informação, o que se estima já beneficia metade da população mundial, na prática, o que se vê é a crescente redução das barreiras de contenção daqueles que se utilizam da rede das redes para a prática de ilícitos e de comportamentos danosos, como fraudes, assédio moral, bullying, emprego de códigos maliciosos, ataques de denegação de serviço, pornografia infantil, desinformação e propagação de notícias falsas ("fake news"), que se disseminam conjuntamente com conteúdos úteis e provenientes de fontes confiáveis.

Na mesma obra, Raul Echeberría anota que, ainda que metade da população global esteja conectada à internet, o que se tornou pressuposto para o desenvolvimento das atividades humanas, um desafio anterior se impõe, que é o de reduzir a diferença de oportunidades que se gera às pessoas conectadas e àquelas que não possuem esse acesso. E o verdadeiro e maior desafio será conectar todo mundo, de forma que a conectividade possa impactar a vida dos indivíduos, de forma positiva, e em tempos razoáveis.

1. GOVERNANÇA DA INTERNET

1.1. O que é a Governança da Internet ?

Como esclarece Jovan Kurbalija[56] se desejamos tratar da Governança da Internet, seja no Brasil, ou no mundo, precisamos, de início, conceituar ambos os termos. A rede mundial de computadores, ou Internet, surgiu em plena Guerra Fria. Concebida com objetivos militares, seria uma das formas das forças armadas norte-americanas

55 Prefácio da obra "Gobernanza y regulaciones de Internet en América Latina", BELLI Luca e CAVALLI, Olga (Coordenadores), FGV Direito, Rio, 2018.

56 KURBALIJA, Jovan; "Uma Introdução à Governança da Internet"; tradução Carolina Carvalho, Comitê Gestor da Internet no Brasil, 2016.

de manter as comunicações em caso de ataques inimigos que destruíssem os meios convencionais de telecomunicações.

Nas décadas de 1970 e 1980, além de ser utilizada para fins militares, a Internet também foi um importante meio de comunicação acadêmico, *locus* de onde se viu brotar a sua difusão em modo planetário. Estudantes e professores universitários, inicialmente nos EUA, e depois em todo o mundo, trocavam ideias, mensagens e conhecimento científico pelas linhas da rede mundial.

A partir de 1990, a Internet começa a ter amplo alcance, chegando à população em geral, graças ao desenvolvimento da World Wide Web pelo engenheiro inglês Tim Bernes-Lee, possibilitando a utilização de uma interface gráfica, além da criação de sites dinâmicos e visualmente interessantes. Desde então, a Internet cresceu em ritmo acelerado, estando atualmente presente na vida de todo e qualquer cidadão do mundo que de fato faça parte da aldeia global, e participe da sociedade da informação.

E o sucesso da internet foi tão avassalador que este termo transcendeu seu objeto original da rede das redes. Embora a chamada sociedade da informação e a tecnologia da informação e da comunicação (TIC) possam ser entendidos como conceitos mais abrangentes, o uso comum do termo 'Internet' encontrou apoio na rápida transição da comunicação global em direção ao uso do Protocolo da Internet (IP) como principal padrão técnico de comunicação.

A Internet já se tornou onipresente e continua expandindo-se a uma velocidade rápida, não somente em termos de número de usuários, mas também em razão dos serviços OTT que oferece, como o protocolo de voz através da Internet (VoIP), que vem assumindo importante papel nas comunicações interpessoais, substituindo enormemente a telefonia convencional.

Se nos primeiros vinte anos de existência da Internet comercial a preocupação maior dos técnicos e pesquisadores que lhe deram forma foi com a engenharia e a estabilidade da rede, nos últimos dez anos observamos a crescente relevância e preocupação com outros aspectos, mais ligados à vida cotidiana e aos direitos dos indivíduos que utilizam a rede para obter informações, fazer negócios, e mesmo se relacionar com outras pessoas.

Nunca houve dúvida, por parte dos técnicos e professores das universidades onde ela surgiu, tampouco por cientistas usuários da internet, quanto à importância de se assegurar o acesso livre, irrestrito, e sobretudo seguro à rede. Os governos, que possuem a obrigação de fornecer serviços públicos, como educação, segurança, e infraestrutura, também buscam preservar a estabilidade pública da rede. Ativistas da sociedade civil e de organizações não governamentais também estão preocupados com a proteção da privacidade e de outros direitos humanos.

Os gênios criativos de futuros aplicativos como Google, Skype, Facebook, Twitter, ou empresários disruptivos como os criadores de Amazon e Alibaba, estão

espalhados em algum lugar do mundo, navegando e trocando informações na Internet. A criatividade e inovação dessas pessoas não devem ser reprimidas, e, ao revés, devem ser incentivadas, desenvolvendo novas formas mais criativas de se usar a Internet.

Tudo isso importa. E no meio de tantos interesses legítimos, mas por vezes conflituosos, a Governança da Internet pode ser compreendida como sintetiza Kurbalija, como "o conjunto de atividades desenvolvidas por uma ampla e complexa teia de agentes, privados e públicos, nacionais e internacionais, que gerenciam e coordenam os recursos técnicos, protocolos, processos, conteúdos, aplicativos e sistemas que contribuem e sobre os quais foi edificada a rede".

A percepção, cada vez mais ampla, da natureza e profundidade dessa riqueza, altera sobremaneira a forma como governos e sociedade civil se relacionam e mesmo esperam que seja tratada a internet.

1.2. O surgimento e histórico da Governança da Internet

A ideia de Governança da Internet não é uma construção meramente teórica e surge dos debates da Cúpula Mundial da Sociedade da Informação (WSIS/CMSI 2003). Embora tal denominação possa sugerir a existência de alguma autoridade central que gerencie o funcionamento da rede, acessível, isso não é de rigor.

E como vimos da citada fala de Vint Cerf, a governança da internet já não diz respeito exclusivamente à questão do acesso à rede, por qualquer público. Seu alcance abarca toda a Internet e as interações humanas que ali se materializam.

De modo magistral, Stefano Quintarelli[57] esclarece que, embora a internet seja comumente defini a como um espaço de mundos e de relações virtuais, tal entendimento não é rigoroso, pois a internet é absolutamente real, sendo o lar da dimensão imaterial do mundo, e neste século XXI representa a pedra angular das relações sociais e econômicas entre pessoas e empresas.

Aponta o autor que isso também traz preocupações, e que não podemos banalizar ou ignorar esse motor de grandes transformações na sociedade e na economia, rotulando, simplesmente tal fenômeno como esotérico, futurístico, ligados às novas tecnologias, e assim pretender se furtar ao enfrentamento da responsabilidade por seus efeitos. E conclui que cada um de nós deve se preocupar com os efeitos das tecnologias sobre tais mudanças, não sendo possível simplesmente delegar tal responsabilidade a governos, mercado, ou mesmo organizações internacionais.

Por isso tudo, a governança da internet pressupõe que governos, setor privado e sociedade civil exerçam os seus respectivos papéis, aplicando, e colocando em prática,

57 QUINTARELLI, Stefano; "Instruções para um Futuro Imaterial", Editora Elefante, São Paulo, 2019

princípios, normas, regras, e programas em comum que definem a evolução e o uso da Internet.

A Governança da Internet se constrói internacionalmente, por meio de esforços conjuntos, expressados em espaços multilaterais e multissetoriais, onde se busca o consenso para o estabelecimento de critérios comuns de governança que permitam assegurar que a Internet continue a ser "uma rede de redes globalmente coerente, interconectada, estável, não fragmentada, escalável e acessível, baseada em um conjunto comum de identificadores únicos e que permita que datagramas e informação fluam livremente de ponta a ponta independentemente de seu conteúdo legal", como expresso pela declaração do Encontro NETmundial realizado no Brasil em 2014.

Em setembro de 2015, a Assembleia Geral da ONU aprovou 17 Objetivos de Desenvolvimento Sustentável, com 169 metas específicas a serem cumpridas pelos Estados-membros até 2030. A realização dessas metas está intimamente relacionada com as iniciativas de governança da Internet. Garantir os direitos universais é preocupação e meta fundamental da governança da Internet. Mas não é só isso. Hoje em dia, praticamente todos os setores de atividade das sociedades humanas estão relacionados com a internet.

A importância do acesso à internet, como forma de pleno exercício da cidadania é reconhecida pelo Conselho de Direitos Humanos da ONU, que aprovou resolução, em 1 de julho de 2016, no âmbito do direito à comunicação, para garantir "A promoção, proteção e desfrute dos direitos humanos na Internet," afirmando que a liberdade de expressão é um direito universal que não deve ser limitado por fronteiras ou pelos meios utilizados para sua expressão, reconhecendo-se a característica aberta e livre como intrínsecas à própria Internet.

1.3. Dificuldade terminológica

Ocorre que nem tudo é tranquilo na internet - que já contabiliza mais de 4,2 bilhões de usuários, a começar pela definição do que seria a sua governança. Desde o início dos debates sobre governança da Internet, especialmente na fase inicial da CMSI 2003, existe controvérsia em relação ao termo 'governança' e suas várias possíveis interpretações.

De acordo algumas visões, o termo "governança" seria sinônimo de "governo". Muitas delegações nacionais presente naquela Conferência tinham este entendimento inicial, o que sugeriria que a governança da Internet deveria ser assunto próprio dos governos nacionais, e consequentemente, essa matéria deveria ser abordada no nível intergovernamental com a participação limitada de outros atores, especialmente aqueles não diretamente relacionados aos Estados.

Tal interpretação, estrita e estreita, não se alinha com o significado mais amplo do termo "governança", que inclui a coordenação e direção dos assuntos de qualquer instituição, conceito que transcende as instituições governamentais. Este foi o significado aceito pelas comunidades da Internet, uma vez que coincide com a forma como a Internet foi criada, cresceu e tem sido governada desde o seu início.

A dificuldade terminológica agravou-se ainda mais quando da tradução do termo inglês "governance" para outros idiomas. Em espanhol, o termo refere-se basicamente a atividades públicas ou ao governo ("gestión pública, gestión del sector público, e función de gobierno"). Na mesma linha, a referência a atividades públicas, ou ao governo, também aparece no francês ("gestion des affaires publiques, efficacit de l'administration, qualité de l'administration, e mode de gouvernement"). O mesmo padrão está presente no português ao se referir ao setor público e ao governo (gestão pública e administração pública).

1.4. Arquitetura da Governança da Internet

Outro aspecto que também gera questionamentos é a forma como deveria se estruturar a governança da internet.

Uma primeira proposta seria a de uma estrutura de governança descentralizada, a refletir a própria natureza da Internet, que é a rede das redes. Este modelo considera que a Internet é tão complexa que não pode nem deve ser colocada sob uma governança única, centralizada, como por exemplo de uma organização internacional, e que a governança descentralizada é exatamente um dos principais fatores que possibilitam o crescimento da Internet. Esse ponto de vista é basicamente apoiado pela comunidade técnica da Internet e por muitos países desenvolvidos.

Modelo alternativo seria o de uma abordagem centralizada, que encontra apoio, em parte, pela dificuld de prática de vários países que não dispõem de recursos humanos e financeiros suficientes para o acompanhamento das discussões sobre a governança da Internet em um cenário altamente descentralizado e pluri institucional. Tais países, além de não contarem com quadros experientes no tema, têm dificuldade em comparecer às reuniões que se celebram em distintos centros da diplomacia mundial (como Genebra e Nova York), e tampouco acompanhar as múltiplas atividades de outras instituições, como a ICANN, o W3C (World Wide Web Consortium), IETF, e mais recentemente, a Rede Internet & Jurisdiction. Por tal razão, esses países, em sua maioria em desenvolvimento, defendem um único ponto de cobertura (one-stop-shop), preferencialmente dentro da estrutura de uma organização internacional.

Outro ponto complicador é a compatibilização de interesses públicos e privados na governança da internet. Um dos principais atributos da Internet é sua natureza

pública, que possibilitou sua rápida expansão e que incentiva criatividade e inclusão. A forma de proteger a natureza pública da Internet é, e continuará sendo, um dos temas centrais do debate sobre governança da Internet.

Este problema mostra-se especialmente complicado porque uma parte significativa da infraestrutura básica da Internet – backbones, redes locais, satélites – é estritamente privada. A possibilidade de empresas privadas serem requisitadas para administrar seus ativos em conformidade com o interesse público e terem que se submeter a limitações típicas de direito administrativo é uma questão complexa, ainda em discussão, como no caso da tão discutida neutralidade da rede.

1.5. Desafios geográficos e políticos

Acrescendo complexidade ao problema, temos por premissa que a Internet não conhece fronteiras nacionais e que subverte, ou desafia, o princípio da soberania. A comunicação via Internet transcende fronteiras nacionais e o anonimato do usuário incorporado à própria concepção da Internet sugeriu, ao menos inicialmente, que os governos não teriam o direito de controlar os usuários.

Hoje, ainda é difícil identificar exatamente quem está por trás da tela, mas já é razoavelmente simples identificar sua localização geográfica. Quanto mais a Internet considera as bases geográficas, menos eficaz é sua governança, e que se torna ainda mais a complexa, considerada a questão da jurisdição na Internet, que não pode ser resolvida de modo eficaz pelas leis xistentes.

A impotência do exercício do controle sobre usuários e dos conteúdos que circulam na internet tem levado alguns países a buscar, e de fato implementar controles e limitações de uso por seus cidadãos, subvertendo por completo a natureza livre da rede, num processo também conhecido por "Splinternet".

A exemplo da "Muralha" ou firewall construído pelo governo chinês, para bloquear o acesso por seus habitantes a conteúdos tidos por impróprios ou perigosos, a Rússia acaba de aprovar uma lei, dita de "Soberania da Internet", que entrará em vigor em novembro de 2019, que asseguraria ao país ter uma internet "sustentável, segura e completamente funcional". Em realidade, isso passaria pela criação de um domínio nacional centralizado, que além de garantir a manutenção da rede em caso de blecaute em outras regiões, também permita ao governo administrar e supervisionar todo o seu conteúdo[58].

A tecnologia da Internet se desenvolve muito rapidamente. Novos serviços são introduzidos quase que diariamente, criando dificuldades adicionais na organização do debate sobre governança da Internet.

58 Disponível em https://meiobit.com/401172/russia-putin-lei-internet-soberana-isolada/. Acesso em 06 de maio de 2019.

O surgimento de plataformas que exercem coleta massiva e efetivo controle de dados pessoais suscita preocupação com a proteção da privacidade, da liberdade de expressão e proteção da propriedade intelectual, apenas para falar dos problemas mais evidentes e discutidos atualmente, como se denota do amplo debate surgiso em torno da aprovação e início de vigência do RGPD – Regulamento Geral de Proteção de Dados na União Europeia e da LGDP – Lei Geral de Proteção de Dados, n. 13.709/18.

Como em todo conflito humano, a busca do equilíbrio certamente se mostra como a solução mais adequada nos debates sobre governança e políticas da Internet, buscando estabelecer um equilíbrio entre vários interesses e distintos pontos de vista. A busca deste equilíbrio é com frequência a base para o consenso. Só assim será possível ter uma internet segura, inclusiva e que estimule a liberdade econômica, política e o desenvolvimento humano.

2. A GOVERNANÇA DA INTERNET NO BRASIL

2.1. Os primeiros passos para uma governança da internet no país

Como esclarece Carlos Afonso, no posfácio à citada obra de Kurbalija, o modelo de governança da Internet é pioneiro e mundialmente apreciado, por seu multisetorialismo, que deriva da intensa articulação realizada pela comunidade acadêmica e por organizações da sociedade civil na década de 90.

Merecem nota nesse processo as iniciativas de redes acadêmicas que resultaram na RNP-Rede Nacional de Pesquisa e as iniciativas de entidades civis, notadamente o Instituto Brasileiro de Análises Sociais e Econômicas-Ibase, que participou da organização da Eco 92, fazendo com que a Internet pudesse ser parte de uma estrutura de comunicação que ampliasse a participação internacional na conferência. Foi isso que permitiu ao país contar com duas conexões permanentes internacionais à Internet nos EUA, uma das quais permitiu o acesso à Internet dos três telecentros da Eco 92. A conferência marcou o momento em que a Internet chegou ao Brasil para fica , em um processo que levou à formação do Comitê Gestor da Internet no Brasil (CGI.br) em maio de 1995.

2.2. O CGI.br – Comitê Gestor da Internet no Brasil

A criação e a trajetória do CGI.br são marcadas também por outros fatos importantes. O CGI.br foi originalmente composto por nove voluntários escolhidos pelo governo federal, incluindo representantes deste, de operadoras de telecomunicações, de provedores de acesso, da comunidade acadêmica e representante dos usuários.

Coube aos ministérios da Ciência e Tecnologia e das Comunicações a formalização do comitê, cuja missão primordial tem sido exercer as funções de coordenação e governança da infraestrutura lógica da Internet no país, incluindo a administração dos nomes de domínio ".br" e a distribuição dos endereços IP no Brasil.

Desde a sua formação, o CGI.br formulou uma política de governança que define o nome de domínio de topo brasileiro (ccTLD) ".br" como um bem comum, que traduz a identidade do Brasil na Internet. A defesa do ".br" como a identidade da nação brasileira na Internet vai além dos símbolos da nacionalidade. Com o emprego do ".br" a comunidade brasileira expressa a sua diversidade, sua cultura, sua economia, e sua política, para todo o planeta. O uso do ".br" é restrito a pessoas físicas e jurídicas brasileiras, ou com residência permanente no país. Em consequência dessa visão, a função central de gestão de domínios e números IP tem sido desde o início um serviço sem fins lucrativos, sendo que a retribuição anual pelo uso de um nome de domínio custa o mesmo valor qualquer que seja o nome de domínio. Essa anuidade, atualmente em R$ 40,00, ou US$ 10, aproximadamente, é necessária para cobrir os custos anuais de operação e desenvolvimento do sistema de governança, que apresentamos mais detalhadamente a seguir.

O CGI.br também promove estudos e recomenda procedimentos para a segurança da Internet, realiza pesquisas e desenvolvimentos que permitem a manutenção da qualidade técnica e inovação no uso da Internet, bem como promove constantes iniciativas de educação para o uso seguro da internet.

As principais funções do sistema brasileiro de governança capitaneado pelo CGI.br são, estão delineadas no Decreto nº 4.829[59], de 3 de setembro de 2003, a saber:

- estabelecer diretrizes estratégicas relacionadas com o uso e o desenvolvimento da Internet no Brasil;
- estabelecer diretrizes para a organização do relacionamento entre o governo e a sociedade na administração do registro de nomes de domínio, distribuição de números IP e administração do ccTLD br em prol dos interesses do desenvolvimento da Internet no país;
- propor programas de pesquisa e desenvolvimento relativos à Internet em conformidade com elevados padrões e inovações técnicas, bem como estimular a disseminação da Internet por todo o Brasil, buscando oportunidades para agregar valor aos bens e serviços relativos à rede;
- promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais relativos à segurança adequada para redes e serviços;
- coordenar ações ligadas à formulação de normas e procedimentos para a regulação de atividades relacionadas com a Internet;

59 Texto integral em <http://www.planalto.gov.br/ccivil_03/decreto/2003/D4829.htm>

- participar de fóruns técnicos de âmbito nacional e internacional relativos à Internet;
- adotar os procedimentos administrativos e operacionais necessários para que a governança da Internet no Brasil seja realizada conforme padrões internacionais aceitos pelos organismos de governança globais, podendo assinar convênios, contratos e instrumentos semelhantes.

A forma de composição do CGI.br é bastante debatida. Quando de sua criação, até 2004, todos os conselheiros eram escolhidos pelo governo federal. Com forte participação da comunidade acadêmica e entidades civis, iniciaram-se discussões de propostas que objetivam que seus representantes fossem, em sua maioria, membros não governamentais, e que também todos os conselheiros não governamentais fossem eleitos por seus respectivos grupos de interesse.

Como resultado deste processo, o governo federal estabeleceu, por meio do Decreto 4.829/2003, que o número de membros do comitê passasse para 21, assim distribuídos por suas *constituencies*:

- o governo federal indica oito conselheiros;
- as secretarias estaduais de Ciência e Tecnologia indicam um conselheiro;
- entidades civis sem fins de lucro e não empresariais (o chamado "terceiro setor") elegem quatro conselheiros;
- associações empresariais elegem um conselheiro que representa cada um dos seguintes setores:
    - provedores de acesso e conteúdo da Internet;
    - provedores de infraestrutura de telecomunicações;
    - indústria de bens de informática, de bens de telecomunicações e de software;
    - e setor empresarial usuário;
- as associações acadêmicas elegem três conselheiros;
- por fim, um conselheiro considerado de notório saber no campo das tecnologias de informação e comunicação é escolhido por consenso, vaga ocupada por Demi Getschko, tido como o "Pai da Internet " brasileira, desde a criação do CGI.

2.3. O Nic.br - Núcleo de Informação e Coordenação do Ponto BR

Em 2004, com o objetivo de operacionalizar a implementação de várias atividades atribuídas ao CGI.br ou no seu interesse, foi e criada uma associação de direito privado, sem fins de lucro, o Núcleo de Informação e Coordenação do Ponto BR, conhecido pela sigla NIC.br, assumindo funções operacionais e administrativas.

O NIC.br, além de braço executivo do CGI.br, tem entre suas atribuições[60]:

- o registro e manutenção dos nomes de domínios que usam o ".br" , e a distribuição de números de Sistema Autônomo (ASN) e endereços IPv4 e IPv6 no País, por meio do Registro.br;
- o tratamento e resposta a incidentes de segurança em computadores envolvendo redes conectadas à Internet no Brasil, por meio das atividades do CERT.br;
- projetos que apoiem ou aperfeiçoem a infraestrutura de redes no País, como a interconexão direta entre redes (IX.br) e a distribuição da Hora Legal brasileira (NTP.br). Esses projetos estão a cargo do Ceptro.br;
- a produção e divulgação de indicadores, estatísticas e informações estratégicas sobre o desenvolvimento da Internet no Brasil, sob responsabilidade do CETIC.br;
- a promoção de estudos e recomendação de procedimentos, normas e padrões técnicos e operacionais, para a segurança das redes e serviços de Internet, bem assim para a sua crescente e adequada utilização pela sociedade;
- viabilizar a participação da comunidade brasileira no desenvolvimento global da Web, atividade desenvolvida pelo Ceweb.br;
- oferecer suporte técnico e operacional ao LACNIC, Registro de Endereços da Internet para a América Latina e Caribe;
- hospedagem do escritório brasileiro do W3C, que tem como principal atribuição desenvolver padrões para Web.

2.4. Atividades do Nic.br e algumas conquistas

Atualmente são mais de 4 milhões de nomes registrados, o que coloca o domínio brasileiro entre os maiores do mundo. Dentre os cerca de 300 domínios de país que existem (ccTLDs), o ".br" é o 7º mais popular. Em sua evolução, o ".br" manteve suas características específicas, como a preservação da semântica das categorias de nomes. Assim, com a criação de novos subdomínios, passou a ter mais de 120 opções. Há categorias para interesses específicos (como "ong.br", "art.br", "eco.br"), para profissionais liberais ("bio.br", "adm.br", "mus.br", "med.br", "eng.br", entre outros), que identificam cidades (por exemplo, "rio.br", "manaus.br", "cuiaba.br", "floripa.b ", "foz.br"), entre outras. No Brasil, 92% das empresas que possuem *websites* usam o domínio ".br", de acordo com a pesquisa TIC Empresas 2017, do CGI.br, realizada pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br) do NIC.br.

60 Disponível em https://www.nic.br/atividades/ . Acesso em 06 de maio de 2019.

O ".br" está completando 30 anos de existência, com assegurada solidez técnica e operacional. O ".br" diferencia-se de outros domínios, inicialmente por ser restrito a indivíduos e empresas localizadas no país, e por adotar recursos de segurança como autenticação em duas etapas (*token*), resolução de DNS com garantia de segurança e criptografia (DNSSEC).

A resiliência do sistema é aumentada com as numerosas cópias de servidores que possui no Brasil, além de manter servidores estrategicamente espalhados pelo mundo (Estados Unidos, Europa e Ásia). O valor praticado pelo registro, além de estar entre os mais baixos internacionalmente, mantem-se estável por longos períodos.

2.5. Conclusão

Como visto, a abordagem brasileira para a governança da Internet é um exemplo inovador e exitoso de gestão pluralista de bens da comunidade. O CGI.br acompanha ativamente todos os debates sobre temas da governança da Internet, e lidera a maioria das iniciativas nesse segmento, no país, atuando ativa e propositivamente na discussão do tema, com protagonismo regional e mesmo mundial, manifestado por sua ativa participação em processos e eventos como o Fórum de Governança da Internet da ONU (IGF).

Também busca, por seus assessores e conselheiros, acompanhar todos os temas candentes envolvendo a internet (conteúdo, acesso, inclusão digital, privacidade, regulação, uso indevido, entre outros), participando de forma destacada nos principais fóruns, conferências, organismos e eventos internacionais relacionados ao desenvolvimento e governança da Internet. Foi a principal entidade organizadora do IGF 2007 no Rio de Janeiro, do IGF 2015 em João Pessoa, e do Encontro NETmundial, em 2014, em São Paulo.

Em 2009, depois de quase dois anos de diálogo interno, o CGI.br aprovou e publicou seus "Dez Princípios para a Governança e Uso da Internet"[61] – uma carta de referência sobre os princípios estruturantes da governança da Internet construída por consenso de todos os setores participantes do comitê.

Esses princípios foram inspiradores da proposta do Marco Civil da Internet, fruto de vários anos de consultas públicas e debates, entre todos os setores representados no CGI.br, até culminar na Lei 12.965/2014[62], sancionada pela Presidente da República durante o Encontro NETmundial, em 23 de abril de 2014.

Apesar de promover todas essas atividades e realizações cruciais para o desenvolvimento da Internet no país, e da reputação internacional adquirida tanto

61 Disponível em https://principios.cgi.br/ Acesso em 06 de maio de 2019.

62 Disponível em http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm Acesso em 06 de maio de 2019.

pela qualidade como pelo pioneirismo de suas atividades e abordagem de governança, O CGI.br ainda possui o desafio de divulgar esta experiência e seus excepcionais resultados. E procura servir de exemplo de modelo de governança pluralista para a internet a outros países, e mesmo para outros setores que estejam envolvidos na formulação e decisão sobre políticas públicas.

E por fim, tendo tido a honrosa oportunidade de integrar o CGI.br, em indicação de vaga reservada no Setor Governamental ao MCTIC – Ministério da Ciência, Tecnologia, Inovações e Comunicações, participamos com afinco de suas atividades, em foros nacionais e internacionais, buscando, especialmente, a divulgação de suas relevantes atividades junto a órgãos públicos, como o Poder Judiciário, além de entidades empresariais, institucionais (OAB – Ordem dos Advogados do Brasil, e AASP – Associação dos Advogados de São Paulo, por exemplo), além de universidade nacionais e estrangeiras de nossa relação, promovendo troca de conhecimento e aproximação, tão importantes para consolidação de sua presença no cenário nacional e estrangeiro.

ANÁLISIS JURÍDICO-POLÍTICO DE LA GOBERNANZA DE INTERNET Y LA EFICACIA DE LOS DERECHOS HUMANOS EN PERÚ

Eje temático: Gobernanza de Internet

Autora:
Cynthia Raquel Rudas Murga
Docente de la Universidad Nacional Mayor de San Marcos, Lima-Perú. Directora CEO del Instituto de Investigaciones Jurídicas y Cibernéticas (IPIJC) escritora e investigadora del C.A.C. Cuerpo Académico Consolidado Derechos del Siglo XXI, en México y Perú (CTI) dra.crrm@outlook.com; contacto@ipijc.com

"no habrán normas jurídicas justas sin seres humanos justos"

RESUMEN
En la era del "Régimen Global Mixto", la Gobernanza de Internet sigue siendo una piedra angular para el derecho y la política. Asimismo, la Gobernanza de Internet está evolucionando de forma objetiva y participativa en nuestra región, más aún cuando se pretende garantizar la eficacia de los derechos humanos del usuario de la red. Derechos humanos como la privacidad, intimidad, autodeterminación informativa, libertad de expresión, cruce de información y datos, *bigdata*, datos personales, flujo transfronterizo de datos sensibles, *ciberseguridad*, etc. Así, el objetivo de la presente investigación no sólo pretende aportar dos posturas de estudio jurídico y político que permita fijar un modelo sostenible, sólido y eficaz de política nacional instrumentalizada en un Plan Nacional, en la consolidación de una normativa nacional coherente al derecho internacional además de fortalecer la doctrina LawTech.
Por su parte, la UIT y la ONU, consideran necesario la participación del Gobierno, la Sociedad Civil, la Academia, la Comunidad Técnica y el Sector Privado a fin de construir una Gobernanza de Internet, misma que debe ser inclusiva.
Por ende, la Gobernanza de Internet debe coexistir salvaguardando la eficacia de los derechos humanos a fin de cumplir con el objetivo democratizador de la sociedad del conocimiento a través de la regulación e implementación de políticas de Estado aplicables en Perú, en América Latina y en el Caribe, bajo sendos contextos.

I. CONTEXTO HISTÓRICO Y ANTECEDENTES

El comportamiento social en internet, *smart world, cloud computing, big data, datamining*, APPs, el internet de las cosas, ciudades inteligentes, la era digital, la nanotecnología, la biomedicina, la inteligencia artificial y la imaginación prospectiva

tecnológica del futuro están transformando nuestros hábitos de convivencia y supervivencia.

Históricamente la evolución científic -tecnológica después de la segunda mitad del siglo XX, planteo retos, 1980 la distribución de procesadores; 1990 el internet masivo; 2000 uso de los dispositivos móviles; 2010 el internet de las cosas, estimándose para el 2020 el *Smart World* 4.0 naciones y *ciberciudadanos (cybercities)*

La Cumbre Mundial sobre la Sociedad de la Información (CMSI) se desarrolló en dos fases: La primera fase tuvo lugar en Ginebra acogida por el Gobierno de Suiza, del 10 al 12 de diciembre de 2003. La segunda acogida por el Gobierno de Túnez, del 16 al 18 de noviembre de 2005. (PÉREZ, 2008)

Entre los principales hitos creados por la CMSI se tiene el IGF *(Internet Governance Forum)* que es un espacio abierto y descentralizado para el debate sobre políticas que favorezcan la sostenibilidad y solides de internet, que reúne a los gobiernos, el sector privado, colectivos académicos, de investigación, y la sociedad civil.

El Foro de la Gobernanza de Internet (IGF) se construye sobre el esquema de *cooperación multistakeholder.* Este Foro surge como un resultado directo de la CMSI y de los grupos interesados (gobiernos, sector privado, sociedad civil, comunidades científicas y técnicas) para estimular el debate y la discusión, intercambiar información y compartir buenas prácticas. El IGF se realiza todos los años en diferentes partes del mundo, y los participantes contribuyen en condiciones de igualdad en un diálogo sobre cuestiones de políticas públicas relacionadas con internet y su gobernanza. Aunque IGF no tiene la autoridad para la toma de decisiones, puede informar e inspirar a aquéllos que sí están en posición de tomarlas.

Así, el Foro Peruano de Gobernanza de Internet (FPGI) es un espacio de diálogo sobre Gobernanza de Internet en el cual distintos representantes del Gobierno, la Sociedad Civil, la Academia, la Comunidad Técnica y el Sector Privado dialogan sobre el uso y los lineamientos de internet en correlación con los derechos humanos.

Esta interacción con internet, dentro del conjunto descentralizado de redes de comunicación interconectadas con protocolos TCP/IP, de alcance mundial. (VERA, 2010, p. 4) y la interacción de las Tecnologías de la Información y la comunicación (TIC) confl yen en una enigmática convergencia tecnológica-electrónica, de *softwares* e infraestructuras de telecomunicaciones, data e información ambivalente.

II. HACIA UNA NOCIÓN DE GOBERNANZA DE INTERNET

Entre algunas definicio es, "La Gobernanza de Internet (GI) es el desarrollo y la aplicación por los gobiernos, el sector privado, y la sociedad civil, en las funciones que les competen respectivamente, de principios, normas, reglas, procedimientos de

adopción de decisiones y programas comunes que configuran la evolución y utilización de internet". (VERA, 2010, p.4)

Para la UNESCO, la Gobernanza de Internet (GI) es un tema prioritario y potencial para fomentar un desarrollo humano sostenible, construir sociedades del conocimiento inclusivas a bien de mejorar la libre circulación de la información y las ideas en el mundo.

Asimismo, la UNESCO defiende una visión abierta y transparente GI basada en el principio de apertura, que incluye la libertad de expresión, el respeto a la vida privada, el acceso universal y la interoperabilidad técnica. La ética y el respeto de la diversidad cultural y lingüística en el ciberespacio son otras de las principales preocupaciones de la Organización. (UNESCO, 2018)

En esta perspectiva, la GI debido a su naturaleza, estructura, características, elementos y modelos de aplicación es una "política global" conformada por directrices, procedimientos, normas, estrategias y tácticas políticas, con metodología y procedimientos propios de un Estado discurridos en una plataforma inclusiva para la sociedad del conocimiento.

III. LOS DERECHOS HUMANOS EN LA GOBERNANZA DE INTERNET

El tema de los derechos humanos ha sido muy debatido en la CMSI y en IGF, señalando como el conjunto básico de los derechos humanos relacionados con internet a los derechos a la privacidad, libertad de expresión, recibir información, diversidad cultural, identidad lingüística, inclusión de minorías, entre otros derechos, el derecho a la educación necesaria para este mundo digital. (BRUNET, 2015, p. 190)

Por su parte, la AEPD (Agencia Española de Protección de Protección de Datos) en un estudio sobre cómo la huella digital de los dispositivos afecta a la privacidad de los ciudadanos; señala que, en:

> *"más de 14.000 páginas web dirigidas al público español, describe cómo se identifica y rastrea a los usuarios a través de sus dispositivos. El estudio afirma, entre otras conclusiones, que el conjunto de datos recogidos puede ser tan extensos, o enriquecerse de tal forma, que puede llegar a recabar incluso categorías especiales de datos sin que los usuarios sean conscientes de ello. El documento incluye las medidas que pueden poner en marcha los usuarios para tratar de evitar este tipo de seguimiento y una serie de recomendaciones a la industria, tanto a fabricantes y desarrolladores como a las compañías que explotan dato obtenidos a partir de la huella de los dispositivos" (feb.2019)*

Uno de los frecuentes debates versa en la seguridad y privacidad en internet, sobre el mismo, la AEPD publicó, junto al Instituto Nacional de *Ciberseguridad* (INCIBE) y la oficina de Seguridad de Internauta (OSI), la guía "Privacidad y Seguridad en Internet" pues, se trata de un conjunto de 18 fichas prácti as sobre los peligros de la Red y que

contiene respuestas, recomendaciones y consejos para afrontar estas amenazas. La guía se complementa con una serie tutoriales.

Pero qué derecho se defiende, la privacidad o la intimidad. "En el derecho estadounidense el concepto de intimidad se reconoce en el *right of privacy* conforme al *Common Law;* institución que aparece hacia finales del XIX cuando Luis Brandeis y Samuel Warren publican su obra *The right of privacy,* y a partir de entonces ha tenido un abundante desarrollo doctrinal y jurisprudencial." (CIENFUEGOS, 2003, p.47)

Asimismo, "la importancia del derecho a la intimidad radica en el reconocimiento de que, no es suficiente proteger los derechos tradicionales como derecho a la vida, sino que también es necesario remover los obstáculos para disfrutar de una vida plena, sin intromisiones ni obstáculos de ninguna especie"(CIENFUEGOS, 2003, p.2) es así, que a pesar de las diversas normas jurídica que prohíben la intervención de las telefonías o las redes sociales, es el usuario quien debe conocer las implicancias del uso de sus datos en internet.

En la Constitución del Perú (1993) Art. 2, núm. 7, encontramos la figura literal como derecho a la "intimidad personal y familiar"; y el tenor de "privacidad" se otorgan a los documentos (de forma literal). Y sin mayor complicación, ambos conceptos – *claramente diferenciados*- deben ser salvaguardados en internet, a través de la búsqueda de fórmulas más efectivas que nos permitan abordar el problema de los conflictos de jurisdicciones en internet, rol no sólo de los Estados sino de los *Stakeholders* y sociedad civil. Teniendo presente la idea de consenso aproximado, o *"rough consensus"* en el ámbito social, donde cada vez son más las partes implicadas en el ámbito del *"policy-making"*.

En Perú, al respecto se han tomado algunas medidas de protección de los derechos humanos con la publicación de la Ley de Protección de Datos Personales N° 29733, del 2011, su Reglamento del 2013 y modificatorias.

Asimismo, este derecho a la protección de datos personales nace como "reacción al impacto de una tecnología, la cámara fotográfica, capaz de obtener información sin la participación del afectado y ha sido históricamente permeable al influjo de la evolución tecnológica." (SERRANO, 2015, p. 114)

Así, junto al internet se fortaleció la concepción de autodeterminación informativa, control de la información, libertad informativa, habeas data y la consolidación en el derecho fundamental a la protección de datos. Por lo que, garantizar la intimidad y la privacidad no solo constituye una precondición para ganar la seguridad y la confianza del usuario. Bajo esta mención, las revelaciones en 2014 del ex agente de los servicios de seguridad estadounidense NSA y de la CIA, Edward Snowden sobre la seguridad en internet fueron el último elemento que contribuyó a la puesta en marcha de este cambio tan significativo del modelo de gestión de los recursos críticos.(SERRANO, 2015, p.11)

Es así, que el compromiso que asume cada Estado versa en garantizar los derechos humanos bajo el principio del *cyberbienestar* en la red, respetando la existente connotación que se tenga sobre intimidad o privacidad.

La GI también implica el estudio de los derechos humanos en la edificación de las "Ciudades Inteligente", asumiendo un sistema de energía, agua, gas conectados a la red, dispositivos eléctricos interconectados, postes de luz con *wifi*, semáforos inteligentes, transporte público *smart*, sistemas de drenaje en red, etc. ¿Qué nos motiva a pensar en el desarrollo del *cyberciudadano?* Interconectado con "todo", en nuestra realidad de megalópolis de analfabetismo y posibles ataques en red, situación que más allá de estructurar ciudades "inteligentes" deberíamos formar personas "inteligentes".

Otra cuestión sobre este punto versa en quién o quiénes financiarían esta mega inversión, las entidades públicas o las entidades privadas; y, quiénes tomarías finalmente las decisiones.

Otro derecho muy defendido es la neutralidad en la red, prohibiéndose de manera expresa las prácticas de bloqueo o degradación de contenido en determinados países. (SERRANO, 2015, p. 200) En Perú, se está trabajando al respecto, pero lo más próximo es la existencia de la Directiva N° 001-2019-PCM/SEGDI, "Directiva para compartir y usar Software Público Peruano", del 17 de abril de 2019.

Todas estas prácticas en el espacio cibernético se manifiestan a través, de la cultura informática, Eduardo Castellanos, afirma: "es todo un reto para el Estado y para la sociedad en general, comprender que esta serie de datos nos permita establecer que en el presente siglo se ha creado más riqueza que en cualquier otra época". (2006, p. 30)

En efecto, el ecosistema digital nos ha transformado y la revolución digital con todo su digitalismo, continuará alimentando el sin sentido más deshumanizante mientras siga impasible ante tantos y tantos náufragos. (PÉREZ, 1998, p, 225)

A continuación, se presentan algunos indicadores del Servicio Móvil, que evidencian la extrapolación el ecosistema digital en el acceso a la red en porcentajes por departamentos en Perú.

Información a fin de periodo de líneas en servicio con el Código de Área de Localización (LAC).

Región	2013	2014	2015	2016	2017	2018	mar-19
Amazonas	0.86%	0.89%	0.92%	0.94%	0.95%	0.90%	0.90%
Ancash	3.46%	3.57%	3.33%	3.44%	3.56%	3.60%	3.57%
Apurímac	1.19%	1.19%	1.18%	1.15%	1.08%	1.02%	1.14%
Arequipa	5.65%	5.56%	5.47%	5.34%	5.29%	5.27%	5.28%
Ayacucho	1.89%	1.93%	1.97%	2.00%	2.00%	2.02%	2.01%
Cajamarca	3.61%	3.70%	3.76%	3.80%	3.94%	3.77%	3.72%

Callao	1.48%	2.63%	3.21%	3.32%	3.23%	3.34%	3.51%
Cusco	4.03%	4.01%	4.02%	3.82%	3.54%	3.26%	3.79%
Huancavelica	0.85%	0.89%	0.92%	0.89%	0.92%	0.81%	0.84%
Huánuco	2.04%	2.03%	2.12%	2.08%	2.05%	1.90%	2.05%
Ica	2.99%	2.94%	2.93%	2.99%	3.09%	3.22%	3.06%
Junín	3.91%	3.89%	3.94%	4.03%	4.06%	3.92%	3.92%
La Libertad	5.94%	5.93%	5.79%	5.78%	5.91%	5.97%	6.01%
Lambayeque	3.81%	3.77%	3.74%	3.75%	3.61%	3.54%	3.72%
Lima	40.45%	39.04%	38.41%	38.24%	38.17%	39.56%	37.90%
Loreto	1.52%	1.58%	1.68%	1.74%	1.75%	1.74%	1.82%
Madre de Dios	0.64%	0.60%	0.60%	0.62%	0.56%	0.52%	0.65%
Moquegua	0.72%	0.71%	0.71%	0.72%	0.74%	0.70%	0.68%
Pasco	0.72%	0.76%	0.78%	0.77%	0.74%	0.69%	0.71%
Piura	4.88%	5.02%	4.97%	4.96%	4.95%	4.84%	5.06%
Puno	4.11%	4.07%	4.09%	4.10%	4.14%	3.94%	3.94%
San Martín	1.98%	2.07%	2.15%	2.16%	2.24%	2.11%	2.26%
Tacna	1.31%	1.27%	1.31%	1.35%	1.43%	1.40%	1.38%
Tumbes	0.73%	0.74%	0.70%	0.72%	0.71%	0.67%	0.70%
Ucayali	1.24%	1.22%	1.29%	1.31%	1.33%	1.30%	1.39%
Total Perú	100%	100%	100%	100%	100%	100%	100%

Fuente: OSIPTEL, Perú.

Dichos indicadores fluctúan alrededor de los 5 millones. El 17 de junio de 2019, la empresa Entel Perú S.A. ha efectuado correcciones en la cantidad de líneas por departamento en la modalidad de control, correspondiente a los meses de enero y marzo de 2019, se concluye que la mínima variable es 0.65% del Departamento de Madre de Dios y la máxima de 37.90% para Lima. Situación crítica para el Perú, y que pone en vitrina un tópic de la Gobernanza en esta parte de Iberoamérica.

Sobre la Gobernanza de Internet (GI) se tiene lo siguiente:

- Características principales de la GI: Descentralizado, Modelo multiparticipativo (*multistakeholders*), un Marco Colaborativo, y el Principio de subsidiariedad.
- Temáticas de la GI: Tecnología, Temas socioeconómicos, Desarrollo, Legislación y Política.
- Principios rectores de la GI: Actores (participación abierta, inclusiva y trasparente); Cooperación (supervisión y empoderamiento colectivo); Pericia y experiencia (toma de decisiones basada en el consenso); Información objetiva y empírica (enfoques pragmáticos y basados en la evidencia); Voluntarismo

(éxito determinado por usuarios) e Innovación libre (sin aprobación de una autoridad central). (Quirós, web, p. 17)

- Elementos de la GI: Sociedad digital y los derechos humanos; La cyberseguridad y los mecanismos óptimos para combatir la cyberdelincuencia; La privacidad y la vigilancia masiva; El conflicto e jurisdicción; Guerra Comercial Cibernética; El desarme digital; y el Cifrado para la nube: dos retos de seguridad. 1. La pérdida de control y 2. La pérdida de confidencialidad de los datos

> *"En el primero de los casos, la preocupación surge por la necesidad del cumplimiento regulatorio en relación con los datos de carácter personal además del cumplimiento de los acuerdos de niveles de servicio. En el segundo de los casos, y sobre todo para las modalidades SaaS (Software as a Service) y PaaS (Platform as a Service), el tratamiento de los datos, en la nube es una fuente de preocupación, con el consiguiente riesgo de robo o filtración. Aún no existen soluciones de probada eficiencia que aplique técnias de cifrado homomórfico para salvar esta circunstancia"* (SERRANO, 2015, p. 73)

IV. MODELOS DE GOBERNANZA DE INTERNET

Entre las propuestas más destacadas de Gobernanza de Internet tenemos: La propuesta de Jovan Kurbalija, el director de DiploFoundation Jovan Kurbalija, propuso un modelo de análisis en tres dimensiones "Qué" temas será materia de debate-multidisciplarios, "Quiénes" representan tenemos los Estado, organizaciones internacionales, sociedad civil y sector privado, y "Dónde" marco geográfico de regulación (local, nacional regional global, etc.) (Pérez, 2008, p. 32) y a esto le suma el "Cómo" que ayude a determinar los mecanismos y técnicas de los temas concretos. Así se conforma su Cubo de la Gobernanza.

Por su parte William J. Drake, propone reglas compartidas, procedimientos y programas que potencien las expectativas y prácticas, asignen roles a los participantes y den forma a sus interacciones. En efecto, en un contexto intraorganizacional la gobernanza incluye, mecanismos de gestión jerárquica centralizada, en un contexto intraorganizacional la cooperación es clave para definir programas, procedimientos y reglas comúnmente aceptadas.

Esta teoría más acertada analiza la posibilidad existencial de imposiciones unilaterales de estados y/o entidades poderosas (cita: EUA y Microsoft) arjé que debe radicar en los mecanismos de cooperación y modelos híbridos (ambos).

Una tercera propuesta está respaldada por Ernest J. Wilson III, que propone un modelo general de "gobernanza" que particulariza para el caso de internet. Establece el proceso en varias fases que varían las relaciones establecidas entre los agentes principales de la sociedad. Sostiene que la Gobernanza de Internet es "fruto directo

de las relaciones entre cuatro colectivos básicos de la economía, de cuya interrelación depende las decisiones y acuerdos sobre determinados aspectos de internet que representa en una formación denominada *Quad*", misma que está compuesta por el Sector público, Sector Privado, ONG y I+D.

Asimismo, tenemos la propuesta del Grupo de Expertos en la tabla de comparación:

Modelos	**Kurbalija**	**Drake**	**Wilson III**	**G.E**
Agentes	Estado Organizaciones internacionales Sector privado Sociedad civil	Organizaciones intergubernamentales Sector privado	Quad: Sector público Sector privado I+D Sociedad civil	Estado Organizaciones internacionales Operadores económicos Sociedad civil
Categorías por temas	"cestas" Infraestructuras y estandarización Legal Económica Del desarrollo sociocultural	Categorías: Infraestructuras Transacciones y contenidos	Dimensiones: Derechos de propiedad Eficiencia del mercado Equidad Participación efectiva	Cadena de valor: Recursos críticos Conectividad e infraestructuras Aplicaciones y servicios Usuario fina

Fuente: (Pérez, 2008, p. 36)

Es así, que la discusión sobre los nuevos modelos de GI, internet *universality*, se explican además con el análisis de las siglas ROAM, que significa *Right* (derechos, OGP) Open (abierto y libre) *Access* (multilingüismo, género entre mujeres) *Multistakeholders*, desarrollado en buena parte por la Unesco y organizaciones internacionales.

Por su parte, la Asociación para el Progreso de las Comunicaciones (APC), (Liddicoat, 2016, pp, 1-15) ha segmentado su estudio en las siguientes líneas:

a) La criminalización de la expresión en línea
b) El bloqueo, control y manipulación de contenido de internet
c) La interferencia con la privacidad y protección de datos
d) Las restricciones y vigilancia ilegal
e) Las limitaciones de acceso a internet

Este trabajo, procura plasmas algunas consideraciones que constituyen una violación de los derechos humanos y las libertades fundamentales de la DUDH y del Art. 19 del Pacto Internacional de Derechos Civiles y Políticos. (Liddicoat, 2016, pp. 1-5)

V. ANÁLISIS JURÍDICO Y POLÍTICO DE LA GOBERNANZA EN PERÚ

Nuestro análisis revisa la normatividad vigente, así como las implicancias de las políticas adoptadas en Perú, sin pretender abarcar todas las temáticas sobre GI citamos los lineamiento adoptados en la segunda Cumbre de 2015, *aceptó que todos los gobiernos debían tener un papel relevante en la Gobernanza de Internet para garantizar la estabilidad, seguridad y continuidad de la Red,* pero no se dijo cuáles tendrían que ser las condiciones jurídicas y políticas. Sin embargo, nace la incertidumbre sobre qué tan cierto será la imparcialidad en la toma de decisiones cuando se analizan los fondos de financia iento del Foro de Gobernanza de Internet (públicas: gobiernos finlandés, suizo, holandés, japonés, noruego, y también de organizaciones como la UIT, ICANN, siemens, AT&T, VeriSign, Cisco, Google, por citar algunos).

En efecto, Perú no ajeno a ello, entre algunas medidas de adecuación normativa a través de la Presidencia del Consejo de Ministros (PCM) se ha emitido el Decreto Supremo N° 093-2019-PCM, que aprueban el Reglamento de la Ley N° 30254, Ley de Promoción para el uso seguro y responsable de las Tecnologías de la Información y Comunicaciones por Niños, Niñas y Adolescentes. Amén de la Ley N° 29022, Ley para la Expansión de Infraestructura en Telecomunicaciones, publicada en el Diario Oficial "El Peruano" el 20 de mayo de 2007, cuyo objeto versa en la instalación y expansión de los servicios públicos de telecomunicaciones a fin de eliminar las barreras.

Ley N° 29904, Ley de Promoción de la Banda Ancha y Construcción de la Red dorsal Nacional de Fibra Óptica, del 19 de julio de 2012, cuyo propósito versa en impulsar el desarrollo, utilización y masificación de la Banda Ancha, promoviendo el despliegue de infraestructura, servicios, contenidos, aplicaciones y habilidad dirigidas, a favorecer y facilitar la inclusión social, el desarrollo socioeconómico, y otros.

Uno de los adelantos jurídico-políticos de la GI en Perú, es la tutela de los datos personales, la privacidad e internet según el Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital, 13 de setiembre de 2018. El objeto consiste en establecer el marco de gobernanza del gobierno digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos; así como, el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de proceso y prestación de servicios digitales por parte de las entidades de Administración Pública. Esta Ley regula el gobierno digital, identidad digital, prestación de servicios digitales, interoperabilidad, gobernanza de datos, seguridad digital, entre otros conceptos.

El Decreto Supremo N° 118-2018-PCM, que regula el desarrollo del Gobierno digital, la innovación y la economía digital con enfoque territorial tiene como principal fin el cruce de información e interconectividad de la Data entre los órganos de servicio público del Estado como EsSalud, RENIEC, JNE, *et al*.

Otra de las políticas en Perú se impulsa con la Resolución de Secretaría de Gobierno Digital N° 001-2019-PCM/SEGDI, para compartir y usar *Software* Público Peruano.

Sin embargo, en la praxis jurídica y política se plantea una crítica al Decreto Legislativo N° 1182, Que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, para la "lucha" contra la delincuencia y el crimen organizado. Esta Ley faculta a la policía acceder a cualquier data personal del presunto culpable sin necesidad de una orden judicial. Bajo este supuesto legal, aunado que a la fecha no se tiene algún informe sobre la modalidad de su ejecución, la sociedad se encuentra en un caos en parte fomentado por los medios de comunicación.

Así, como lo dijo Baltazar Garzón, "No es demasiado difícil manipular a las colectividades a través de los medios de comunicación. Cuando el poder es hegemónico o pretende serlo, lo que no se dice o no se da como noticia, no existe." (2005, p. 349)

VI. CONCLUSIÓN

Es así, que en el presente siglo la realidad virtual ha logrado superar a la ficción jurídica a partir de la Cuarta Revolución del Conocimiento; expresión adoptada de la convergencia tecnológica, la innovación electrónica y la internet; así como, del surgimiento de la robótica, la nanotecnología, la biotecnología, la eugenesia, la inteligencia artificial, la tecnología molecular y sobre todo de las innovaciones tecnológicas de la información y comunicación. En este sentido, los impactos multidimensionales son trascendentales en la vida personal, social y jurídica del *ciberjurísta* a fin de evitar la vulneración de los derechos fundamentales, la intimidad, la privacidad, la libertad de expresión, el acceso a la información, la autodeterminación informativa, la Seguridad Nacional, el orden público, los estándares de legalidad (CIDH, 2009, pp. 75-ss.) y el uso de datos personales en las comunicaciones en Internet.

Una de las extensas problemáticas de la Gobernanza de Internet, es el espionaje cibernético, la defensa del Gobierno, la seguridad en internet, la soberanía del Estado, el ciberespionaje global, en América Latina, en el Caribe y en Perú.

En esta perspectiva, el presente aporte pretende determinar los elementos jurídicos esenciales que viabilicen la Gobernanza en la Internet a fin de salvaguardar con total respeto la efica ia de los Derechos Humanos orientados a la formación de una Sociedad del Conocimiento científico y humanista en la presente era digital. Asimismo, se pretende contribuir con la praxis política y jurídica pública, y con propuestas de preceptos legales en beneficio de la comunidad cibernauta.

La entidad pública es la persona indicada de defender el interés de la sociedad y no emitir leyes de manera parcializada, como a la fecha lo vienen realizando en este país y en el mundo.

La hiperinflación normativa, la descodificación legal, la inexistente jurisprudencia vinculante y la carente doctrina son algunas limitaciones que iremos resolviendo con la Gobernanza en la Internet y los Derechos Humanos conforme a la Constitución Política del Perú y el Bloque de la Constitucionalidad del Siglo XXI.

Finalmente, en la era del "Régimen Global Mixto" para la Gobernanza de Internet se desarrollan foros de políticas multilaterales y con múltiples participaciones, sin embargo, cabe la necesidad de construir teorías de manera inductiva; es decir, desde la perspectiva y practica local hacia la construcción de una gran política parte de la Gobernanza de Internet en el marco Internacional.

VII. ÍNDICE BIBLIOGRÁFICO

AGUERRE, Carolina, *et al.*, (2018) Mapeo de las iniciativas de Gobernanza de Internet nacionales en América Latina, Internet Policy, Universidad de Pensilvania.

BRUNET, Laura, (2015) "Gobernanza de Internet : componentes normativos y socios culturales de un ambiente multistakeholder", *Revista de Derecho de la Universidad de Montevideo,* Núm. 25, Instituto de Derecho Informático, Universidad Mayor de la República de Uruguay.

BURGORGUE-LARSEN, Laurence, MAUÉS, Antonio y SÁNCHEZ Mojica, BEATRIZ Eugenia (Coord.) (2014) DHES, Red Derechos Humanos y Educación Superior. Derechos Humanos y Políticas Públicas.

CASTELLANOS HERNÁNDEZ, Eduardo (Coord.) (2006) Temas de Derecho Informático, Secretaría de Gobernación de México.

CIENFUEGOS SALGADO, David, "El derecho a la intimidad y los actos procesales de imposible reparación. La tesis, 1ª. J17/2003, admisión y desahogo de la prueba pericial en genética", *Revista Lex,* México, núm. 101, noviembre de 2003.

GARZÓN, Baltazar, (2005) Un mundo sin miedo, Random House Mondadori.

LIDDICOAT, Joy (Coord.) 20 APC, Los derechos en internet son derechos humanos, Declaración escrita presentada por la Asociación para el progreso de las comunicaciones, una organización no gubernamental en categoría consultiva general, web obtenido 2016.

MAYORCA PÉREZ, Dante (2017) Satisfacción del usuario de telefonía móvil en zonas urbanas del Perú, OSIPTEL, Lima.

OECD (2019) *Digital Government in Peru: Working Closely with Citizens, OECD Digital Government Studies, OECD Publishing, Paris, https://doi.org/10.1787/0c1eb85b-en*.

PÉREZ TAPIAS, José A., (1998) Internautas y náufragos. La búsqueda del sentido en la cultura digital, Editorial Trotta, Naufragos e Internautas, Vid. Derrida, *Adiós a Emmanuel Lévinas,* Palabra de acogida, Trotta: Madrid.

PÉREZ, Jorge (Coord.) (2008) La Gobernanza de Internet, contribución al debate mundial sobre la gestión y el control de la red, colección Fundación Telefónica, Editorial Ariel: España.

PÉREZ, Jorge y OLMOS, Ana (2008) Gobernanza de Internet, *"Internet Governance Forum – IGF, The first two years", Edited by Avri Doria and Wolfgang Kleinwachter in cooperation with the IGF Secretariat*.

QUIRÓS VARGAS, Nancy, Gobernanza de Internet, Gerente desarrollo de capítulos LAC, quiros@soc.org.

SERRANO CALLE, Silvia, (2015) Gobernanza de Internet en España, Foro de la Gobernanza de Internet en España: España.

UNESCO, 20.11.2018, IGF: Internet de Confianza. "Prevención de la violencia juvenil a través de las TIC" Foro de Gobernanza de Internet, París.

VERA QUINTANA, Carlos (Instr.) Gobernanza de Internet, www.gobernanzainternet, 2010

AEPD, 07 de febrero de 2019, https://www.aepd.es/prensa/2019-02-07.html

CIBERSEGURANÇA

INTERCEPTACIÓN Y DIFUSIÓN NO AUTORIZADAS DE LAS AUDIENCIAS TELEMÁTICAS ANTE LA SALA DE CASACIÓN PENAL VENEZOLANA

Eje temático: Delitos informáticos y ciberseguridad

Autor:
Gustavo Adolfo Amoni Reverón
Abogado especialista
Profesor de la Universidad Central de Venezuela

RESUMEN
La participación de los sujetos procesales mediante el uso de Tecnologías de Información (TI) en las audiencias de casación y extradición de la Sala de Casación Penal (SCP) del Tribunal Supremo de Justicia (TSJ), como sucede en cualquier transmisión telemática, implica el riesgo de interceptación y difusión no autorizadas, parcial o total, de ese acto procesal. La Resolución 2016-001 de la SCP remite a la Ley Especial Contra los Delitos Informáticos donde se prevén ciertos tipos penales en los que pudieran subsumirse tales conductas, así como otras previas y posteriores a su celebración. Esto se entiende claramente en los casos de audiencias reservadas por disposición legal, como sucede en casos que involucren niños y adolescentes al igual que en casos de delitos sexuales. No obstante, cabe preguntarse cuáles son las razones para sancionar tal conducta respecto de una audiencia que debe ser pública porque así lo impone la Constitución. En este caso, la justificación se ubica tanto en razones operativas, para facilitar que se mantenga el orden en la sala, como en razones de tutela judicial efectiva, para fortalecer el derecho a la presunción de inocencia y a la privacidad, evitando que los juzgadores sean presionados socialmente por la opinión pública, puesto que nada impediría seguir el avance de un proceso judicial como si se tratara de un espectáculo para el entretenimiento de masas y no como una garantía para la libertad individual. Por tanto, si bien existe el derecho a asistir a audiencias públicas, este derecho está condicionado a la autorización que otorgue el juez, como director del proceso, para ingresar a la sala de audiencias o al recinto privado desde

el cual se participe y, adicionalmente, a la autoridad del recinto oficial desde la cual se intervenga a distancia. Regla que también aplica a la difusión de la audiencia por medios de comunicación en general, o específicamente telemáticos.

INTRODUCCIÓN

Con la participación a distancia de los sujetos procesales en las audiencias ante la Sala de Casación Penal (SCP) del Tribunal Supremo de Justicia (TSJ) venezolano es factible interceptar y difundir dicho acto procesal sin contar con la debida autorización.

A fin de enfatizar las consecuencias penales de dichas actuaciones, vinculadas a la transmisión remota de la audiencia, la Resolución 2016-001 de la SCP (Res. 2016-001) recurre a la Ley Especial Contra los Delitos Informáticos[63] (LECDI) para recordar su aplicabilidad, siendo necesario, en consecuencia, precisar los tipos penales en los que pudieran subsumirse tales conductas para culminar analizando sus elementos.

1. LA REFERENCIA A LA TIPOLOGÍA PENAL EN LA RESOLUCIÓN 2016-001 DE LA SALA DE CASACIÓN PENAL

El artículo 17 de la Res. 2016-001 remite a la LECDI para sancionar a quien intercepte y difunda sin autorización la audiencia remota celebrada ante la SCP, la participación de alguno de los sujetos procesales intervinientes por medios telemáticos y la difusión del registro sonoro o audiovisual de tal acto procesal.

La norma no tipifica hechos penalmente antijurídicos y personalmente imputables (Mir, 2004, p. 147), lo que sería violatorio del principio de legalidad, por lo que era dispensable incluirla en la Res. 2016-001. De hecho, hay otros delitos, no necesariamente informáticos, que pudieran producirse con ocasión de la audiencia telemática; no obstante, luce oportuno destacar estas conductas para alertar, desde el propio texto que autoriza la participación a distancia, que aun cuando la audiencia es pública, solo se ha admitido su divulgación entre quienes ingresen a la sala de audiencias, según su aforo, y quienes fueran autorizados para acudir al lugar de emisión de la intervención telemática.

En consecuencia, debe recurrirse a la ley especial referida para determinar los eventuales delitos que pudieran perpetrarse en relación con la audiencia telemática ante la SCP. Para ello, se clasificarán en dos categorías: 1) los tipos penales que inciden indirectamente sobre la transmisión de la audiencia y que pueden verificarse antes,

63 Gaceta Oficial de la República Bolivariana de Venezuela n. 37.313 del 30 de octubre de 2001.

durante o después de su celebración; y 2) los que afectan directamente la transmisión de la audiencia por lo que son ejecutables de modo concomitante con ella.

2. TIPOS PENALES INFORMÁTICOS QUE INCIDEN INDIRECTAMENTE SOBRE LA TRANSMISIÓN DE LA AUDIENCIA TELEMÁTICA EN LA SCP

A. Tipos penales sobre el sistema de videoconferencia

La LECDI prevé una serie de tipos penales por los que se sancionan conductas realizadas antes, durante y después de la transmisión. Estos son:

1. El acceso, interferencia o uso indebido de sistemas informáticos. Constituyen acciones típicas cuando recaen sobre el sistema de videoconferencia del que dispone el TSJ sin contar con la autorización correspondiente o excediéndose de la que se hubiera obtenido, puesto que al hacerlo peligraría su funcionamiento.

2. El sabotaje o daño a sistemas. A diferencia del tipo penal anterior, con esta norma se sancionaría a quien dañara el sistema de videoconferencia, en su totalidad o solo en alguno de sus componentes. Ambas acciones pueden realizarse por medios informáticos, en el *software,* o por contacto tangible en el *hardware*, ya que el tipo penal no discrimina. Además, la conducta puede ser dolosa o culposa, en cuyo caso se estaría ante el favorecimiento culposo de sabotaje o daño a sistemas o sus componentes. Igualmente, esto puede ocurrir en cualquier momento impidiendo la audiencia.

3. Sabotaje o daño a datos. Es otra modalidad del tipo penal de sabotaje o daño, que, en lugar de recaer sobre el sistema, afecta el conjunto de datos. En este supuesto se sancionarían conductas dañosas sobre los datos que componen el registro en video o en audio de la audiencia, almacenados en el sistema informático de la SCP.

Este tipo penal se agravaría si se produjera por haber introducido un virus u otro programa análogo. Se trata de dañar, incluso hasta su destrucción, pero dejando rastros del registro de la audiencia, total o parcialmente, de modo que no pueda reproducirse, por lo que en el ejemplo descrito sería un delito posterior a la audiencia o a determinado participación telemática.

Si el acto disvalioso produjera la eliminación total, sin dejar rastro del registro de la audiencia o alguno de sus datos, se estaría ante otro tipo penal: la falsificación de documentos, ya que tales registros son documentos electrónicos[64], agravándose la pena si el agente procurase para sí o para otro algún beneficio o un perjuicio para un tercero.

64 Artículo 2 LECDI: "… e) Documento: registro incorporado en un sistema en forma de… video, audio… que contiene data o información acerca de un hecho o acto capaces de causar efectos jurídicos".

Ahora bien, si el agente extrajera datos del registro de la audiencia, mediante los cuales fuera factible identificar a quien haya participado en una audiencia privada, pudiera estarse ante el delito de violación de la privacidad de la data o información de carácter personal que se agrava si se causara un perjuicio al interesado o a un tercero. Si los datos que se difunden son fotos o videos pornográficos de personas menores de 18 años de edad, aplicaría el tipo penal de exhibición pornográfica de niños o adolescentes.

4. Acceso indebido o sabotaje a sistemas protegidos. Si el sistema de videoconferencia estuviera protegido por medidas de seguridad, entendiendo que la jurisdicción es una de las funciones del Poder Público, también pudiera incurrirse en este delito, bien sea por afectar el *hardware* o el *software*, e incluso sin llegar a afectarlo, tan solo ofreciendo el servicio de sabotaje, equipos o programas para tal fin.

B. Tipos penales sobre el registro de la audiencia

1. Revelación indebida de data o información de carácter personal. Usando la LECDI sería válido encuadrar la disposición no autorizada de la grabación de la audiencia que estará disponible en la SCP en dos tipos penales: la revelación indebida de data e información personales y su modalidad agravada, que solo pudieran materializarse luego de la audiencia o, en todo caso, de determinada participación telemática.

2. Espionaje informático. Se perpetra cuando alguna persona, obtenga, revele o difunda indebidamente el video o audio, almacenado en un sistema informático o en cualquiera de sus componentes, de una de las audiencias celebrada ante la SCP.

Solo quien obtuvo los datos usando TI perpetraría la conducta típica, mientras que la obtención por otros medios, como sería adquirirla de un tercero, por ejemplo, mediante un CD, resultaría atípica. No obstante, si quien obtuvo copia del video de la audiencia lo hizo como parte de un plan, pudiera responder como coautor u otra forma de participación criminal, según las circunstancias. En todo caso, los supuestos de revelación y difusión de la audiencia, sin importar el modo de obtención, son conductas típicas.

3. Espionaje informático agravado. El tipo penal anterior se agravaría si el agente persiguiera un beneficio económico y si se pusiera "… en peligro… la confiabilidad de la operación de las instituciones afectadas…" en este caso, del TSJ.

4. Fraude. Este delito se perpetra por el uso indebido de TI, específicament manipulando sistemas, sus componentes, data o información allí almacenada, insertando instrucciones falsas o fraudulentas. Como ejemplos de fraude electrónico pueden mencionarse el *phishing* (Rico, 2013, p. 214 y Fernández, 2007, p. 219), el

pharming (Rico, 2013, p. 214 y Fernández, 2007, p. 220), así como el *spyware* (Fernández, 2007, p. 2018), o una de sus especies, el *Key Logger* (Banesco, 2019).

Sería fraude informático si una persona manipulara el sistema que use tecnologías de información del TSJ o del lugar desde donde participara la persona citada a la audiencia telemática, para que al intentar intervenir en la audiencia, se conectara a una dirección electrónica distinta a la oficial, creyendo que está actuando ante la SCP. Al finaliza , el agente tendría la posibilidad de utilizar tal exposición, "… para conseguir disposiciones o ventajas económicas en favor del autor de la sustracción o de terceros" (Fernández, 2007, p. 218).

En síntesis, la LECDI incluye tipos penales que permiten sancionar tanto a quien afecte el sistema de videoconferencia como a quien altere o use el registro de la audiencia celebrada ante la SCP antes, durante o después de la audiencia o de la transmisión de cierta intervención. Ahora, corresponde analizar los tipos penales atinentes a la afectación o acceso no autorizado durante el desarrollo de las audiencias telemáticas.

3. TIPOS PENALES INFORMÁTICOS QUE INCIDEN DIRECTAMENTE SOBRE LA TRANSMISIÓN DE LA AUDIENCIA TELEMÁTICA EN LA SALA DE CASACIÓN PENAL

La LECDI tipifica el acceso, captura, interceptación, interferencia, reproducción, modificación, desvío o eliminación no autorizados de comunicaciones ajenas, así como su revelación, difusión o cesión sin la debida autorización. Si bien no hace mención expresa de la transmisión de intervenciones procesales por medios telemáticos, resultaría válido subsumir en ambos tipos penales la interceptación y difusión no autorizadas de la participación telemática en las audiencias ante la SCP, donde un sujeto actúa mediante TI confiando en que sus manifestaciones solo serán conocidas por un público determinado, al igual que lo asumen los demás sujetos procesales.

Y es que la transmisión de la audiencia telemática puede ser interceptada y difundida sin autorización siendo sancionables ambas conductas como "violación de la privacidad de las comunicaciones" y "revelación indebida de data o información de carácter personal". El análisis de ambos tipos penales se abordará en los apartados siguientes, donde se definirá el sujeto activo y pasivo, las partes objetiva y subjetiva de los referidos tipos penales, así como el objeto material y el bien jurídico protegido en cada supuesto.

A. Tipo penal de interceptación no autorizada de comunicaciones ajenas: elementos

a. Sujetos activo y pasivo: Cualquier persona puede perpetrar y ser víctima del delito de interceptación no autorizada de comunicaciones ajenas; por tanto, se trata de un tipo penal de sujetos activo y pasivo comunes o genéricos; sin embargo, en el caso del sujeto activo, debe tener conocimientos suficientes en el uso de TI para actuar sobre telecomunicaciones ajenas, y así interceptar tanto la transmisión de la participación remota a la sala de audiencia como en sentido inverso.

b. Parte objetiva del tipo penal: Se pena a quien se valga de TI para acceder, capturar, interceptar, interferir, reproducir, modifica , desviar o eliminar, total o parcialmente, mensajes de datos o señales de transmisión o comunicaciones ajenos, donde resulta legítimo incluir la transmisión de las audiencias ante la SCP. La particularidad de preverse un medio de comisión telemático permite su perpetración, incluso fuera del país.

c. Parte subjetiva del tipo penal: Es un tipo penal doloso de manera que su perpetración culposa es atípica y, por tanto, no punible. El agente debe querer y conocer que mediante su conducta se producirá un resultado dañoso y solo así respondería penalmente por este delito.

d. Objetos: El objeto material es un "… mensaje de datos o señal de transmisión o comunicación ajena…", lo que en el supuesto bajo revisión es la transmisión de la participación a distancia de cualquiera de los sujetos procesales.

En cuanto al bien jurídico protegido, este es la privacidad de las comunicaciones y en el caso de las audiencias telemáticas, ello se traduce en la privacidad o publicidad reducida[65] de la intervención procesal tanto de quienes intervienen desde la sala de audiencias como de quienes lo hacen de forma remota, aspecto que será ampliado en el tipo penal que se presentará a continuación.

B. Tipo penal de difusión no autorizada de comunicaciones ajenas: elementos

a. Sujetos activo y pasivo: Cualquier persona puede perpetrar el delito de revelación, difusión o cesión, de manera total o parcial, no autorizada, de comunicaciones ajenas, en este caso, de la intervención a distancia que realiza quien está fuera de la sala de audiencias así como la participación de los sujetos procesales que actúan desde dicho recinto. Por tanto, se trata de un tipo penal de sujeto activo común o genérico.

65 Es oportuno destacar que el artículo 2 del Reglamento Europeo de Protección de datos (Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016) excluye el tratamiento de datos personales "…d) por parte de las autoridades competentes con fines de… enjuiciamiento de infracciones penales…", lo cual se rige por la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 que busca "… proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales…". En efecto, la Directiva prevé que "no debe impedir que los Estados miembros regulen el ejercicio de los derechos de los interesados… en el marco de un proceso penal, y las posibles restricciones de tales derechos, mediante el Derecho procesal penal nacional".

La situación del sujeto pasivo no es distinta en el tipo penal descrito. En este caso, tampoco se puede tildar de calificado o especial ya que cualquier persona tiene derecho a que sus comunicaciones personales sean respetadas, manteniéndolas tan públicas como lo desee y la ley lo establezca.

b. Parte objetiva del tipo penal. Son conductas típicas penales: revelar, difundir o ceder, en todo o en parte, las imágenes, el audio o, en general, la data o información obtenida sin autorización, mediante el uso de TI.

Revelar es "Descubrir o manifestar lo ignorado o secreto" (RAE, 2018), difundir significa "Propagar o divulgar conocimientos, noticias, actitudes, costumbres, modas, etc." (RAE, 2018), y ceder, "Dar, transferir o traspasar a alguien una cosa, acción o derecho" (RAE, 2018); esto significa que si una persona accede a la transmisión de la intervención de cualquier sujeto procesal en una audiencia ante la SCP, y la hace pública, más allá del grupo de sujetos autorizados para presenciarla, estaría materializando la parte objetiva del tipo penal de "Revelación indebida de data o información de carácter personal".

El *nomen iuris* hace referencia a data e información personales; no obstante, puede haber data o información con un nivel de publicidad controlado, como sucede con las audiencias ante la SCP, donde la publicidad se le otorga mediante la presencia de otras personas en la misma sala de audiencias o desde donde participa a distancia.

No es igual que 20 o 50 personas escuchen un testimonio sobre una persona que no sea parte y cuya fidelidad u honestidad se cuestione en una audiencia, a transmitirlo y dejarlo disponible en Internet sin que el sujeto afectado pueda defenderse o lograr efectivamente su eliminación. Así mismo, pudiera haber pruebas reservadas o aspectos de la vida privada que no guardan relación directa con el proceso jurisdiccional y nadie está obligado a ventilarlas en público.

Ahora bien, cuando se trate de audiencias privadas por disposición legal, la publicidad se reduce a las partes y a los servidores judiciales mínimos para su desarrollo, teniendo en cuenta, como lo afirman Dako, Montero y Barri (Coord., 2017, 25), razones de orden, serenidad del debate, la dignidad humana o los intereses de terceros.

Para incurrir en este delito no hace falta propagar en su totalidad "… las imágenes, el audio o, en general, la data o información obtenidos…" también es posible que la referida difusión sea parcial. Incluso, la perpetración no tiene que producirse por medios electrónicos. Si una persona toma el video almacenado en un archivo del Poder Judicial y lo difunde (vendiéndolo en un CD o simplemente regalándolo) se trataría de un delito informático en los términos de la LECDI aunque no se usen TI para su perpetración.

Concretando, la parte objetiva del tipo penal prevé que un sujeto revele, difunda o ceda, sin permiso y por cualquier medio, una transmisión ajena efectuada mediante TI, como una audiencia de casación o extradición de la SCP.

1. Agravante objetiva: La LECDI prevé que si resultare algún perjuicio para otro, la pena se aumentará de un tercio a la mitad. No se trata de una previsión que debe haber tenido el actor, ya que no hay necesidad de dolo para que se aplique dicha agravante. Aquí lo importante no sería el elemento psicológico centrado en querer el resultado, sino que se produzca un perjuicio a un tercero, que es la exigencia de la norma.

A efecto de una interpretación coherente, deben entenderse incluidos los daños y no solo los perjuicios que es a lo que se refier expresamente la ley. Para ello, sería válido aceptar con Sarmiento, Medina y Plazas que daño es la lesión al bien jurídico tutelado (2017, 112), mientras que perjuicio es un menoscabo del patrimonio de una persona (2017, 109), concluyendo entonces que no habría ninguna afectación excluida debido a la ausencia del vocablo "daño".

Si por el contrario se entiende que daño es la pérdida sufrida por el acreedor[66] (daño emergente[67]) y perjuicio, la utilidad de la que se le haya privado[68] (lucro cesante[69]), la falta de agravante expresa por daño no impediría admitir que este también se incluye en el concepto de "perjuicio" pues sería ilógico sancionar en mayor medida a una persona por haber impedido la obtención de una ganancia eventual que por haber causado una pérdida cierta.

Otro elemento que debe tenerse en cuenta es que además de los perjuicios patrimoniales expresados, deben incluirse los perjuicios "morales", que pueden ser "… daños morales indirectamente económicos…, y los estrictamente morales… con tal que hayan sido consecuencia natural de la infracción)" (Casado, 2015, p. 20) y que pueden definirse como la perturbación del ámbito psíquico y/o físico del ser humano[70], o de la reputación de las personas jurídicas, que es consecuencia de la lesión de un derecho o bien de la personalidad[71]. Es fundamental tener esto claro ya que el bien jurídico protegido en este tipo penal está directamente vinculado a

66 Artículo 1273 del Código Civil venezolano publicado en la Gaceta Oficial Gaceta Nº 2.990 Extraordinaria del 26 de julio de 1982.

67 "Disminución del patrimonio por la pérdida o detrimentos sufridos" (Alessandri, Somarriva y Vodanovic, 1998, p. 35).

68 Artículo 1273 del Código Civil (1982).

69 "Falta de acrecimiento del patrimonio a causa de haberse frustrado por el hecho dañoso la incorporación a aquél de un valor económico normalmente esperado" (Alessandri, Somarriva y Vodanovic, 1998, p. 35).

70 A partir de las refl xiones sobre atribución de personalidad jurídica a otros sujetos como los animales, inteligencias artificiales y la naturaleza, habría que revisar esta definición (Amoni, 2017, 190).

71 Esta definición es una reconstrucción de la expuesta por Diez-Picazo (2008, 91), con la referencia a las personas jurídicas indicada por Blanca Casado (2015, pág. 23).

la esfera de derechos a los que alude el daño moral, como se expondrá en el título dedicado a este tópico.

c. Parte subjetiva del tipo penal: La revelación, difusión o cesión, total o parcial de los hechos descubiertos, de las imágenes, del audio o en general, de la data o información a la que hubiera accedido, capturado o interceptado mediante el uso de TI, supone que el sujeto activo haya actuado con dolo.

En el asunto bajo análisis, quien haga pública la intervención procesal telemática, más allá de los límites de la presencia tangible en la sala de audiencias, tiene la intención de difundir, total o parcialmente, tal acto procesal.

Lo mismo sucede con quien revele o ceda a otro la información, puesto que al tenerla en su poder, el sujeto receptor podrá disponer de ella a su libre arbitrio, incluyendo extender la publicidad del acto fuera de los límites autorizados por el juez con base en la norma procesal penal. Quien actúe así, conoce y acepta tal resultado como posible, en cuyo caso habría dolo directo.

Por otra parte, si se dejare al azar la difusión de la información, sería válido admitir la presencia del dolo de consecuencia eventual, puesto que al actuar con desprecio por el bien jurídico tutelado, sin evitar un comportamiento capaz de generar un resultado dañoso, teniendo el poder de impedirlo o de actuar en otro sentido, se entiende que se ha querido el resultado y que se ha actuado en consecuencia.

Ahora bien, si el sujeto activo estuviera seguro de que su comportamiento no generaría la difusión de la información, actuando para evitarlo y, aun así, se produjera, se estaría en el terreno de la culpa consciente. En este supuesto no habría sanción ya que el tipo penal no admite culpa, sino dolo.

1. Agravante subjetiva: La perpetración de este delito no supone ningún elemento especial en la conciencia del sujeto activo, pero sí hay una circunstancia agravante subjetiva especial: el fin de lucro. Si la revelación, difusión o cesión se hubieran realizado con un fin de lucro, la pena se aumentará de un tercio a la mitad, bastando la simple intención de lucrarse, de obtener un beneficio material, para sí o para otro, aunque esto no llegase a suceder.

d. Objetos: El objeto material es la totalidad o parte de "… los hechos descubiertos, las imágenes, el audio o, en general, la data y la información obtenidas por alguno de los medios indicados en los artículos 20 y 21…"; y el bien jurídico protegido es la privacidad.

En el caso específico de las audiencias telemáticas, se justificaría sancionar la revelación, difusión o cesión de la transmisión de la audiencia a distancia cuando se tratase de una audiencia privada, porque así lo prevé la ley; pero, en las audiencias públicas, donde la propia Constitución establece la publicidad como principio, se justifica por razones operativas y de tutela judicial efectiva

Son razones operativas: 1) mantener el orden en la sala de audiencias o en el lugar desde el cual se participa y 2) resguardar la seguridad del público y demás sujetos procesales, limitando la participación según el aforo del recinto. Para ello, el magistrado presidente de la SCP, en su condición de director del proceso, podrá restringir el acceso y garantizar el correcto desenvolvimiento de la audiencia, tanto en la sala como en el lugar desde donde se interviene a distancia. De esta manera, no se desconoce el derecho a ejercer control social, presenciando la audiencia, sino que el ejercicio de ese derecho estará condicionado a la autorización del juez presidente de la SCP y basado solo en razones de orden y buen desarrollo del proceso, mas no por arbitrariedad.

En lo que concierne a la tutela judicial efectiva, uno de sus elementos constitutivos es el derecho a la defensa, mediante la garantía de los derechos a la reputación, la honra además de la presunción de inocencia[72]. Se trata de derechos previstos en la Declaración Universal de los Derechos Humanos (Art. 12), Pacto Internacional de los Derechos Civiles y Políticos (Art. 14 y 17 n. 1), y en la Convención Americana sobre Derechos Humanos (Art. 8 y 11 n. 1). En el ordenamiento interno venezolano, la Constitución también los consagra (Art. 49 n. 2 y 60), e igualmente sucede en el Código Orgánico Procesal Penal respecto de la presunción de inocencia (Art. 8).

Al penarse la difusión no autorizada de información ajena, por ejemplo, la transmisión telemática de las intervenciones procesales en las audiencias ante la SCP, se pretende evitar la instauración de una "condena" pública sin juicio previo, donde se forma opinión y se castiga socialmente al imputado sin debido proceso, a partir de las noticias recibidas desde los medios de comunicación (Pásara, 2003, p. 4) o de la apreciación de la audiencia que se difundiera por medios informáticos.

Lo expuesto se justifica por la llamada "pena de banquillo" o "proceso paralelo", aspecto que ha morigerado la publicidad de las actuaciones judiciales y que, a partir de las redes sociales, tiene mayor posibilidad de causar los efectos negativos que pretenden evitarse al limitar la audiencia a la capacidad de la sala.

Entre tales efectos perjudiciales destacan: un trato desigual de la información, privilegiando la imputación; información incompleta violatoria de la presunción de inocencia; la asunción de declaraciones como hechos establecidos; un tratamiento de la información acentuado en las personas y no en los hechos; dificultad de lograr un auténtico derecho a réplica; y una mala comprensión del proceso, en especial del rol de los sujetos procesales, lo que lleva a una necesaria formación jurídica de los comunicadores sociales dedicados al área (Dako, Montero y Barri -Coord.-, 2017, 41).

No toda publicidad del caso resulta dañina, ya que luce probable que existan casos que se hayan investigado y sentenciado por presión social, manifestada por los

72 Sobre la afectación del principio de presunción de inocencia como consecuencia de la difusión de noticias sobre procesos judiciales se ha pronunciado Luis Pásara (2003, 6).

medios de comunicación. De ahí que se demuestre la importancia de que tribunales y medios de comunicación social intervengan en su área de competencia: los tribunales, sentenciando y los medios de comunicación, informando. (Pásara, 2003, p. 5)

Una posible solución parcial, pasaría por una mayor explicación acerca del proceso y el uso de un lenguaje más llano en la sentencia, de manera que sea más sencillo para la colectividad entender el fallo y validar su contenido.

Mientras más secreta sea la información sobre el juicio es probable que se especule en mayor medida al respecto. De ahí que pareciera pertinente ampliar la participación en la audiencia, incluso por medios telemáticos, sobre ciertos aspectos que contribuyan a satisfacer la necesidad de información por parte de la sociedad, excluyendo de la transmisión, las discusiones probatorias que afectarían el honor o la reputación.

Es una tarea nada fácil que corresponderá evaluar al juez, en especial para evitar que la vida privada se convierta en un espectáculo para el entretenimiento masivo.

CONCLUSIÓN

La Res. 2016-001 alude a la LECDI para resaltar que la publicidad de las audiencias ante la SCP está limitada al aforo de la sala de audiencias, del lugar de emisión de la intervención telemática y a la autoridad del director del proceso. Quienes irrespeten el derecho a la privacidad de los intervinientes, o publicidad limitada, además de la autoridad judicial, valiéndose de tecnologías de información, incurrirían en responsabilidad penal por la perpetración de delitos informáticos, tanto cometidos en perjuicio del funcionamiento del sistema de videoconferencia que use la SCP como en detrimento de la transmisión de la audiencia telemática desde y hacia la sala de audiencias.

BIBLIOGRAFÍA

ALESSANDRI, A; SOMARRIVA, M.; y VODANOVIC, A. *Tratado de Derecho civil: parte general y especial* (Tomo I), editorial jurídica de Chile: Chile, 1998.

AMONI, G. "Relectura del 'Curso de Introducción al Derecho' de Luis María Olaso (tomo I), desde la perspectiva del derecho de las tecnologías de información y comunicación". *Revista venezolana de legislación y jurisprudencia.* (No 8), Caracas, 2017.

CASADO, B. "El concepto del daño moral bajo el prisma de la jurisprudencia", en *Revista internacional Doctrina y Jurisprudencia* (Vol. 9), 2015

DAKO, F. ; MONTEIRO, V. ; y BARRY, A. *La couverture médiatique des procédures judiciaires (Selon le droit positif centrafricain)*, República Centroafricana, 2017.

DIEZ-PICAZO, L., *El escándalo del daño moral*, Thomson- Civitas, Pamplona, 2008.

FERNÁNDEZ, J. "Respuesta penal frente a fraudes cometidos en Internet: estafa, estafa informática y los nudos de la red". *R.D.P.C., 2.a Época,* (n. 19), 2007.

MIR, Santiago. *Derecho* Penal (7ª edición), España, Reppertor, 2004.

PÁSARA, L. "El conflicto entre medios de comunicación y justicia". *Reforma judicial,* Comisión Nacional de Tribunales Superiores de Justicia, Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México (n. 3), México, 2003.

PÉREZ, A. "La definici n legal". *Boletín mexicano de Derecho Comparado"* (21), México: UNAM, 1974.

SARMIENTO, D., MEDINA, S. y PLAZAS, R. "Sobre la responsabilidad y su relación con el daño y los perjuicios". *Revista Virtual Via Inveniendi et Iudicandi* (Vol. 12, N.° 2), Colombia, 2017.

CIBERDELINCUENCIA EN LA LEGISLACIÓN PENAL ECUATORIANA A LA LUZ DEL CÓDIGO ORGÁNICO INTEGRAL PENAL (2014)

Eje temático: Delitos Informáticos y Ciberseguridad

Autores:
Jonathan Marcelo Ramos Mera
Abogado – Máster en Derecho Penal mención Derecho Procesal Penal
Universidad Central del Ecuador

José Luis Romo Santana
Abogado - Máster en Derecho Penal mención Derecho Procesal Penal
Universidad Técnica de Ambato
QUITO – ECUADOR

ABSTRACT
La tipificación vigente de los delitos contra la seguridad de los activos de los sistemas de la información y comunicación constante en el Código Orgánico Integral Penal, es analizada en esta investigación, partiendo desde conceptualizaciones básicas y explicaciones técnicas que permiten entender la naturaleza jurídica de estos ilícitos, enfatizando posteriormente el análisis en los elementos del tipo objetivo de estos delitos informáticos constantes en el Código Orgánico Integral Penal Ecuatoriano, evidenciando falencias en sus estructuras principalmente en lo que tiene que ver con las acciones típicas descritas en estos delitos.
La construcción de una tipificación técnico jurídico penal - informática de los delitos contra la seguridad de los activos de los sistemas de información y comunicación, permitirá el establecimiento inequívoco de responsabilidades penales de los sujetos activos de estos ilícitos, es la hipótesis en el que se centra este estudio.
El análisis de los elementos del tipo objetivo de estos delitos, específicamente el de acción típica y bien jurídico, son el núcleo de este trabajo académico, pues con ellos se evidencia la poca motivación técnica y jurídica que utilizaron los legisladores ecuatorianos al momento de tipificar los delitos informáticos.
Los legisladores son los llamados a construir normas penales que atiendan la criminalidad informática, esto debido al monopolio que ostentan por el denominado principio de reserva de ley, y por ser los representantes de la voluntad popular, por ello, es necesario, que desde la academia se promueva una crítica constructiva que impulse a los legisladores a entender que estos delitos ya no se pueden construir solo desde el ámbito jurídico, es necesario entender la interrelación directa que existe con la informática. La creación de la norma penal en estos delitos informáticos debe contemplar como base todos los elementos que confluyen en estas conductas, para posteriormente poder determinar a la misma como delito, y consecuentemente conminarle una pena.
El Estado es el único facultado para crear y aplicar las normas; pensemos entonces que sucede cuando la construcción de la norma penal es deficiente, indefectiblemente la aplicación por parte del poder judicial también lo será, de ahí, la necesidad imperiosa de tener mucho cuidado en la tipificación de este tipo

de delitos. Las consecuencias de una correcta legislación penal son variadas, pasando por la seguridad jurídica, y aplicación natural del principio de legalidad, permitirá a los jueces dictar sentencias con objetividad y uniformidad, evitando la arbitrariedad y uso desmedido del derecho penal; la informática reviste conceptualizaciones diferentes a las tradicionales, por lo tanto, este trabajo académico es un aporte de investigación, que dilucida las falencias que rodean al Código Orgánico Integral Penal Ecuatoriano en torno a ciberdelincuencia. Adicional a ello, se ha estudiado dicha problemática generando soluciones técnicas, que resuelven los vacíos legales, constantes en este tipo de figuras penales.

PALABRAS CLAVE: Delitos Informáticos; Bien Jurídico; Acción Típica; Sistema Informático; Tipos Penales.

1.- BREVE HISTORIA DE LA LEGISLACIÓN INFORMÁTICA EN EL ECUADOR

Ecuador expidió en el 2002 la Ley de Comercio Electrónico, firmas y mensajes de datos, dentro del contenido de esta norma se desarrollaban las llamadas infracciones informáticas, que se determinaron de dos tipos, las primeras con carácter administrativo, y las segundas, delitos que mediante reforma fueron introducidos en el código penal vigente a esa fecha. Esta norma legal ya realizaba una clasificación sobre delitos informáticos, sin embargo, lo relevante es que mediante este instrumento se reformó el Código Penal de aquel entonces.

Hoy en día desde el año 2014 existe el denominado Código Orgánico Integral Penal Ecuatoriano que introduce nuevas formas de delincuencia informática, bajo la sección denominada delitos contra la seguridad de los activos de los sistemas de información y comunicación, dentro del capítulo tercero de los delitos contra los derechos del buen vivir; en este capítulo se tipifica la revelación ilegal de base de datos (artículo 229), la interceptación ilegal de datos (artículo 230), la transferencia electrónica de activo patrimonial (artículo 231), el ataque a la integridad de sistemas informáticos (artículo 232), los delitos contra la información pública reservada legalmente (artículo 233), y el acceso no consentido a un sistema informático, telemático o de telecomunicaciones (artículo 234).

2.- BIENES JURÍDICOS VULNERADOS POR LO DELITOS INFORMÁTICOS SEGÚN LA LEGISLACIÓN PENAL ECUATORIANA

El Código Orgánico Integral Penal Ecuatoriano, al igual que los códigos penales en el mundo han clasificado sus tipos penales tomando en cuenta el bien jurídico que se vulnera cuando se perpetra una determina acción delictual. Esta forma de clasificar los tipos penales tomando en cuenta el bien jurídico deviene de la función sistemática, Santiago Mir (2016) señala que el código penal parte de los distintos bienes jurídicos (…) (p.164), en ese sentido, pensar que es indispensable clasificar estos nuevos

tipos penales sistemáticamente y estrictamente es alejarse de la realidad actual, aun cuando esta función se sigue utilizando de manera general, en la actualidad se ve necesario cambiar la perspectiva parcialmente, pues la clasificación sistemática se rige específicamente a la protección por un lado de bienes individuales, y en otros casos a bienes de carácter colectivo o supraindividuales, sin embargo, pensar que en un tipo penal exista un bien jurídico de origen o individual y también uno supraindividual, no menoscabaría la función sistemática, esto, generaría tipos penales acordes a la realidad vigente.

La tipificación de las figuras delictivas encuentra su clasificación en conexión al bien jurídico que afectan, o vulneran, no hacemos alusión a los términos bien jurídico protegido porque los tipos penales sancionan a quienes cometen delitos, más no previenen delitos. Con esto no se pretende anular la prevención general, uno de los fines de la norma penal, sino entender desde un punto de vista objetivo que el derecho penal castiga no previene. Esta función entonces está solamente dirigida a crear cierto tipo de conciencia en la sociedad, para prevenir que los ciudadanos encuadren sus conductas en las figuras delictivas.

El bien jurídico que vulneran los delitos informáticos, de acuerdo a lo establecido en el actual Código Orgánico Integral Penal es la seguridad de los activos de los sistemas de información y comunicación. La aparición de este bien jurídico, tiene su origen en la Constitución de la República del Ecuador del 2008, el artículo 16 de la Carta Magna otorga a todas las personas el derecho al acceso universal a las tecnologías de la información y comunicación, por ende, este derecho al igual que los demás derechos están protegidos constitucionalmente tanto en su reconocimiento, goce y ejercicio, bajo garantías y principios que hacen realidad el acceso a la tecnologías por parte de los ciudadanos, entonces en este punto, cabe preguntarse si la protección de ese derecho se agota solamente con el acceso, y la respuesta es no, por ello, el Código Orgánico Integral Penal contiene penas para las personas que dificultan o vulneran dicho acceso; sin embargo, esta protección penal como veremos más adelante no es aun lo suficientemente fuerte para evitar este tipo de transgresiones; no hay que dejar de lado que el derecho penal es de ultima ratio, y es el Estado el llamado por medio de otros mecanismos preventivos quien tiene la obligación de generar esa confianza en el acceso a las tecnologías de la información y comunicación, creando políticas de capacitación y prevención en el uso de estas tecnologías.

El ser humano debe sentirse seguro para desenvolverse y desarrollarse en la sociedad actual en la que nos encontramos; por lo tanto, el Estado debe proteger tanto los bienes jurídicos individuales como los colectivos que se vulneran con esta clase de delitos informáticos, haciendo énfasis en que esto, no solamente se lo debe hacer desde el ámbito penal, pues este se activa cuando ya existe una vulneración, ya que sirve para el pasado no para el futuro, por ello, es por medio de otros mecanismos

preventivos que se debe proteger dichos bienes jurídicos. Sin alejarnos del tema central, debemos mencionar que la seguridad de los activos de los sistemas de información y comunicación, en primera instancia vendrían a ser un bien colectivo, un bien supraindividual, debido a que está vinculado a los derechos del buen vivir, a derechos colectivos y comunitarios que tienen los individuos, reconocidos constitucionalmente. Sin dejar de lado que en estos delitos también se transgreden los bienes jurídicos individuales como la intimidad, la privacidad, la propiedad que son igualmente "(…) bienes necesarios para el libre desarrollo del individuo, sin que estos se usurparan a costa del libre desarrollo de los otros, y en seguida, bienes compartidos, necesarios para una convivencia saludable." (García, 2014, p.34), estos últimos que los llamamos anteriormente como colectivos, supraindividuales o comunitarios. Por lo tanto, en este tipo de delitos las teorías monistas quedarían de cierta manera relegadas, pues la afectación no solamente se genera a la seguridad de los activos de los sistemas de información sino a otros bienes jurídicos de carácter individual, debido a ello, este tipo de delitos deben ser observados desde teorías dualistas de afectación.

En ese sentido, diremos que la agrupación de este tipo de delitos si atiende la función sistemática, pero de manera diferente a la tradicional estricta, es decir, en estos delitos el bien jurídico supraindividual que no se separa del individual, sería la seguridad de los sistemas informáticos, con esto indudablemente el estado estaría protegiendo por prevención general que los ciudadanos utilicen correctamente los sistemas informáticos, este estaría correlacionado directamente con el bien jurídico individual, que en los casos de estudio vendrían a ser la propiedad, la privacidad, entre otros.

Consideramos entonces al bien jurídico, "seguridad de los sistemas" como un bien colectivo, no solamente por su ubicación en el Código Orgánico Integral Penal, y lo determinado en la Constitución en cuanto a la protección del acceso a las tecnologías, sino, a que la afectación del mismo supone una consecuencia general y global, no solamente particular para el titular del bien, sino para la generalidad, en cuanto al sentimiento de inseguridad generado en la utilización de estos sistemas.

3.- ANÁLISIS DE LA TIPICIDAD CON ÉNFASIS EN EL PRINCIPIO DE LEGALIDAD DE LOS DELITOS CONTRA LA SEGURIDAD DE LOS ACTIVOS DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN

La tipicidad está conectada con el principio de legalidad, en ese sentido tal y como lo determina nuestra Constitución de la República *"Nadie puede ser juzgado ni sancionado por un acto u omisión que, al momento de cometerse, no este tipificado en la ley como infracción penal, (…) ni se le aplicara una sanción no prevista por la Constitución o la Ley";* en

ese sentido, esta categoría dogmático penal, debe ser entendida como el primer filtro de la teoría del delito, por el cual debe pasar el acto, sea de acción o de omisión, para posteriormente determinar si la misma es antijurídica, y se puede responsabilizar a una persona con una pena por dicha conducta.

Es sabido que en décadas pasadas se juzgaba a determinadas personas por sus acciones atípicas, es decir, se concluía que esas acciones eran lesivas, sin embargo, y aun cuando no estaban tipificadas esas conductas se determinaban responsabilidades. Hay que recordar que Beling (1930) fue quien se percató de las consecuencias que traía consigo el reconocimiento y aplicación del principio de legalidad, es así que, como lo destaca el mismo antes del aparecimiento de este principio "el juez podía castigar toda ilicitud culpable" (p.36), ya que cualquier conducta que se presumía antijurídica y culpable de por sí debía tener como conclusión el establecimiento de una pena, es decir, era escasa y casi nula la existencia de tipos delictivos, se penaba a las personas de manera arbitraria y desproporcional, eliminando cualquier rasgo de seguridad jurídica; en este punto y sobre el tema de la arbitrariedad es necesario hacer alusión a lo que señala el maestro Nodier Agudelo (2014) en su obra "Estudios Preliminares y Notas - Cesare Beccaria De los Delitos y de las Penas", cuando mencionaba: "Que quien vea establecida la misma pena de muerte, por ejemplo, para quien mate un faisán, para quien asesine a un hombre o para quien falsifique un escrito importante, no distinguirá entre esos delitos, destruyéndose de ese modo los sentimientos morales" (p.189); es claramente lo que sucedía en las épocas en las que el principio de legalidad no tenía la relevancia que actualmente posee.

Los delitos contra la seguridad de los activos de los sistemas de la información y comunicación, son analizados teniendo como base el principio de legalidad, estudiando a esta clase de delincuencia no solo conceptualmente sino técnicamente; hemos de decir en primer lugar que, toda actuación y procedimiento punitivo deberá regirse estrictamente por el imperio de la legalidad, por lo tanto, el juez deberá tener como instrumento una ley previa, expresa, general y prohibitiva de toda clase de analogía.

Estas exigencias o aristas del principio de legalidad garantizaran el derecho a la seguridad jurídica, que como está establecido en nuestra constitución responde al respeto a la Constitución y a la existencia de normas jurídicas previas, claras, públicas y aplicadas por autoridades competentes.

Por lo tanto, el Estado, como ente del poder público de las relaciones en sociedad, no sólo establece los lineamientos y normas a seguir, sino que en un sentido más amplio tiene la obligación de establecer "seguridad jurídica" al ejercer su "poder" político, jurídico y legislativo. La seguridad jurídica es la garantía dada al individuo, por el Estado, de que su persona, sus bienes y sus derechos no serán violentados o que, si esto llegara a producirse, le serán asegurados por la sociedad, protección y reparación; en resumen, la seguridad jurídica es la certeza que tiene el individuo de

que su situación jurídica no será modificada más que por procedimientos regulares y conductos establecidos previamente. Como se ha dicho antes, el derecho a la seguridad jurídica encuentra su fundamento en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes, por expresa disposición constitucional"[73]. [Énfasis Añadido].

El principio de legalidad es un elemento generador de garantías, una de ellas la ya mencionada seguridad jurídica; por ello, el legislador debe ser cuidadoso al momento de crear una norma más aun cuando se trata de delitos en los que ha ingresado una nueva ciencia como la informática, misma que cambia constantemente por la evolución de la sociedad de la información; hay que tener en claro que un pequeño descuido o la falta de técnica legislativa en conjunto con el poco entendimiento de dogmática penal pueden generar normas carentes de eficacia y efectividad, lo que se traduce en que las mismas no conseguirán el objetivo que pretenden; por lo tanto, se debe entender que estos delitos evolucionan, en efecto el derecho debe evolucionar, los legisladores deben ir a la par en el estudio e investigación de los posibles nacimientos de nuevas conductas delictivas con el uso de la informática, bajo fundamentos consolidados de política criminal y política penal, con el fin de proteger efectivamente los bienes jurídicos susceptibles de transgresión y vulneración; sin olvidarnos que además, estas normas correctamente estructuradas serán los instrumentos por medio de los cuales los jueces impartan bajo el imperio de la ley, la justicia.

La construcción de la norma penal en este tipo de delitos debe dejar de lado el pensamiento de que a mayor cantidad de términos que encuadren acciones típicas o verbos rectores, mayor es la eficacia al momento de juzgar, veremos cuan inútil resulta el hecho de introducir varios verbos rectores, en un delito, sin entender la naturaleza del mismo, generando únicamente el distanciamiento de la consolidación de la seguridad jurídica.

El 14 de junio del 2012, la Asamblea Nacional del Ecuador elaboró el informe para el primer debate del proyecto del ¨Código Orgánico Integral Penal", en el mismo se describía a los hoy en día denominados delitos contra la seguridad de los activos de los sistemas de información y comunicación, "delitos contra la información", en donde se establecían denominaciones de tipos penales diferentes a los que hoy encontramos en el vigente Código Orgánico Integral Penal, por ejemplo, el proyecto contemplaba, el delito de daño informático, el de obtención de información, la modificación de programas, la inutilización de programas, sin embargo, estos cambiaron considerablemente cuando en el 2013 se produjo el segundo debate, dentro del mismo se hace alusión sin alejarnos al tema de la tipificación que: "(…) se han diseñado los tipos penales

73 Corte Constitucional del Ecuador, Sentencia N.° 088-13-SEP-CC y Corte Constitucional del Ecuador, para el período de transición, Sentencia N.° 007-10-SEP-CC.

considerando las garantías constitucionales, la efectividad del combate del delito, y la precisión en los elementos de la tipicidad"; este último aspecto parece haberse quedado en una muy interesante intención, pues como veremos más adelante esa precisión lejos de combatir el delito, ha dejado vacíos que delincuentes informáticos utilizan para perpetrar sus acciones, desviando el castigo penal por falta de tipicidad. Los delitos de la sección tercera de los derechos contra el buen vivir, finalmente con el segundo debate quedaron tal y como hoy en día los observamos en el Código Orgánico Integral Penal.

Se ha dedicado estas primeras líneas a la explicación de la tipicidad con énfasis en el principio de legalidad, con el objeto de prevenir, y avizorar que no solamente es necesario tener un Código Orgánico Integral Penal que contemple delitos informáticos, y con ello pretender creer que el problema está solucionado; es necesaria la tipificación de este tipo de delitos atendiendo el principio analizado, con la colaboración de expertos en materia informática; las técnicas utilizadas dentro de este tipo de ilícitos, muchas veces son traducidas por los juzgadores utilizando diccionarios convencionales, recayendo equivocadamente en conceptualizaciones que muchas veces se alejan de la realidad conceptual en el ámbito informático.

Analizada la importancia del principio de legalidad dentro de la categoría dogmático penal de la tipicidad, nos incumbe ahora realizar un análisis crítico de la tipicidad referente a los delitos contra la seguridad de los activos de los sistemas de información y comunicación.

3.1 Análisis crítico propositivo de los delitos contra la seguridad de los activos de los sistemas de información y comunicación

Este análisis crítico de cada uno de los delitos contra la seguridad de los activos de los sistemas de información y comunicación se desarrolla en un orden diferente al establecido sistemáticamente en el Código Orgánico Integral Penal, debido a que partimos del análisis del delito de ataque a la integridad de sistemas informáticos, pues del mismo se desprende quizá la mayor critica al Código Orgánico Integral Penal, sin dejar de lado, que el análisis de este delito influye como veremos más adelante en el estudio de los demás delitos tipificados en la sección estudiada, sin más preludio iniciamos el análisis.

Artículo 232

Ataque a la integridad de sistemas informáticos

> La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.
> Con igual pena será sancionada la persona que:
> 1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.
> 2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.
> Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.

Análisis:

Dentro del artículo 232 del Código Orgánico Integral Penal se establecen ciertas acciones, verbos rectores que dan lugar a la figura penal de ataque a la integridad de sistemas informáticos, estos son: destruir, dañar, borrar, deteriorar, alterar, suspender, trabar, causar mal funcionamiento, comportamiento no deseado, suprimir datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, adicional a ello, este tipo penal sanciona con la misma pena si se producen otras acciones que son, diseñar, desarrollar, programar, adquirir, enviar, introducir, ejecutar, vender, distribuir dispositivos o programas maliciosos que causen los efectos señalados en el primer párrafo de este artículo, también y con la misma pena a quien destruya o altere sin la autorización la infraestructura tecnológica para la transmisión, recepción o procesamiento de información en general. Este tipo penal contempla ciertos elementos adicionales uno de ellos, por ejemplo, el de "sin autorización" cuando se destruya o altera infraestructura tecnológica.

Si observamos, el proyecto del Código Orgánico Integral Penal referente a esta figura delictiva en primer debate tenemos, algo totalmente distinto, pues se lo estableció primero bajo la descripción de daño informático, con conductas externas diferentes, incluyendo las acciones del delito de interceptación ilegal de datos, modificación de programas e inutilización de programas, así describía el primer debate a algunos tipos penales.

En la transición del primer y segundo debate sucede algo interesante y es que, se contemplaba los delitos de modificación de programas e inutilización de programas, sin embargo, cuando se redacta el texto del segundo debate estos son eliminados

y de cierta manera las acciones pasan a la descripción de tipos penales con nuevas denominaciones. Cabe preguntarse, ¿qué es lo interesante?, y es que, aunque un poco alejado de las conceptualizaciones técnicas actuales, el primer debate, si determinó que quien impida el acceso normal de forma temporal o definitiva a un programa, datos, bases de datos, redes era responsable de delito de inutilización de programas, la mayoría del contenido de este artículo se convirtió en lo que hoy está tipificado como "Ataque a la integridad de sistemas informáticos".

¿Qué sucedió para eliminar estas acciones?, en el texto vigente no aparece, ninguna explicación y justificación técnica, no se entiende como la acción de volver inaccesible un programa o sistema informático no esté tipificado. Si bien el primer debate, se acercó, tampoco era técnicamente correcto, pues el volver inaccesible un programa es diferente a volverlo inutilizable, esto último recae más en las acciones de dañar y alterar.

Las acciones descritas en la figura penal estudiada, harían entender que cuando una persona torna inaccesible un programa, lo está dañando o alterando, sin embargo, esto está muy alejado de ser cierto.

Las explicaciones técnicas sobre esta afirmación, radican en el siguiente análisis, ¿un juzgador podría sancionar a quien hace inaccesible un sistema informático?, y la respuesta rotunda es no, sin embargo, y debido a la falta de entendimiento de conceptos técnicos de informática hay quienes sostienen que sí se puede sancionar, con las acciones de alterar, dañar, o la de causar comportamiento no deseado. Es necesario, entender que las acciones descritas deben ser lo más claras posible, atendiendo las aristas del principio de legalidad, para este caso específico la taxatividad, los conceptos de estas acciones no pueden ser extraídos de diccionarios clásicos tradicionales, pues fácilmente harán equivocar al juzgador en su pretensión de determinar correctamente responsabilidades.

Entonces regresando al tipo penal objeto de análisis, diremos que el proyecto en primer debate sí determinaba de cierto modo la acción de volver inaccesible anclada a la generalidad del resultado que sería la inutilización, sin embargo, tampoco era correcta porque no necesariamente la acción de volver inutilizable, se encuadra en la inaccesibilidad, el delincuente informático puede volverlo inaccesible sin inutilizarlo.

Ahora bien, ¿la inaccesibilidad puede ser entendida como la acción de alterar?, la respuesta es no, pues puede darse el caso de que los propios datos sean modificados, evitando el acceso a los mismos, en este punto no estaríamos hablando de hacer inaccesibles sino de una alteración al propio dato que, aunque no afecta la información contenida en el mismo lo torno inaccesible, es necesario, entender que la inaccesibilidad debe enfocarse en un segundo plano pues no se vulnera ni afecta la integridad de los datos como tal, sino que mediante programas externos los vuelves inaccesibles.

Es necesaria entonces la reforma de esta figura penal, pues el legislador solo contemplo las acciones del que "*destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima*", sin contemplar la de volverlos inaccesibles.

El legislador ha insertado las acciones de destruir, dañar, borrar, y suprimir, entre otras, sin embargo, no se percató, de que algunas acciones descritas se subsumen por conceptos informáticos a otras, dejando de lado la inclusión de aquellas que en realidad si eran merecedoras de ser tipificadas como la mencionada acción de inaccesibilidad.

La acción de destruir se debe subsumir en la acción de dañar, la destrucción por lo general se enfoca en el derecho tradicional en la afectación de un bien físico, no estrictamente por cierto, pero por poner un ejemplo, alguien destruye un computador, una laptop, se podría decir que se afectaron los datos o la información de ese ordenador, pues debería realizarse un peritaje con el efecto de identificar los daños, ya que puede haberse generado solo daños materiales físicos, sin afectación de los datos y programas, sin embargo, la acción de destruir tiene como fin dañar, entonces este término daño, se subsumiría en cada una de las acciones insertadas en el tipo, pues en general, las conductas externas unas con mayor intensidad que otras tienen como resultado un daño.

Hay que acotar en este punto que España sustituyo en su legislación la acción destruir por la de borrar y suprimir, bajo el criterio de que el enfoque realizado anteriormente de destrucción estaba destinado más a objetos materiales que inmateriales, sin embargo, estos dos términos fueron incluidos pues se enfocaban más específicamente al ámbito de la informática, destinados a la protección de bienes inmateriales; se identifica, además, que la acción destruir podría encasillarse en la acción de volver inaccesible, pues en el ejemplo expuesto, se produce una acción externa que podría entorpecer el acceso a los datos, sin embargo, no podría considerarse que destruir podría a la inversa convertirse en la acción que subsuma a la inaccesibilidad, pues esta posee otro tipo de características que hacen necesaria su tipificación como tal.

La acción de deteriorar se ve relacionada con la acción de alterar, sin embargo, se enfoca igualmente en el resultado que es dañar, en este caso sería un daño parcial, un daño que altera un programa afectándolo parcialmente en su utilidad, que aun cuando sigue funcionando lo hace de manera defectuosa. En este caso, el deteriorar se subsume a la acción de alterar, pues no aporta conceptual ni técnicamente diferenciarlo debido a que la alteración de un programa trae como consecuencia el deterioro del mismo, entre otras. Las técnicas o programas inicialmente están dirigidas a la alteración, mas no a deteriorar, esta última se correlacionada como consecuencia de la primera.

Las demás acciones insertas en la figura penal, prácticamente pierden relevancia puesto que técnicamente no se realizó el análisis respectivo, para incluirlas, el causar

un mal funcionamiento, por ejemplo, se subsume a la acción de alterar; los programas maliciosos que se utilizan en esta acción tienden a afectar el funcionamiento de los programas, por ejemplo, la técnica del caballo de troya, que introduce programación no deseada en un ordenador alterando su funcionamiento, si bien las funciones se afectan esto es producto de la acción de alterar; lo mismo sucede con la acciones de comportamiento no deseado, y las de trabar y suspender, son acciones que se subsumen a la acción típica de alterar.

Entonces lo relevante en este tipo penal es que se transforma en indispensable la reforma que incluya a la acción de volver inaccesible, pues ni la de alterar, ni la de destruir, ni la de dañar, ni ninguna otra reemplaza este vació técnico legal, pues, como ya hemos explicado el volver inaccesible los sistemas, depende de un factor exterior; podría aquí decirse, por ejemplo, que trabar debe también quedar tipificada pues también podría depender de un agente externo, sin embargo, esta última al igual que las otras analizadas se subsumen porque se refiere a la integridad intrínseca de un dato o programa, que afecta el funcionamiento, en la inaccesibilidad no se afecta el funcionamiento, lo que se provoca es un bloqueo en el acceso que no altera la integridad esencial del programa.

Entonces queda claro, que el factor externo es el elemento indispensable para volver inaccesible un sistema, mientras que volver inaccesible el dato en sí, recae en la acción de alterar. La problemática y limitaciones de este artículo no se agota en este punto, pues existen dos elementos adicionales que deben también tomarse en cuenta, pues generan un resultado diferente al del tipo penal de ataque, a consecuencia de ello, es necesaria la creación de un tipo penal nuevo.

Estas dos acciones a las que hacemos referencia son las de la obstaculización y la interrupción, pensemos en este punto bajo que figura el juzgador podría sancionar los ataques de denegación de servicios o también llamados DDoS, sí tomamos en cuenta que esta acción se enfoca íntegramente en un ataque activo de interrupción, nos remitiríamos al artículo 232 del Código Orgánico Integral Penal para tratar de encuadrar la acción que permita sancionar a alguien que produce un ataque de denegación, objetivo que quedaría sin solución pues en este tipo de ataque, si bien confluyen las acciones analizadas anteriormente, lo hacen, causando resultados diferentes y concretos; estos van dirigidos a la interrupción u obstaculización del sistema, por lo tanto, no podrían ser utilizadas las acciones anteriores, pues en estos casos observaremos que las primeras se subsumen a las segundas.

Mirkovic (2004), respecto a este ataque señala que el mismo:

> Tiene como objetivo reducir la disponibilidad de un determinado activo en el sistema mediante la realización de un ataque bien a la fuente de información, bien al canal de trasmisión, o incluso a ambos. (p.40)

Es decir, este ataque se produce cuando se dirigen ciertos comandos o mensajes a la fuente de información, al canal de trasmisión o a ambos, con el objetivo de interrumpir u obstaculizar el normal funcionamiento de un sistema informático. Por lo tanto, existe una trasmisión de datos, acción que no contempla el artículo anteriormente mencionado, generando en este caso que la denegación de servicios no pueda ser juzgada, sino arbitrariamente y analógicamente usando las acciones descritas en el artículo objeto de análisis.

El ataque de denegación de servicios entonces utiliza una primera acción que es la trasmisión de datos, con el objeto de interrumpir y obstaculizar el correcto funcionamiento de un sistema informático, no afectando la integridad de los datos, sino al sistema en sí. Por lo tanto, y como manifestamos anteriormente varias de las acciones descritas en el artículo 232 del Código Orgánico Integral Penal están dirigidas a atacar la integridad de los datos, esto provocaría que esas acciones no permitan ser utilizadas en este caso pues no se altera como ya lo dijimos la integridad de los datos, sino la funcionalidad de los sistemas, por lo tanto, la inclusión de un tipo penal que atienda esta necesidad es indispensable pues no solamente se debe castigar la vulneración o afectación a la integridad de los datos y sistemas, sino también el correcto funcionamiento de estos últimos.

Las acciones por ejemplo de *dañar, borrar, alterar, o hacer inaccesible,* se deben incluir en la redacción del tipo penal que proteja la funcionalidad de los sistemas, sin embargo, lo debe hacer atendiendo a que el resultado en estos casos no es el daño del sistema, sino más bien la interrupción y obstaculización del mismo.

Continuando con el análisis de este tipo penal observamos que en su contenido se determina también que:

Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.
2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

El primer numeral referente al diseño, desarrollo, adquisición, envió, venta y distribución de dispositivos o programas informáticos maliciosos, debe necesariamente transformarse en un nuevo tipo penal, debido a que no solamente las acciones descritas en este tipo pertenecen estrictamente al delito de ataque a la integridad de sistemas informáticos, al contrario puede presentarse esta situación en todos los demás delitos desarrollados en la sección de ilícitos contra la seguridad de los activos de los sistemas de información y comunicación, por poner un ejemplo, para sancionar a la persona

que diseña, desarrolla, adquiera, envía, venda o distribuya programas destinados al cometimiento del delito de sabotaje a los sistemas informáticos, deberíamos al igual que en el delito de ataque introducir un inciso especificando este particular, cabe aclarar que el delito de sabotaje es una propuesta que hemos introducido en esta investigación, sin embargo, y de la misma forma si alguien vende un programa destinado a cometer el delito revelación ilegal de base de datos que si está tipificado actualmente en el Código Orgánico Integral Penal, ¿podría ser sancionada?, la respuesta es no, porque en el contenido de este delito no se contempla tal posibilidad.

El delito de interceptación en su último numeral si contempla tal situación, pero de manera más escueta que el de ataque, adicional a ello, la misma situación de atipicidad se presentaría en los casos de que alguien venda programas para el cometimiento de los delitos de transferencia electrónica de activo patrimonial, de acceso no consentido a un sistema informático, telemático o de telecomunicaciones y de ilícitos contra la información pública reservada legalmente, pues en su contenido tampoco se ha previsto tal posibilidad. Por ello, es necesario tipificar un nuevo tipo penal bajo la denominación de "abuso de dispositivos", que se remita a sancionar a la persona que *"diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados"* al cometimiento de los ilícitos contemplados en la sección referente a los delitos contra la seguridad de los activos de los sistemas de información y comunicación.

Es decir, no solamente la propuesta del delito de sabotaje es justificación para la creación de este nuevo tipo penal, pues como hemos visto los demás delitos de la sección objeto de análisis en este proyecto también necesitan de esa protección, no abultando a cada artículo con este contenido sino remitiéndose a uno autónomo que incluye a todos. Ahora bien, en lo referente a la penalidad, tanto en el delito de ataque como en el de interceptación, la pena es la misma para quien comete el delito, como para quien vende o diseña un programa para el cometimiento de ese delito. Referente a la penalidad siguiendo la estructura del Código Orgánico Integral Penal, y entendiendo teológicamente lo que quiso hacer el legislador deberíamos determinar que la pena en este delito sea la misma que la que se ha establecido para los delitos principales, acogiendo esta refl xión, el tipo penal sería tipificado de la siguiente forma:

> La persona que diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados al cometimiento de uno de los delitos contemplados en esta sección, será sancionada con la pena primaria no agravada establecida en cada tipo penal.

Puntualizando que en los delitos principales con una misma pena la aplicación de este delito no sería dific ltosa, tampoco en los que tienen un tipo penal agravado pues

la persona que diseña por ejemplo un programa para sabotear un sistema informático podrá o no saber que lo vende a un servidor público, no por ello, deberá ser sancionado con el tipo agravado, sería algo prácticamente desproporcional y arbitrario. En el caso del delito contemplado en el artículo 233 la aplicación se debe atender observando la denominación de este ilícito "Delitos contra la información pública reservada legalmente", es decir, este tipo penal incluye algunos delitos autónomos relacionado con la información reservada legalmente, por lo tanto, no se refiere a un delito agravado, la aplicación del delito propuesto de abuso de dispositivos debe aplicarse independientemente atendiendo cada uno de los delitos descritos en este artículo.

El segundo numeral de este artículo deberá permanecer intacto en la redacción del delito de ataque, sin perjuicio de argumentar críticamente que el mismo se debería subsumir en el contenido primario del delito, pero quizás el legislador en un esfuerzo ha querido especificar por sobre el daño particular del sistema a la infraestructura tecnológica, dotándole protección si se quiere más específica, quedan entonces las dos acciones de destruir y alterar, pues como ya lo he dicho, en el caso de presentarse otras acciones que afecten esta infraestructura tecnológica que también está compuesta por sistemas informáticos, nos remitiríamos al contenido principal del delito.

Artículo 229

Revelación ilegal de base de datos

> La persona que, en provecho propio o de un tercero, revele información registrada, contenida en fich ros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.
> Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

Análisis:

La revelación ilegal de datos se produce como podemos observar cuando una persona revela un secreto contenido en un sistema informático básicamente, materializando voluntaria e intencionalmente la violación del secreto, la intimidad y privacidad de las personas, cabría preguntarse entonces cual sería el justificativo

que utilizó el legislador para ubicar este delito dentro de esta sección, si claramente bajo los argumentos ya estudiados en el delito anterior, podemos dilucidar que tal y como está redactado claramente debería ser ubicado en los delitos contra la intimidad personal y familiar. Decimos esto, claramente porque los sistemas informáticos en este delito son utilizados como instrumento para afectar bienes jurídicos como la intimidad y la privacidad de las personas de manera primaria, aquí, el bien jurídico, seguridad de los activos de los sistemas de la información, se vería afectado con una incidencia claramente menor, no queda duda de ello pues la descripción del tipo penal hace relevante e indispensable el hecho de materializar con las acciones descritas en el inicio del tipo la violación del secreto, la intimidad y la privacidad de las personas. Por lo tanto, la ubicación de este tipo penal en esta sección en primera instancia resultaría errónea.

No cabe duda, que como ya lo explicamos cuando analizamos el delito de ataque, la afectación primordialmente es directa y principal a la seguridad de los activos de los sistemas de información y comunicación, por ello, el delito se encuentra en la sección estudiada. Por el contrario, cuando el ataque es primordial a otros bienes jurídicos, en donde solamente se instrumentaliza a la informática, el tipo es ubicado acorde al bien jurídico que vulnera diferente al relacionado con la informática.

Dentro del Código Orgánico Integral Penal específicamente en el artículo 178 se tipifica el delito de violación a la intimidad, sancionando a la persona que

> (…) sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio (…)

Un juzgador tendría la difícil tarea de encuadrar una acción que violente la privacidad, en unos de estos dos tipos penales el 178 o el 229, cuáles serían las características o los elementos que le permitirían decantarse por una o por otra, sin afectar o vulnerar el principio de legalidad. Es muy difícil dilucidar porque su contenido es estrictamente parecido, en el artículo 178 se sanciona a quien revela información registrada en un sistema informático, en el 229 se sanciona a quien difunda datos personales e información contenida en sistemas informáticos, hasta ahí, prácticamente son lo mismo, en la segunda parte el delito de violación a la intimidad describe el hecho de que esa difusión y publicidad sea por cualquier medio, a diferencia del 229 que describe que esa revelación deberá ser dirigida a través de un sistema informático, es decir, que una persona necesariamente deberá revelar la información a través de un sistema informático, esto estaría cubierto también por el artículo 178 cuando en su contenido inserta los términos cualquier medio. El artículo 229 creemos debió si se

quiere complementarse de cierto modo con el 178 evitando la tipificación de dos tipos penales que prácticamente sancionan la misma conducta penalmente relevante, hasta con la misma pena.

Sin embargo, en esta investigación se logra solventar este inconveniente sin eliminar el delito ya tipificado, y sin reubicarlo o complementarlo con el delito de violación a la intimidad. Esta solución está conectada intrínsecamente con el contenido del siguiente tipo penal:

Artículo 234

Acceso no consentido a un sistema informático, telemático o de telecomunicaciones

> La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.

Análisis:

El acceso ilícito o no consentido está relacionado con el delito de revelación ilegal de datos, ya que en primera instancia se transforma en un delito de protección si se quiere anticipada y preventiva de bienes jurídicos como los de privacidad e intimidad, construido claramente para sancionar a quien afecta directamente la seguridad de los activos de los sistemas de información y comunicación, pues con mecanismos técnicos informáticos se describen en el tipo acciones que vulneran seguridades de dichos sistemas afectándolos en su funcionamiento, accediendo de manera no autorizada al sistema, explotando indistintamente el acceso logrado.

Evidentemente la persona que accede ilícitamente a un sistema informático, de por sí está afectando el bien jurídico intimidad y privacidad, pero claramente se afecta en primer orden la seguridad de los sistemas informáticos y en segundo los otros bienes jurídicos mencionados, la intensidad de afectación dependerá del acto que se cometa, pues en algunos casos se afectara absolutamente la seguridad del sistema y la intimidad personal no tanto, no solamente con el acceso logrado se puede afectar este bien jurídico, podrían verse afectado otros, y con mucha más gravedad.

Conforme lo expuesto, la solución más pacifica se traduce en generar una fusión entre estos dos tipos penales sin afectar la estructura del último, en donde se proteja la seguridad de los activos de los sistemas de información y comunicación, así como los demás bienes jurídicos como la intimidad y la privacidad, esta fusión justificará de sobre manera que el delito de revelación ilegal de datos permanezca en esta sección subsumido en el delito de acceso ilícito. El delito de acceso ilícito con esta fusión se ve claramente fortalecido; el simple acceso debe ser punible y de eso estamos claros, no debe necesitarse consecuencias adicionales, sin embargo, cuando se dan igualmente deben ser penadas, cabe recordar que la ubicación dada a estos delitos radica en que la vulneración a la seguridad de los sistemas es directa y de mayor incidencia que otros bienes jurídicos; bajo estos criterios el delito construido quedaría de la siguiente manera.

Delitos de acceso ilícito y revelación ilegal de datos:

> La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho **a excluirlo**, será sancionada con la pena privativa de la libertad de uno a tres años.

Análisis:

En primer lugar, este delito debe mostrar en su contenido este primer párrafo, puesto que el simple acceso indebido, ilícito y no consentido vulnerando si se quiere las seguridades del sistema informático, debe ser penado. El acceso ilícito de por sí, se genera utilizando mecanismos informáticos que afectan a los sistemas en su integridad, accesibilidad, y funcionamiento, creando como consecuencia la vulneración directa del bien jurídico protegido en la sección estudiada. Posterior a ello, se afectarán otros bienes jurídicos, sin embargo, es necesario atender coherentemente la construcción sistemática en función del bien jurídico que ha querido dar el legislador a estos delitos. Se incluye adicionalmente los términos "a excluirlo" pues con ello se completa la redacción entendiendo, que quien tiene derecho a excluirlo valga la redundancia, es el propietario del sistema informático. La penalidad se reduce, puesto que, se sanciona en sentido estricto el simple acceso al sistema informático.

Ahora bien, la protección no se agota en el acceso, por lo tanto, la segunda parte del delito dirá:

> La persona que, **en beneficio propio o de un tercero, haya accedido sin autorización al sistema informático para explotar el acceso logrado, revelando información registrada contenida, en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de tres a cinco años.**

Aquí se encuentra el núcleo esencial de la fusión de los dos delitos analizados, esto evidentemente hace merecer al tipo penal la ubicación actual en la sección de delitos informáticos, debido a que, se sanciona en primer lugar el acceso, acceso que, en sí, ya supone en primera línea la vulneración de la seguridad de los activos sistemas de la información y comunicación, enlazando en segundo plano otras acciones conectadas con el acceso, destinadas a vulnerar otros bienes jurídicos protegidos, característica intrínseca que se presenta en esta clase de delitos y que ya la discutimos extensamente en el delito de ataque a la integridad de sistemas informáticos.

Por último, este delito no debe dejar de lado o en el aire la parte final que determina el actual delito de acceso ilícito, y el segundo párrafo del delito revelación de datos, por ende, el texto de este tipo propuesto deberá decir:

> Con la misma pena será sancionada la persona que, **en beneficio propio o de un tercero, haya accedido sin autorización al sistema informático para modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos.**
> Si las conductas descritas se comenten por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financie a o contratistas, será sancionada con pena privativa de libertad de cinco a siete años.

La gradualidad de las penas en este tipo penal propuesto responde decisivamente al delito de acceso ilícito, pues en los párrafos descritos todas las acciones y consecuencias están conectadas a ese acceso no consentido, y al ser estas las que afectan la seguridad de los sistemas, en conjunto con otros bienes jurídicos protegidos, es necesario el aumento de la pena en comparación con el delito de revelación. Con este análisis se evita la proliferación y expansión del derecho penal simbólico, que lo único que hace es crear normas penales con letra muerta e inaplicable.

Adicional a estos ilícitos analizados en la sección de los delitos contra la seguridad de los activos de los sistemas de la información y comunicación, se encuentra también el de interceptación ilegal de base de datos, delito que no requiere mayor análisis en nuestra investigación, pues consideramos que su tipificación responde a los parámetros internacionalmente establecidos, y a la realidad normativa actual, sin dejar de lado que presenta una construcción técnica precisa, pues hace referencia a

acciones que necesariamente en la totalidad de los casos o en su gran mayoría afectan la confiabilidad y accesibilidad de los sistemas informáticos, estas acciones permiten al delincuente informático, interceptar, escuchar, grabar, desviar, u observar, datos informáticos, específicamente dice el tipo, para obtener la información, en su origen, destino o en el interior del sistema; claramente este delito debe ubicarse en esta sección, pues vulnera la seguridad de los sistemas, sin dejar de lado que también afectará otros bienes, uno de ellos la intimidad.

Prácticamente este bien jurídico aparece como bien afectado en algunos de los delitos analizados en este proyecto de investigación. Es importante mantener la tipificación vigente de este delito puesto que, aquí se afectan también las reglas y protocolos que utilizan las redes, que permiten la conexión entre sistemas, los mismos que a su vez comparten información. De ahí, que introduce también otras acciones que se enfocan igualmente en la modificación de datos y sistemas informáticos, para inducir a la persona a acceder digitalmente a sitios no voluntariamente queridos, así como la venta de información contenido de las tarjetas de crédito, débito o similares, técnica denominada manipulación de datos de salida, que también afecta a la seguridad de los activos de la información y comunicación. El numeral 4 de este delito se suprime, puesto que, este contenido ya es atendido con la creación del delito de abuso de dispositivos, no así el numeral 2 de este tipo penal que tiene características intrínsecas propias y autónomas que obligan necesariamente a mantener su tipificación vigente.

Otro de los delitos que aparece en la sección objeto de estudio es el delito de transferencia electrónica de activo patrimonial, este delito tampoco requiere de mayor análisis, puesto que, en primer lugar, su ubicación es correcta, responde claramente a la naturaleza descriptiva de este tipo de delitos, pues, desarrolla las acciones de alterar, manipular o modificar el funcionamiento de los sistemas informáticos, que bien podrían subsumirse a la de alterar, pero para efectos de este delito no reviste mayor importancia excluirlos; estas acciones tienen la finalidad de procurarse la transferencia de activos patrimoniales perjudicando a terceros, es decir, está claro que la afectación primaria radica en la seguridad de los activos de los sistemas de la información y comunicación, pero posteriormente se vulnera otro bien jurídico que es el patrimonio. El segundo inciso sanciona igualmente a quien proporciona su cuenta en una suerte de testaferrismo electrónico, para recibir el activo patrimonial obtenido de manera ilegítima. En el caso de que una persona venda un programa para el cometimiento de este delito, el artículo propuesto de abuso de dispositivos, suplirá la falta de previsión de esta particularidad en el texto vigente de este tipo penal.

Nos queda un delito, por analizar, el mismo se denomina *"Delitos contra la información pública reservada legalmente";* con la tipificación de este delito se pretende que quien destruye o inutilice información reservada legalmente sea sancionado con una pena privativa de libertad considerable de cinco a siete años, es el tipo

penal de esta sección que tiene la pena más grave, puesto que evidentemente los efectos de destruir información clasificada, puede generar una afectación diversa a las particulares contempladas en los otros delitos. En este tipo no se detallan cuáles serán las acciones que deberán tomarse en cuenta en lo referente a llevar a cabo una destrucción o inutilización de información, podría en primera instancia entenderse que tales acciones están destinadas a la afectación física de los sistemas informáticos o componentes de los mismos que contienen información, sin embargo, y como ya lo hemos explicado adoptar esa percepción sería recaer en una vulneración primaria del derecho de propiedad, dejando a un lado el de la seguridad de los activos de los sistemas de la información y comunicación, tornando en errónea la ubicación de este delito en esta sección.

Sin embargo, y a efectos de adoptar integralmente los criterios analizados en este trabajo académico, deberemos ser propositivos y enfáticos en señalar que en el primer párrafo de este delito se deberá incluir necesariamente las acciones de alterar, dañar, suprimir, borrar, no se incluye la de volver inaccesible porque evidentemente no estamos hablando de un sistema informático, sino de la información en sentido estricto, por lo tanto, en el caso de que se vuelva inaccesible un dato que contiene información, estaremos cubriendo tal situación con la acción de alterar, pues se vulnera directamente la integridad de la información, a diferencia del hecho de volver inaccesible un sistema que no afecta la integridad de la información sino que mediante un agente externo, evita la accesibilidad a dicha información, afectando en sí, al sistema más no a la información.

Hemos visto que la acción de destruir, en las legislaciones internacionales ha sido reemplazada por las de borrar y suprimir, evidentemente porque su enfoque se torna más específico y materialmente acorde, en este caso cuando se trata de daños a bienes jurídicos inmateriales como el de información; la destrucción, así como está incluida en el tipo hace más alusión a daños físicos sobre objetos materiales. La inutilización de la información debe subsumirse a la acción de alterar, esto como ya lo hemos explicado, debido a que un dato puede ser objeto de acciones que lo tornen inaccesible en su integridad, generando como una de las posibles consecuencias directas la inutilización, mantener el contenido inutilizar, es un poco ambiguo, esto recordemos lo analizamos en el delito de ataque, en donde esta acción de inutilizar ha sido reemplazada por la acción de volver inaccesible, ya que en un sistema puede darse el caso de que se torne inaccesible el mismo mediante un agente exterior, sin inutilizar la información que contiene este; a diferencia del tipo que analizamos en el que la acción de inutilizar la información se traduce en la acción de alterar, cuando se torna inaccesible un dato o información.

El segundo párrafo no reviste mayor análisis puesto que se pena a quien utiliza un medio informático para obtener esta información, el sistema informático es el medio

el instrumento para el cometimiento del delito, si bien la afectación podría recaer en otros bienes jurídicos, no es menos cierto que en este caso aparece la información, si se quiere como objeto de tutela jurídica penal, cabe recalcar que manteniendo la uniformidad de criterios lo que se debe entender es que en el caso de la perpetración de este ilícito lo que se está afectando es la integridad de esa información, provocando como consecuencia evidentemente que el mismo sea merecedor de la ubicación que ostenta actualmente, pues en efecto esto devendría en una afectación a la seguridad de los activos de la información y comunicación; observar a la información como un bien jurídico independiente o autónomo, generaría un complejo análisis desde el derecho penal, delimitar frenos al ius puniendi, establecerle límites al mismo, tomando en consideración a que información en más incidente o influyente para el libre desarrollo de la personalidad de los seres humanos en un estado democrático, sería un problema mucho más serio para el derecho penal, por ello, y aunque en este delito no estamos estrictamente ante información personal, sino en su gran mayoría estatal con su cláusula de reserva legal, debemos observar a la información desde su integridad.

El ultimo inciso de este tipo penal tiene una pena que va de los siete a los diez años, para el sujeto calificado servidor público que revela información reserva que comprometa la seguridad del estado, aquí no se delimitan las acciones para revelar esa información, sin embargo, creemos que no es necesario incluirlas, porque podría solventarse estos casos con la aplicación del concurso ideal de infracciones, cuando se evidencie una unidad de acción en el accionar por parte del sujeto activo, es decir, podría sancionarse al servidor público que en unidad de acción lineal accede ilícitamente al sistema informático, para revelar información reservada, que compromete la seguridad del estado. Cabe acotar, que anteriormente en esta investigación se hacía alusión al atacante interno, mismo que aprovechándose de su condición de trabajador (servidor público) accedía a los sistemas validado por sus atribuciones legitimas con fines no legítimos.

Hemos analizado, todos los tipos penales constantes en la sección de delitos contra la seguridad de los activos de los sistemas de información y comunicación, mostrando de cierto modo que cada tipo penal necesita una construcción más técnica, que se erija no solamente desde el ámbito jurídico sino también del técnico informático, los vacíos que contienen son muchos como hemos visto en este apartado. Sin lugar a duda, el análisis del delito de ataque, contribuyo con relevancia en el desarrollo de esta investigación, pues a partir del mismo, se fueron identificando los problemas que presentaban los demás tipos penales, específica ente en lo que tiene que ver con la tipicidad de las acciones delictuales.

3.- CONCLUSIONES

Los primeros ataques utilizando la informática, fueron desatendidos por mucho tiempo en el campo del derecho penal, sin embargo, hoy en día los códigos penales de los países en el mundo, han introducido en sus contenidos, figuras penales que atienden esta clase de criminalidad, lamentablemente en algunas, de forma errada debido a la concepción equivocada de que esta clase de delitos son autónomos en su totalidad, sin tomar en consideración el análisis sistemático a partir del bien jurídico que vulneran. Lo que genera impunidad y desconfianza en los sistemas penales modernos; estos delitos vulneran bienes jurídicos distintos, no solamente se los debe observar desde teorías monistas de afectación.

Los delitos informáticos son conductas típicas, antijurídicas, culpables y punibles cometidas a través de acciones informáticas que afectan el bien jurídico, seguridad de los activos de los sistemas de información y comunicación, así como otro tipo de bienes jurídicos como la privacidad, intimidad, propiedad, entre otros. Es decir, dentro de este tipo de ilícitos en algún momento del camino del delito, interviene una acción típica informática que vulnera la seguridad de los sistemas informáticos, datos, redes e infraestructuras tecnológicas; su afectación es primordial, ya que, de ahí, se diferenciará si se trata o no de un delito autónomo informático, o de un delito tradicional.

El estudio de la modific ción de la estructura típica objetiva de los delitos contra la seguridad de los activos de los sistemas de información y comunicación, fue enfocado y sustentado no solo conceptualmente sino técnica jurídica e informáticamente. La construcción de la norma penal de este tipo de delitos debe dejar de lado el pensamiento de que a mayor cantidad de términos que encuadren acciones típicas, mayor será la eficacia de la norma. La introducción indiscriminada de verbos rectores en los tipos penales como se ha demostrado no es garantía de tipos delictivos eficientes; la correcta tipificación debe partir del entendimiento de la naturaleza jurídica de este tipo de delitos, y de la construcción de bases a partir de conceptualizaciones informáticas relacionadas con las jurídicas y legislativas.

El bien jurídico que vulneran los delitos informáticos es la seguridad de los activos de los sistemas de información y comunicación, a ello se debe, la agrupación sistemática de estos delitos actualmente en el Código Orgánico Integral Penal; este bien jurídico debe ser entendido desde el esquema del bien jurídico supraindividual, ligado al bien jurídico individual, este último, donde se encuentran bienes jurídicos como la privacidad, la intimidad, la propiedad, entre otros. Esta forma de comprender este tipo de delitos, permite al Estado proteger por prevención general que los ciudadanos utilicen correctamente los sistemas informáticos, previniendo la afectación de bienes jurídicos individuales.

El bien jurídico "seguridad de los activos de los sistemas de información y comunicación" que vulneran estos delitos informáticos, tiene su origen en la

Constitución del 2008, el derecho que tiene toda persona al acceso universal a las tecnologías de la información y comunicación, debe ser protegido indudablemente por la esfera penal, el real acceso a la tecnologías de la información y comunicación por parte de los ciudadanos, no debe agotarse en la accesibilidad, se debe castigar aquellas personas que dificultan o vulneren dicho acceso. La protección penal actual es ineficiente como hemos demostrado, no es actualmente una herramienta consolidada que sirva para sancionar eficiente ente a los delincuentes informáticos; sin duda y como sabemos el derecho penal es de ultima ratio, por lo tanto, adicional a la modifi ación de los tipos penales, el Estado es el llamado por medio de otros mecanismos preventivos quien tiene la obligación de generar esa confianza en el acceso a las tecnologías de la información y comunicación, creando políticas de capacitación y prevención en el uso de estas tecnologías.

La regulación vigente sin lugar a duda es un avance en comparación a la mantenida en el anterior Código Penal Ecuatoriano, sin embargo, con el análisis realizado a la tipicidad con énfasis en el principio de legalidad, así como los elementos que integran el tipo objetivo de los delitos contra la seguridad de los activos de los sistemas de la información y comunicación, específicamente en lo que tiene que ver con las acciones típicas, hemos evidenciado que existen ciertos vacíos legales, ciertas acciones, no contempladas en cada uno de los tipos penales analizados, mismas que a la postre serán generadoras de imposibilitar al juzgador para sancionar, obligando a los juzgadores bajo el justificativo de no dejar en la impunidad estos actos, al uso de la analogía, lo que evidentemente recaería en la vulneración del principio de legalidad al momento de juzgar.

La informática es una ciencia aun no analizada a profundidad por el derecho, debido a su aparición y evolución constante, los legisladores son los llamados a brindar conceptualizaciones necesarias, así como, tipos penales informáticos construidos desde bases técnicas, que permitan a los jueces dictar sentencias con objetividad y uniformidad, evitando como ya lo hemos dicho la arbitrariedad y uso desmedido del derecho penal; la informática reviste conceptualizaciones diferentes a las tradicionales, por lo tanto, este trabajo académico es un aporte de investigación, que dilucida las falencias que rodean al Código Orgánico Integral Penal en torno a ciberdelincuencia. Se ha estudiado y analizado dicha problemática generando soluciones técnicas, que resuelven los vacíos legales, constantes en este tipo de figuras penales.

4.- BIBLIOGRAFÍA

MIR PUIG, SANTIAGO. Derecho Penal – Parte General. Editorial Reppertor. Barcelona. 2006

MIR PUIG, SANTIAGO. Traducción de la clasificación de la OCDE - Delincuencia Informática, Ed. PPU, 1ª edición, Barcelona.

GARCÍA, Ramiro, *Código Orgánico Integral Penal Comentado*. Ecuador: Latitud Cero Editores, 2014. Impreso

BELING, Ernst von. *Esquema de Derecho Penal. La doctrina del Delito-Tipo. Trad. De Sebastián Soler, de las obras originales alemanas Grundzüge des Strafrechts, 11ª ed. 1930 y Die Lehre von Tatbestand, 1930*. Buenos Aires, Palma, 1944. Impreso

AGUDELO, Nodier. *Cesare Beccaria-De los delitos y de las penas*. Medellín-Colombia, 2014. Impreso

CIBERSEGURIDAD VS CIBERDELINCUENCIA

Eje Temático: Gobernanza en Internet, DDHH.

Autor:
Katty Pérez Ordóñez
Abogado, Doctoris Scientiae en Derecho
Universidad Andina Néstor Cáceres Velásquez – Puno – Perú.

RESUMEN
El programa "Hacia un Perú Digital" que patrocina el Ministerio de Transportes y Comunicaciones del Perú. Recomienda que "Las estrategias de ciberseguridad nacional deben armonizarse con los valores y derechos fundamentales como la privacidad, la libertad de expresión y el debido proceso" y advierte que entre los riesgos de la constante y cotidiana innovación tecnológica, también se producirá un incremento de las actividades delictivas *on line* así como el abuso informático y por lo mismo, la Ciberseguridad se convertirá en un asunto claro y transversal de la sociedad, por cuanto las nuevas tecnologías gestionarán y procesarán información vital para lograr la eficiencia de los servicios críticos y sensibles. La transformación digital, ejemplifica la versión de nuevos ataques informáticos como el RAMSOMWARE, ataques de degeneración de servicios usando dispositivos LOT, robo de cuentas y datos personales por debilidades en las configuraciones, ataques y grupos organizados para el espionaje cibernético (Poseidón, Lazarousgroup, hackingteam, pishing, etc)
Y como respuesta se percibe que en la configuración y avance de las Estrategias de Ciberseguridad Nacional, (que deben armonizar los derechos fundamentales con el debido proceso) no documentan con precisión, ni procesan con rigurosidad científica y tecnológica, asuntos relacionados con la gestión y participación de la prueba digital en el debido proceso, en tanto que, la gestión de la prueba digital, constituye uno de los elementos esenciales para la judicialización de cualquier delito igualmente informático.
Por tanto, **el tema** a desarrollar, configura la relación de la prueba digital, con los procesos y procedimientos referidos a los delitos informáticos, en vista que uno de los fines y objetivos más importantes del nuevo Código procesal penal, consiste en comprobar o desvirtuar la existencia de un delito en base de pruebas que constituyen instrumentos de contenido y esencia irrefutable.
La estructura de la ponencia, destaca el requerimiento de los pasos y fases que establece todo proceso enmarcado en el nuevo Código procesal penal desde las diligencias de Investigación Preliminar, la observación de pruebas en la Investigación Preparatoria y la fijación de supuestos para declarar casos virtuales como complejos. La **Hipótesis** de trabajo, sostiene que, en el ámbito de aplicación del Nuevo Código, la Estrategia de Ciberseguridad Nacional y la pretensión del DEBIDO PROCESO, no guardan relación armónica con las diligencias informáticas forenses, propias de la Gestión jurídica de la Prueba Digital.
El Objetivo más importante del presente artículo es, Investigar si las diligencias y Peritajes de Resguardo y Protección de la Prueba Digital, corresponden a las demandas del procesamiento, transporte, almacenamiento y reproducción de información de evidencias probatorias.

Palabras Clave: Ciberseguridad y Ciberdelincuencia, Peritajes de Resguardo y Protección de la Prueba.

ABSTRACT
The "Towards a Digital Peru" program sponsored by the Ministry of Transportation and Communications of Peru. Recommends that "National cybersecurity strategies must be harmonized with fundamental values and rights such as privacy, freedom of expression and due process" and warns that among the risks of constant and daily technological innovation, there will also be an increase in Online criminal activities as well as computer abuse and therefore, Cybersecurity will become a clear and transversal

issue of society, as new technologies will manage and process vital information to achieve the efficienc of critical and sensitive services. The digital transformation exemplifies the version of new computer attacks such as RAMSOMWARE, service degeneration attacks using LOT devices, account theft and personal data due to weaknesses in configurations, attacks and organized groups for cyber espionage (Poseidon, Lazarousgroup, hackingteam , pishing, etc)
And in response, it is perceived that in the configuration and advancement of the National Cybersecurity Strategies, (which must harmonize fundamental rights with due process) they do not accurately document, nor process with scientific and technological rigor, matters related to management and participation of the digital evidence in due process, while the management of the digital evidence constitutes one of the essential elements for the prosecution of any equally computer crime.
Therefore, the topic to be developed, configures the relationship of the digital evidence, with the processes and procedures referred to computer crimes, since one of the most important purposes and objectives of the new Criminal Procedure Code, is to verify or distort the existence of a crime based on evidence that constitutes instruments of irrefutable content and essence.
The structure of the paper highlights the requirement of the steps and phases established by any process framed in the new Criminal Procedure Code from the Preliminary Investigation proceedings, the observation of evidence in the Preparatory Investigation and the setting of assumptions to declare virtual cases as complex. The Working Hypothesis, argues that, in the scope of the New Code, the National Cybersecurity Strategy and the claim of the DUE PROCESS, have no harmonious relationship with the forensic computer proceedings, typical of the Legal Management of the Digital Proof.
The most important objective of this article is to investigate whether the procedures and Expertise of the Protection and Protection of the Digital Proof correspond to the demands of the processing, transport, storage and reproduction of evidence evidence.

Keywords: Cybersecurity and Cybercrime, Security Surveys and Test Protection.

INTRODUCCIÖN

En la cuestión previa de la Criminalidad Informática, Jiménez Herrera (2017) Comenta que, para la INTERPOL, "la ciberdelinciancia constituye uno de los ámbitos delictivos de más rápido crecimiento, y esto se ha notado de manera permanente en estos últimos años. Cada vez mas delincuentes se aprovechas de la rapidez, la comodidad y el anonimato que ofrecen las tecnologías modernas para llevar a cabo diversos tipos de actividades delictivas.. estas incluyen ataques contra sistemas y datos informáticos, usurpación de la identidad, distribución de imágenes de agresiones sexuales contra menores, estafas relacionadas con las subastas realizadas a través de internet, intrusión de servicios financieros en línea, difusión de virus, botnets (redes de ordenadores infectados controlados por usuarios remotos) y distintos tipos de estafas cometidas por correo electrónico, como el phishing (adquisición fraudulenta de información personal confidencial)".

Conductas antijurídicas, todas ellas relacionadas al uso de las tecnologías de la información y las comunicaciones, para afectar bienes jurídicos, económico-patrimoniales e informáticos, así como los derechos fundamentales de la persona. Según Tiedemann (1985) "La criminalidad mediante el uso de computadoras, alude a todos los actos antijurídicos, según la ley penal vigente, realizados con el empleo de un equipo automático de procesamiento de datos En consecuencia, se producen ataques

contra el derecho a la intimidad, infracciones a la propiedad intelectual y/o derechos de autor, sabotajes informáticos que ocasionan daños a programas o documentos electrofónicos contenidos en redes, fraudes informáticos, como las estafas que se realizan por medio de la manipulación de datos y programas, calumnias, ofensas y amenazas de extorsión y pornografía y prostitución infantil, así como la trata de menores".

Ahora bien, para combatir aquellas constantes y cambiantes amenazas provenientes de la cibercriminalidad, el 2001 el Consejo de Europa a través del Convenio sobre el Cibercrimen, exige poner límites a la extensión transnacional de los delitos vinculados a las tecnologías de la información, aceptando y creando por primera vez, los términos Cibercrimen y Ciberseguridad, teniendo en consideración la naturaleza global y transfronteriza de tales fenómenos, estos hechos facilitan la cooperación judicial, primero entre los miembros de la comunidad europea (en la formalización del EUROJUST, el G-8) para luego extenderse por todo el plantea. Es en ésta coyuntura que surge el Convenio de Budapest, o Convención sobre Delitos Informáticos o Convenio sobre Ciberdelincuencia y que en nuestro caso involucra al Derecho Penal, al Código Penal y al Código Procesal Penal.

El convenio de Budapest, que instrumenta tres objetivos globales: Armonizar el Derecho Penal con los derechos fundamentales, establecer medidas procesales para el medio digital y poner en funcionamiento un régimen de cooperación internacional. ha determinado así mismo, que el bien jurídico a proteger es: la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos.

Los Delitos Tipo reconocidos por el Convenio, son los siguientes:

- Acceso ilícito, el bien jurídico lesionado o puesto en peligro va a ser la "seguridad informática" o la "confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos"
- Atentado a la integridad de datos informáticos, el bien jurídico lesionado o puesto en peligro va a ser la "confidencialidad, integridad y disponibilidad de los datos informáticos" o la "seguridad informática".
- Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos, el bien jurídico lesionado o puesto en peligro va a ser la "indemnidad sexual" o al "libertad sexual"
- Interceptación de datos informáticos, el bien jurídico lesionado o puesto en peligro va a ser el "secreto de las comunicaciones" o la "confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos".
- Fraude informático, el bien jurídico lesionado o puesto en peligro va a ser el "patrimonio".
- Suplantación de identidad, el bien jurídico lesionado o puesto en peligro va a ser la "Fe Publica".

El año 2013 se dio la Ley Nº 30096 y su modificatoria 30171, para tipificar con precisión los siguientes Delitos digitales: acceso ilícito, atentado a la integridad de datos informáticos; atentado a la integridad de los sistemas informáticos, proposiciones a niños, niñas y adolescentes con fines sexuales, la interceptación de datos informáticos, fraude informático, suplantación de identidad y abuso de mecanismos y dispositivos informáticos. Además protege los siguientes bienes jurídicos: El patrimonio, la Seguridad Informática, la confidencialidad, disponibilidad e integridad de datos o sistemas informáticos, el secreto de las comunicaciones, la fe pública, la libertad sexual y la indemnidad sexual.

¿CUÁL ES LA SITUACIÓN DE LA CIBERSEGURIDAD EN EL PERÚ?

El Banco Interamericano de Desarrollo (BID) y la OEA emitieron el Informe "Ciberseguridad 2016, ¿Estamos preparados en América Latina y el Caribe?". En dicho informe se evaluaron los avances en cada país de la región, ubicando al Perú en un puesto intermedio e identificando los principales retos a afronta:

- Desde 2005 existe en la Policía la DIVINDAT (División de Investigación de Delitos de Alta Tecnología) que se especializa en combatir delitos informáticos. Hasta antes de la creación de tipos penales específicos, la mayor parte de casos recibidos eran procesados como nuevas modalidades de estafa.
- Desde 2009 contamos con el PeCERT, un órgano de coordinación dentro de la Administración Pública dedicado a enfrentar los ciberataques dirigidos contra los sistemas del Estado. Este modelo de CERTs es además el más común en el mundo.
- Desde 2011 tenemos la Ley de Protección de Datos Personales que busca crear un ámbito de protección sobre la disposición y uso de dichos datos por terceros.
- En el 2013, se renovó la Ley de Delitos Informáticos que cubre el vacío normativo que existía sobre algunos de los ataques más comunes: la vulneración de sistemas informáticos, entre otros. Esta norma posteriormente fue perfeccionada en el 2014.

El Perú, actualmente se encuentra en proceso de adherencia al Convenio de Budapest, que es un Tratado internacional de cooperación sobre delitos informáticos. El órgano responsable de gestionar su aprobación e implementación es la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI).

Pues, según los profesionales en seguridad de ISACA (InformationSystems Audit and Control Association) La ciberseguridad se debe definir ahora, como una capa de protección para los archivos de información, a partir de ella, se trabaja para evitar

todo tipo de amenazas, las cuales ponen en riesgo la información que es procesada, transportada y almacenada en cualquier dispositivo.

A partir de tal definición, el Informe de **Seguridad Informática** de Telefónica del Perú, (2018) indica que para dar una respuesta técnica a un ataque, es primordial seguir cinco pasos con los que se podrá **prevenir un robo de datos** o acotar el impacto negativo del ataque: desconectar el equipo de internet, instalar un programa antivirus, realizar un análisis completo del sistema, modificar las contraseñas y hacer una limpieza manual del equipo.

Pero también existe una tendencia para establecer Reglas globales que necesariamente afectan las relaciones privadas y las cuestiones públicas; si bien ambas deben ser protegidas o promovidas a partir de la firma de tratados entre Estados, existe un camino institucional sumamente relevante por desarrollar, el Convenio de Budapest sobre Ciberseguridad. Sobre cuya firma, el 30 de enero de 2019, el Pleno del Congreso del Perú, aprobó la suscripción del Convenio de Budapest. Dicho tratado busca optimizar la regulación interna en materia de ciberseguridad, con mayor énfasis en materia penal, de tal manera que sus organismos correspondientes puedan tener mayor capacidad para poder perseguir este tipo de delitos.

¿QUÉ ES, Y QUÉ REGULA EL CONVENIO DE BUDAPEST?

El Convenio de Budapest es un tratado multilateral adoptado en el Consejo de Europa en el año 2001, con la finalidad de aplicar una política penal común y poder hacer frente a la "ciberdelincuencia".

Los Estados son conscientes y se encuentran sumamente preocupados por los riesgos que han generado las redes informáticas. Aún peor, determinados países aún no poseen una regulación adecuada e idónea para poder investigar y procesar este tipo de delitos. Por ello, el Convenio posee una sección especial que orienta a los países adherentes a tener una regulación penal especial para poder perseguir este tipo de delitos.

En ese sentido, el Convenio tiene como uno de sus principales objetivos la implementación de tipos penales, a fin de que los organismos pertinentes de cada Estado puedan perseguir la ciberdelincuencia.

¿QUÉ REGULA EL CONVENIO DE BUDAPEST?

Teniendo en cuenta todos los problemas, delitos y, sobre todo, los objetivos de los Estados Miembros del Consejo de Europa, el Convenio recomienda una serie de secciones que permitirán a los Estados mejorar su regulación interna y la cooperación..

Asimismo, el Convenio de Budapest ha incorporado una sección especial (Primer Capítulo) con el fin de disponer que los países deberían tipificar determinados delitos y así, de forma indirecta, tener una regulación similar entre todos los países. En dicha sección, se han dispuesto categorías que engloban a los siguientes delitos: (i) delitos contra la confidencialid d, la integridad y la disponibilidad de los datos y sistemas informáticos, (ii) delitos informáticos, (iii) delitos relacionados con el contenido, y (iv) delitos relacionados con infracciones de la propiedad intelectual y de derechos afines.

Cabe precisar que el principal problema, consiste en la adecuación de las referidas categorías con la regulación interna de cada país.

Finalmente, es relevante indicar que el Convenio ha dispuesto una sección referida a la cooperación internacional, a fin de dotar con mayor capacidad de acción a cada Estado en la lucha contra el cibercrimen. De esta forma, se ha dispuesto, como una obligación, el apoyo y cooperación entre los países en relación a los temas de extradición, asistencia mutua (incluso en ausencia de acuerdos internacionales), confidencialidad, entre otros. Por ello, es importante establecer relaciones con actores tecnológicos como Google, Facebook, Apple y Alibaba, con *startups* y con epicentros como Silicon Valley, Shenzhen y otros lugares. (Para mayor detalle ver https://www.bbc.com/mundo/noticias-38917336(visitado el 01/03/19)

Pues según el Equipo de Seguridad de Microsoft, (2018) los ataques más comunes de la Ciberdelincuencia son:

1. ATAQUES DE PHISHING

Muchos de los sitios web de phishing ahora utilizan certificados de seguridad. Según el AntiphishingWorkingGroup, durante el segundo trimestre de 2018, cerca del 35% de los ataques de phishing registrados se alojaron en sitios web con protocolo HTTPS, un importante incremento en comparación con el casi 5% de los casos de sitios falsificados con certificados SSL, reportados a finales de 2016.

2. CRIPTOJACKING

Esta amenaza se comenzó a identificar en agosto de 2017 y tiene como principio el secuestro de la capacidad de procesamiento de un equipo ajeno para ganar dinero mediante la minería de criptomonedas. Una de las formas de infectar los dispositivos es a través de scripts que se ejecutan en el navegador de los usuarios, basta con que un usuario visite un sitio web que contenga el código para que su procesador sea utilizado para minar alguna criptodivisa. El criptojacking comenzó a tener una gran actividad

hacia finales del año pasado, siendo la amenaza más detectada por la telemetría de ESET a nivel mundial entre diciembre de 2017 y junio de 2018.

En lo que va de 2018, en la región latinoamericana, casi la mitad de las detecciones de JS/CoinMiner se concentra en dos países: Perú (30,72%) y México (17,41%), seguidos por Ecuador (8,89%), Brasil (7,73%) y Argentina (7,08%).

3. MALWARE

Los códigos maliciosos continúan siendo una de las principales amenazas, al tiempo que también son utilizados para llevar a cabo ataques. De acuerdo con el ESET Security Report 2018, las infecciones por malware se presentan como la principal causa de incidentes de seguridad en las empresas latinoamericanas.

Los Laboratorios de Investigación de ESET reciben diariamente más de 300,000 muestras únicas de malware, observando que se desarrollan amenazas de este estilo para prácticamente todos los sistemas operativos utilizados de la actualidad. Por ejemplo, los laboratorios de ESET afirman que identifican mensualmente, en promedio, alrededor de 300 muestras de malware para Android. Además, comenzaron a aparecer muestras de malware especialmente diseñadas para afectar a los dispositivos de la denominada Internet de la Cosas; que luego de ser comprometidos son utilizados para llevar a cabo otros ataques.

4. CIBEREXTORSIONES

Durante 2018 aparecieron diversas estafas vía correo electrónico enfocadas en engañar a los usuarios a partir de la supuesta obtención de información que los comprometía. En varias de estas campañas existía un dato específico, que hacía creer al usuario que podría no tratarse de un engaño.

Un ejemplo es la campaña en la que la contraseña de los usuarios era el asunto del mensaje, en un intento por demostrar que tenían sus datos personales y que la extorsión que detallaban en el texto del correo era real. Se estima que esta campaña en particular logró recaudar cerca de medio millón de dólares. Otro ejemplo de este tipo de estafas tenía la particularidad de que el correo electrónico llegaba al usuario desde su propia cuenta, lo que hacía suponer que el atacante tenía acceso a la cuenta de la potencial víctima.

5. EXPLOTACIÓN DE VULNERABILIDADES

Hacia final s de 2017, ESET destacaba que se trataba del año con el mayor número de vulnerabilidades reportadas (14,714), superando por mucho los registros de años anteriores, sin embargo, en lo que va de 2018 esta cifra ha sido superada. De acuerdo a CVE Details, "a pesar de que aún no concluye el año, ya se han registrado más 15,300 vulnerabilidades". En este contexto, la explotación de algunas vulnerabilidades también se encuentra al alza. Por poner un ejemplo, la detección de EternalBlue, un exploit utilizado durante la propagación de WannaCry, ha tenido aumentos. Si se comparan las detecciones de este exploit durante mayo de 2017 con las de julio de 2018 (periodo con mayor actividad), hubo un incremento de casi 600%, en donde diversas familias de ramsomware y otros tipos de malware intentan aprovecharse de las vulnerabilidades en los sistemas desactualizados.

Según el informe, el equipo de seguridad de Microsoft desglosa cuatro tendencias globales principales:

Los ataques de Ransomware están disminuyendo: los ataques han disminuido en un 78% en América, lo que hace que la tasa sea un 40% más baja que el promedio mundial.

La minería de moneda criptográfica es frecuente: con una barrera de entrada baja, los delincuentes cibernéticos aprovechan la amplia disponibilidad de software de minería y los reenvasan en malware, sin embargo, en las Américas, la minería de criptomoneda es un 58% más baja que el promedio mundial.

Las cadenas de suministro de software están en riesgo: al incorporar un componente comprometido en una aplicación o paquete de actualización legítimos, que luego se distribuye a los usuarios a través del software, los atacantes pueden aprovechar la confianza que los usuarios tienen en sus proveedores de software, lo que lo hace muy difícil de detectar.

Los hallazgos de ejemplos anteriores, incluida la campaña Dofoil, ilustran el alcance de este tipo de ataques y lo que Microsoft está haciendo para prevenirlos y responder a ellos.

El phishing que sigue siendo un método de ataque preferido, al igual que el ransomware, han cambiado las tácticas en respuesta a las herramientas y técnicas más sofistic das que se han implementado para disuadir los ataques y proteger a los usuarios.

Los hallazgos adicionales destacan cambios positivos clave, como la disminución en las tasas de encuentro de Malware en un 47% en el conjunto de las Américas, lo que hace que la tasa de encuentro de la región sea un 27% más baja que la tasa global.

Diana Kelley, CTO del campo de seguridad cibernética de Microsoft, afirma que "con los nuevos hallazgos, como el aumento de la actividad de la cadena de suministro, la extracción de monedas y las prácticas de phishing, Microsoft asegura que 2018 fue

un año lleno de importantes avances positivos. Un hallazgo clave en Perú es que lidera la tasa de ataques con malware de minería de criptomonedas, superando a Bolivia y Venezuela. Esto se debe en parte a la mala higiene de la seguridad cibernética, y la poca conciencia de seguridad de los usuarios en estos mercados pueden llevar a una mayor infección de malware".

En esa línea, Perú también se ubica como el tercer país de América en la tasa de ataques con malware en general. Entre los principales riesgos está el deterioro de uso, pérdida de datos, robo de propiedad intelectual y pérdida monetaria.

Sin embargo, pequeñas acciones pueden hacer una enorme diferencia en la salud de nuestra ciberseguridad en general, ayudándonos a reducir estas tendencias. Aquí, Microsoft ha recopilado las más importantes Reglas de Ciberseguridad:

A nivel organizacional, hay dos prácticas ideales para protegerse:

- **Prevención:** los controles preventivos aumentan el costo de los ataques de los ciberdelincuentes y previenen técnicas de ataque cibernético eficace
- **Detección y respuesta:** aprovechar la tecnología en la nube para limitar el acceso de los atacantes a los datos y ayude a las operaciones de seguridad a responder mejor a los ataques.

Por otro lado, a nivel de usuarios, Microsoft ofrece 5 recomendaciones:

- **Higiene cibernética:** use una solución antivirus y mantenga actualizado el software y los sistemas operativos.
- **Software original:** evite usar software pirateado y solo use software de fuentes confiables.
- **Gestión de contraseñas:** utilice una contraseña segura para cada cuenta y cámbielas regularmente.
- **Copia de seguridad de archivos personales:** realice copias de seguridad de fotos y otros datos personales importantes en una plataforma de almacenamiento en la nube confiable.
- **Manténgase alerta:** las actividades en las que se transmitirá información personal solo deben realizarse en los dispositivos de los propios usuarios, en una red de confianza.

PERICIAS DE RESGUARDO Y PROTECCIÓN DE LA PRUEBA

Uno de los procedimientos para la obtención de información preliminar de un hecho jurídico virtual, se halla en la Guía de Actuación Fiscal en el Código Procesal penal de la Escuela del Ministerio Público de la Fiscalía de la Nación (2013) demanda que para el Protocolo de Intervención, Grabación o Registro de Comunicaciones telefónicas, radiales y otras, tiene por objetivo intervenir y grabar las comunicaciones

del investigado o tercero, relacionado a un delito penado mayor a cuatro años de privación de la libertad. Para cuyas diligencias:

- La autoridad encargada registra con grabación magnetofónica u otro medio técnico y entrega al fiscal;
- El fiscal debe;
- Disponer las medidas de seguridad para la conservación de las grabaciones y para que no sean conocidas por otras personas;
- Disponer la transcripción de las grabaciones sin perjuicio de conservar los originales, levantando el acta correspondiente;
- Notificar lo actuado al afectado, una vez terminada la diligencia, siempre que el objeto de la investigación lo permita y no se ponga en peligro la vida o integridad de otras personas.

Por tanto, las empresas telefónicas y de telecomunicaciones, deben posibilitar la intervención, grabación o registro de las citadas comunicaciones.

Pues, las funciones del fiscal, la policía y el juez, en el proceso de la investigación, son coordinadas bajo el siguiente procedimiento:

FUNCIONES DEL FISCAL

- Dirección de la investigación;
- Protección de los derechos y garantías en el proceso penal;
- Poder coercitivo y deber de la carga de prueba, por la cual, al averiguar el hecho, recaba elementos de convicción de cargo y de descargo.

FUNCIONES DE LA POLICÍA

- Realiza la investigación operativa y apoya al fiscal en la investigació

El Juez de la investigación Preparatoria, resuelve los requerimientos y solicitudes de las partes, se pronuncia sobre las medidas y medios de defensa.

En este contexto las FASES DE LA INVESTIGACIÓN, son las siguientes:

Realización de las Diligencias Preliminares. Con la finalidad de obtener y asegurar los elementos materiales de prueba, individualizar a los involucrados y agraviados y lograr el recojo de evidencias y el aseguramiento de la cadena de custodia.

Luego se procede con el Inicio de las diligencias preliminares, la Fijación del plazo de las Diligencias preliminares, la Conclusión de la Investigación preliminar y el Control del Plazo.

Finalizadas las Diligencias preliminares se apertura la investigación preparatoria con la finalidad de profundizar los actos de investigación y lograr mayor información., se fija la Finalidad de la Investigación y se da Inicio de la Investigación Preparatoria Formalizada, se fijan los plazos, la Conclusión de la Investigación y el Control del Plazo.

En cambio, la Investigación científica y las metodologías de la Informática Jurídica, consideran que para realizar una investigación, para la consecución de Pruebas digitales, es imprescindible desarrollar Cursos de capacitación y Certificación de nivel universitario en Informática forense, para lograr un alto nivel de profesionalismo y entrenamiento continuo, que soporten investigaciones de crímenes de alta tecnología y consecuente innovación continua de equipos y tecnología, en el escenario más sorprendente de su uso delictivo y represivo Por ejemplo, las metodologías que aplica la Certificación ISFCEl exige conocimiento en múltiples áreas técnicas y jurídicas, experiencia práctica y demostración de habilidades y dominio de la informática forense, es una entidad dedicada a los temas de Computación Forense, denominada Key ComputerService, LLC, ofrece la Certificación. CCE-CertifiedComputerExaminer en sus niveles básico, avanzado y maestro.(Referimos a éste orden de conocimientos, por considerar adecuados al nivel de uso promedio de la población)

Las habilidades requeridas para el nivel básico son:

- Buen entendimiento de las reglas de la evidencia, relacionadas con:
    - La identificación y adquisición de medios magnéticos de última generación. Y el manejo, etiquetado y almacenamiento de evidencias digitales.
    - Conocimiento de la Cadena de Custodia y Derecho a la Privacidad de la Libertad.

Buen entendimiento de cómo eliminar, verificar y validar medios de almacenamiento de información.; de cómo proteger el medio original de escrituras accidentales, del cómo hacer y verificar copias exactas de medios de almacenamiento de información, conocimiento básico de cómo quebrar contraseñas, habilidades para organizar y presentar informes, gráficas y resultados de reportes, presentar copias exactas de data. de almacenamiento de información, conocimientos básicos de las redes de computadoras y de internet, de las aplicaciones de última generación y cómo acceder a la metadata almacenada, etc.

Por su parte el Instituto de Administradores de Sistemas, Auditoría, Redes y Seguridad SANC, que es una institución creada para la formación, entrenamiento y generación de conocimientos en temas de Seguridad de la Información, para alcanzar

esta certificación, y el Título de Investigador forense en Informática, los temas que se estudian son los siguientes: (sólo se mencionan los de nuestro interés)

- Estructura de sistemas de archivos y su metadata.
- Característica de los sistemas de archivos
- Prácticas en el manejo de evidencias digitales.
- Adquisición de evidencias de discos duros y datos volátiles.
- Análisis de tiempo sobre sistemas de archivos.
- Recuperación de datos utilizando cadenas y encabezados de archivos.
- Comparación de hash de archivos contra bases de datos de hash
- Análisis del >Registro del sistema, rastros en Internet y metadata de archivos.
- Análisis de huellas de las aplicaciones.
- Análisis forence de USB, Windows y otros de últina generación.

El estudio de las áreas tecnológicas en Informática y Electrónica, incluyen el estudio de Lenguajes de Programación, Teoría de sistemas operacionales y sistemas de archivos; Protocolos e Infraestructuras de comunicación, Fundamentos de Circuitos eléctricos y electrónicos. Arquitectura de Computadoras y Fundamentos de bases de datos.

En el Área de Seguridad Informática: Principios de Seguridad Informática, Políticas, estándares y procedimientos en seguridad informática, Análisis y administración de Riesgos Informáticos, Re, Técnicas de Hacking y vulneración de sistemas, Mecanismos, medios y tecnología de seguridad.

CONCLUSIONES

Primera. La gradual transformación digital de la sociedad peruana, conlleva la aparición de Dos categorías jurídicas que giran en torno de la ciberseguridad y la ciberdelincuencia, producto de la globalización de la cultura jurídica y la Siderización cotidiana de las innovaciones de las TICs, de las Redes sociales y de los medios físicos de telecomunicación electrónica robotizada, en este contexto de adopción necesaria y permanente de desarrollo de las nuevas tecnologías, especialmente Internet, la justicia procesal en el país, prevé el tratamiento del tema de la Ciberseguridad como un asunto socio económico y jurídico transversal, para la lucha contra la ciberdelincuencia.

Segunda.- La relación del Derecho Procesal penal. con la problemática de la ciberseguridad – ciberdelincuencia, se halla en la Certificación, garantía y seguridad, que ofertan las innovaciones tecnológicas para la obtención de la Prueba digital. La misma se constituye en un instrumento ineludible e inseparable, tanto para la tipificación del delito, como para su judicialización y consecuencias jurídicas.

Tercera. Las diligencias o pesquisas, que actualmente realiza la PNP y las fiscalías dedicadas a la gestión de Procesos penal.- digitales, no utilizan procedimientos de data científi a-forense-informática, para la obtención de información constitutiva de una prueba digital.

REFERENCIAS BIBLIOGRÁFICAS

YRIVARREN J. (2011) *Gobierno Electrónico. Análisis de los conceptos de tecnología, comodidad y democracia.* Lima: Universidad Peruana de Ciencias Aplicadas (UPC)

Jiménez, J. (2017) *Manual de Derecho Penal Informático.* Lima: Jurista Editores E.I.R.L.

Sánchez, P. (2004) *Manual de Derecho Procesal Penal.* Lima: IDEM S.A.

Mittermaier, K. (1979) *Tratado de la prueba en materia criminal".* Buenos Aires: Ed. HAMMURABI.

FerreitosC. FerreryrosH. Mauricio D. (2016) *Derecho de personas e Informática.* Lima: Grijley.

Pérez, A. (2004) *¿Ciberciudadaní@ o Ciudadaní@.com?.*Barcelona: Editorial Gedisa S.A.

Correa C. Batto H. Czar de Zalduendo, S y Nazat F. (1994) *Derecho Informático.* Buenos Aires: Ediciones DePalma.

LOS ESTADOS, LAS CRIPTOMONEDAS Y LA CIBERSEGURIDAD

Eje temático: Cibersegurança

Autor:
Humberto Martín Ruani
Presidente de la Asociación Argentina de Informática Jurídica
Argentina

Palabras Clave:
Criptomonedas - Delitos Informáticos - Delitos Económicos - Comercio Electrónico transfronterizo - Dinero electrónico - Transferencia de divisas.

Síntesis: Este trabajo aborda la actualidad de los activos conocidos como criptomonedas en la actualidad, realizando un análisis de sus antecedentes, objetivos y mecanismos de acción. A su vez propone un criterio ético que concluye en una serie de recomendaciones para su regulación a nivel internacional.

Síntese: Este artigo trata da atualidade dos ativos conhecidos como criptomoedas no momento, realizando uma análise de seus antecedentes, objetivos e mecanismos de ação. Ao mesmo tempo, propõe um critério ético que conclui com uma série de recomendações para sua regulamentação em nível internacional.

INTRODUCCIÓN

Hoy día es innegable el valor que han adquirido las criptomonedas y cualquiera que haya operado con las mismas puede dar fe de que este mecanismo, es la practicidad hecha dinero. Aparte quedan temas como si es una inversión segura o rentable, la realidad es que poder enviar dinero a casi cualquier parte del mundo en cuestión de segundos y con un costo ridículo como pueden ser la cantidad de 0,02 dólares por transferencia. (ethgasstation, 2019) Sin impuestos, sin tasas ni contribuciones, sin controles de ningún tipo, es una realidad que hasta hace apenas una década atrás, pareciera inalcanzable.

Por otro lado (el lado oscuro…), es usual que tras el desarrollo de nuevas tecnologías, aparezcan personas que adapten las mismas en función de obtener un beneficio propio. El problema real se da, cuando ese beneficio es en perjuicio de otros. En este sentido, precisamente las ventajas que ofrecen las criptomonedas, como ser el anonimato, la falta de control de un ente centralizado y la falta de regulación a nivel internacional, hacen que sea una excelente vía para la ejecución de delitos administrativos y económicos, ya que no hay un registro formal de las operaciones, ni identific - ción fehaciente de las partes.

Aquí, lo que realmente hace ruido, es que el desarrollo de una herramienta

como esta, en la cual no se identifican las partes, se transfieren créditos con valor pecuniario a cualquier parte del mundo, sin que se registren las operaciones, sin que los sistemas fiscales e impositivos puedan controlar los ingresos y egresos de las personas, ¿PODRÍA HIPOTÉTICAMENTE HABERSE CREADO PARA USUARIOS QUE CUMPLEN CON SUS DECLARACIONES DE IMPUESTOS Y CON LA NORMATIVA FISCAL DE SUS PAÍSES?

Bueno, en Argentina y otros países de habla hispana, utilizamos a menudo la frase "Se inventó el avión a chorro y el chorro afana en avión". La respuesta al párrafo anterior, quedará a criterio cada quien... pero en mi opinión, pareciera que en vez de inventarse el avión a chorro y que el "chorro", después "afanara" en avión, aquí más bien se inventó un arma digital y después se lo disfrazó de avión.

Mucho podemos hablar de la ciberseguridad, de la aplicación de la tecnología y de los beneficios de poder realizar transferencias seguras –Y lo haremos más adelante-. Pero muchas veces podemos estar frente a una arma de doble filo, cuando las herramientas desarrolladas, sirven tanto para agilizar actividades licitas, como ilícitas.

2. DEFINICIÓN Y ANTECEDENTES

2.1 Concepto de Criptomonedas

La denominación de Criptomonedas, define este concepto per sé, se trata de una moneda encriptada, codificada. Básicamente es una red de datos, protegida con fuerte seguridad, que permite controlar la creación de unidades originarias y adicionales. También permite verificar la transferencia de activos, pero sin la necesidad de un intermediario formal, es decir que tienen un control descentralizado, a diferencia de los bancos y entidades financieras.

Otra diferencia con el sistema tradicional, es que las transacciones de criptomonedas, no se realizan en forma individual, sino que se agrupan varias transacciones y se conforma un bloque que se controla al cerrarse y se adjunta a otros bloques, controlados y cerrados, formando así las conocidas cadenas de bloques o en inglés, "blockchain", que son el equivalente a un registro público de transacciones, con la salvedad de que aquí no hay nombres, ni identificación de personas humanas.

La última gran diferencia que tendremos en cuenta, es que con las monedas tradicionales, la única manera de obtenerlas, es a través de una transacción comercial o laboral; mientras que las criptomonedas, como necesitan de trabajo humano para revisar las transacciones, pagan por ello. De esta manera, aquellos que tienen algunos conocimientos específicos, pueden obtener criptomonedas como pago por su ayuda para con el sistema. Estos constructores de paquetes que preparan los bloques para que viaje la información, son conocidos como mineros.

Este sistema de procesar información que utiliza miles de usuarios y ordenadores, genera una enorme red de seguridad, la cual si bien es matemáticamente quebrantable,

requeriría de una capacidad de procesamiento realmente grande, de hecho tendría que ser mayor que el de todo el entramado (red-enjambre) de todos los mineros del sistema, y aun así, solo tendría una probabilidad de éxito del 50% (n.º de ronda de autenticación).

2.2 Origen de las Criptomondeas

Como muchos otros inventos, -incluso Internet- las criptomonedas no se generaron por una única idea en un momento determinado, sino que han tenido su evolución en distintos momentos. Básicamente podemos remontarnos a 1983, cuando el criptógrafo David Chaum desarrolló un sistema criptográfico monetario electrónico llamado ecash (Nombre que al menos en Argentina), aún utiliza una empresa de pagos electrónicos). Más de 10 años después, Desarrolló "Digi Cash", este sistema, bastante más similar al concepto de criptomonedas actuales, utilizaba la criptografía para dar anonimato a las transacciones de dinero. Este sistema, contaba con un software que al tomar dinero de una entidad financiera, codifi aba, encriptaba las operaciones antes de que puedan transferirse a alguien más y de esta manera conseguía evitar que se rastreara el trazado del dinero. Sin embargo, carecía de algo esencial que tienen las criptomonedas actuales y es precisamente la descentralización del control, ya que las operaciones de dicho sistema requerían un control central.

Más allá de los antecedentes referidos en el párrafo anterior, muchos -la mayoría- identifican la primer publicación de la idea actual de criptomonedas, con el Ingeniero Informático Wei Dai, quien en 1998 propuso crear un nuevo tipo de dinero, cuya plataforma no fuera físico y principalmente, una herramienta de intercambio económico que no dependiera de un organismo central, sino que se regulara de manera descentralizada. El ingeniero Dai propuso que una de las formas de darle seguridad a dicha herramienta, era la utilización de la criptografía como medio de control. Unos años más tarde, bajo el pseudónimo de Satoshi Nakamoto, se creó el conocido por todos "Bitcoin", entre 2008 y 2009. Que más adelante, desató una enorme controversia por el anonimato detrás del pseudónimo, así como también lo hizo por el hecho de tratarse de un código abierto que cualquier persona con conocimientos de programación y desarrollo de software puede revisar y comprender. Es más, este sistema permite modifi aciones en su código sin que un ente central las apruebe o rechace. La única condición, es la aprobación de los demás usuarios.

3. LEGALIDAD Y LEGITIMIDAD

Estos dos conceptos, que suenan tan parecidos, tienen definiciones similares, toda vez que la primer definición según la (Real Academia Española, 2019) es precisamente que algo legítimo, es aquello acorde a la ley. Sin embargo, cuanto más indagamos respecto de este vocablo, más nos encontramos con una idea de lo que es debido, de lo lógico, de lo correcto; Mientras que lo legal, sigue estrictamente la letra de la normativa escrita y la adecuación de las conductas a dicha normativa.

El conocido principio de legalidad nos indica que "Todo lo que no está prohibido, está permitido". En otras palabras, es tan importante la seguridad jurídica, que aun cuando la lógica indique que una acción es socialmente negativa, si la misma no está prohibida expresamente por la normativa vigente, entonces será legal y por lo tanto no reprochable por el sistema de administración de justicia.

En esta inteligencia, el uso de las criptomonedas estará en sí mismo permitido, siempre y cuando no esté prohibido. Ahora bien, salteando la parte de definir las criptomonedas y siguiendo el principio de la primacía de la realidad, en el cual nos encontramos que resultan ser bienes intangibles, susceptibles de apreciación pecuniaria, independientemente de la legalidad que puedan alcanzar, no es menos cierto que debieran cumplimentar con todas las formalidades que en cada país regulan este tipo de bienes.

Por otro lado, el uso de estas criptomonedas, que de por sí puede ser cuestionado en cuanto a su específico diseño formulado para ser impersonal y favorecer el anonimato, es también con frecuencia utilizado en actividades ilegales, además de imposibilitar el establecimiento de políticas impositivas sobre transacciones realizadas a través de dicho medio por parte de los gobiernos.

4. LA CIBERSEGURIDAD Y LAS CRIPTOMONEDAS

En la actualidad, es realmente amplio el campo de la Ciberseguridad y como dijimos anteriormente en la introducción, es realmente mucho lo que se puede hablar de esta disciplina. Es que tratándose de un producto netamente digital, las criptomonedas realmente se destacan en este campo. Están concebidas no solo para resistir ataques, sino también para ser escrutadas por los usuarios e interesados, en algunos casos incluso poseen un código abierto, a través del cual, la mismísima comunidad de usuarios es capaz de modificar el funcionamiento del software con la condición de que dicha modificación sea aceptada por los demás usuarios. Lo que por un lado otorga una confiabilidad y transparencia envidiable, mientras que por el otro expone completamente su mecanismo y eventuales vulnerabilidades.

Resulta imposible a esta altura, garantizar la seguridad de un sistema operativo en un cien por ciento. Así como uno puede en su casa colocar una reja, un sistema

de alarmas, un custodio en la puerta o mudarse a una isla; permanentemente se está aumentando el nivel de seguridad, pero en ninguno de los casos se podría evitar la muerte ante la caída cercana de una bomba atómica… Esta exageración tal vez algo burda, es un ejemplo claro de cómo, con ciertas medidas, podemos "achicar ventanas", reducir riesgos, evitar ciertos tipos de ataques y prevenir eventuales accidentes.

El concepto de "Achicar ventanas" es una metáfora que define muy aproximadamente el objetivo de la seguridad en general y que aplica específicamente a la ciberseguridad. En este sentido, tanto en lo que refiere al software como incluso al hardware, siempre podemos elevar el nivel de seguridad, aunque a veces no podamos prevenir o resistir un ataque nuclear, posible mente podamos evitar otros ataques menores, pero a la vez más probables, o frecuentes.

En el caso de las criptomonedas, consideremos que en hay gran diversidad de sistemas como hemos visto anteriormente, pero que se trata de un valor que hasta hoy es incluso más valioso y apetecible que los datos personales, estamos hablando de dinero *contante y sonante,* dinero que persiguen aquellos que desarrollan una plataforma de moneda electrónica, o al menos con seguridad lo persiguen quienes hacen uso de estos medios.

Podría ser redundante decir que el eslabón más débil por lo general es el humano, ya que en general cuando se trata de información protegida intencionalmente con asesoramiento de profesionales en la materia, no es tan sencillo romper las barreras de seguridad del software o del hardware. Pero la realidad es que una vez mas, tratándose de criptomonedas, el eslabón más débil es el mismo que en el resto de las situaciones.

La amenaza más vigente, no ataca directamente el software de la criptomoneda, ni las cuentas de los usuarios. En el universo de las monedas electrónicas, donde existen actividades que producen *per se,* una renta activa, la violación de seguridad más común, refiere a la utilización no autorizada, ilícita, de la capacidad de procesamiento de ordenadores, teléfonos o dispositivos afines, ajenos a quien realiza la actividad. Por ejemplo, mientras yo estoy durmiendo con mi teléfono al costado de la cama, cargando su batería para el día siguiente, resulta que el Smartphone, ha sido hackeado y alguien está utilizando su capacidad de procesamiento para llevar adelante actividades de minería, produciendo así un redito en criptomonedas que luego podrá ser canjeado por bienes, servicios, o incluso monedas de curso legal.

Naturalmente, con el tamaño y la implicancia del objeto víctima de un ciberataque, concurre una exponencial capacidad de daño. Recordemos que partiendo de la base de que las criptomonedas son una forma de financ amiento prácticamente imposible de ratrear, pueden formar parte de un ciberataque desde la concepción llana y simple de una forma de pago.

5. INTERVENCION DE LOS ESTADOS Y DERECHO COMPARADO

Haciendo un muy breve resumen en atención a la extensión del presente artículo y a la constante variación de la normativa internacional al respecto, podemos decir que:

BOLIVIA se ha convertido en el primer país americano en prohibir explícitamente el uso de criptomonedas. En este sentido, el Banco Central de Bolivia, el 6 de mayo de 2014 emitió la Resolución 044/2014 que en su art. 1 indica: "A partir de la fecha queda prohibido el uso de monedas no emitidas o reguladas por estados, países o zonas económicas, y de órdenes de pago electrónicas en monedas y denominaciones monetarias no autorizadas por el Banco Central de Bolivia en el ámbito del sistema de pagos nacional" (MARTY, Belén). Esta autora, señala también que "El documento, firmado por el directorio del Banco Central, explica que esta resolución, como todas las realizadas por esta entidad, tienen como objeto "procurar la estabilidad del poder adquisitivo interno", y que con ese fin se llevan a cabo las políticas monetarias.", aunque sin embargo, también contempla la posibilidad de que estos cripto activos, sean precisamente un resguardo de los eventuales desequilibrios monetarios que los estados pueden ejecutar en algunos casos de manera voluntaria para perseguir diversos objetivos.

BRASIL, es uno de los tantos países que venían evaluando la regulación de estos activos y finalmente, este año la Receita Federal do Brasil, dictó la *Instrução Normativa N° 1888/ 2019*, cuyos efectos no habían comenzado a ser obligatorios al momento de escribir este artículo, pero sí debieran serlo al momento de la publicación de este trabajo, ya que a partir del mes de Agosto de 2019, los brasileros, deberán declarar sus operaciones de criptomonedas. Esto no es un dato menor, un estudio de abogados (MACHADO MEYERS ADVOGADOS), cita la Consulta Pública RFB nº 6/2018, cuyo resultado indica, según la fuente citada, que el movimiento de estos activos durante 2018 fue de entre 18 y 45 billones de Reales, SOLO en Bitcoins. (entre 4,7 y 12 billones de dólares aproximadamente).

El caso más controversial, es el del gran gigante asiático, China, que supo liderar el mercado mundial de criptomonedas, hasta que en 2017 comenzó una categórica prohibición del venta anticipada de monedas, que se complementó con la prohibición del intercambio de Yuanes por criptomonedas, impactando negativa y sustancialmente en el valor de estos activos y repartiendo su liderazgo luego, entre Japón y Corea del Sur. Si bien el mercado espera que esta prohibición caiga de un momento para otro; No es menos cierto que la principal plataforma social y de pagos "We Chat", en Mayo de 2019 cambió su política de pagos, dejando de aceptar transacciones en criptomonedas, por considerar dichas operaciones ilegales.

El análisis de la situación en ESPAÑA, no puede hacerse con independencia de la COMUNIDAD EUROPEA, por lo que resumidamente diremos que si bien, las Cortes Generales no han aprobado ninguna ley sobre las criptomonedas, es decir que no existe regulación legal local de las monedas virtuales en la actualidad, que provengan de este país, la realidad es que sí hay un marco normativo general. Por ejemplo, el Tribunal de Justicia de la Unión Europea (TJUE), en la sentencia de fecha 22 de octubre de 2015, asunto C-264/14, (Tribunal Superior de la Comunidad europea, Sala Quinta, 2019) decretó que,

> *"la divisa virtual de flujo bidireccional «bitcoin», que se intercambiará por divisas tradicionales en las operaciones de cambio, no puede calificarse de «bien corporal» en el sentido del artículo 14 de la Directiva del IVA, puesto que, como puso de manifiesto la Abogado General en el punto 17 de sus conclusiones, no tiene ninguna finalidad distinta de la de ser un medio de pago."* (Tribunal Superior de la Comunidad europea, Sala Quinta, 2019)

Finalmente, en sus conclusiones, la referida jurisprudencia indica en el punto 2, que,

> *"2) El artículo 135, apartado 1, letra e), de la Directiva 2006/112 debe interpretarse en el sentido de que constituyen operaciones exentas del IVA con arreglo a dicha disposición unas prestaciones de servicios como las controvertidas en el litigio principal, consistentes en un intercambio de divisas tradicionales por unidades de la divisa virtual «bitcoin», y viceversa, y realizadas a cambio del pago de un importe equivalente al margen constituido por la diferencia entre, por una parte, el precio al que el operador de que se trate compre las divisas y, por otra, el precio al que las venda a sus clientes."* (Tribunal Superior de la Comunidad europea, Sala Quinta, 2019)

En resumidas cuentas, el TSJ de la Comunidad Europea, determina mediante este fallo que el empleo de la moneda Bitcoin y consecuentemente las criptomonedas, quedarán exentas del tributo del Impuesto al Valor Agregado (IVA).

Asimismo, en junio de 2018, se aprobó la Directiva 2018/843/UE, que será de obligatorio cumplimiento para los países miembros a partir del 10 de enero de 2020 cuya finalidad es combatir el blanqueo de capitales, determina la obligación de las sociedades intermediarias de "criptomonedas" de desarrollar medidas de diligencia debida, como la identificación de sus usuarios con un documento oficial de identidad. Siendo sujetos obligados los proveedores de servicios de cambio de moneda virtual en moneda fiduciaria y a los proveedores de servicios de custodia de monederos electrónicos entre otros. Debiendo informar las actividades sospechosas y restringiendo al menos parcialmente el anonimato que permiten las criptomonedas. (PARLAMENTO DE LA UNION EUROPEA Y CONSEJO, 2019).

Los anteriores, como hemos dicho, son ejemplos de las directrices europeas que condicionan el marco regulatorio de España, pero ya adentrándonos concretamente

en este país, podemos tomar como referencia, las disposiciones de la Agencia Estatal de Administración Tributaria que ya en enero de 2018 publicó en el Boletín Oficial de España, un Plan de Control Tributario y Aduanero, donde se establece directrices para el control de modelos de negocio por Internet y pagos a través de medios como los monederos electrónicos.

Las obligaciones establecidas, varían según el tipo de transacción y los beneficios por el intercambio de criptomonedas, debiendo también ser declaradas y tributar en su carácter de patrimoniales. Por lo que beneficios y pérdidas obtenidos en las operaciones de compra y venta de estos activos tributarán como ganancia o pérdida patrimonial en el IRPF. Tomando como modelo, los criterios de valoración de las operaciones con acciones. Recientemente y en igual sentido, el 20 de Junio de 2019 el TRIBUNAL SUPREMO a través de su Sala de lo Penal, mediante Sentencia núm. 326/2019 al RECURSO CASACIÓN/998/2018. Manifestó expresamente que las criptomonedas, en este caso Bitcoins, no son en modo alguno dinero; también afirmó que se trata de "… un activo patrimonial inmaterial".

En cuanto a la minería de criptomonedas hay obligación de darse de alta en el Impuesto sobre Actividades Económicas asimilando las actividades relacionadas con criptomonedas a las propias de los servicios financieros.

Por su parte, ESTADOS UNIDOS ha publicado recientemente -9 de mayo de 2019-, a través de la Red de Control de Delitos Financieros de Estados Unidos (FinCEN), una guía de interpretación que incluye una parte importante de los modelos de negocios con criptomonedas, dentro de la BSA (Ley de Secreto Bancario), estableciendo pautas necesarias para cumplir con la política conocida como "KYC", por sus siglas en inglés que se traducen "conozca su cliente". Esto afectaría a casas de cambio y aplicaciones que trabajen con transferencias de dinero y la finalidad es principalmente el control de ciertas personas o empresas que puedan estar bajo sospecha para las autoridades de ese país.

RUSIA por su parte, ya tiene proyecto de ley desde el año pasado (2018), que fue aprobado en su primer lectura, y posteriormente pese a tener el apoyo total del ejecutivo, ha debido dar un pequeño paso atrás, ya que el GAFI (Grupo de Acción Financiera Internacional), Le solicitó que ampliara su proyecto legislativo, ya que este omitía temas centrales como la minería por ejemplo. Razón por la que ha vuelto a la primer lectura. Se espera que Rusia respete las indicaciones del GAFI, ya sea en el actual proyecto de ley o complementando este proyecto con otro nuevo en el corto plazo. Sin embargo, la agencia Rusa Fontanka (https://www.fontanka.ru/2019/05/15/073/) informó en su portal el pasado 16 de Mayo de 2019 que el primer ministro Ruso, Dmitry Medvedev, ha manifestado que este tema no es una prioridad para el gobierno ruso y que el motivo de esta situación es la pérdida de popularidad de las criptomonedas en ese país.

Por otro lado, en VENEZUELA, donde se ha llegado a arrestar, en 2017, a varias personas que realizaban explotaciones de "Minería" por legitimación de capitales, enriquecimiento ilícito, delitos informáticos, financiamiento al terrorismo, fraude cambiario y daños al sistema eléctrico nacional, a partir del 9 de abril de 2018 por medio de Decreto, la Asamblea Nacional Constituyente legalizó toda existencia y creación de todo criptoactivo incluyendo al "Petro". También permite que cualquier persona natural o jurídica, privada o pública, pueda publicar su propio "Libro Blanco", siendo el primer paso para iniciar el proceso de registro y control de la nueva criptomoneda a crear ante el Ejecutivo Nacional. Así mismo se ordena a todos los entes del Estado a preparar su estructura burocrática a fin de recibir y pagar con las criptomonedas que estén debidamente registradas.

6. CONCLUSIONES

6.1 A nivel práctico, las criptomonedas juegan un rol superlativo en cuanto a transacciones se refiera. Se producen intercambios con un alto nivel de seguridad, dentro de un marco transparente por su código abierto (caso bitcoin), las cuales tienen un cortísimo plazo de acreditación y no reconocen fronteras. Por si esto fuera poco, el dinero de las comisiones va en parte a usuarios que facilitan el control de las transacciones y la única manera de modificar los protocolos del sistema es, ni más ni menos, que con el acuerdo necesario de todos los usuarios. Poco más se les podría pedir.

6.2 En relación a la legalidad, evidentemente dependerá de cada estado, entendiendo que es tal la magnitud del impacto que han tenido estas monedas electrónicas que eventualmente terminará por normalizarse legislativa o jurisprudencialmente en la inmensa mayoría de los países.

6.3 En cuanto a la legitimidad, es realmente dudosa. ¿Cuál es el objeto de hacer una herramienta comercial que favorezca y permita el anonimato si se pretende cumplir con las normativas de cada estado? ¿Cuál es el objetivo de generar una red punto a punto, donde se manejan enormes cantidades de dinero y en la que no exista un responsable por las operaciones? uno se pregunta si es posible que al momento de desarrollar el sistema puede haberse omitido el hecho de que trasladar bienes susceptibles de apreciación pecuniaria de un estado a otro y sin posibilidad de control por parte de los estados, infringiría necesariamente sus normativas.

6.4 Cabe concluir que aún cuando los estados puedan permitir su uso, es difícil creer que estas criptomonedas hayan sido desarrolladas con la mira en actividades lícitas. Por otro lado, hemos dicho que su practicidad resulta extraordinariamente conveniente. Pareciera que la mejor alternativa viable, será considerar la posibilidad

de una reglamentación paulatina, que ya han comenzado algunos estados y que progresivamente se promueva la unificación y complementación de las diferentes normativas. Un ejemplo de avance en este sentido es el Consorcio, desarrollado para averiguar cómo aprovechar la cadena de bloques en los sistemas financieros tradicionales. Uno de los primeros problemas de la aplicación de este esquema es el anonimato que proporciona el diseño de la cadena de bloques, algo que han resuelto con el llamado "libro de contabilidad autorizado" ('permissioned ledger'), una variante muy peculiar de la cadena de bloques de bitcoin, por ejemplo, que sí que identifica a los usuarios que añaden bloques y que hace que las transacciones del sistema solo puedan consultarse por ciertas partes.

6.5 Como una última conclusión y posiblemente la mas relevante, es que las criptomonedas, no pueden escapar de la vista de los estados. Hablamos de un sistema que permite desde defraudaciones tributarias y hackeos de celulares para la obtención de créditos por minería utilizando procesadores ajenos, hasta el financiamiento del terrorismo de manera inmediata y anónima. Por eso entendemos que su regulación no es solo conveniente, sino extremadamente necesaria.

7. DE LEGE FERENDA

Ha quedado ya claro que difícilmente estas monedas hayan sido creadas con objetivos legítimos y en muchos casos resulta dudosa incluso su legalidad, pero suponiendo que se sortearan esos obstáculos y que quedará en cada uno la responsabilidad por sus actos, lo cierto es que las criptomonedas tienen un valor pecuniario y por lo tanto pueden ser objeto de derecho. Entonces la segunda cuestión es cómo debiera regularse su utilización y en caso de que tributen, la otra gran pregunta es a quién. Supongamos que en un avión de American Airlines, sobrevolando algún país de Sudamérica, desde un celular con conexión satelital transfiero dos millones de dólares (en criptomonedas) a España. ¿Corresponde tributar en algún país? ¿en todos? ¿debe tributar el que recibe el dinero? ¿el que lo envía? ¿Cómo se establece el precio de las criptomonedas a los fines de grabarlos impositivamente? ¿Qué tributos, tasas o impuestos deben grabar estos bienes?

Muchas preguntas y pocas respuestas, en principio la recomendación de este capítulo, es seguir el concepto de que quien dispone del objeto, en este caso criptomonedas, debe tributar según corresponda en la jurisdicción desde donde se realiza el acto de disposición. Es decir que si bien las criptomonedas no están en un lugar específico, sino en un complejo software; también es cierto que en el ejemplo del párrafo anterior, la disposición se estaría efectuando desde jurisdicción de los Estados Unidos, por ser la bandera de la Aerolínea. Por esta razón entenderíamos

según esta recomendación, que deberían realizarse las declaraciones pertinentes, pago de impuestos y justificación de ingresos, según la normativa de ese país para criptomonedas y por el acto de la transferencia, con independencia de los tributos que correspondan a las personas en sus respectivos países por las criptomonedas como activos patrimoniales por el período que hayan poseído estos dentro de su patrimonio.

Seguramente, distintos países tendrán diversa normativa al respecto. En algunos se tendrá que justificar el origen del capital de manera más rigurosa, en otros será más alta la tasa impositiva por disponer del capital, etc. Sin embargo resultaría posible y deseable que los países y bloques económicos pudieran acordar al menos las pautas de qué jurisdicción deban ser aplicables, para que resulte posible hacer uso de esta herramienta sin que se defraude a la administración pública y se elimine el anonimato que conlleva una motivación para el movimiento de capitales provenientes o destinados a actividades ilícitas por estos medios. De esta manera podría preservarse una fuente de trabajo (mineros), una herramienta eficiente, rápida y económica para el movimiento de capitales y a su vez salvaguardar la buena práctica, la razonabilidad y por sobre todo transformar este sistema en una herramienta legítima y legal.

8. BIBLIOGRAFÍA

CRISTENSEN, K. D. (2004). La Piratería Informática en el Ciberespacio: Recursos Jurídicos y Tecnológicos Para Combatirla. En G. (. CABANELLAS DE LAS CUEVAS, *Derecho de Internet* (págs. 159-208). Buenos Aires: Heliasta.

ethgasstation. (16 de JUNIO de 2019). *ETH GAS STATION*. Obtenido de HTTP:// ethgasstation.info

PERRIT, H. H. (2004). Internet ¿Una Amenaza Para la Soberanía? En G. (. CABANELLAS DE LAS CUEVAS, *Derecho de Internet* (págs. 66-90). Buenos Aires: Heliasta.

Real Academia Española. (21 de JULIO de 2019). *REAL ACADEMIA ESPAÑOLA*. Obtenido de WWW.RAE.ES

Tribunal Superior de la Comunidad europea, Sala Quinta. (22 de Julio de 2019). *Infocuria*. Obtenido de http://curia.europa.eu/juris/document/document.jsf?docid=170305&doclang=ES

USO DE DRONES POR POLICÍA Y JUECES PARA LA INVESTIGACIÓN DE DELITOS

Eje temático: Ciberseguridad

Autor:
Federico Bueno de Mata
Profesor Titular de Derecho Procesal. Universidad de Salamanca- ESPAÑA

RESUMEN
En este artículo se analiza la figura del dron como diligencia de investigación tecnológica para el esclarecimiento de hechos delictivos g. Así se explican los tipos de usos permitidos para operadores jurídicos: policía o por jueces a través de lo regulado en las últimas reformas de la normativa española. De este modo, existen aún muchas dudas por despejar sobre el tratamiento procesal del dron. Debemos pensar que en muchas ocasiones estos dispositivos se erigirán como una pieza fundamental en la seguridad de los ciudadanos de la UE y por tanto podrán ser usados como diligencias de investigación tecnológica y como posible dispositivo para la captura de pruebas electrónicas como videos o fotografías digitales.

1. LOS NUEVOS GUARDIANES DEL AIRE

Fue la vigésimo tercera edición del DRAE la que nos sorprendió adaptando el sustantivo inglés "drone", literalmente "zángano", para referirse a una aeronave no tripulada en términos genéricos.

Dejando a un lado esta anécdota, al definir y conceptualizar a los drones debemos partir de que nos movemos en el terreno de la robótica y de la inteligencia artificial, dos elementos que unidos suponen una auténtica revolución en el sector judicial. Así, nos referimos en este caso a una aeronave no pilotada o pilotada de forma remota, pero igualmente a un sistema de servidores y satélites que permiten la gestión del tráfico y la limitación de su vuelo por determinadas localizaciones geográfica.

Los drones presentan cierto debate a nivel terminológico, al utilizarse diferentes acepciones, y aunque todas ellas sean válidas, creemos que es necesario optar por una terminología concreta. Por ello pensamos que el término VANT "Vehículo Aéreo No Tripulado" en castellano o también conocidos como UAS si lo traducimos al inglés, puede conllevar una nomenclatura más amplia que las también conocidas como UAVs (Unmanned Aerial Vehicle) o RPAs (Remotely-Piloted Aircraft). Esto es así debido a que con la nomenclatura VANT no hacemos referencia a si la aeronave tiene un control remoto o tiene la autonomía suficiente para ser autodirigida mediante sistemas de

inteligencia artificial, confeccionando una concepción abierta que hace que no quede rápidamente desfasada por el paso del tiempo y el avance tecnológico.

El legislador español ha utilizado sin embargo el control remoto como el sistema común de pilotaje y así lo demuestra en los arts. 50 y 51 de la Ley 18/2014, reguladora del uso civil de los RPAs, con referencia únicamente a la posibilidad del control remoto para aeronaves cuya masa máxima al despegue sea inferior a los 150 kilos, puesto que en los casos que superen estas dimensiones la competencia recaerá en la Agencia Europea de Seguridad Aérea.[74] Así, la definició de dron en la ley, subraya el control remoto como única opción al definir estas aeronaves como "cualquier maquinaria pilotada por control remoto que pueda sustentarse en la atmósfera por reacciones del aire que no sean reacciones del mismo contra la superficie de la tierra [75].

A principios de 2018 entró en vigor el Real Decreto 1036/2017 de 15 de diciembre[76], por el que se regula la utilización civil de las aeronaves pilotadas por control remoto. Avanzamos así hacia una normativa más pareja con nuestros países vecinos, eliminando muchas de las restricciones que establecía la Ley 18/2014 y que limitaba en exceso las posibilidades de uso de estos dispositivos. Con este nuevo texto legal contamos con disposiciones mucho más tolerante y detallada de su uso, ampliando su utilización con fines lúdicos y recreativos y acotando de manera concreta su utilización por los diferentes operadores jurídicos para una serie de operaciones policiales como el control de aduanas, la extinción de incendios o la búsqueda o el salvamento de personas.

A lo largo de las siguientes líneas realizaremos un estudio de la última normativa sobre drones al tiempo que analizaremos el distinto régimen de su uso como dispositivo con fines recreativos por particulares o como diligencia de investigación por los distintos operadores.

En marzo de 2018 el Ministerio de Fomento presentó el Plan Estratégico para el desarrollo del sector civil de los drones en España 2018-2021[77]. Un documento marcado por su carácter innovador en el que se proyecta el potencial que el uso de estos dispositivos puede tener para un mercado que se encuentra en plena expansión y que llevará aparejados la creación de nuevos puestos de trabajo, así como un desafió normativo de primer nivel.

Podemos decir que el documento marca la hoja de ruta o el camino a seguir por el Estado en los próximos años. De esta forma el plan se divide en cuatro ejes

74 CUERNO REJADO, C. (et al.), "Evolución histórica de los vehículos aéreos no tripulados hasta la actualidad", *Dyna,* Vol. 91, Nº 3, 2016, págs. 282 – 283.

75 ARIZA COLMENAREJO, M.J, DEL, "La utilización de drones como herramienta en la investigación penal", *Fodertics 4.0*, Comares, Granada, 2015, pág. 107.

76 Vid. https://www.boe.es/buscar/doc.php?id=BOE-A-2017-15721 (Fecha de consulta: 14 de marzo de 2018).

77 Vid. https://www.fomento.gob.es/MFOM/LANG_CASTELLANO/PLANES/PLAN_DRONES_2018_2021/ (Fecha de consulta 26 de mayo de 2018)-.

estratégicos: creación de marco normativo, fomento del I+D+i, cultura de drones y coordinación entre las diferentes Administraciones Públicas e impacto para los derechos de los ciudadanos.

Se parte de que los drones y sus distintas funcionalidades se erigen como un auténtico desconocido para la mayor parte de la población, la cual los percibe más como una amenaza para sus derechos que como un instrumento que puede ofrecer muchos y muy interesantes servicios a la ciudadanía en su conjunto o a las distintas Administraciones Públicas. Por ello es preciso que se creen los cimientos para potenciar una verdadera "cultura de drones" en nuestro país, al tiempo que el desarrollo de la ciencia y la tecnología investiga tanto la parte técnica como la parte jurídico-social que conlleva la introducción de un nuevo elemento en nuestra sociedad.

En este sentido, la apuesta por la investigación vinculada a los drones no solo hará fortalecer nuestro tejido empresarial, sino que servirá como eje central del que se nutran el resto de los ejes.

Así, se podrá avanzar hacia un conocimiento mejorado por parte del sector aeronáutico de esta figura y se podrán crear certificaciones más específicas para el uso y manejo de estos dispositivos al tiempo que se crearán nuevos puestos de trabajo vinculados al sector. Por otro lado, los ciudadanos dejarán de percibir a los drones como unos dispositivos que favorecen el espionaje o el Estado policial para comprender que serán elementos que les harán más fácil su día a día al tiempo que favorecerán su seguridad y la del país.

Según el Plan, en el año 2035 se necesitarán más dieciséis mil de estos dispositivos, de los cuales la mitad servirá para labores de vigilancia y la otra mitad para actividades de primera respuesta. Los cálculos reflejan que existirá un dron por cada cuatro coches de policía y otro por cada dos vehículos de bomberos.

Por otro lado, la creación de un centro de Excelencia es una de las ideas más positivas que incluye el Plan, al promover la colaboración entre empresas y universidades y potenciar así una verdadera transferencia del conocimiento entre ambas instituciones. Esta sería una buena forma de trasladar posteriormente los resultados a los distintos ámbitos implicados y que tuviera posteriormente un reflejo en la sociedad a través de su divulgación.

La difusión a través de diversos canales como Internet fomenta sin lugar a dudas el conocimiento por parte de la ciudadanía, por ello, la creación de la aplicación web ENAIRE Drones constituye un primer escaparate por el que los potenciales usuarios, a través de la descarga gratuita de la aplicación tendrán la posibilidad de planificar el vuelo, leer avisos y alertas con antelación a volar un dron. Igualmente podrán saber sobre qué zonas pueden volar el dron y en cuáles les estará prohibido o requerirán de permiso adicional.

En definitiva, podemos decir que este Plan acabará desembocando en la creación de un marco normativo integral sobre el uso de drones en nuestro país. Como paso previo contamos con la promulgación de un Real Decreto 1036/2017 que nos ofrece una primera cobertura jurídica para la certificac ón de las areonaves, la formación de los pilotos o los requisitos que deben cumplir los operadores.

2. EL USO DE DRONES CON FINES DE INVESTIGACIÓN TRAS LA LO 13/2015

En nuestro país existe un antes y un después en materia de investigación tecnológica con la aprobación de la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la LECrim. A través de ella se dota de fuerza legal para limitar derechos fundamentales, concretamente los recogidos en el art. 18 CE, a través de la previa autorización judicial para el uso de distintas medidas de investigación[78].

Con esta reforma se refuerza por un lado una medida como la de interceptación de comunicaciones, anteriormente regulada mediante ley ordinaria y que ahora no solo habla de conexiones telefónicas sino integrales, con lo que se da soporte y cobertura jurídica a interceptar también aplicaciones instaladas en *smartphones* u otros dispositivos; y por otro se adicionan tres bloques más de medidas tecnológicas de investigación: la captación y grabación de comunicaciones orales e imágenes mediante la utilización de dispositivos electrónicos; la utilización de dispositivos técnicos de seguimiento, localización y captación de imágenes; y por último, el registro de dispositivos de almacenamiento masivo de información. Como hemos apuntado en investigaciones anteriores sobre la materia creemos que la terminología empleada constituye un acierto del legislador español al catalogar las diligencias en cuatro bloques, al utilizar un lenguaje abierto que hace que la regulación no caiga en la obsolescencia con el paso de los años debido a la evolución propia de la tecnología[79].

Respecto al uso del dron como diligencia de investigación policial en esta ley orgánica es necesario apuntar que no hay una alusión concreta a los drones de manera concreta, debido al carácter abierto de la norma. Por ello debemos acudir al bloque denominado "utilización de dispositivos técnicos de seguimiento, localización y captación de imágenes". Concretamente el artículo 588 *quinquies* a) permite a la Policía Judicial la captación de imágenes en lugares o espacios públicos a través de la grabación "por cualquier medio técnico imágenes de la persona investigada cuando

78 ARIZA COLMENAREJO, M.J, DEL, "La utilización de drones como herramienta en la investigación penal", *Fodertics 4.0*, Comares, Granada, 2015, pág. 107 y ss.

79 BUENO DE MATA, F., "Comentarios de legislación: Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica [BOE n. º 239, 6-X-2015]", *Ars Iuris Salmanticensis*, Vol. 4, Nº. 1, 2016.

se encuentre en un lugar o espacio público, si ello fuera necesario para facilitar su identificación, para localizar los instrumentos o efectos del delito u obtener datos relevantes para el esclarecimiento de los hechos".

Del mismo modo la letra c de este mismo artículo, al margen de manifestar que la duración de la medida puede durar hasta 18 meses mediante prórrogas sucesivas, su apartado segundo ya establece que la Policía Judicial deberá entregar al juez "los soportes originales o copias electrónicas auténticas que contengan la información recogida cuando éste se lo solicite y, en todo caso, cuando terminen las investigaciones", a lo que suma en su apartado tercero aplicar mecanismos de aseguramiento que garanticen una buena cadena de custodia[80]a al indicar que "la información obtenida a través de los dispositivos técnicos de seguimiento y localización a los que se refieren los artículos anteriores deberá ser debidamente custodiada para evitar su utilización indebida". Con todo ello vemos como la normativa permite utilizar un dron como medidas de investigación policial y posteriormente aportarlo como prueba al proceso a fin de reproducir su contenido durante la vista oral. De esta forma tendremos que ver de qué forma se aporta y bajo qué manera se reproduce estas potenciales piezas de convicción en juicio.

Igualmente, tal y como hemos apuntado anteriormente esta normativa se complementa con el Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, que le da un marco de actuación más puntual para su utilización para operaciones de policía de las Fuerzas y Cuerpos de Seguridad, funciones de guardacostas y servicios de aduanas, misiones de vigilancia del tránsito viario, y operaciones del Centro Nacional de Inteligencia, así lo especifica de manera concreta en su art. 2 a decir que se aplicara a las aeronaves pilotadas por control remoto "cualquiera que sea su masa máxima al despegue, que efectúen actividades de aduanas, policía, búsqueda y salvamento, lucha contra incendios, guardacostas".

3. LAS DISTINTAS POSIBILIDADES DE USO DE DRONES POR CIVILES Y OPERADORES JURÍDICOS

3.1 El dron como diligencia de investigación policial

En nuestro país existe un antes y un después en materia de investigación tecnológica con la aprobación de la Ley orgánica 13/2015, de 5 de octubre, de modificación de la LECrim. A través de ella se dota de fuerza legal para limitar derechos

80 Vid. ESCLAPÉS MEMBRIVES, S., "Los drones y su uso generalizado: un nuevo reto para el derecho", *Fodertics 5.0*, Comares, Granada, 2016.

fundamentales, concretamente los recogidos en el art. 18 CE, a través de la previa autorización judicial para el uso de distintas medidas de investigación.

Con esta reforma se refuerza por un lado una medida como la de interceptación de comunicaciones, anteriormente regulada mediante ley ordinaria y que ahora no solo habla de conexiones telefónicas sino integrales, con lo que se da soporte y cobertura jurídica a interceptar también aplicaciones instaladas en smartphones u otros dispositivos; y por otro se adicionan tres bloques más de medidas tecnológicas de investigación: la captación y grabación de comunicaciones orales e imágenes mediante la utilización de dispositivos electrónicos; la utilización de dispositivos técnicos de seguimiento, localización y captación de imágenes; y por último, el registro de dispositivos de almacenamiento masivo de información. Como hemos apuntado en investigaciones anteriores sobre la materia creemos que la terminología empleada constituye un acierto del legislador español al catalogar las diligencias en cuatro bloques, al utilizar un lenguaje abierto que hace que la regulación no caiga en la obsolescencia con el paso de los años debido a la evolución propia de la tecnología[81].

Respecto al uso del dron como diligencia de investigación policial en esta ley orgánica es necesario apuntar que no hay una alusión concreta a los drones de manera concreta, debido al carácter abierto de la norma. Por ello debemos acudir al bloque denominado "utilización de dispositivos técnicos de seguimiento, localización y captación de imágenes". Concretamente el artículo 588 *quinquies* a) permite a la Policía Judicial la captación de imágenes en lugares o espacios públicos a través de la grabación "por cualquier medio técnico imágenes de la persona investigada cuando se encuentre en un lugar o espacio público, si ello fuera necesario para facilitar su identificación, para localizar los instrumentos o efectos del delito u obtener datos relevantes para el esclarecimiento de los hechos".

Del mismo modo la letra c de este mismo artículo, al margen de manifestar que la duración de la medida puede durar hasta 18 meses mediante prórrogas sucesivas, su apartado segundo ya establece que la Policía Judicial deberá entregar al juez "los soportes originales o copias electrónicas auténticas que contengan la información recogida cuando éste se lo solicite y, en todo caso, cuando terminen las investigaciones", a lo que suma en su apartado tercero aplicar mecanismos de aseguramiento que garanticen una buena cadena de custodi[82]a al indicar que "la información obtenida a través de los dispositivos técnicos de seguimiento y localización a los que se refieren

81 BUENO DE MATA, F., "Comentarios de legislación: Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica [BOE n. º 239, 6-X-2015]", *Ars Iuris Salmanticensis*, Vol. 4, Nº. 1, 2016.

82 Vid. ESCLAPÉS MEMBRIVES, S., "Los drones y su uso generalizado: un nuevo reto para el derecho", *Fodertics 5.0*, Comares, Granada, 2016.

los artículos anteriores deberá ser debidamente custodiada para evitar su utilización indebida". Con todo ello vemos como la normativa permite utilizar un dron como medidas de investigación policial y posteriormente aportarlo como prueba al proceso a fin de reproducir su contenido durante la vista oral. De esta forma tendremos que ver de qué forma se aporta y bajo qué manera se reproduce estas potenciales piezas de convicción en juicio.

Igualmente, tal y como hemos apuntado anteriormente esta normativa se complementa con el Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, que le da un marco de actuación más puntual para su utilización para operaciones de policía de las Fuerzas y Cuerpos de Seguridad, funciones de guardacostas y servicios de aduanas, misiones de vigilancia del tránsito viario, y operaciones del Centro Nacional de Inteligencia, así lo especifica de manera concreta en su art. 2 a decir que se aplicara a las aeronoves pilotadas por control remoto "cualquiera que sea su masa máxima al despegue, que efectúen actividades de aduanas, policía, búsqueda y salvamento, lucha contra incendios, guardacostas".

3.2 El Dron Como Diligencia Judicial

El art. 299 LECiv en su apartado cinco reconoce el reconocimiento judicial como un tipo de prueba., para que posteriormente los artículos 353 a 359 del mismo texto legal detallen y regulen las características propias del mismo.

En este sentido, según el art. 353.1 LECiv se utiliza cuando para el esclarecimiento y apreciación de los hechos sea necesario o conveniente que el tribunal examine por sí mismo algún lugar, objeto o persona. Por esta razón, sólo el reconocimiento judicial puede ser considerado como prueba directa, pues con ella el juez percibe o toma conocimiento directo y personal del objeto mismo de la prueba. En todos los demás casos de pruebas admitidas en nuestro ordenamiento jurídico, serán consideradas indirectas, debido a que el medio de prueba se realiza por medio de un tribunal ante el juez en sede judicial.

La fuente del reconocimiento judicial es el objeto o la persona que puede ser reconocida; mientras que el medio es el régimen legal de la actividad de reconocimiento por parte del juez y acompañado por el Letrado de la Administración de Justicia y en ocasiones por las propias partes y los letrados. De este modo, el reconocimiento judicial es un medio de la prueba mediante el cual el juez se traslada a un determinado lugar fuera de la sede judicial para tener un contacto directo con un material probatorio. Por ejemplo, cuando debe acudir a ver un edificio en ruinas o debe realizar una exploración

a un menor fuera del juzgado para que su entrada en las dependencias de justicia no se suponga una victimización secundaria.

En el caso de los "ciberreconocimientos", o uso de dispositivos telemáticos para su uso, ya se ha contemplado por parte de la jurisprudencia este tipo de situaciones. En ellas el juez es el que se aproxima de una manera directa a la pantalla del dispositivo originario con el fin de evitar manipulaciones en las pruebas electrónicas aportadas. En otras ocasiones este reconocimiento tiene a su vez conectado una exhibición o cotejo de terminales en las que el propio juzgador compara la conversación o el mensaje electrónico aportado en los terminales para ver que el contenido es el mismo.

Pero ¿y si el juez utilizara un dron como mecanismo para ejercer un reconocimiento judicial? Es decir, en estas ocasiones no sería el juez quien se acercará a la pantalla si no que usaría el dispositivo para que ese visor se desplazara hasta el lugar o la persona que quiere reconocer. De una manera previa pensamos que no debe existir limitación a la hora de practicar los medios de prueba puesto que si no se estaría vulnerando frontalmente el art. 24 de nuestra CE. Aún así, la práctica debe realizarse con fiel respeto a las garantías procesales y no veríamos conveniente el uso de estos dispositivos para reconocer personas puesto que el mismo tipo de reconocimiento se podría realizar a través de un sistema de videoconferencia, con la especial incidencia que tendría al tiempo para el principio de inmediación pero cuyo debate ya se ha visto superado hace años al admitir de manera generalizada la telepresencia virtual para ejercer este tipo de medios de prueba.

Aún así, puede que, en el caso de reconocer edificios de gran altura o escenarios recónditos, con difícil acceso, el dron o los dispositivos aéreos de control remoto pueden ser una buena opción. Para ello se necesitaría dispositivos sofisticados y obtener la previa autorización por parte de AESA para un tipo de vuelo BVLOS (*Beyond Line of Sight*), operaciones más allá del alcance visual del piloto, con aeronaves más sofisticas. De igual manera el vuelo no podría realizarse en primera persona y debería ser atendido por un piloto externo y unos observadores aéreos, al menos uno en el sitio de despegue y otro en el lugar donde la infraestructura fuera a ser reconocida.

Del mismo modo deberíamos plantearnos la presencia del Letrado de la Administración de Justicia. Entendemos que sería suficiente que el LAJ estuviera al lado del juez a la hora de practicar la diligencia y que no sería necesaria que estuviera otro profesional de su misma categoría en el lugar físico del reconocimiento. Esta cuestión no podría equiparse en sentido estricto a las prácticas de declaraciones por videoconferencia, puesto que en ellas se necesitan dos LAJ al consistir en una práctica de una prueba personal. En cambio, al referirnos de forma exhaustiva a un reconocimiento material la presencia del LAJ en el lugar de la infraestructura se supliría con la presencia de un observador de vuelo quien aseguraría las condiciones correctas de aeronavegabilidad.

Aún así, puede que el uso de estos dispositivos, ya asumido por los ciudadanos cuando los mismos son utilizados por FCSE, nos resulte excesivamente futuristas al ser practicados por jueces y magistrados. Esta reticencia inicial nos hace plantear una serie de ventajas e inconvenientes en su uso como diligencia judicial.

En este sentido podríamos observar una ventaja inicial que es la concerniente al uso de tecnología con el fin de ahorrar el tiempo que los profesionales de la justicia invierten en desplazarse a lugares para reconocer determinados objetos o cosas, pues en muchas ocasiones si se contabiliza la ida y la vuelta pueden llegar a consumir gran parte de su jornada laboral. Al mismo tiempo existen algunos lugares que por su altura o su holografía hacen imposible que el contacto visual directo y espacialmente aproximado resulte imposible, lo que se supliría fácilmente con elevar un dron a decenas de metros y poder mediante una cámara de visión directa del objeto de reconocimiento.

Por otro lado, podríamos atisbar una serie de inconvenientes que, desde nuestro de punto de vista, están ya superados o podrían tener una solución relativamente sencilla.

En primer lugar, el fiel respeto a los principios procesales a la hora de su práctica, y de manera concreta su posible afectación al principio de inmediación. Este principio se caracteriza por el contacto directo del juez con el material probatorio que va a examinar, algo que en este medio aún se enfatiza más por ser el único considerado como medio de prueba totalmente directo. Aún así, pensamos que un reconocimiento por videoconferencia de una persona puede conllevar más lesión para este principio que un reconocimiento de una cosa, infraestructura u objeto por medio de un dron. En este escenario no entran el juego cuestiones propias de las pruebas personales como es el lenguaje paraverbal que en ocasiones no es captado por la cámara o la posibilidad de disimular ciertas situaciones de estrés o nerviosismo por la calidad de imagen o el campo de grabación de la lente. En esta ocasión tenemos una videocámara móvil, que por tanto puede subir, bajar, acercarse, alejarse o rotar para la dirección que el juez desee hasta obtener un completo reconocimiento del objeto a ser reconocido. Por estas razones no creemos que exista una colisión directa con este principio, sino más bien una potenciación del mismo, al poder utilizar un dispositivo que llegaría a obtener de manera más eficiente un reconocimiento de la infraestructura. Si a todo ello le sumamos la posibilidad del uso de termografía o tecnología vinculada a rayos X con la que poder visualizar defectos de construcción interno, fugas de gas o un cableado mal conectado que pueda dar lugar a fallos electrónicos, entre otros, esta opción debería ser usada cuanto antes dentro de nuestro sistema judicial.

Por otro lado, podemos pensar que aún no tenemos una normativa concreta que contemple de manera propia al dron como medio de prueba. Efectivamente no existe texto legal específico que enmarque el uso del dron como diligencia judicial ni como

medio para la obtención de pruebas, pero todo esto tiene una relación basada en la analogía con ciertas normas legales ya aludidas en este artículo.

Por un lado, el RD de 2017 permite su uso por autoridades públicas, por lo que la judicatura podría entrar dentro de estos sectores siempre que su fin fuera justificado. Si se permite de manera concreta el uso de drones para el control de aduanas, ¿por qué no podrá usarlo un juez como funcionario público para realizar reconocimientos de infraestructuras? Del mismo modo hemos visto como las diligencias de investigación tecnológica regulan de forma amplia la utilización de dispositivos técnicos de seguimiento, localización y captación de imágenes por parte de Policia Judicial. Aunque no haga una referencia concreta a la figura de la judicitatura tampoco encontramos una ley que prohiba su uso por lo que podríamos decir que no existe ninguna norma de rango legal que limite esta posibilidad.

Si por último acudimos a la LECiv, texto legal donde se regulan las disposiciones generales para el procedimiento probatorio de forma genérica y cuya aplicación debe darse de manera supletoria siempre que no exista una norma concreta al respecto, encontraremos en su art. 354 una respuesta de permisividad clara.

En este artículo, al tratar la forma de realización del reconocimiento judicial, se dictamina en su apartado primero que "el tribunal podrá acordar cualesquiera medidas que sean necesarias para lograr la efectividad del reconocimiento". Con esta afirmación se abre la posibilidad de usar cualquier técnica, tecnología o mecanismo para llevar a cabo el reconocimiento como medio de prueba, lo que a su vez se justifica a uno de los contenidos de nuestro derecho a la jurisdicción, al dar la posibilidad a todo ciudadano "a utilizar los medios de prueba pertinentes para su defensa", según el art. 24 de la Constitución Española.

El problema en cuestión viene justamente en el apartado segundo de este mismo artículo, al hacer referencia al coste personal que tiene la ejecución de la medida, pues para garantizar el principio de contradicción se exige que el resto de las partes tengan la posibilidad de estar presentes en el reconocimiento. Así se establece que "las partes, sus procuradores y abogados podrán concurrir al reconocimiento judicial y hacer al tribunal, de palabra, las observaciones que estimen oportunas". Pero ¿en qué punto geográfico deben estar presentes todas estas personas? La respuesta que debemos ofrecer debe ir en concordancia con la línea de argumentación apuntada a lo largo de este estudio. Con ello debemos partir de que la telepresencia judicial es admitida, por lo que el principio de inmediación se cumple, aunque el juez permanezca en el juzgado. Así, si admitimos que la persona principal que debe estar en contacto con el material probatorio logra ese acercamiento a la pieza de convicción a través de la cámara de visión del dron, el resto de los sujetos intervinientes a los que se refiere el art. 354.2 no deben ejercitar el principio de inmediación, sino únicamente el principio de contradicción en el que se incardina a su vez el principio de defensa y para ello

bastaría con estar en la misma sala que el juez y no presencialmente en el lugar donde esté sobrevolando el dron.

Aún así, al margen de que los jueces, los operadores jurídicos, las partes, los abogados y procuradores estuvieran en la sala, sería necesaria una inversión económica tanto en dispositivos como en personal del juzgado. Por un lado, sería necesario invertir en RPAS con una tecnología puntera, con matrícula e iluminación suficiente para poder sobrevolar de día y de noche, al tiempo que pudiera captar, grabar imágenes e incorporar tecnología ortofotográfica. Cuestión esta última que se enlaza con la nueva tecnología utilizada para drones denominada LIDAR (*Light Detection and Ranging* o *Laser Imaging Detection and Ranging),* consistente en establecer la distancia desde un dispositivo que emite un láser hasta un objeto o superficie concreta a través de un láser pulsado[83]. Igualmente, el coste personal también sería elevado puesto que al menos se necesitaría un piloto que controlara el avión, que estaría junto con el juez para controlar el vuelo y por otro lado una serie de observadores que controlaran como el dron sobrevuela desde su punto de salida hasta el lugar donde debe ejecutarse el reconocimiento. Eso querrá decir que, a más distancia, se necesitarán más observadores y por lo tanto un coste en personal cada vez más alto.

Sin duda, de los inconvenientes apuntados éste último es el que menos complejidad presenta pero puede ser el más difícil de alcanzar debido a la realidad política y económica de nuestro país, en el que no se cuentan con mayorías parlamentarias fuertes lo que hace que los trámites parlamentarios se demoren de manera excesiva o que no se consigan grandes pactos para solucionar problemas acuciantes como es la financiación constante que se debería realizar en modernización judicial y que prácticamente lleva en una inversión sostenida en los últimos cuatro años. Esta falta de financiación y de reciclaje de tecnologías y equipos no vislumbra un futuro ambicioso para la informatización o mecanización de algunas labores de los operadores jurídicos y con el que se lograría reducir aún más los tiempos de respuesta judicial. Por este motivo, pensamos que si superamos los obstáculos de naturaleza financiera puede que este tipo de tecnología se aplique en la realización de reconocimientos judiciales de objetos, cosas o infraestructuras en un futuro próximo. Igualmente sería bueno aprobar un plan de concienciación y formación para jueces sobre esta materia y comenzar a confeccionar protocolos para su implementación y uso como diligencia judicial.

83 Vid. REUTEBUCH, STEPHEN E.; ANDERSEN, HANS-ERIK; MCGAUGHEY, ROBERT J., "Light Detection and Ranging (LIDAR): An Emerging Tool for Multiple Resource Inventory", *Journal of Forestry*, Volumen103, numero 6, 2005, pags. 286-292.

BIBLIOGRAFÍA CONSULTADA

ARIZA COLMENAREJO, M.J, DEL, "La utilización de drones como herramienta en la investigación penal", *Fodertics 4.0*, Comares, S.L. Granada, 2015.

BUENO DE MATA, F., "Comentarios de legislación: Ley Orgánica 13/2015, de 5 de octubre, de modificació de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica [BOE n. º 239, 6-X-2015]", *Ars Iuris Salmanticensis*, Vol. 4, Nº. 1, 2016.

CUERNO REJADO, C. (et al.), "Evolución histórica de los vehículos aéreos no tripulados hasta la actualidad", *Dyna,* Vol. 91, Nº 3, 2016.

ESCLAPÉS MEMBRIVES, S., "Los drones y su uso generalizado: un nuevo reto para el derecho", *Fodertics 5.0*, Comares, Granada, 2016.

GÓMEZ-JUÁREZ SIDERA, I., "Drones y privacidad: desafíos de la protección de datos en la utilización civil de aeronaves pilotadas por control remoto", *Fodertics 4.0*, Comares, Granada, 2015.

MUERZA ESPARZA, J. DEL, "Aspectos básicos de las nuevas reformas de la Ley de Enjuiciamiento Criminal", *Dossier reforma de la Ley de Enjuiciamiento Criminal,* 2015.

SEMPERE SAMANIEGO, J. DEL, "Usos y régimen jurídico aplicable a los drones", *Diario La Ley*, La Ley, Nº 8343, Sección Tribuna, 2014.

SERRANO FERRER, M.A, DEL, "Los avances en la tecnología e importancia procesal", *El reflejo de las nuevas tecnologías en el derecho penal y otros destellos*, Aranzadi, 2016.

INTELIGENCIA ARTIFICIAL, E LEGAL TECHS

PYME O STARTUP: ¿LA FORMA ES FONDO?

BASES LEGALES EN SU ORGANIZACIÓN ACTUAL

Eje Temático: Legaltechs, Fintechs, Starups

Autor:
José Heriberto García Peña[84*]
Doctor en Derecho por la UNAM de México
Profesor Investigador del Tecnológico de Monterrey

"Allí donde hay una empresa de éxito,
alguien tomó alguna vez una decisión valiente…"
Peter Drucker[85]

RESUMEN
Una de las cuestiones más delicadas que se pueden presentar en la toma de decisiones de carácter empresarial es la concepción de cómo será un futuro negocio. Del correcto enfoque de esta cuestión, que afecta a la organización entendida en el sentido más amplio, depende en gran medida el futuro éxito o fracaso de la empresa que se está gestando. La apuesta hoy sería tratar de crear las condiciones para desarrollar Empresas Pequeñas y Medianas (se identifican con las siglas PYME) más modernas, con uso intensivo de tecnología, elevado nivel de productividad y alta capacidad de innovación y aprendizaje. Las mismas tienen que adecuarse a una nueva forma de organización, redefinir sus procesos productivos, y asumir una nueva visión de los trabajadores, de los clientes y del medio ambiente como una nueva manera de entender la economía emergente y cómo cambiar y mejorar a corto plazo con las nuevas tecnologías para su beneficio (se reconocen entonces como STARTUP). Pero, para poder realizarlo, se requiere de un marco legal y políticas públicas eficientes que permitan su inclusión equitativa en la competencia del mercado y el desarrollo nacional. Se trata, en lo particular, de brindar las nociones esenciales y valorar la actual incidencia que tienen hoy este modelo empresarial en el contexto legal mexicano y latinoamericano, de tal suerte que el emprendedor/empresario puedan contar con elementos adicionales para una mejor y más amplia comprensión desde una perspectiva jurídica; y, al mismo tiempo, plasmar una discusión crítica en cuanto a los pros y contras de esta nueva realidad de la conocida como *"empresa virtual"* que plantea un amplio conjunto de ideas complejas que se

84 * El autor es miembro permanente y participante asiduo como ponente en los eventos de la Federación Iberoamericana de Asociaciones de Derecho e Informática (FIADI). En México es miembro de la AMDETIC y de la ISOC Capítulo México. Miembro del Sistema Nacional de Investigadores de México, actualmente posee el nivel II. Su E-mail: jhgarcia@tec.mx

85 Fue consultor y profesor de negocios, tratadista austriaco y abogado de carrera, considerado el mayor filósofo de la administración (también conocida como *management*) del siglo XX. Hoy es considerado el padre del *management* como disciplina y sigue siendo objeto de estudio en las más prestigiosas escuelas de negocios a nivel mundial.

entrelazan desde diferentes perspectivas, pero que tienen un impacto real al sustentarse sobre nuevas bases legales. **Palabras claves:** Pyme, Startup, Nuevas Tecnologías, Economía emergente, Empresas virtuales, Bases Legales.

I. A MANERA DE INTRODUCCIÓN

En México las Micro, Pequeñas y Medianas empresas (MIPyMEs) generan importantes contribuciones al desarrollo económico y el desarrollo social. Alrededor del mundo las MIPyMEs suelen ser las responsables de la mayor creación de puestos de trabajo; además, constituyen una fuente primordial de innovación, crecimiento y oferta fl xible para las grandes empresas[86]. La información para una Encuesta en México se levantó durante los meses de junio y julio de 2015 en **26,997** unidades económicas a nivel nacional, conformadas por Micro, Pequeñas y Medianas empresas (MIPyMEs)**…**ver algunos datos que ilustran[87]

Las nuevas tecnologías se integran cada vez más a la empresa en la actual economía global. Hemos ido avanzando de la ERA DE LA PRODUCCIÓN EN MASA **(**costo, disponibilidad y economías de escala), pasando por la ERA DE LA CALIDAD (conformidad, confiabilidad, durabilidad y servicios de garantía) para llegar a la ERA DEL CLIENTE VIRTUAL (Globalización, Productos diferenciados vs Rotación y entrega, Productos personalizados vs Reales precios de mercado; hay mayor Participación del cliente: *"Los clientes deciden: qué, cómo, cuándo y dónde comprarán productos y servicios",* aumenta la Responsabilidad social corporativa y se crean Pymes a gran escala.

Los negocios… su presente y futuro… ¿en lo virtual?

La sociedad en general y en concreto el mundo empresarial están evolucionando con gran rapidez, planteando nuevos retos de futuro a distintos niveles. El mundo de la empresa y el emprendimiento han visto imprescindible la utilización de la innovación tecnológica en sus procesos empresariales y una necesaria adaptación de sus estructuras a la nueva realidad: la relación de la tecnología con el fomento del emprendimiento empresarial. *La tecnología ha tenido un papel disruptivo y ha marcado el*

86 SISTEMA PARA APERTURA RAPIDA DE EMPRESAS EN MÉXICO (2012). LATIN--REG es la red Latinoamericana de Mejora Regulatoria y Competitividad. Esta publicación esta disponible en https://www.gob.mx/conamer [Fecha de consulta: 19 de octubre de 2018]

87 Instituto Nacional de Estadística y Geografía (INEGI), el Instituto Nacional del Emprendedor (INADEM) y el Banco Nacional de Comercio Exterior (BANCOMEXT), presentan la Encuesta Nacional sobre Productividad y Competitividad de las Micro, Pequeñas y Medianas Empresas (ENAPROCE) 2015. - Se difunden estadísticas detalladas sobre las micro, pequeñas y medianas empresas del país (BOLETÍN DE PRENSA NÚM. 285/16) www3.inegi.org.mx/rnm/index.php/catalog/330/download/9792 [Fecha de publicación: 13 de julio de 2016]

inicio de una nueva revolución industrial, la revolución digital (Pardo, 2017)[88]. Es aquí dónde nace un "dilema" hoy llamado STARTUP.

El origen del movimiento STARTUP (o *STARUPs*) tuvo lugar en Silicon Valley (California) en los años 50 y a día de hoy sigue dominando el panorama mundial. Actualmente, además de Silicon Valley, se agregan ciudades como New York y Boston; y a nivel mundial otras ciudades como Londres y Beijing se encuentra entre los cinco (5) mejores ecosistemas para emprender según el informe *Global Startup Ecosystem Ranking* (Startupxplore, 2019)[89].

De acuerdo con la Revista Fortune –Si bien California sigue siendo la cuna de las Starups disruptivas a nivel mundial (nueve de las 20 Starups con mayor valoración de mercado se encuentran en California, entre ellas UBER, AIRBNB Y PINTEREST– (2016)[90] ; Hoy numerosos países cuentan con una cultura emprendedora en expansión. Y América Latina no se está quedando atrás. Los gobiernos, el sector privado y las universidades se activan para apoyar la creación de Starups y confían cada vez más en su potencial transformador para las economías de la región. A continuación…. algunos datos que ilustran[91] con algunas Citas Textuales:

"Pese a los escasos avances en materia de dinamismo de los sistemas de innovación, el mundo de las Starups nos muestra una cara más dinámica de América Latina. Los países de la región siguen invirtiendo poco en ciencia, tecnología e innovación… América Latina ha avanzado en la adopción de tecnologías de la información y la comunicación (TIC) en la última década, pero una brecha importante con los países de la OCDE perdura (CEPAL, 2013). Cuando se llevó a cabo el primer estudio de la experiencia de América Latina en fomento a las Starups, la creación y el desarrollo de…estas… aparecía como un tema "ajeno" a la cultura de los países de la región (OCDE, 2013). Hoy en día la percepción es diferente y hay Starups creándose y creciendo en América Latina. La industria de capital de riesgo en América Latina se encuentra en expansión y ha doblado su tamaño en términos de inversiones entre 2011 y 2015 (LAVCA, 2016). Sin embargo… Todavía falta una medición exhaustiva y comparable de la dinámica y el impacto del fenómeno de las Starups en América Latina. No hay bancos de datos oficiales sobre Starups, y la multiplicidad de las definiciones usadas para definir las Starups no ayuda a avanzar en la medición".

Lo cierto es que la implementación de los programas de fomento a Starups está generando cada vez más una nueva información sobre este fenómeno. Según AngelList

88 PARDO, D. (2016). El sector tecnológico en España reclama 100.000 profesionales especializados. El Economista (blog). Entrada del día: 26 de octubre de 2017. Disponible en: http://infoautonomos.eleconomista.es/blog/profesionales-sector-tecnologico/[consulta: 19 de mayo de 2018]

89 Sitito Web: https://startupgenome.com/reports/global-startup-ecosystem-report-2019 [consulta 3 julio 2019].

90 Fortune (2016), The Unicorn List, [en línea], disponible en: http://fortune.com/unicorns/ [consulta julio 2018].

91 STARTUP AMÉRICA LATINA 2015-2016: CONSTRUYENDO UN FUTURO INNOVADOR © OCDE (https://www.oecd.org/dev/americas/Startups2016_Si-ntesis-y-recomendaciones.pdf) [consulta: 19 octubre 2018]

(2016)[92], que es una base de datos utilizada por inversores que buscan información sobre Starups para sus decisiones de inversión: Brasil es el país con el mayor número de Starups en América Latina, seguido por México. México es el país donde los ecosistemas de Starups están más distribuidos en el territorio con 32% de las Starups en México DF[93], 10% en Guadalajara y 8% en Monterrey. Chile es el país con la mayor concentración territorial de Starups, con el 80% de las mismas registradas en Santiago de Chile. Pero lo cierto es que en los cuatro países hay nuevos esquemas de fomento a las Starups, más modernos e integrados, que responden mejor a las demandas de los *Startuppers (Iniciantes)*. Por ejemplo, se introducen los espacios de trabajo colaborativo y se reforman instrumentos para agilizar las nuevas formas de financiamiento como el fondeo colectivo. El abanico de instrumentos de política tiende a ofrecer servicios integrados, combinando acceso a infraestructura, financiamiento y servicios, así como acceso a redes de contacto. Además, se opera en alianza con el sector privado, las empresas y los institutos de investigación y tecnológicos, mejorando así la efectividad de las políticas y satisfaciendo las necesidades de las propias Starups. Asimismo, se nota un avance en simplificar trámites y en reformar el marco legal hacia uno más amigable para la creación y expansión de las empresas. Destaca la adopción en Chile y México de la Ley de Empresas en un Día, aunque permanecen debilidades en los cuatro países, a nivel de complejidad de trámites e incentivos fiscales para empresas de reciente creación y altamente innovadoras.

II. PYME O STARTUP: ¿LA FORMA ES FONDO?

La revolución digital global está modificando la estructura tradicional de sociedades y economías. Las Startups buscan la creación de valor diferencial con modelos de negocio disruptivos normalmente en sectores con predominio de elementos tecnológicos aunque no exclusivamente con un beneficio directo para consumidores y usuarios. Estas empresas emergentes basadas en la innovación tecnológica constituyen una importante atracción de capital y creación de trabajo de calidad siendo una alternativa más allá de las salidas profesionales tradicionales.

La complejidad del marco regulatorio que se les aplica, en conjunto con sus respectivos costos, inhiben de manera desproporcionada la creación y expansión de estas nuevas empresas. Así, hoy las acciones de los gobiernos deben estar encaminadas a construir y facilitar la cultura empresarial a través de una regulación adecuada.

92 Sitio Web: https://angel.co/companies [Fecha de consulta: 19 de octubre de 2018]

93 El Expresidente de México, Enrique Peña Nieto, promulgó el **29 de enero de 2016** la reforma a la Constitución que establece que el Distrito Federal ya no existe más, porque pasó a llamarse Ciudad de México. La **Ciudad de México** se convirtió así en el estado número 32 del país, merced a una **reforma de la Constitución**, con lo que obtiene autonomía para configurarse política y administrativamente. Entro en vigor el **17 de septiembre de 2018.**

Efectivamente, hoy la mayoría de las Starups pueden considerarse Pymes, pero son Pymes muy distintas a las que comúnmente existen en nuestro país. Las plataformas y operaciones en línea también están generando información sobre las Starups de la región. Las Diferencias están en los diversos factores: *Condición de escalabilidad, Grado de innovación, Una operación basada en tecnología, pero sobre todo el Potencial para afectar a un sector, un producto, un servicio o un sistema.*

Veamos dos ejemplos:

Imaginemos un par de Pymes que nos ayuden a obviar estas diferencias:

1. Una tienda de computadoras**:** En principio, podría pensarse que ser distribuidor de computadoras en pleno centro de la ciudad de México es una Startup, ya que basa su negocio en tecnología y, sin embargo,… dista mucho de serlo…

2. Por el lado contrario, algo que en primera instancia no parecería una Startup, ¿qué tal una Florería? Y, sin embargo, SI puede serlo…

La cuestión fundamental es que la diferencia radica no en el producto o servicio como tal, sino —como lo mencionaba anteriormente— en la escalabilidad, el grado de innovación e impacto… En el PRIMER CASO, la Tienda se trata de una Pyme tradicional: Si bien distribuye computadoras, al final, cuenta con un local, un equipo de vendedores y su escalabilidad es aritmética; pues para duplicar las ventas, tendría que abrir una nueva sucursal, contratar un nuevo equipo de ventas y duplicar los costos, ETC… El SEGUNDO CASO de la Florería se trata de una Startup: Si bien realiza una actividad bastante tradicional como es vender flores, lo hace a través de Internet, apoyándose en medios de pago en línea, con redes de distribución locales coordinadas y a través plataformas online. Esta Startup tiene un impacto importante en el sector, cambiando la forma en que las personas compran, surten y envían flores

¿Cómo se define a una PYME?

La percepción de la micro, pequeña y mediana empresa *(también conocida por las siglas MyPYMEs)* ha cambiado en los últimos años por el impacto económico y social que tienen a nivel mundial. De ser consideradas un problema por erradicar debido a su informalidad, ahora se observan como una oportunidad a partir de los empleos generados y su aportación al desarrollo económico donde se encuentren ubicadas. Su definición varía dependiendo del país en el que nos ubiquemos, no existiendo un concepto universal aplicable a todas las regiones.

"Las Pymes en México se caracterizan por ser de tipo familiar, ya que el dueño es el que aporta el capital necesario para las operaciones normales de la empresa y mayoría tienden a no cambiar su lugar de operaciones, es decir, se mantienen en el mismo donde se iniciaron. Ellas crecen principalmente a través de la reinversión de utilidades, ya que no cuentan con apoyo técnico–

financiero significativo de instituciones privadas ni del gobierno. En México existen dos tipos de incorporación fiscal de acuerdo con el monto de ingresos que registren

en sus estados financieros: el primero, régimen fiscal, que es para aquellas personas físicas o morales con un ingreso de hasta 2 millones de pesos anuales y que se define que es un conjunto de derechos y obligaciones a los que se hace acreedor un ciudadano a partir de desempeñar una actividad específica, según la actividad que desarrolle y sus características propias se organizan en diferentes grupos. Y el segundo que es el régimen general, para personas morales con ingresos superiores a los 2 millones de pesos anuales y que es aquel que se aplica a las sociedades que realicen actividades lucrativas, como son las sociedades mercantiles (por ejemplo: sociedad anónima, sociedad de responsabilidad limitada, etc.), sociedades civiles, Instituciones de crédito (por ejemplo: casas de bolsa y bancos) y organismos descentralizados que comercialicen bienes o servicios (Paredes-Barceló *et al,* 2016, p. 198-199)[94]

Una de las cuestiones más delicadas que se pueden presentar en la toma de decisiones de carácter empresarial es la concepción de cómo será un futuro negocio. Del correcto enfoque de esta cuestión, que afecta a la organización entendida en el sentido más amplio, depende en gran medida el futuro éxito o fracaso de la empresa que se está gestando.

En este contexto, deben distinguirse varios factores:

1) Nacimiento de la empresa: Toda empresa nace de la conjunción entre una o varias personas emprendedoras, una idea que ponen en práctica y un capital. La idea puede ser, por ejemplo, una empresa de transportes, un comercio, etc.

2) Ubicación: Otro de los grandes problemas que ha de resolverse es el relativo al lugar donde se instalará el negocio, ya que ninguna empresa se puede aislar de su contexto geográfico, social y económico.

3) Forma Jurídica: Desde el enfoque jurídico, la persona se define como aquel que tiene representación propia en el Derecho, ya sea como ente físico, como persona individual o moral o jurídica como conjunto de personas. Es quizás la decisión que "*a priori*" parece más importante. Ésta ha de estar en consonancia con las características de sus promotores, sus objetivos y el volumen estimado de operaciones. En principio, probablemente habrá que elegir entre la Empresa individual y la Sociedad mercantil. Más adelante, a lo largo de la vida del negocio, y dependiendo de su crecimiento, su situación financiera y fiscal, etc., se puede aconsejar que admita nuevos socios que puedan aportar capital y, por tanto, entren a formar parte de la organización. "*Toda persona moral o sociedad mercantil tiene una personalidad jurídica, la cual es definida como una investidura o la posición*

94 Paredes-Barceló, Raúl G. · Peña-Ahumada, Nuria B. Vacio-Hernández, Iván A. Tópicos Selectos de Micro y Pequeñas Empresas: *La Micro y Pequeña Empresa: Un análisis desde la perspectiva económico-administrativa T-I,* ECORFAN Editores, Universidad Tecnológica de San Juan del Río, México, noviembre, 2016. Sitio Web: https://www.ecorfan.org/actas/A_1/EXTENSO/A1.pdf [Fecha de consulta: 19 de octubre de 2018].

legal que tiene, que se le atribuye a cualquier corporación o colectividad, jurídicamente organizada, como empresa, asociación, organización, institución o conjunto de personas con la capacidad de contraer derechos y obligaciones y que generan responsabilidades para el mismo o terceros, que se validan y se legitiman, dando el derecho de adquirir y poseer bienes y ejercitar acciones judiciales. La personalidad jurídica está inmersa en un marco legal,…,enfoque definido como un instrumento regulador de la creación,…del ente activo: la empresa.". (Nuño de León, 2012, p. 17)[95] En cualquier caso, la forma jurídica que se decida adoptar deberá estar en función, tanto de las preferencias de sus fundadores como de la legislación vigente. Es importante señalar que no todo tipo de organización o combinaciones de formas son adecuadas para cualquier negocio. Al escoger una forma de negocio, se debe considerar los miembros involucrados, sus gustos, sus disgustos y disposiciones, sus necesidades inmediatas y a largo plazo, así como sus situaciones fiscales. Se deberá pensar detenidamente respecto al tipo de negocio en que opera, exactamente qué es lo que hace y qué no hace, y qué tipo de organización será mejor para sus planes. Rara vez, un solo factor determinará completamente la forma de organización de un negocio. Actualmente para alcanzar los fines para los cuales fue creada una empresa, debe existir un ordenamiento de las partes que la componen. En esto consiste la organización, es decir, es la estructura de una empresa y el ordenamiento lógico de sus partes componentes, de tal manera que cumpla los fines para los cuales fue creada.

¿Qué medidas es necesario adoptar en las PYMEs para adecuar su marco legal?

La apuesta hoy sería tratar de crear las condiciones para desarrollar Empresas PYMEs más modernas, con uso intensivo de tecnología, elevado nivel de productividad y alta capacidad de innovación y aprendizaje, utilizando mano de obra calificada y especializada e incorporadas al progreso técnico. Las mismas tienen que adecuarse a una nueva forma de organización, redefinir sus procesos productivos, y asumir una nueva visión de los trabajadores, de los clientes y del medio ambiente con una nueva manera de entender cómo cambian y se mejoran las tecnologías a corto plazo para su beneficio. Pero para poder realizarlo, se requiere de un marco legal y políticas públicas eficientes que permitan su inclusión equitativa en la competencia del mercado y el desarrollo nacional. Se trata en particular de valorar la actual incidencia que tienen hoy el contexto legal de tal suerte que tanto el emprendedor/empresario puedan contar

95 Nuño de León, Pierina del R., *Administración de pequeñas empresas*, Primera edición, RED TERCER MILENIO S.C., México 2012 (Sitio Web en otra pagina) http://aliat.org.mx/BibliotecasDigitales/economico_administrativo/Administracion_de_pequenas_empresas.pdf`_uG [Fecha de consulta: 19 de octubre de 2018].

con elementos adicionales para una mejor y más amplia comprensión del fenómeno desde una perspectiva jurídica moderna. Como resultado de una revisión comparativa en algunos países latinoamericanos importantes (García Peña, 2011, p. 105)[96] se comprobó que: *"se deberá elegir el tipo jurídico apropiado para cada empresa. Una forma puede ser la más adecuada para cierto tipo de empresas, pero podrá presentar grandes desventajas para otras con objetivos diferentes.*

Para la elección del tipo jurídico se debe considerar: 1. Simplicidad o complejidad de la empresa: las formas jurídicas más simples son las apropiadas para las empresas pequeñas.

2. Recursos financieros de que se pueda disponer: el monto de los capitales con que cuenta la empresa al iniciarse influye en la forma jurídica que se adopte. No todas las formas jurídicas ofrecen las mismas ventajas para recurrir posteriormente a la adquisición de mayores recursos financieros; las formas más simples y sencillas no ofrecen grandes posibilidades para la adquisición de nuevos y mayores recursos.

3. Responsabilidad de los socios: depende de la responsabilidad que quieran adquirir los socios. Si los propietarios están dispuestos a tomar un riesgo, hasta por sus bienes personales, la forma que se elegirá será una "sociedad en nombre colectivo" en donde los socios tienen una responsabilidad ilimitada y buscarán el control absoluto de las operaciones. Respecto a los socios que sólo quieren arriesgar su parte invertida, su responsabilidad es limitada, y la administración podrá ser más elástica, más evolucionada, como las sociedades comanditas y las anónimas.

4. Estabilidad: la forma jurídica seleccionada deberá dar a la empresa la estabilidad que ésta requiera. Si la duración que tendrá la empresa sobrepasara la vida de sus fundadores, deberá elegirse preferentemente una forma cuya duración pueda ser indefinida, por ejemplo: la Sociedad Anónima.

5. Intervención del gobierno: puede darse de manera más o menos directa como es el caso de las instituciones bancarias, hipotecarias, fiduciarias, de seguros, de fianzas y en general empresas de crédito, a las cuales el gobierno les otorga un control determinado en beneficio y en garantía de los intereses públicos que le están confiados. También se da a través de las obligaciones fiscales. La selección de tal o cual tipo jurídico puede traer consigo más o menos obligaciones de carácter fiscal".

Los tipos básicos de organizaciones legales de negocios existentes a nivel de Latinoamérica para el hombre de negocios pequeño y mediano, son variados. A continuación se analizan los rasgos esenciales de algunos de las tipologías básicas de organización legal enunciados por las leyes de diversos países:

1. El propietario individual Constituye la organización de empresa más sencilla y por ende la más económica, donde el propietario es el único dueño, quien normalmente lo administra con fines de obtención de utilidades y responde por los contratos, así como por los actos de negligencia y otros errores cometidos por él y por sus empleados en lo que concierne a su negocio.

96 García Peña, José H., *Derecho Empresarial. Tópicos y Categorías: Una revisión comparada en el Sector Pyme Latinoamericano,* Porrúa, México, 2011

2. La Sociedad Personalista (también se le llama sociedad en nombre colectivo) Se define como una asociación de dos o más personas para conducir un negocio con fines lucrativos y su creación involucra la contribución del capital o la fundación del negocio en propiedades, dinero, habilidad, trabajo, etc., por los socios.

3. Asociación estatutaria Difiere de la sociedad en comandita en que todos los miembros tienen una responsabilidad limitada y los intereses de las empresas son transferibles. Este tipo de organización frecuentemente se le llama "Sociedad de Responsabilidad Limitada", y adquiere el título de "S. de R.L."

4. Asociación no incorporada La asociación no incorporada se conoce también como "Asociación en participación o de acciones conjuntas", y combina algunas de las características de la sociedad personalista y algunas de la sociedad anónima. Las normas constitutivas de este tipo de compañías, así como las de una sociedad, constan en un contrato privado.

5. El trust Comercial (también conocido como Fideicomiso) El fideicomis (trust) comercial es una organización creada por un testamento o declaración de fideicomiso en la cual los activos pertenecientes a una empresa son transferidos a una fiduc aria para que sean administrados en beneficio o provecho de las personas que sean titulares de los certificados.

6. Sociedad de Capital (SA) Una sociedad anónima (siglas S.A.) es una agrupación de personas que tiene una personalidad jurídica distinta de los miembros que la integran (accionistas). Los derechos, las obligaciones y demás relaciones legales que surgen de una empresa se consideran como si fuera una entidad separada. Los accionistas tienen, en teoría, tan solo un interés indirecto en los activos de la sociedad que está representada por su derecho a participar en los dividendos y en la distribución de los activos de la sociedad al liquidarse. Posee propiedades, celebra contratos, transfiere propiedades y conduce asuntos legales con capacidad distinta a la de los accionistas. Esta separación de la sociedad con sus socios es también reconocida para fine fiscales, reconociéndose a la sociedad como un "ente sujeto a impuestos". Esto significa que la sociedad tan sólo podrá constituirse, si se da cumplimiento a la legislación establecida por el Estado en donde se vaya a organizar. Resulta importante que la estructura financiera de la sociedad y su administración estén en conformidad, hasta cierto grado, con sus estatutos. En algunos países puede darse también la posibilidad de constituir una llamada Sociedad Anónima familiar. Adopta la forma de una sociedad "cerrada" que posee uno o unos cuantos accionistas y la cantidad o

monto de capital que se obtiene está limitada. Este tipo de sociedad "cerrada" es particularmente propia para los negocios pequeños porque provee estatutos y cláusulas especiales incluidas en el acta constitutiva. Permite ciertos convenios entre los accionistas. Sin embargo, tiene restricciones para la transferencia de las acciones. Y en ella existe el derecho de veto por parte de los accionistas preferentes.

Es importante analizar también, algunos de los factores que deben considerarse al seleccionar el tipo de organización de un negocio, siendo los más importantes: *la limitación de responsabilidad; el asegurar la continuidad del negocio y la aplicación de la concesión como método de operación de un negocio*.

Sin embargo, incluir a las PYME en el nivel de competitividad que condiciona el mercado actual, implica un arduo trabajo; se requiere dotarlas de tecnología para elevar su nivel de productividad, utilizar mano de obra especializada y un marco legal propicio para tener acceso a todo ello y competir de manera equitativa con el resto de las empresas.

¿Qué es una STARTUP?

Una startup podría definirse como una empresa de nueva creación que presenta unas grandes posibilidades de *crecimiento y, en ocasiones, un modelo de negocio escalable*.

Aunque el término Startup (en plural se le denomina *Starups*) puede referirse a compañías de cualquier ámbito, normalmente suele utilizarse para aquellas que tienen un fuerte componente tecnológico y que están relacionadas con el mundo de Internet y las TICs. Debido a estas características las Startups tecnológicas suelen diferenciarse de otras empresas jóvenes en sus posibilidades de crecimiento y necesidades de capital. Las empresas tecnológicas y de Internet tienen asociados unos *costos de desarrollo menores* que empresas de otros ámbitos. Esto hace que las necesidades de financiación para su puesta en marcha sean sensiblemente inferiores, lo que facilita otro aspecto clave mencionado anteriormente: su mayor crecimiento en el medio y largo plazo.

La tipología de inversores en el mundo del emprendimiento es muy amplia y va desde los *FFF* (*friends, family y fools*), que suelen ser claves en los primeros años de vida, hasta el *Venture Capital o Private Equity* que aportan fondos en etapas más avanzadas. Ejemplos de Starups existen muchos, tanto a nivel internacional como a nivel local. Google, Twitter, Facebook, Tuenti o Privalia comenzaron siendo Starups y con el paso de los años se han convertido en gigantes empresariales con cientos de empleados y un número importante de ingresos y beneficio . Un debate que suele asociarse con este concepto es el momento en el que una Startup deja de serlo y pasa a convertirse en una empresa *al uso*. Sobre esta cuestión no existe ninguna conclusión definitiva. En

ocasiones suele afirmarse que en etapas avanzadas el concepto de Startup pasa a estar ligado a la estructura corporativa, forma de trabajar y ambiente de una empresa, en vez de las características mencionadas anteriormente.

Startups con modelo de negocio formal ¿o no?

En la apertura de este punto, comentábamos que, *en ocasiones*, las Starups presentan un modelo de negocio escalable. Dicha apreciación es importante porque *existen muchos ejemplos de Starups que nacen sin un modelo de negocio y que incluso son vendidas antes de encontrar uno*[97].

Pero, ¿a qué nos estamos refiriendo cuando hablamos de una "Startup"? Si nos atenemos a su traducción literal, este término acuñado en Estados Unidos expresa conceptos tales como *"comienzo hacia arriba", "puesta en marcha", "encendido", "activación" o "arranque"*, pero estas acepciones no son las que más nos interesan para comprender que es una empresa denominada Startup. No existe una definición universal, pero diferentes autores han dado su explicación particular y todas ellas comparten varios elementos comunes.

Me gustaría tomar la de Startupxplore – *la comunidad de inversión en Startups que conecta a todos los actores del ecosistema*–(2019) la cual recoge en su blog una definición del término: *"una **Startup** es una empresa de reciente creación con ciertas posibilidades de generar un gran crecimiento y volumen de negocio en un espacio de tiempo reducido. El término se suele aplicar sobre todo en los ámbitos tecnológicos, cuyas compañías, debido a la reducción de costes que entraña ser digital, suelen tener más posibilidades de crecer rápidamente, de forma escalable, aunque no es exclusivo"*.

En los últimos años y a raíz del "boom emprendedor" ha tenido lugar una proliferación de actores que intervienen en el ecosistema Starups y las relaciones que entre ellos se generan. Se entiende por ecosistema a una comunidad de compañías y actores cuyos procesos empresariales se relacionan entre sí y se desarrollan en función de los factores y circunstancias de un mismo ambiente económico. Las Starups es el elemento en torno al cual gira todo el ecosistema *Empresa emergente*: *desde proveedores de servicios, inversores, incubadoras, aceleradoras, etc.*

Con respecto al modelo de negocio de las Startup es importante apuntar que un buen número terminan siendo vendidas a otras empresas más grandes. A pesar de que todo parezca de color de rosa, lo cierto es que la gran mayoría de Starups mueren

97 El caso más conocido por todos es el de Instagram, que fue comprada por Facebook hace un año aproximadamente por más de 700 millones de dólares. Instagram "no tenía (ni tiene) un modelo de negocio" http://www.elblogsalmon.com/empresas/instagram-el-caso-de-la-empresa-sin--apenas-ingresos-que-vale-1000-millones-de-euros y sin embargo Mark Zuckerberg decidió desprenderse de unos cuantos millones para hacerse con ella. ¿Por qué? Por las posibilidades de crecimiento que la empresa de Kevin Systrom presentaba en esos momentos.

a los pocos meses o años de vida. Un estudio publicado en septiembre de 2012 por Shikhar Ghosh y recogido en el "Wall Street Journal"[98] se afirma que *tres de cada cuatro startups financiadas por Venture Capital no consiguen devolver el dinero prestado*. Cifras que en cualquier otro contexto empresarial podrían asustar pero que, dados los bajos costos que en la mayoría de ocasiones supone poner en marcha una startup, no resultan tan impactantes.

¿Por qué son importantes las Startup?

La OCDE en su estudio las identifica como las nuevas empresas intensivas en innovación o de alto impacto, para las cuales se están diseñando mecanismos de apoyo en los países de América Latina. Cada Startup está respaldada por una idea que busca simplificar procesos y trabajos complicados, con el objetivo de que el mercado tenga una experiencia de uso simplificada y fácil. Generalmente son negocios que quieren innovar, desarrollar tecnologías y diseñar procesos web. Principalmente, son empresas de capital-riesgo. No todo el mundo debe o tiene la oportunidad de trabajar en grandes empresas, y ese es el grado de importancia que tiene una Startup.

Sus Características esenciales son: Se relaciona con empresas emergentes; Tienen una fuerte relación laboral con la tecnología; Se trata de negocios con ideas innovadoras, que sobresalgan en el mercado siempre apoyadas por las nuevas tecnologías.

Veamos ahora como operan legalmente.

III. PRINCIPALES BASES LEGALES A TENER EN CUENTA PARA FUNDAR TU STARTUP

La prosperidad económica depende de la existencia de un ambiente propicio para los negocios. Hacerles la vida más sencilla a las empresas y facilitar la entrada al mercado de nuevas organizaciones fomenta la competitividad y el crecimiento. Si bien es necesaria la regulación para abrir nuevas empresas, en ocasiones su implementación puede volverse un proceso difícil y costoso, lo cual desalienta la actividad empresarial. Uno de los problemas que plantea el desarrollo de la tecnología es que las empresas y los modelos de negocio avancen mucho más rápido de lo que evoluciona la legislación.

98 Sitio Web: http://online.wsj.com/article/SB10000872396390443720204578004980476429190.html [Fecha de consulta: 19 de octubre de 2018].

Por esta razón, nuestro ordenamiento carece de una normativa específica para la regulación de las Starups y a las pequeñas nuevas empresas de base tecnológica.

Pese a la ausencia de una normativa *ad hoc*, existe una serie de aspectos jurídicos y cuestiones legales que deben ser considerados en la constitución de una Startup y que vamos a desarrollar a continuación.

¿Cuestiones legales a tener en cuenta al aperturar una Startup?

El nacimiento de estas pequeñas empresas no suele estar reglado, dando lugar a una infinidad de variables. Es por ello por lo que resulta preciso abordar la protección jurídica desde su inicio y tener muy presente que, en ocasiones, el descuido de esta faceta puede afectar al proyecto a medio o largo plazo.

Si bien, los aspectos legales siempre deben formar parte del plan de negocio, se necesita una estrategia adecuada que permita establecer la estructura legal más conveniente para la empresa. Entre dichos aspectos legales se encuentra: *la relación con los socios e inversores, la relación con los clientes, el ámbito fiscal, aquellos relativos a la privacidad o comercio electrónico, los potenciales riesgos a los que se enfrenta la empresa legalmente o la estrategia de protección que se debe seguir*. Cuestiones como: la Propiedad Intelectual: ¿Hasta dónde puedo y no puedo proteger mi Startup?; la Propiedad industrial: ¿Es necesario registrar la marca?; Startup en la Red: Registrar el DNS; Contener un Aviso Legal; Política de cookies; Especial consideración con los datos de carácter personal a los que se va a acceder; Proteger la información; Acuerdos de confidencialidad; Cuestiones transfronterizas; Aspectos de derecho internacional: (protección al consumidor y contratación); son entre otros muchos elementos claves a considerar. Lo cierto es que a la hora de crear una estructura legal del negocio hay que diferenciar entre aspectos internos y aspectos externos. Los aspectos internos son aquellos que se refieren a la organización propia de la actividad (forma jurídica, socios, trabajadores, instalaciones y recursos, etc.). Los aspectos externos son aquellos que se refieren a todas las relaciones que mantendrá la empresa con el exterior (clientes, proveedores, autoridades, competidores, etc.).

En cuanto a las formas jurídicas más habituales para constituir una Startup aparecen las siguientes:

- Empresario individual, es decir, persona física con actividad empresarial;
- Sociedad civil;
- Sociedad cooperativa;
- Sociedad limitada (o más bien Sociedad de responsabilidad limitada);
- Sociedad Anónima (con sus diversas variantes).

Tal vez la más conveniente en estos casos, son la de Responsabilidad limitada y la Anónima, pues en el caso de que existan deudas o se llegue a la quiebra, el dueño o dueños del negocio harán frente a ellas únicamente con los activos del negocio y no con todo su patrimonio como si ocurre cuando la responsabilidad es ilimitada.

Para que una Startup sea legal es indispensable que su modelo de negocio también lo sea. Ante las nuevas posibilidades técnicas y los nuevos modelos de negocio, en muchos casos no contemplados específicamente en el ordenamiento jurídico de cada país, se hace fundamental fijar dichas cuestiones a fin de no condicionar su crecimiento futuro.

Lo cierto es que si bien una Startup no tiene por qué ser ilegal en la definición de su modelo de negocio, *en muchos casos se convierte en un modelo de negocio no legal por incumplir la normativa del sector u omitir determinados requisitos legales, acabando con la viabilidad del proyecto antes de comenzar la actividad* (Vázquez, 2015)[99].

Otros aspectos de especial atención son: el tipo de modelo de negocio, se deben tener en cuenta una serie de consideraciones según el tipo de mercado al cual se dirija la Startup (no es lo mismo si se trata de consumo colaborativo, de hardware, de software o de plataformas de comercio electrónico); además los destinatarios del producto o servicio ofrecido, ante posibles casos de confli to según la tipología de los clientes (consumidores u otras empresas) tendrán unas responsabilidades y obligaciones a cumplimentar, o la posibilidad de acudir a unos tribunales u otros; y por último el origen, trascendencia y tratamiento de los datos personales.

El Pacto de Socios es una de las cuestiones más complejas. Se trata de determinar las reglas internas de la sociedad y la relación entre los socios que deberá prevalecer. Si bien se define primero el Estatuto Social que es la norma que marca el régimen interno de la empresa a nivel legal como documento que recoge el conjunto de normas por las cuales se rige el funcionamiento de la Sociedad, regulando los aspectos básicos de la organización, los derechos de los socios y las relaciones con terceros, y que, junto a la Escritura pública o acta de constitución firmada por todos los socios ante Fedatario y otros documentos conexos, serán los trámites previos e imprescindibles para la inscripción de la empresa en el Registro Mercantil; el Pacto de Socios busca garantizar la seguridad jurídica de la Startup y prevenir posibles conflictos que pongan en peligro el desarrollo del proyecto por lo que se considera imprescindible. Es también llamado Acuerdo entre socios o Pactos parasociales, y se establece como todo contrato privado que suscriben voluntariamente los socios de un proyecto con el objetivo de regular sus relaciones, sus obligaciones y derechos, y el funcionamiento general de la Sociedad. Se trata de un contrato con autonomía de la voulntad propia, es independiente al estatuto de la sociedad, y suele ser complementario a este ya que permite mayor

99 VÁZQUEZ, R. (2015). Startup Legal III: *Constitución Startup*. Disponible en: http://mcaconsultores.com/legal-startup-iii-constitucion-startup/ [Última consulta 19 de octubre de 2018].

fl xibilidad en su regulación. Dicho pacto no se encuentra regulado por ninguna ley. Al tratarse de un documento privado su validez y eficacia no dependen de ningún requisito formal, es decir, no es necesario inscribirlo ante ninguna autoridad pública (aunque la recomendación es que si se suscriba con fé pública una vez firmado por las partes). Podrá suscribirse en cualquier momento, siendo lo más recomendable realizarlo desde el inicio del proyecto. En cuanto a su contenido, dependerá de las circunstancias y características propias de cada proyecto.

Según la tipología podemos distinguir diversidad de claúsulas en los mismos: *pactos de relación que regulan las relaciones entre los socios sin intermediación de la sociedad; pactos de atribución que otorgan un derecho o privilegio a la sociedad y pactos de organización dirigidos a regular el funcionamiento y organización de la sociedad, entre otros*… (Ruiz Chicote, 2017, p. 57) .[100] En definitiva, un Pacto de Socios debe prever y regular aquellas circunstancias que puedan afectar negativamente a la continuidad de la empresa, hablando y negociando entras las partes los acuerdos necesarios y plasmándolo por escrito en un documento vinculante para todas ellas.

Además de lo anterior se deberá cuidar muy de cerca varios puntos que detallo a contnuación:

1. La protección de los Activos (sobre todo los intangibles). Debemos tener en cuenta que los principales activos de una Startup son la innovación, la investigación, la información y el conocimiento técnico. Todos ellos forman el Know-how o Secreto industrial de una Startup. Dichos activos intangibles constituyen una ventaja competitiva en el mercado y su protección y uso requiere una especial atención. La primera medida que debe tomar la empresa es limitar el acceso a la información confidencial al personal estrictamente necesario para el desarrollo del producto o servicio. Firmar Acuerdos de Confidencialidad según las cuales se obliga a ambas partes a no divulgar información confidencial comprendida en el marco del contrato y desarrollo de las actividades correspondientes. También es necesario hacer una especial mención de los dos grandes mecanismos de protección de la Propiedad industrial (que protege las invenciones o creaciones intelectuales que tengan aplicación industrial como son las patentes, modelos de utilidad, marcas y diseños industriales) por un lado, y la propiedad intelectual (que protege el derecho de autor, es decir, las creaciones del intelecto humano de carácter literario, artístico o científico, como es el caso de las obras literarias, audiovisuales, musicales, ETC). Actualmente

100 Ruiz Chicote, N.; *La Innovación Empresarial y el Emprendimiento; el Fenómeno de las Starups*, Trabajo de fin de Grado, Facultad de Ciencias Empresariales y del Trabajo de Soria, Universidad de Valladolid, España, Julio 2017, Sitio de enlace: https://core.ac.uk/download/pdf/154403215.pdf [Fecha de consulta: 19 de octubre de 2018]

también se incluye el software y las bases de datos por este otro lado.

2. La protección en el entorno Digital: Actualmente, como consecuencia de la evolución de la sociedad de la información, las marcas de productos o servicios no solo existen y se desarrollan en un entorno físico sino que también lo hacen en el entorno digital, siendo este último posiblemente en el cuál tengan mayor repercusión. Por ello, cualquiera que sea el negocio de la Startup tiene que cuidar especialmente su presencia en la red, la protección de su página web así como los datos que ésta vaya a manejar en el desarrollo de su actividad y el cumplimiento en todo momento de la legislación vigente como otra cuestión legal básica. La primera medida que debe tomar la Startup para situarse en la red es realizar el Registro del Nombre de Dominio (DNS, por sus siglas en inglés, *Domain Name System*) de la página web a través de la cual vaya a operar la compañía. La página web corporativa es una herramienta que la empresa emplea como canal de comunicación, incluso de desarrollo del negocio y como medio de remisión de documentos e información a los socios o terceros interesados. En segundo lugar, requiere una especial atención el contenido mínimo del página Web. Es necesario cumplir con lo dispuesto en la legislación en materia de la Sociedad de la información, por ello la página web debe contar con varios textos legales, como el aviso legal y/o las condiciones generales de uso. También se debe informar al usuario de la política de cookies de la web, así como los tipos de cookies utilizadas, su funcionalidad y el modo de deshabilitarlas. Es necesario el consentimiento de los usuarios para su utilización, dándose incluso por cumplido con la mera navegación por la web durante un periodo prolongado. Asimismo, en el caso de que los usuarios puedan contratar productos y servicios a través del sitio web (es decir, que exista e-commerce), éstos tendrán aceptar de forma expresa los términos y condiciones de contratación. En tercer lugar, hay que tener especial consideración con los datos de carácter personal. Es necesario disponer de una política a través de un aviso de privacidad con el fin de cumplir con los requisitos establecidos en la Ley. Con el nuevo Reglamento de Protección de Datos (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de dichos datos, siendo su aplicación efectiva en mayo de 2018, las empresas deberán haberse adaptado a la nueva normativa, implementando de manera efectiva las medidas jurídicas y técnicas que sean necesarias pues entre sus novedades se destaca, la incorporación del derecho de transparencia, el derecho al olvido y la portabilidad de datos a losya instaurados Derechos ARCO[101].

3. Cuestiones transfronterizas (aspectos del derecho internacional)

101 Derechos ARCO (Acceso, Rectificación, Cancel ción y Oposición).

Según sea el desarrollo y evolución de la Startup es posible que resulte necesario ocuparse de algunos aspectos relativos al Derecho Internacional pues cada vez resulta más común que una empresa tenga su sede en un territorio determinado pero que sus usuarios se encuentren repartidos por todo el mundo. Sobre la ley aplicable a obligaciones contractuales, prevalece el principio general la autonomía de la voluntad de las partes, es decir, las partes pueden escoger la ley aplicable a su contrato. A falta de esta determinación, se aplicará la ley de la residencia habitual o del centro principal o habitual de negocios de la parte que tiene a su cargo la prestación característica del contrato, es decir, la empresa o Startup del país donde se firmo el contrato decidirá la regulación aplicable. Para conocer el tribunal competente ante posibles incidencias, el criterio que prevalece es que *la autonomía de la voluntad está limitada en materia de garantías y protección de los consumidores, por lo que el órgano jurisdiccional competente será el del lugar donde esté domiciliado el usuario como regla.*

Por último, sugerimos que las Starups deberán escoger la forma jurídica bajo la cual operará para hacer frente a las obligaciones fiscales pertinentes y prestar atención a las diversas fórmulas de financiación disponibles, verificando incluso, si es posible, acceder a ayudas públicas.

Contexto Mexicano

En México, hasta hace unos meses, para iniciar una empresa había que sujetarse a trámites complicados que derivaban en retrasos y costos adicionales. Es por eso por lo que el gobierno mexicano se planteó el objetivo de orientar las regulaciones de acuerdo con el punto de vista de los ciudadanos para favorecer el crecimiento económico y el desarrollo. El resultado es el portal **tuempresa.gob.mx**[102], un importante logro en la estrategia de simplificación administrativa de la interacción entre los ciudadanos y el gobierno. El portal emplea tecnologías de información de punta que reducen significativamente el papeleo actual y minimizan los costos de apertura de las nuevas empresas. Esos complicados trámites y los retrasos con frecuencia obligaban a algunos empresarios a claudicar y abandonar sus proyectos; otros decidían continuar sin sujetarse a todos los trámites requeridos; de hecho, muchos terminaban desarrollando su actividad empresarial en el sector informal, al menos por algún tiempo, "*para ver cómo resultaban las cosas*". Lo cierto es que la informalidad no sólo crea inseguridad para

102 OCDE.org, Facilidad y rapidez en la creación de empresas en México, lanzado en 2009 y luego reformulado en su versión 2.0 en 2012. Este folleto fue divulgado por Secretaria de Economía en 2013 y resulto ampliado en 2016 con la creación de la SAS. Sitio Web: https://www.oecd.org/centrodemexico/medios/43843217.pdf [Fecha de consulta: 19 de octubre de 2018].

las empresas y los trabajadores, sino que también los priva del acceso a los apoyos gubernamentales.

El portal está diseñado para brindar asistencia práctica a las personas que quieren iniciar una empresa comercial a través de las figuras de Sociedad Anónima y Sociedad de Responsabilidad Limitada[103]; pero no aplicaba a personas físicas con actividad empresarial, quienes están sujetos a procedimientos más sencillos. El objetivo del portal es buscar simplifi ar los trámites federales, evitando que el ciudadano haga filas en diversas ventanillas y se desplace a distintas oficinas gubernamentales. El portal le da incluso la oportunidad al ciudadano de generar los "Estatutos Sociales (de Ley)" de su empresa en un archivo electrónico, los cuales pueden ser modificados por el ciudadano o por el notario o corredor público antes de la constitución de la empresa.

Los pasos para constituir una empresa a través del portal son muy sencillos:

1. Registrarse; 2. Seleccionar el Nombre o Denominación social (5 referentes); 3. Llenar los datos para constituir la empresa; 4. Pagar los derechos federales correspondientes; y 5. Seleccionar un fedatario público y acudir a su oficina para formalizar la constitución de la empresa.

Los documentos que obtiene el ciudadano al finalizar el proceso en el portal y después de acudir con el fedatario son: Estatutos de la empresa y acta constitutiva; Permiso de uso de nombre o denominación social; Aviso del permiso de uso de nombre o denominación social; Boleta de inscripción del acta constitutiva en el Registro Público de Comercio correspondiente; Inscripción en el Registro Federal de Contribuyentes y la Cita ante la Subdelegación del Instituto Mexicano del Seguro Social para recoger la Tarjeta de Identificación Patronal. Finalmente, estos portales electrónicos de resolución de trámites hacen uso de las tecnologías de información y comunicación (TIC) más avanzadas y ofrecen una muy amplia gama de servicios.

En el ámbito internacional, muchos países han instrumentado portales electrónicos para ayudar a la creación e inicio de operaciones de las nuevas empresas.

- En América Latina, Chile clic es la iniciativa más reciente introducida por el gobierno de Chile para ayudar a las empresas (y a los ciudadanos) a cumplir con trámites administrativos a través de portales en internet. Esta iniciativa busca estar más orientada al cliente, a diferencia de los modelos desarrollados anteriormente.
- En Norteamérica, el portal BizPal de Canadá ofrece información y asesoría vía internet. Este portal funciona en un ambiente de negocios complejo, dado que Canadá, como México, tiene tres niveles de gobierno.
- En Europa, el portal de internet Circe de España, combinado con una

103 Más del 80% de las sociedades mercantiles que se constituyen anualmente en México utilizan la figura de la Sociedad Anónima y/o de la Sociedad de Responsabilidad Limitada (esto en términos no absolutos).

simplificación de trámites, ha sido efectivo en la creación de empresas, especialmente aquéllas muy pequeñas.

• Portugal también ha llevado a cabo un programa de reformas para facilitar la creación de nuevas empresas, incluido un registro centralizado en internet para todas las licencias y para el desarrollo de ventanillas únicas de resolución de trámites.

México se coloca hoy a la vanguardia en la simplificación y disminución de trámites y cargas administrativas para la creación e inicio de nuevas empresas, así como para trámites vinculados con su operación. Con ello busca avanzar firmemente en la implementación de portales electrónicos de trámites contribuirá al fortalecimiento de la competitividad en México. Todo esto dio sentido entonces al nacimiento de una nueva forma empresarial que resulta emblemática ya, la que surgió a partir de 2016[104] y vino a cambiar la percepción del concepto mismo de empresario PYME hacia una concepción más moderna y atractiva. Nació la idea del Negocio más allá de lo "Virtual" plasmado en la unipersonalidad pero con una formalidad legal más incluyente. Nace así la posibilidad de creación de una nueva variante que pudiera ser ya llamada como ¿la **Startup Mexicana**?

IV. STARTUPS LEGALES: UNA NUEVA TENDENCIA INNOVADORA

La "revolución del sector legal" puede también llegar de la mano de una Startup[105] *"Gracias a una biblioteca digital, los usuarios pueden acceder a documentos creados por otros participantes y facilitar sus tareas rellenando documentos extremadamente sencillos que luego generarán el documento que ellos necesitan. Si bien los conocimientos legales no son necesarios, la plataforma se encuentra actualizada respecto a la legislación española vigente, por lo que con los datos ingresados se crearán documentos completamente válidos. Los expertos indican que con procedimientos de este estilo se puede obtener el material*

104 El 14 de marzo de 2016 se publicó en el Diario Oficial de la Federación el Decreto por el que se reformaron y adicionaron diversas disposiciones a la Ley General de Sociedades Mercantiles en México. La constitución de una Sociedad por Acciones Simplificada (conocida por la siglas SAS), es un nuevo régimen jurídico que a partir de una persona física o en asociación con otras más que pueden constituir una empresa a través de medios electrónicos con todos los efectos legales y donde la intervención del Fedatario Público es opcional. La única forma para realizar este trámite es mediante el Sistema Electrónico de Constitución de Sociedades por Acciones Simplificadas, el cual está a cargo de la Secretaría de Economía, cuyo funcionamiento y operación se regirá por las Reglas de Carácter General para el Funcionamiento y Operación del Sistema Electrónico de la SAS publicadas en el Diario Oficial antes mencionado. Sitio Web (otra página). https://www.gob.mx/cms/uploads/attachment/file/237280/1.4_GUIA_DEL_US_ARIO.pdf[Consulta: 19 octubre 2018].

105 Universia España, Aunque parezca extraño, incluso una de las profesiones más tradicionales y anticuadas en el mundo: el Derecho, también se ve revolucionada por la creación de una página web de la Startup llamada **Bigle Legal**: https://biglelegal.com/es/ Fecha de consulta: 27 de mayo de 2016]

que se necesita con un proceso un 95% más rápido que del modo tradicional".

Sucede que tradicionalmente los abogados/as han sido reticentes a adoptar innovaciones y nuevas tecnologías. Ahora, estas innovaciones están siendo dirigidas por el creciente ecosistema de proveedores de **tecnología legal** (LEGALTECH) que buscan convulsionar y reinventar la industria. La tecnología ya no es opcional en el mundo legal. Cualquier bufete puede alcanzar resultados increíbles gracias a la adopción de innovaciones y usarlas para impulsar su transformación digital.

Es por ello que una Startup también debe y puede ofrecer servicios legales accesibles y tener como uno de sus objetivos ayudar a disminuir la informalidad, al proporcionar información para la debida y legal operación de los negocios y facilitar herramientas que apoyen a empresarios en el cumplimiento de sus obligaciones legales y regulatorias. Para ello deberá seguir los siguientes pasos: *1. Consultar a un asesor desde cualquier lugar; 2. Obtener un diagnóstico de la situación legal del negocio; 3. Crear documentos legales individualizados y confiables para cubrir necesidades específicas; y 4. Administrar y dar seguimiento a contratos y acuerdos legales adoptados.*

Todo ello teniendo como base una plataforma digital con libre acceso a Internet que viabilice su operación y funcionamiento. De ese modo se evitarían errores legales muy frecuente, como son: elegir una fórmula societaria inadecuada; no elegir bien el lugar de constitución de la sociedad; confiar en quien no se debe (Socio); no firmar un pacto de socios y despreciar la importancia del valor actual de los intangibles.

V. CONSIDERACIONES FINALES (CON ALGUNAS RECOMENDACIONES)

PRIMERO: Se puede considerar que basado en la definición de PYME enunciada, se requiere homogeneizar el tipo de forma legal de acuerdo a la dimensión o tamaño de la empresa y tomando en cuenta el alcance o proyección del negocio bajo la fórmula de empresario social. Al respecto, se pretende exponer la idea que valore la estructura de la pequeña y mediana empresa ya no solo como las clásicas Sociedades Personalistas (sobre todo la micro o familiar) sino como Sociedades Mercantiles de responsabilidad limitada (sobre todo la S.R.L. o la S.A. de manera excepcional) para el resto de los negocios.

SEGUNDO: Principalmente un buen plan de creación de una PYME habrá de recoger: La descripción del negocio que pretendemos crear; un profundo y serio estudio acerca de la viabilidad real de la idea, viabilidad que ha de ser tanto técnica como económica y financiera; los objetivos que se persiguen con la creación de la empresa, y una detallada descripción de las estrategias que se habrán de seguir para la consecución de tales objetivos; También el conseguir o no suficientes recursos

financieros que nos permitan poner en marcha nuestra iniciativa; y por último, pero no menos importante, ha de ser la elección de la *forma jurídica a adoptar por la empresa.*

TERCERO: Cabe destacar que en nuestro ordenamiento jurídico todavía no existe una normativa *ad hoc* que apoye, fomente y regule cuestiones específicas relativas a las Startups y su ámbito de actuación. Pero, por otro lado, la ausencia de una normativa específica no exime a las Starups de cumplir y tener en cuenta una serie de aspectos en lo referente a la legalidad del modelo de negocio y su constitución, el pacto de socios, la protección de los activos y del entorno digital. Asimismo, en caso de que tenga lugar la expansión internacional se tendrán que tomar en consideración la regulación de cada país concreto.

CUARTO: Entre las acciones principales para convertir una PYME en STARTUP esta el hecho que debe basarse en la viabilidad jurídica y el pleno respeto a la legalidad de su proyecto. Un mal análisis legal puede afectar al desarrollo natural del negocio. En este sentido, la actividad empresarial nunca podrá llevarse a cabo si no se ajusta dentro de lo que los abogados llamamos "marco legal de referencia". Queda claro, pues, que resulta imprescindible tener muy claros los aspectos jurídicos a observar para que la PYME como Startup sea viable. No sólo desde una perspectiva legal, sino también a nivel operativo. En el momento de la creación de la Startup es muy importante contar con un entorno legal bien definido y sólido.

QUINTO: Debido a la relativa novedad de este modelo de empresa y sus especiales características no se dispone todavía una regulación que se adapte a sus necesidades, por lo que recomendamos que: desde el propio ecosistema Startup se solicite que se eliminen las trabas existentes para la creación de una empresa, empezando por los excesivos trámites burocráticos, y se adapte la creación de una figura o forma mercantil más concreta para esta modalidad, incluso fomentando la constitución online (en línea) e incluyendo aspectos relativos al ámbito fiscal que busque fomentar un sistema de deducciones que por un lado favorezca la inversión y por otro no penalice los resultados obtenidos por la empresa en sus inicios.

SEXTO: Esta modificación de la normativa legal propiciará un entorno más práctico y eficiente, pero a su vez también necesario buscando se produzca cierto cambio en la mentalidad del negocio que todavía no está adaptada a la realidad que presenta la innovación y asi poder entender la nueva realidad emprendedora y desarrollar las capacidades técnicas y tecnológicas necesarias. Aunado a esto, el asesoramiento jurídico en todo tipo de Startup debe anticiparse a las necesidades que puedan surgir del proyecto adoptando un rol proactivo que coadyuve en beneficio y protección actual de los pequeños y medianos negocios.

VI. REFERENCIAS BIBLIOGRÁFICAS

ASOCIACIÓN PARA LA INVERSIÓN DE CAPITAL PRIVADO EN AMÉRICA LATINA (LAVCA). Sitio Web: https://lavca.org/about-lavca/ [Fecha de consulta: 19 de octubre de 2018]

ANGELLIST Where the world meets startups. Sitio Web: https://angel.co/companies [Fecha de consulta: 19 de octubre de 2018]

FORTUNE (2016), The Unicorn List, [en línea], disponible en: http://fortune.com/unicorns/ [consulta julio 2018].

GARCÍA PEÑA, José H., *Derecho Empresarial. Tópicos y Categorías: Una revisión comparada en el Sector Pyme Latinoamericano,* Tecnológico de Monterrey-Editorial Porrúa, México, 2011.

GOBIERNO DE MÉXICO, Instituto Nacional de Estadística y Geografía (INEGI), el Instituto Nacional del Emprendedor (INADEM) y el Banco Nacional de Comercio Exterior (BANCOMEXT), presentan la Encuesta Nacional sobre Productividad y Competitividad de las Micro, Pequeñas y Medianas Empresas (ENAPROCE) 2015. - Se difunden estadísticas detalladas sobre las micro, pequeñas y medianas empresas del país (BOLETÍN DE PRENSA NÚM. 285/16) www3.inegi.org.mx/rnm/index.php/catalog/330/download/9792 [Fecha de publicación: 13 de julio de 2016]

GLOBAL STARTUP ECOSYSTEM RANKING, 2019 Sitio Web: https://startupgenome.com/reports/global-startup-ecosystem-report-2019 [consulta 3 julio 2019].

NUÑO DE LEÓN, Pierina del R., *Administración de pequeñas empresas*, Primera edición, RED TERCER MILENIO S.C., México 2012.

OCDE.ORG, Facilidad y rapidez en la creación de empresas en México, lanzado en 2009 y luego reformulado en su versión 2.0 en 2012. Este folleto fue divulgado por Secretaria de Economía en 2013 y resulto ampliado en 2016 con la creación de la SAS. Sitio Web: https://www.oecd.org/centrodemexico/medios/43843217.pdf [Fecha de consulta: 19 de octubre de 2018].

PARDO, D. (2016). El sector tecnológico en España reclama 100.000 profesionales especializados. El Economista (blog). Entrada del día: 26 de octubre de 2017. Disponible en: http://infoautonomos.eleconomista.es/blog/profesionales-sector-tecnologico/[consulta: 19 de mayo de 2018]

PAREDES-BARCELÓ, Raúl G. · Peña-Ahumada, Nuria B. Vacio-Hernández, Iván A. *Tópicos Selectos de Micro y Pequeñas Empresas La Micro y Pequeña Empresa: Un análisis desde la*

perspectiva económico-administrativa T-I, ECORFAN Editores, Universidad Tecnológica de San Juan del Río, México, noviembre, 2016.

RUIZ CHICOTE, N.; *La Innovación Empresarial y el Emprendimiento; el Fenómeno de las Starups*, Trabajo de fin de Grado, Facultad de Ciencias Empresariales y del Trabajo de Soria, Universidad de Valladolid, España, Julio 2017, Sitio de enlace: https://core.ac.uk/download/pdf/154403215.pdf [Fecha de consulta: 19 de octubre de 2018]

SHIKHAR GHOSH (estudio recogido en Wall Street Journal) Sitio Web: http://online.wsj.com/article/SB10000872396390443720204578004980476429190.html [Fecha de consulta: 19 de octubre de 2018].

SISTEMA PARA APERTURA RAPIDA DE EMPRESAS EN MÉXICO (2012). LATIN-REG es la red Latinoamericana de Mejora Regulatoria y Competitividad. Esta publicación esta disponible en https://www.gob.mx/conamer [Fecha de consulta: 19 de octubre de 2018]

STARTUP AMÉRICA LATINA 2015-2016: CONSTRUYENDO UN FUTURO INNOVADOR © OCDE (https://www.oecd.org/dev/americas/Startups2016_Sintesis-y-recomendaciones.pdf) [consulta: 19 octubre 2018]

TU EMPRESA | Campaña | gob.mx - Gobierno de México:

PLATAFORMA DIGITAL TU EMPRESA: https://youtu.be/j7_eFtNmU-A

CONSTITUYE TU EMPRESA EN LINEA: https://youtu.be/29Tig1lEMoQ

UNIVERSIA ESPAÑA, Noticias, https://noticias.universia.es/ciencia-tecnologia/noticia/2016/05/27/1140181/revolucion-sector-legal-llega-mano-startup.html [Fecha de consulta: 27 de mayo de 2016]

VÁZQUEZ, R. (2015). Startup Legal III: *Constitución Startup*. Disponible en: http://mcaconsultores.com/legal-startup-iii-constitucion-startup/ [Última consulta 19 de octubre de 2018].

LAS OPERACIONES CON RECURSOS DE PROCEDENCIA ILÍCITA Y LAS FINTECH

(RESPONSABILIDAD PENAL DE LAS PERSONAS MORALES)

Eje temático: Inteligência Artificial, egalTechs

Autores:
Alberto Enrique Nava Garcés
Doctor en Derecho; Miembro del Sistema Nacional de Investigadores (Conacyt); Profesor por Oposición de Derecho Penal en la Facultad de Derecho de la Universidad Nacional Autónoma de México; Investigador y miembro del Comité de Investigación del Instituto Nacional de Ciencias Penales (INACIPE); Miembro del Consejo editorial de las revistas: El mundo del abogado y Criminogénesis; Miembro de la Sociedad Mexicana de Criminología y de la Asociación Nacional de Doctores en Derecho y Miembro invitado del Instituto de Derecho Informático del Colegio de Abogados de Mar del Plata, Argentina.

Juliette Núñez Ruiz
Licenciada en Derecho, Maestrante en Ciencia Jurìdico Penal. Investigadora Asistente en el Instituto Nacional de Ciencias Penales.

SUMARIO

1. Introducción, 2. La responsabilidad penal de las personas morales, 3. Empresas tecnológicas, 4. Inicios de una Starup, 5. Evolución de Starup a Fintech, 6. Qué es una Fintech, 7. Características, 8. Servicios Ofrecidos, 9. El acierto de regular las Fintech, 10. La regulación en las fintech México, 11. Conclusiones, 12. Bibliografía.

ABSTRACT

El concepto de empresa ha ido evolucionando a lo largo del tiempo, dica capacidad de mutación ha influenciado el mundo impactando no solo de forma económica sino también social y culturalmente, lo anterior ya que no se ha limitado a los tipos de empresas o sociedades que conocíamos sino que se ha dado un nuevo concepto derivado de la búsqueda de innovación y un modelo de negocios rentable.
En consecuencia de lo anterior es que se crea el sector Fintech, mismo que ha ido ganando terreno en la economía, negocios e incluso en las legilaciones, por ello, se identificará la evolución de este sector y el grado de reglamentación que ocupa en México, para ello hemos de verificar la evolución que han tenido las empresas y los inicios de la Starup misma que ha servido de base para crear las Fintech. En este esquema se ha de identificar aquellos elementos característicos de la empresa catalogada como innovadora pues tal como se verá en párrafos subsiguientes, el esquema es tan amplio, que es necesario que las legislaciones comiencen limitando el concepto de este sector e identificando qué servicios serán ofrecidos por las empresas que se cataloguen dentro de este sector.
Una vez identificado es necesario el estudio de la regulación de este sector en México pues de esta forma lograremos identificar los aciertos y oportunidades de mejora que nuestros legisladores tiene ya

que como es sabido por el lector, la poca regulación de estas empresas, ha causado que (no sólo México) sino alrededor del mundo existan huecos legales que afectan al sistema de pagos, al sector económico, la competencia entre empresas e incluso a los consumidores, situación que diversos sujetos activos han sabido aprovechar para hacer uso de diversos recursos e inmiscuirse en nuevas conductas antijurídicas, lo que como consecuencia ha tenido que los países deban reformar sus legislaciones penales en busca de cerrar los causes que provocan las operaciones con recursos de procedencia ilícita.

Palabras clave: Delitos informáticos, responsabilidad de las personas morales, Fintech, crowfounding, lavado de dinero, blanqueo de capitales.

1. INTRODUCCIÓN

El Derecho Penal y las nuevas tecnologías tienen puntos de convergencia más a menudo. Éstas últimas han incidido tanto en la creación de nuevos tipos penales como en el cambio de óptica respecto de figuras que parecían inamovibles como la responsabilidad penal de las empresas que hoy en día ha abierto un debate por demás interesante y enriquecedor.

Antonio Mazzitelli (Representante en México de la Oficina de las Naciones Unidas contra la Droga y el Delito en México, UNODC) lo ha señalado con gran claridad en diversos foros:

> **La lucha contra el crimen organizado, y la corrupción es un tema de ir detrás del dinero**, si queremos de verdad golpear al crimen organizado, la actividad más importante es tratar de extraer su fortaleza, esto es, su capacidad de infiltrarse, de controlar y de legitimar una cultura criminal.
> No nos adentraremos en los temas específicos y técnicos de las lucha contra el lavado de activos, el objetivo de esta ponencia es mostrar cómo el crimen organizado se está estructurando, evolucionando y mostrando nuevas caras, así como su infiltración en la sociedad. […
> En diciembre de 2011, se trató de elaborar un primer informe, estimando los flujos financieros relacionados con las actividades criminales, trabajo de compilación, sustentado en el análisis de cuánto dinero pueden generar los mercados criminales, es decir, se trata de ver al crimen organizado desde una perspectiva diferente y no solamente a sus bienes, las drogas, la trata de personas, el robo, sino a los mercados criminales, partiendo del presupuesto del concepto de los mercados y operadores que tratan de maniobrar dichos mercados.[106]

El flujo de activos, ahora en esta época, virtuales, así como la creación de nuevos modelos de empresa, obligan a conocer el funcionamiento de ésta así como la preparación de una regulación que permita conocer el origen de los recursos que administra o transfiere

2. LA RESPONSABILIDAD PENAL DE LAS PERSONAS MORALES

106 Cfr. http://www.cinu.mx/noticias/la/antonio-mazzitelli-el-experto-/ consultado el 8 de junio de 2019, 14:44 hs.

Cuando nos referimos al sujeto activo estamos acostumbrados a pensar en la persona física que, por sí misma o a través de otra, actualiza el verbo núcleo del tipo pero, en los últimos años se ha hecho énfasis en que la persona jurídica o moral tenga una concepción similar para hacerla responsable penalmente. Y al respecto adelanto mi posición, la persona moral delinque a través de las personas que actúan en su nombre y, además, la persona moral puede ser el constructo jurídico para dar apariencia de empresa a lo que en realidad es una organización orientada a la comisión de un delito.

Hace algunos años, el doctor Fernando Flores García (1989) escribió unas líneas extraordinarias, cuando el tema no cobraba la vigencia que tiene hoy. En la conclusión de su análisis el maestro escribió:

> Se han logrado considerables avances y establecido puntos de coincidencia. Es de desearse que en futuros congresos jurídicos, en libros, ensayos, proyectos legislativos, etc., se renueven los esfuerzos para dar una solución que resuelva los problemas que en la vida real representan las actividades ilícitas de las personas jurídicas colectivas. [107]

Y es que al hablar de responsabilidad debe quedar claro si el concepto parte de la sustitución del juicio de reproche o bien, es la consecuencia procesal de un acto en particular.

En todo caso, la voluntariedad y conocimiento que exige la culpabilidad, siempre serán un gran reto para quien diserte sobre este tema.

Recientemente se han desarrollado distintas iniciativas de ley, derivadas de los instrumentos internacionales que ha firmado México, entre los cuales destacan la Convención de las Naciones Unidas Contra la Delincuencia Organizada Transnacional y la Convención de las Naciones Unidas Contra la Corrupción que contienen la posibilidad de que los Estados legislen sobre la responsabilidad penal de las personas jurídicas.

La Convención de las Naciones Unidas Contra la Delincuencia Organizada Transnacional en su artículo 10 señala:

- La obligación de los estados a adoptar medidas necesarias y establecer la responsabilidad de las personas jurídicas.
- La materias competentes para conocer de la responsabilidad se limitarán a penal, civil o administrativa.
- Las responsabilidades serán excluyentes a la que se relaciona con la materia penal.

107 Véase Flores García, Fernando, *La responsabilidad penal de la persona jurídica colectiva* en *Ensayos jurídicos*, Facultad de Derecho (Cincuentenario de la Revista de la Facultad de Derecho de México), UNAM, 1989, pp. 99 – 143. Véase también: Flores García, Fernando, *Principales Corrientes acerca de la Responsabilidad Penal de la Persona Jurídica Colectiva*, en *Liber Ad Honorem Sergio García Ramírez*, Tomo II, UNAM, Instituto de Investigaciones Jurídicas, México, 1998.

• Los estados velarán por la imposición de sanciones penales[108].

Por su parte, la Convención de las Naciones Unidas Contra la Corrupción establece lo siguiente:

• Los estados deberán adoptar medidas para establecer la responsabilidad de las personas jurídicas cuando se participe en las conductas tipificadas por la convención.

• LaS materias competentes para conocer de la responsabilidad se limitarán a penal, civil o administrativa.

• Las responsabilidades serán excluyentes a la que se relaciona con la materia penal.

• Los estados velarán por la imposición de sanciones penales[109].

Asimismo, en el ámbito nacional se han abordado en varias iniciativas de ley lo relativo a la responsabilidad de las personas morales, con distintas perspectivas doctrinales, con distintas soluciones. Además, se ha abonado lo relativo a los derechos humanos que le son propios a las personas jurídicas[110], sin embargo, de la lectura de los pocos artículos que le dedica al tema el Código Nacional de Procedimientos Penales (artículos 421 al 425), podemos vislumbrar que el procedimiento penal a las personas jurídicas apenas está en sus comienzos y deberá ser en la legislación sustantiva dónde deba ser regulado.[111]

108 Artículo 10. Responsabilidad de las personas jurídicas. 1. Cada Estado Parte adoptará las medidas que sean necesarias, de conformidad con sus principios jurídicos, a fin de establecer la responsabilidad de personas jurídicas por participación en delitos graves en que esté involucrado un grupo delictivo organizado, así como por los delitos tipificados con arreglo a los artículos 5, 6, 8 y 23 de la presente Convención. 2. Con sujeción a los principios jurídicos del Estado Parte, la responsabilidad de las personas jurídicas podrá ser de índole penal, civil o administrativa. 3. Dicha responsabilidad existirá sin perjuicio de la responsabilidad penal que incumba a las personas naturales que hayan perpetrado los delitos. 4. Cada Estado Parte velará en particular por que se impongan sanciones penales o no penales eficaces, proporcionadas y disuasivas, incluidas sanciones monetarias, a las personas jurídicas consideradas responsables con arreglo al presente artículo.

109 Artículo 26. Responsabilidad de las personas jurídicas 1. Cada Estado Parte adoptará las medidas que sean necesarias, en consonancia con sus principios jurídicos, a fin de establecer la responsabilidad de personas jurídicas por su participación en delitos tipificados con arreglo a la presente Convención. 2. Con sujeción a los principios jurídicos del Estado Parte, la responsabilidad de las personas jurídicas podrá ser de índole penal, civil o administrativa. 3. Dicha responsabilidad existirá sin perjuicio de la responsabilidad penal que incumba a las personas naturales que hayan cometido los delitos.4. Cada Estado Parte velará en particular por que se impongan sanciones penales o no penales eficaces, proporcionadas y disuasivas, incluidas sanciones monetarias, a las personas jurídicas consideradas responsables con arreglo al presente artículo.

110 "Las personas morales gozan de aquellos derechos fundamentales que conforme a su naturaleza le resulten necesarios para la realización de sus fines con el fin de proteger su existencia, su identidad y asegurar el libre desarrollo de su actividad." Así lo estableció el Pleno de la Suprema Corte de Justicia de la Nación el 21 de abril de 2014, al resolver la Contradicción de Tesis 360/2013.

111 Ramón Eduardo Ribas escribe sobre el el procedimiento penal a las personas jurídicas: "La construcción de un sistema de responsabilidad penal de las personas morales puede encauzarse jurídicamente a través de dos vías fundamentales:

Sin embargo, bajo este tenor, las empresas Fintech podrían ser imputadas penalmente si incurriesen en algún delito, en especial el blanqueo de capitales o lavado de dinero cuya denominación en la legislación mexicana es operaciones con recursos de procedencia ilícita.[112]

En primer lugar, acudiendo a las categorías y criterios de imputación penales ya conocidos.

Creando, en segundo término, un nuevo Derecho Penal, exclusivo de las entidades colectivas.

La primera de estas soluciones consiste en *adoptar* el Derecho Penal clásico, de base individualista, y aplicarlo a los comportamientos criminales protagonizados por entidades colectivas. Obviamente, dicha adopción y la subsiguiente aplicación no pueden realizarse de forma mecánica o automática; sería preciso ajustar, antes, mediante una reinterpretación funcionalista, la teoría del delito individual. Sin esta nueva normativización de los conceptos penales, la inadecuación de éstos para enfrentarse a formas de criminalidad colectiva obligaría a una *resignación descriptiva* o a crear un sistema de responsabilidad penal específico para empresas o personas colectivas. Característico de estos planteamientos es, en fin, su intento de adecuar las categorías penales a las personas jurídicas antes que sustituirlas por otras.

Radicalmente contraria a la fl xibilización de las categorías penales existentes se muestra Zúñiga rodríguez. En su opinión, dicha fl xibilización comportaría el riesgo de «contaminar» todo el sistema de responsabilidad individual de esas ansias de «adaptabilidad», pudiendo desembocar en la pérdida de la validez de las garantías ganadas y construidas durante dos siglos. También Tamarit Sumalia considera, ante los riesgos de «contaminación conceptual» que pudieran derivarse de la integración de la responsabilidad de las personas jurídicas en el sistema penal, que sería aconsejable un «dualismo no disgregador del sistema.

La segunda solución, a mi juicio más plausible, toma como punto de partida la siguiente idea: las personas jurídicas, por ser sujetos diferentes, necesitan de un derecho penal distinto del de las personas físicas, precisamente porque el problema es que éste no les resulte aplicable. Asumida la necesidad de un Derecho Penal distinto, será necesario determinar que deberá tener este nuevo Derecho *antiguo* para seguir conceptuándolo como Penal: si no tuviera nada, no nos hallaríamos ante un Derecho Penal distinto, sino, como indica García Arán, ante algo distinto del Derecho Penal." (Ribas, Ramón Eduardo, *La persona jurídica en el derecho penal. Responsabilidad civil y criminal de la empresa*, Editorial Comares, Granada, 2009, pp. 281 – 282).

112 **Operaciones con recursos de procedencia ilícita**

Artículo 400 Bis. Se impondrá de cinco a quince años de prisión y de mil a cinco mil días multa al que, por sí o por interpósita persona realice cualquiera de las siguientes conductas:

I. Adquiera, enajene, administre, custodie, posea, cambie, convierta, deposite, retire, dé o reciba por cualquier motivo, invierta, traspase, transporte o transfiera, dentro del territorio nacional, de éste hacia el extranjero o a la inversa, recursos, derechos o bienes de cualquier naturaleza, cuando tenga conocimiento de que proceden o representan el producto de una actividad ilícita, o

II. Oculte, encubra o pretenda ocultar o encubrir la naturaleza, origen, ubicación, destino, movimiento, propiedad o titularidad de recursos, derechos o bienes, cuando tenga conocimiento de que proceden o representan el producto de una actividad ilícita.

Para efectos de este Capítulo, se entenderá que son producto de una actividad ilícita, los recursos, derechos o bienes de cualquier naturaleza, cuando existan indicios fundados o certeza de que provienen directa o indirectamente, o representan las ganancias derivadas de la comisión de algún delito y no pueda acreditarse su legítima procedencia.

En caso de conductas previstas en este Capítulo, en las que se utilicen servicios de instituciones que integran el sistema financiero, para proceder penalmente se requerirá la denuncia previa de la Se-

3. EMPRESAS TECNOLÓGICAS

Jorge Barrera Graf (2010) define a la empresa como un "conjunto de personas y cosas organizadas por el titular con el fin de realizar una actividad onerosa, generalmente lucrativa de producción o de intercambio de bienes y servicios destinados al mercado".[113] O bien, como lo define la Real Academia Española como una "unidad de organización dedicada a actividades industriales, mercantiles o de prestación de servicios con fines lucrativos".[114] Pero también encontramos definiciones que son más extensas por integrar un número más amplio de conceptos a los cuales se dedica, tal es el caso de Julio García y Cristóbal Casanueva (2001) que en su libro Prácticas de la Gestión empresarial la definen como una "entidad que mediante la organización de elemento humanos, materiales, técnicos y financieros proporciona bienes o servicios a cambio de un precio que le permite reposición de los recursos empleados y la consecución de unos objetivos determinados".[115]

La capacidad de mutación que la empresa ha demostrado durante el transcurso de los años ha permeado hasta nuestros tiempos de forma que gracias a ello gran parte de la economía que perciben los países se ha visto beneficiada por ellas, por lo que se han generado diversas oportunidades para la creación de las mismas que ya no se limitan a sociedades civiles, colectivas, anónimas, o bien por tamaños siendo pequeña, mediana o grande empresa, sino que han surgido diversos tipos como lo son las Fintech.

El tema que se expondrá en forma referencial, teórica y analítica requiere del entendimiento de diversos conceptos básicos de la materia para la comprensión mínima y correcta, por lo que a fin de entender el término Fintech en su totalidad y para pasar a una crítica de esta tecnología de financiamiento, nos vemos obligados a entrar al tema no sin antes definir lo que entendemos por "startup" esto ya que como es sabido, muchas empresas comienzan siéndolo y cambian al sector Fintech.

4. INICIOS DE UNA STARTUP

---

cretaría de Hacienda y Crédito Público.

Cuando la Secretaría de Hacienda y Crédito Público, en ejercicio de sus facultades de fiscaliz - ción, encuentre elementos que permitan presumir la comisión de alguno de los delitos referidos en este Capítulo, deberá ejercer respecto de los mismos las facultades de comprobación que le confieren las leyes y denunciar los hechos que probablemente puedan constituir dichos ilícitos.

113 Citado en Dávalos Torres, María S. Manual de Introducción al Derecho Mercantil. Cultura jurídica, México, 2010, pp. 101.

114 Consultado de https://dle.rae.es/?id=EsuT8Fg, 25 de mayo de 2019.

115 García Del Junco,Julio. Prácticas De La Gestion Empresarial. Mc Graw Hill, Madrid, 2001.

El término comienza a utilizarse en razón del surgimiento de diversas empresas pequeñas que ofrecen servicios innovadores, por ello podemos identificarlas como aquel proyecto original mismo que se identific por no tener un símil y aunque el mundo empresarial la alcance, contará con un buissnes plan y una ventaja competitiva que la ayudara a destacar de las otras empresas.

Steve Blank y Bob Dorf (2000) la definen como una "organización temporal en busca de un modelo de negocio rentable, que puede repetirse y que es escalable" [116], pero también debemos tomar en consideración el concepto de startup, según Cambridge Dictionary se entiende como "pequeño negocio que apenas ha empezado"[117], o bien como lo establece Montoya Pineda (2015) "es casi una hipótesis todavía en conducción y aún no demostrada en su totalidad, aunque también se asume en la región como una compañía consolidada demostrada en la práctica y vigente en los tiempos cambiantes"[118].

El término de startup fue acuñado en los años 50 del siglo pasado en Silicon Valley, en donde aproximadamente en 1957 se crea la primera empresa orientada a este concepto conocida como Fairchild Semiconductor[119].

116 Steve Blank; Bob Dorf. El Manual Del Emprendedor. Ediciones Gestion 2000. Centro Libros PAPF, S. L. U., 2013

117 Consultado en https://dictionary.cambridge.org/es/diccionario/ingles/start-up?q=startup, el día 26 de mayo de 2019.

118 Montoya, D. Startups: tendencias en America Latina y su potencialidad para el crecimiento empresarial. Universidad de Gran Colombia. 2015.

119 Los párrafos anteriores nos permiten tener una serie de características que deben portar las Startups que en términos generales envistamos no sin antes mencionar que es enunciativa, más no limitativa, por lo que podemos resumir en: Ideas innovadoras; Rápido servicio; Fácil de evolucionar; Generalmente apuestan por proyectos relacionados con la tecnología.

La creación de las startup ha generado diversas empresas que en la actualidad son populares y muy utilizadas como en el caso de Facebook, Amazon, Google, Privalia, Edreams, por mencionar algunas. Estas empresas se han valido de costos de inicio más bajos que para otros negocios de índole tradicional, esto limita las necesidades de financiamiento y ayuda a que a bajo costo se pueda crear la empresa. Lo anterior ha hecho creer a expertos en la economía que estas empresas se denominen como una "nueva economía" esto derivado de que exista la evolución de una economía basada en los progresos tecnológicos principalmente con ayuda los las TIC.

Por lo anterior es que diversos organismos nacionales e internacionales se han interesado en dicho segmento en especial los países miembros de la OCDE pues según CEPAL en 2013 se marcó una clara diferencia entre la economía de los países misma que tuvo influencia de estas Startup

Lo cual se ve marcado en el Estudio Económico citado con antelación ya que en dicho año la creación y desarrollo de dichas empresas no se sentía propio en los países de América Latina. Sin embargo, en 2016 podemos apreciar que se sumaron esfuerzos para la creación de estas empresas y se cuenta con un "32% de startups en México dividido en 10% CD.MX., 8% en Guadalajara y 8% en Monterrey. Pero otros países del continente también ha dado paso a ellas, tal es el ejemplo de Chile con un 80%, también Brasil cuenta con 60% en São Paulo y 12% en Río de Janeiro" OCDE. Estudios del Centro de Desarrollo Startup América Latina 2016 Construyendo un futuro innovador. Síntesis y recomendaciones de política. OCDE. 2016.

5. EVOLUCIÓN DE STARTUP A FINTECH

Una empresa Startup deja de serlo para convertirse en parte del sector Fintech. lo anterior ocurre como consecuencia de varios factores que comienzan a ocurrir: la cotización en bolsa, competencia en el mercado sobre el producto que se ofrece al público, deja de ser independiente sino que en la mayoría de los casos es adquirida por una empresa.

Pero la lista no termina ahí derivado de la gran cantidad de Startups que se han convertido a Fintech como la empresa Irlandesa Sedicii que se ha encargado de generar un sistema para verificar la identidad de los usuarios, además su sistema previene el robo de identidad; pero también tenemos otras que con base en una red global ayuda a las empresas en tiempo real a fin de poder ofrecer financiamiento a los clientes.

6. ¿QUÉ ES UNA FINTECH?

Una vez comprendidos los términos anteriores es de vital importancia definir lo que es una Fintech, para lo cual nos apoyamos en el Buró de entidades financieras "Fintech deriva de las palabras "financial technology" y se utiliza para denominar a las empresas que ofrecen productos financieros, haciendo uso de tecnologías de la información y comunicación, como páginas de internet, redes sociales y aplicaciones para celulares"[120].

Estas instituciones de tecnología financiera han aprovechado la innovación tecnológica y, la mayoría, su incorporación a grandes compañías a fin de desarrollar diversos productos y servicios que van desde la gestión de materia, ofrecimiento de seguridad financiera e incluso monederos digitales, los cuales muchas veces se acompañan de un asesoramiento online.

Las Fintech se muestran en nuestra vida diaria en forma de páginas web, aplicaciones para Smartphones o por medio de métodos que van de la mano con la tecnología, lo anterior con ayuda de los bajos costos que manejan y aprovechando en todo momento la tecnología que tienen a su alcance, situación que incluso implementaron como una ventaja aunado a lo amigables que son sus servicios que a contrario de los bancos han sabido aprovechar para ganar más terreno en los negocios y la economía.

---

120 CONDUSEF. ¿Qué son las Fintech?. Consultado en https://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/educacion-financiera/763-que-son-las-finte . En 28 de mayo de 2019.

7. CARACTERÍSTICAS

Las Fintech poseen ciertas particularidades:

- Bajo costo;
- Financiamiento por diversos métodos de capital que incluso incluyen el de riesgos;
- Información digitalizada;
- Desafíos al sector bancario;
- Productos únicos e innovadores;
- Generalmente no se acude a ninguna sucursal;
- Se componen por personas dispuestas a prestar su dinero a cambio de cierto rendimiento económico.

Estas entidades mediante las características planteadas resultan ser novedosas y en lo general atrapan a jóvenes que en su mayoría son el Target de estas empresas, esto pues son las personas que regularmente se encuentran más cerca de los proyectos tecnológicos que ofrecen con su innovación y trascendencia de servicio.

8. SERVICIOS OFRECIDOS

Si bien es cierto que las Fintech se han caracterizado por realizar préstamos a cambio de cierto monto de rendimiento, también lo es que han sabido ampliar más allá el mercado meta a fin de ofrecer distintos tipos de servicios, de esta forma su crecimiento se ha visto favorecido.

Lo anterior ha tenido como consecuencia que las Fintech se agrupen en distintos campos de especialización, lo cual ha beneficiado a que distintos segmentos que no han sido explotados o que han quedado atendidos de forma parcial, se vean beneficiado, sin embargo, esto también representa riesgo financiero pues su situación no necesariamente será encontrada por las estadísticas que reflejen los sistemas financieros; esto de forma independiente sobre ciertas conductas delictivas que deriven de ellas como el lavado de dinero.

9. EL ACIERTO DE REGULAR LAS FINTECH

Como consecuencia de los servicios que presta una Fintech, está obligada a:

1. Establecer medidas y procedimientos para prevenir y detectar actos, omisiones u operaciones que pudieran ubicarse en los supuestos previstos en el Capítulo II del Título Vigésimo Tercero del Código Penal Federal.

2. identificar a sus clientes y usuarios; de conformidad con lo establecido por los artículos 115 de la Ley de Instituciones de Crédito; 87-D, 95 y 95 Bis de la Ley General de Organizaciones y Actividades Auxiliares del Crédito.
3. Presentar ante la Secretaría los reportes sobre actos, operaciones y servicios que realicen con sus clientes y lleven a cabo funcionarios y empleados de la propia entidad.
4. Entregar a la Secretaría de Hacienda y Crédito Público, por conducto del órgano desconcentrado competente, información y documentación relacionada con los actos, operaciones y servicios a que se refiere este artículo.
5. Conservar, por al menos 10 años, la información y documentación relativas a la identificación de sus clientes y usuarios o quienes lo hayan sido, así como la de aquellos actos, operaciones y servicios reportados.
6. Prohibición de uso de efectivo en las actividades vulnerables en caso de actualizar determinados montos, el cual dependerá de la actividad a realizar.

La supervisión, verifica ión y vigilancia del cumplimiento de las obligaciones a que se refiere esta Sección y las disposiciones de las leyes que especialmente regulen a las Entidades Financieras se llevarán a cabo, según corresponda, por la Comisión Nacional Bancaria y de Valores, la Comisión Nacional de Seguros y Fianzas, la Comisión Nacional del Sistema de Ahorro para el Retiro o el Servicio de Administración Tributaria.

Como es sabido, la actividad realizada por estas empresas se ha dado de forma posterior a que las mismas se vieran implementadas y en operaciones, está deficiencia se ha visto en varios países no sólo de América sino de todo el mundo; y como consecuencia se han tenido que regular sus actividades para no afectar al sistema de pagos, al sector económico, la competencia entre empresas e incluso a los consumidores[121].

El beneficio que ha existido al crear la regulación de las Fintech consiste en poder seguir cuidando la solidez de las instituciones que se tienen en el país pues como ya se había tocado el tema, existen múltiples beneficios que estas empresas han ofrecido al contrario de otras como los sistemas bancarios que se han quedado rezagados cuando el tema de la tecnología ha entrado en acción; a su vez se ha dado la posibilidad de seguir dando crecimiento a estos temas de innovación sin dejarlos de lado como ocurrió antes de su regulación cuando se fue creando las normas después de que las acciones fueron visualizadas.

121 El país pionero en la regulación de las Fintech es Reino Unido quien en 2014 creó la Financial Conduct Authority y misma que dedicó a las empresas que habían obtenido su capital de inversionistas y estos requerían sus ganancias. Así comenzó a otorgar permisos y planes para los casos de quiebra, hasta 2017 en donde aumentó los requisitos, sin embargo, también otorgó un periodo de prueba para las empresas a fin de que su terminación no terminará con sus activos. FUNDEF. La evolución del Sector Fintech, Modelos de Negocio, Regulación y Retos. FUNDEF. México. 2017.

10. LA REGULACIÓN EN LAS FINTECH MÉXICO

Como un acierto se toma que México sea de los primeros dos países en América Latina junto con Brasil en apoyar el desarrollo de las Fintech, pues según Fintech en América Latina 2018: crecimiento y consolidación en 2018 "Brasil aporta 380 emprendimientos de esta categoría mientras que México 273".[122] En razón de lo anterior, es por lo que México logró consolidar aquellas iniciativas en materia de regulación de las Fintech siendo así uno de los pocos países que contemplan una ley para la materia.

La legislación a la que hacemos referencia es la Ley para Regular las Instituciones de Tecnología Financiera misma que contempla la innovación y estabilidad financiera, la sana competencia entre las empresas de esta índole, la protección a los consumidores y además, la prevención del delito de Operaciones con recursos de procedencia ilícita.

Dentro de esta legislación se contemplan diversos términos que ayudan a que una empresa no llegue a la quiebra de forma temprana por las implicaciones que esto conlleva, por ello se tiene un Sandbox que no es otra cosa que los Modelos Novedosos el cual permite que la empresa creada tenga un periodo de prueba a fin de no realizar ciertos trámites regulatorios pues existe la posibilidad que la empresa no tenga una vida duradera por lo que existe un comité que evalúa su plan de negocios.

Estas Instituciones de Tecnología Financiera, como lo denomina la ley sustantiva, las divide en dos tipos una de ellas como colectivas y las otras de fondo de pago electrónico, ambas deberán cumplir con las disposiciones de la CNBV quien tendrá un órgano especializado para asegurar que se cumplen las reglas impuestas en la norma, a su vez cuenta con las facultades de investigación inspección y revocación, sin embargo, no es la única autoridad que las rige en México pues también deben estar acordes a las autoridades financieras como Banxico, SCHP y Conduse .

A) Instituciones de financiamiento Colectivo

Son aquellas que realizan actividades con el fin de contactar a diversos sujetos con la finalidad de otorgarse financiamiento colectivo de deuda, capital y copropiedad o regalías, esto por medio de aplicaciones informáticas, interfaces, internet o cualquier medio de comunicación electrónica o digital. Estas instituciones actúan como mandatarias o comisionistas de sus clientes. Además se regulan las obligaciones que tendrán que cumplir, mismas que entre otras se encuentran dar a conocer los medios que utilicen para operar, analizar e informar posibles inversionistas, entregar recursos a los inversionistas. Incluso se muestran limitantes a su actividad como resulta

122 *Íbidem.*

asegurar retornos o rendimientos sobre la inversión o garantizar el resultado o éxito de las inversiones.

B) Instituciones de Fondos de Pago Electrónico

Son aquellas empresas que emiten, administran y transmiten fondos de pago automático de acuerdo a diversas aplicaciones informáticas, páginas de internet o medio de comunicación electrónico o digital.

La ley establece qué debemos considerar como fondos de pago electrónico y las facultades que tienen, pero a su vez las hipótesis en que podrán otorgar los créditos y préstamos. Por último tenemos las prohibiciones como lo es no otorgar rendimiento o beneficio monetario a los clientes por el saldo que se acumule o mantenga en un momento dado.

Pero, para los efectos de esta ponencia, resulta de especial interés la ingente cantidad de delitos que la ley de la materia ha establecido para las instituciones de tecnología financiera. A sabe :

Delitos para la Protección del Patrimonio de los Clientes de las ITF y de las Sociedades Autorizadas para operar con Modelos Novedosos

- A quien en forma indebida utilice, obtenga, transfiera o de cualquier otra forma, disponga de los recursos, fondos de pago electrónico o activos virtuales de los Clientes de las ITF, de las sociedades autorizadas para operar con Modelos Novedosos o de los recursos, fondos de pago electrónico o activos virtuales de éstas.[123]
- Quien se encuentre facultado para disponer de los recursos a cargo de una ITF o una sociedad, Entidad Financiera u otro sujeto supervisado por alguna Comisión Supervisora o por el Banco de México, autorizado para operar con Modelos Novedosos y no realice la devolución de éstos a sus clientes, estando obligado a hacerlo o se niegue sin causa justificada. [124]

123 Artículo 119.- A quien en forma indebida utilice, obtenga, transfiera o de cualquier otra forma, disponga de los recursos, fondos de pago electrónico o activos virtuales de los Clientes de las ITF, de las sociedades autorizadas para operar con Modelos Novedosos o de los recursos, fondos de pago electrónico o activos virtuales de éstas, será sancionado con prisión de tres a nueve años de prisión y multa de 5,000 a 150,000

UMA. Si quien realiza la conducta prevista en el párrafo anterior es accionista, socio, consejero, funcionario, directivo, administrador, empleado o proveedor de una ITF, de una sociedad autorizada para operar con Modelos Novedosos o es un tercero ajeno pero con acceso autorizado por éstas a sus propios sistemas, será sancionado con prisión de seis a dieciocho años y multa de 10,000 a 300,000 UMA.

124 Artículo 120.- Será sancionado con prisión de tres a nueve años y multa de 5,000 a

• Los accionistas, socios, consejeros, funcionarios, directivos, administradores, empleados o proveedores de una ITF o de una sociedad o Entidad Financiera u otro sujeto supervisado por alguna Comisión Supervisora o por el Banco de México, autorizado para operar con Modelos Novedosos, que desvíen los recursos, fondos de pago o activos virtuales de sus Clientes o de las propias ITF, para cualquier fin distinto al que se haya pactado [125]

• A quienes utilicen o divulguen la información financiera o confidencial de los Clientes para cualquier fin distinto al de la realización de las Operaciones, sin contar con autorización previa y expresa del Cliente.[126]

Delitos contra la adecuada operación de las ITF, o de las Empresas Autorizadas para operar con Modelos Novedosos

• Todo aquel que, habiendo sido removido o suspendido, por resolución firm de la CNBV, continúe desempeñando las funciones respecto de las cuales fue removido o suspendido o bien, ocupe un empleo, cargo o comisión, dentro del sistema financiero m xicano, a pesar de encontrarse suspendido para ello.[127]

• Lleve a cabo operaciones o actividades de las reservadas para las ITF o para las sociedades o Entidades Financieras u otros sujetos supervisados por alguna

150,000 UMA, quien se encuentre facultado para disponer de los recursos a cargo de una ITF o una sociedad, Entidad Financiera u otro sujeto supervisado por alguna Comisión Supervisora o por el Banco de México, autorizado para operar con Modelos Novedosos y no realice la devolución de éstos a sus clientes, estando obligado a hacerlo o se niegue sin causa justificada

125 Artículo 121.- Serán sancionados con prisión de tres a nueve años y multa de 5,000 a 150,000 UMA, los accionistas, socios, consejeros, funcionarios, directivos, administradores, empleados o proveedores de una ITF o de una sociedad o Entidad Financiera u otro sujeto supervisado por alguna Comisión Supervisora o por el Banco de México, autorizado para operar con Modelos Novedosos, que desvíen los recursos, fondos de pago o activos virtuales de sus Clientes o de las propias ITF, para cualquier fin distinto al que se haya pactado. Cuando el desvío contemplado en el párrafo anterior, tenga como consecuencia el quebranto o perjuicio de la ITF o de una sociedad o Entidad Financiera u otro sujeto supervisado por alguna Comisión Supervisora o por el Banco de México, autorizado para operar con Modelos Novedosos, se impondrán las siguientes sanciones: I. Cuando el monto del quebranto o perjuicio patrimonial, según corresponda, exceda de 2,200 UMA y no de 57,000 UMA; se sancionará con prisión de cuatro a diez años y multa de 7,000 a 170,000 UMA. II. Cuando el monto del quebranto o perjuicio patrimonial según corresponda, exceda de 57,000, pero no de 400,000 UMA, se sancionará con prisión de cinco a once años y multa de 9,000 a 200,000 UMA. III. Cuando el monto del quebranto o perjuicio patrimonial según corresponda, exceda de 400,000, UMA, se sancionará con prisión de seis a doce años y multa de 10,000 a 250,000 UMA.

126 **Artículo 122.-** Serán sancionados con prisión de dos a seis años y multa de 1,000 a 50,000 UMA, a quienes utilicen o divulguen la información financiera o confidencial de los Clientes para cualquier fin distinto al de la realización de las Operaciones, sin contar con autorización previa y expresa del Cliente.

127 **Artículo 123.-** Serán sancionados con prisión de dos a siete años y multa de 5,000 a 150,000 UMA todo aquel que, habiendo sido removido o suspendido, por resolución firme de la CNBV, en términos de lo previsto en el artículo 62 de esta Ley, continúe desempeñando las funciones respecto de las cuales fue removido o suspendido o bien, ocupe un empleo, cargo o comisión, dentro del sistema financiero m xicano, a pesar de encontrarse suspendido para ello.

Comisión Supervisora o por el Banco de México, autorizados para operar modelos novedosos, sin contar con la autorización prevista en esta Ley, y Habiendo sido autorizado para operar como ITF, realice actividades con activos virtuales o divisas, sin contar con la autorización a que se refiere el artículo 30 o bien, tratándose de instituciones de crédito, sin la autorización.[128]

• Quien para obtener la autorización para operar como ITF o con Modelos Novedosos o con activos virtuales, proporcione información falsa a la autoridad financiera que corresponda. [129]

• **A** quien proporcione a las Autoridades Financieras que correspondan, información falsa respecto de su situación contable, financiera, económica y jurídica, que le sea requerida en términos de esta Ley.[130]

• **A** quien por sí o a través de un tercero, difunda, publique o proporcione al público de la ITF o sociedad autorizada para operar con Modelos Novedosos, información falsa o alterada o que induzca al error.[131]

• **A** quien destruya, modifique total o parcialmente, los sistemas o registros contables o la documentación que dé origen a los asientos contables de una ITF o sociedad autorizada para operar con Modelos Novedosos, con anterioridad al vencimiento de los plazos legales de conservación.[132]

• A quien se ostente frente al público en general como una ITF o sociedad o Entidad Financiera u otro sujeto supervisado por alguna Comisión Supervisora

---

128 **Artículo 124.-** Será sancionado con pena de prisión de siete a quince años y multa de 5,000 a 150,000 UMA quien: **I.** Lleve a cabo operaciones o actividades de las reservadas para las ITF o para las sociedades o Entidades Financieras u otros sujetos supervisados por alguna Comisión Supervisora o por el Banco de México, autorizados para operar modelos novedosos, sin contar con la autorización prevista en esta Ley, y **II.**Habiendo sido autorizado para operar como ITF, realice actividades con activos virtuales o divisas, sin contar con la autorización a que se refiere el artículo 30 o bien, tratándose de instituciones de crédito, sin la autorización a que alude el artículo 88.

129 **Artículo 125.-** Será sancionado con pena de prisión de siete a quince años y multa de 5,000 a 150,000 UMA quien para obtener la autorización para operar como ITF o con Modelos Novedosos o con activos virtuales, proporcione información falsa a la autoridad financiera que corresponda.

130 **Artículo 126.-** Serán sancionados con prisión de dos a diez años y multa de 5,000 a 150,000 UMA a quien proporcione a las Autoridades Financieras que correspondan, información falsa respecto de su situación contable, financiera, económica y jurídica, que le sea requerida en términos de esta Ley.

131 **Artículo 127.-** Serán sancionados con prisión de dos a diez años y multa de 5,000 a 150,000 UMA a quien por sí o a través de un tercero, difunda, publique o proporcione al público de la ITF o sociedad autorizada para operar con Modelos Novedosos, información falsa o alterada o que induzca al error.

La misma sanción resultará aplicable a los solicitantes de financiamiento colectivo o a los miembros del consejo de administración, directivos, funcionarios o empleados de dichos solicitantes, que se ubiquen en el supuesto del párrafo anterior al proporcionar información falsa o que induzca al error a la ITF o sociedad autorizada para operar con Modelos Novedosos.

132 **Artículo 128.-** Serán sancionados con prisión de dos a diez años y multa de 5,000 a 150,000 UMA a quien destruya, modifique total o parcialmente, los sistemas o registros contables o la documentación que dé origen a los asientos contables de una ITF o sociedad autorizada para operar con Modelos Novedosos, con anterioridad al vencimiento de los plazos legales de conservación.

o por el Banco de México, autorizado para operar con Modelos Novedosos.[133]

Delitos para la Protección del Patrimonio de las ITF y de las Sociedades Autorizadas para operar con Modelos Novedosos

• **A** quien valiéndose de cualquier medio físico, documental, electrónico, óptico, magnético, sonoro, audiovisual, informático o de cualquier otra clase de tecnología, suplante la identidad, representación o personalidad de cualquiera de las Autoridades Financieras o de alguna de sus unidades administrativas o áreas o de un servidor público, de las ITF o sociedades autorizadas para operar con Modelos Novedosos o de alguno de sus directivos, consejeros, empleados, funcionarios, dependientes o representantes legales.[134]

• **A** quien utilice, realice u obtenga, por sí o a través de interpósita persona, cualquier servicio, Operación o producto proporcionado por alguna de las ITF o sociedad o Entidad Financiera u otro sujeto supervisado por alguna Comisión Supervisora o por el Banco de México, autorizado para operar con Modelos Novedosos previstas en esta Ley bajo una identidad falsa o suplantada.[135]

Artículo 132.- Se sancionará con prisión de tres a nueve años y multa de 5,000 a 150,000 UMA, al que sin causa legítima o sin consentimiento de quien esté facultado para ello, acceda a los equipos o medios electrónicos, ópticos, informáticos o de cualquier otra tecnología de las ITF o sociedades autorizadas para operar con Modelos Novedosos.

• Al que sin autorización obtenga, extraiga o desvíe recursos, fondos de pago electrónicos o activos virtuales por medio de los sistemas o equipos de informática de las ITF o de las sociedades o Entidades Financieras u otros

133 **Artículo 129.-** Será sancionado con prisión de uno a seis años, y multa de 5,000 a 150,000 UMA a quien se ostente frente al público en general como una ITF o sociedad o Entidad Financiera u otro sujeto supervisado por alguna Comisión Supervisora o por el Banco de México, autorizado para operar con Modelos Novedosos en términos de esta Ley, sin contar con la autorización que corresponda.

134 **Artículo 130.-** Se sancionará con prisión de tres a nueve años y multa de 5,000 a 150,000 UMA, a quien valiéndose de cualquier medio físico, documental, electrónico, óptico, magnético, sonoro, audiovisual, informático o de cualquier otra clase de tecnología, suplante la identidad, representación o personalidad de cualquiera de las Autoridades Financieras o de alguna de sus unidades administrativas o áreas o de un servidor público, de las ITF o sociedades autorizadas para operar con Modelos Novedosos o de alguno de sus directivos, consejeros, empleados, funcionarios, dependientes o representantes legales.

A quien lleve a cabo el supuesto delictivo previsto en el párrafo anterior y obtenga un beneficio para sí o para un tercero, será sancionado con prisión de seis a doce años y multa de 10,000 a 250,000 UMA.

135 **Artículo 131.-** Se sancionará con prisión de tres a nueve años y multa de 5,000 a 150,000 UMA, a quien utilice, realice u obtenga, por sí o a través de interpósita persona, cualquier servicio, Operación o producto proporcionado por alguna de las ITF o sociedad o Entidad Financiera u otro sujeto supervisado por alguna Comisión Supervisora o por el Banco de México, autorizado para operar con Modelos Novedosos previstas en esta Ley bajo una identidad falsa o suplantada.

sujetos supervisados por alguna Comisión Supervisora o por el Banco de México, autorizados para operar con Modelos Novedosos[136].

Este nuevo catálogo de delitos especiales, debe observarse de manera conjunta con la legislación establecida para combatir las operaciones con recursos de procedencia ilícita. Con lo que, lejos de considerar que se ha cubierto adecuadamente el problema, podemos considerar que se ha abierto un veradero berenjenal para acreditar adecuadamente alguna de estas actividades.

11. CONCLUSIONES

Las Fintech, a la par de las nuevas tecnologías, vinieron a cambiar de manera toral el mercado al que sirven. Dieron una nueva faz a la empresa, tal y como la conocimos apenas hace algunos años.

Pero, de manera proporcional a la novedad de estas empresas, la utilidad que potencialmente pudieran tener para el blanqueo de capitales, el flujo de activos y el financiamiento de actividades ilícitas, reviste el mayor interés para conocer su funcionamiento y contar con mecanismos de supervisión.

Al respecto se han creado leyes particulares para abarcar estos aspectos, prevenir el delito y sancionar el mismo acorde con una legislación que esté al día en la materia. Sin embargo, estamos ante el cambio emergente de las distintas actividades y procesos que abarcan, de modo tal que, en los años por venir, habrán de pasar por el tamiz de la eficacia del derecho o, de lo contrario, estaremos en presencia de un problema mayor: el flujo impune de activos virtuales.

Creemos que lejos de considerar que se ha cubierto adecuadamente el problema, podemos considerar que se ha abierto un veradero berenjenal para acreditar adecuadamente alguna de estas actividades. La taxatividad será el tema ante los

136 **Artículo 133.-** Al que sin autorización obtenga, extraiga o desvíe recursos, fondos de pago electrónicos o activos virtuales por medio de los sistemas o equipos de informática de las ITF o de las sociedades o Entidades Financieras u otros sujetos supervisados por alguna Comisión Supervisora o por el Banco de México, autorizados para operar con Modelos Novedosos, se le impondrán las siguientes sanciones:

I. Cuando el monto de los recursos o el valor de los fondos de pago electrónicos o activos virtuales en el momento en que se cometa la conducta a que se refiere el presente artículo, según corresponda, exceda de 2,200 y no de 57,000 UMA; se sancionará con prisión de cuatro a diez años y multa de 7,000 a 170,000 UMA.

II. Cuando el monto de los recursos o el valor de los fondos de pago electrónicos o activos virtuales en el momento en que se cometa la conducta a que se refiere el presente artículo, según corresponda, exceda de 57,000, pero no de 400,000 UMA, se sancionará con prisión de cinco a once años y multa de 9,000 a 200,000 UMA.

III. Cuando el monto de los recursos o el valor de los fondos de pago electrónicos o activos virtuales en el momento en que se cometa la conducta a que se refiere el presente artículo, según corresponda, exceda de 400,000 UMA, se sancionará con prisión de seis a doce años y multa de 10,000 a 250,000 UMA.

tribunales encargados de validar los tipos penales a la luz del principio constitucional de exacta aplicación de la ley.

Pronto sabremos si la misma está a la altura de los retos que representa este sector finaciero y tecnológico.

12. BIBLIOGRAFÍA

Daza Gómez, Carlos, *Teoría General del Delito*, 2ª reimpresión, Cárdenas Editor, México, 2001.

Díaz Aranda, Enrique, *Teoría del Delito,* Straf, México, 2006.

Flores García, Fernando, *La responsabilidad penal de la persona jurídica colectiva* en *Ensayos jurídicos*, Facultad de Derecho (Cincuentenario de la Revista de la Facultad de Derecho de México), UNAM, 1989.

FUNDEF, *La evolución del Sector Fintech, Modelos de Negocio, Regulación y Retos*, FUNDEF, México, 2017.

Jiménez Huerta, Mariano, *Derecho Penal Mexicano*, Tomo I, 6ª ed., Porrúa, México, 2000.

Malo Camacho, Gustavo, *Derecho Penal Mexicano*, 3ª. ed., Porrúa, México, 2000.

Pavón Vasconcelos, Francisco, *Delitos contra el patrimonio*, Porrúa, México, 2005.

Zamora Pierce, Jesús, *Delitos Patrimoniales*, Porrúa, México, 2007.

Código Nacional de Procedimientos Penales

Convención de las Naciones Unidas Contra la Corrupción

Convención de las Naciones Unidas Contra la Delincuencia Organizada Transnacional

Ley para Regular las Instituciones de Tecnología Financiera

VALORACIÓN CRÍTICA DE PROMETEA, A LA LUZ DE LA FILOSOFÍA DE LA MENTE DE JOHN SEARLE

Eje temático: Inteligencia Artificial: riesgos y desafíos jurídicos

Autor:
Manuel Leonardo Prada Rodríguez
teólogo, magíster en filosofía latinoamericana y candidato a doctor en filosofí
Universidad Santo Tomás – Sede Villavicencio.

RESUMEN
La Corte Constitucional de Colombia está implementando una inteligencia artificial llamada Prometea, para hacer más expedito y preciso el proceso de revisión de fallos de tutelas relativas al sistema colombiano de salud. Debido a que diariamente se interponen, en promedio, 2700 sentencias, es de esperar que Prometea ayude a los jueces a descongestionar su trabajo. En otras palabras, los problemas legales relativos a la salud de muchos colombianos están siendo puestos en manos de una tecnología, motivo por el cual es pertinente refl xionar acerca de si ella es semejante a la inteligencia de un humano o si se trata de una inteligencia incompleta, en la que no es conveniente confiar a ciegas todavía
Para responder si Prometea es totalmente confiable o no, que es la pregunta problema que orienta esta ponencia, se explica en primer lugar en qué consiste dicha inteligencia artificial.
En segundo lugar, se expone la filosofía de la mente de John Searle, haciendo una breve alusión a la noología de Xavier Zubiri. Del pensamiento searleano se puede deducir que una inteligencia artificial no tiene intencionalidad original, sino derivada. La intencionalidad original corresponde exclusivamente al ser humano que la impone en la inteligencia artificial, tal como la impone en las letras que conforman palabras organizadas sintácticamente en oraciones. O sea, el ser humano tiene semántica, producto de su intencionalidad biológica, mientras que la inteligencia artificial sólo tiene sintaxis, tal como Searle lo explica con el experimento mental denominado por él como *Caja china*. Con dicho experimento, Searle contra-argumenta la postura de Alan Turing, matemático para el que se puede afirmar que los computadores piensan cuando sostienen una conversación con una persona, haciéndole creer que el que dialoga es otro ser humano, mas no una máquina. Así, del pensamiento searleano se puede derivar que las inteligencias artificiales pueden organizar datos, mas no imponer intencionalidad en ellos, por lo cual están incapacitadas para darles significado.
En tercer lugar, a partir del pensamiento searleano se concluye que Prometea no es en sentido estricto una inteligencia completa, semejante a una inteligencia humana, por cuanto es incapaz de imponer intencionalidad en las tutelas que evalúa. De ahí que no se considere pertinente delegar a una inteligencia no humana la función de seleccionar las sentencias más relevantes entre millares de acciones de tutela interpuestas por colombianos esperanzados en que sus problemas de salud por fin serán atendidos adecuadamente. Prometea no puede entender empáticamente a las personas que necesitan urgentemente que su sistema de salud funcione bien, por cuanto dicha inteligencia artificial no tiene capacidad biológica de imponer intencionalidad en las letras de las tutelas que lee a gran velocidad y que selecciona siguiendo unos criterios meramente sintácticos, mas no semánticos. Por dicha razón, es necesario considerar a Prometea como una herramienta tecnológica útil para que los jueces decidan cuáles tutelas son prioritarias, mas no como un juez artificial que puede reemplazar las labores de sus colegas humanos, que es hacia donde tiende esta tecnología aplicada al ámbito jurídico.

1. ¿QUÉ ES PROMETEA?

Prometea es: "un proyecto de la Facultad de Jurisprudencia de la Universidad del Rosario, el Laboratorio de Inteligencia Artificial (IA) de la Universidad de Buenos Aires, el Ministerio Público Fiscal de Buenos Aires y la Corte Constitucional de Colombia" (Peña, 2019). Este programa es una inteligencia artificial que puede leer tutelas y preseleccionar las que son prioritarias en poco tiempo, antes de transferirlas al supremo juez constitucional. En otras palabras, dicha inteligencia artificial: "es capaz de leer, analizar, detectar y sugerir los casos más prioritarios y urgentes a tratar en materia de salud. Para ello, es capaz de leer miles de sentencias que provienen de más de 4.000 jueces de todo el país" (Rivadeneria, 2019). Para realizar la selección de tutelas, Prometea sigue los criterios que: "el alto tribunal ha establecido en sentencias anteriores y los establecidos por la Constitución Política. También tiene en cuenta la Ley 1751 de 2015, que regula el derecho fundamental a la salud, y la Ley 1384 de 2010, que establece las acciones para la atención integral del cáncer en el país" (El Espectador, 2019). Es importante aclarar que:

> PROMETEA es un sistema tecnológico que busca ayudar al juez constitucional, mediante el manejo estadístico de bases de datos e información, a facilitar la toma de decisiones, sin condicionarlas. Es decir, PROMETEA no toma decisiones por el juez, al contrario, es él, quien, apoyándose en la herramienta, toma las decisiones pertinentes. (...) El sistema lee de manera automática sentencias de anteriores instancias, y selecciona los casos prioritarios. En este análisis semántico y gramatical, PROMETEA detecta las principales causas y circunstancias específicas de cada caso, las cuales determinan si el caso debe recibir respuesta rápida y eficaz o no, dependiendo de la afectación del derecho (Universidad de Los Andes, 2019).

Finalmente, el nombre de esta inteligencia artificial tiene que ver con Prometeo, uno de los titanes más inteligentes de su época que, de acuerdo a la mitología griega, robó el fuego, símbolo de la técnica, a Hefestos. Según Juan Gustavo Corvalán, fiscal general adjunto en lo Contencioso Administrativo y Tributario del Ministerio Público Fiscal y codirector del Laboratorio de Innovación e Inteligencia Artificial de la Universidad de Buenos Aires: "Nosotros, como este es el siglo de las mujeres, quisimos reivindicarlas cambiando el nombre a Prometea" (Murgo, 2019).

2. ¿QUÉ ES UNA INTELIGENCIA, SEGÚN LA FILOSOFIA DE LA MENTE DE JOHN SEARLE?

En su primera etapa de pensamiento, representada por el texto: Speech Acts: An essay in the Philosophy of language (1969), John Searle afirma que el significado de un enunciado puede ser explicado mediante convenciones regladas por una

comunidad lingüística. Por eso, él investiga el lado no formal (giro pragmático) de la filosofía analítica (giro lingüístico), enfatizando en los actos de habla que se dan en la cotidianidad, y profundiza en los actos ilocutivos, propuestos por John Austin, que se dan en los enunciados performativos, o sea, actos que son llevados a cabo con expresiones del lenguaje ordinario, de tal manera que un mismo contenido proposicional puede tener diversas fuerzas ilocutivas. Así, un mismo contenido proposicional puede manifestarse en una aseveración, una pregunta o una orden (Searle, 1994, p. 31):

> No hay, por lo tanto, dos estudios semánticos distintos e irreductibles: por un lado un estudio de los significados de oraciones y por otro un estudio de las realizaciones de los actos de habla. Pues de la misma manera que forma parte de nuestra noción del significado de una oración el que una emisión literal de esa oración con ese significado en un cierto contexto constituya la realización de un acto de habla particular, así también forma parte de nuestra noción de acto de habla el que exista una oración (u oraciones) posibles, la emisión de las cuales, en cierto contexto, constituiría en virtud de su (o sus) significado(s) una realización de ese acto de habla (Searle, 1994, p. 27).

No obstante, desde que escribió su libro: Intentionality: An essay in the Philosophy of Mind (1983), Searle no considera que el significado dependa sólo de la convención hecha por una comunidad lingüística, sino también de la intencionalidad –esa capacidad de la mente para referirse a los estados de cosas que están afuera de ella, en el mundo–, que es un fenómeno biológico cuyas formas primitivas no son lingüísticas, tal como lo propone la tradición analítica, sino pre-lingüísticas (Searle, 1985, p. 85). Las formas primitivas tienen estructura lógica y se desarrollan hasta el punto de imponerse sobre entidades que no son intencionales.

Cuando se está realizando un acto de habla, la mente impone intencionalmente en la expresión física (sonidos o marcas, por ejemplo) las condiciones de satisfacción del estado mental que dicha expresión representa, ya que el significado del lenguaje es intencionalidad derivada y tiene que ser derivada de la intencionalidad original de la mente. Por eso, los estados intencionales (creencias, deseos, intenciones, entre otros) son propicios para explicar el significado de los actos de habla. Con base en lo anterior, es posible decir que Searle une al giro pragmático con la filosofía de la mente, a la que considera como filosofía primera:

> Para Searle (1983), la filosofía del lenguaje es una rama de la filosofía de la mente. El argumento es, más o menos, que puesto que el lenguaje es la expresión del pensamiento, nuestras teorías acerca de la naturaleza de la mente determinarán nuestra filosofía del lenguaje. Ahora bien, la trayectoria del propio Searle no ha sido precisamente ésa, sino incluso la contraria: sólo tras elaborar una teoría del lenguaje ha pasado a ambicionar la invasión del territorio mental (Rodríguez, 2003, p. 60).

En en el marco de las observaciones anteriores, aunque la mente, según Searle, hace parte de la realidad porque emerge (macro-nivel) de las relaciones sinápticas del cerebro (micro-nivel), no se reduce ontológicamente a él (naturalismo biológico). Dicho de otra forma, a pesar de que la mente tiene causas físicas (el cerebro), sus características ontológicas son independientes e inmateriales, por lo cual la postura searleana ha sido considerada como un dualismo biológio (Arias, 2013, p. 188), a pesar de que el propósito de Searle es, precisamente, evitar el dualismo cartesiano.

Según Searle, la mente humana impone intencionalidad en las cosas, que no son intencionales. La intencionalidad, que es: "aquella característica de la mente mediante la cual los estados mentales se dirigen a, o tratan de, o se refieren a, o apuntan a estados de cosas en el mundo… no es preciso que el objeto exista" (Searle, 2001, pp. 65-66), tiene la capacidad de personificar los aparatos tecnológicos como si en verdad fueran humanos y también tuvieran intencionalidad. Pero, dado que Searle no considera que las cosas tenga intencionalidad original, elabora su argumento conocido como la caja china contra la inteligencia artificial fuerte y el est de Turing.

En su texto: Computing Machinery and Intelligence, el matemático Alan Turing propone un test para saber si una máquina piensa o no como los seres humanos (1950, p. 433), en el que hay dos personas y una máquina diseñada para generar respuestas similares a las de un ser humano. Una persona, que no puede ver ni a la máquina ni a la otra persona, elabora preguntas, con el fin de saber cuál de las dos entidades es la humana y cuál es la máquina. Si después de cinco minutos de conversación textual la máquina sigue "engañando" al interrogador, "haciéndole creer" que ella es humana, entonces eso significa que ella piensa[137]. Cuando se lleva a cabo el juego de la imitación, la mejor estrategia para la máquina es, posiblemente, algo diferente a la imitación del comportamiento de un hombre (Turing, 1997, p. 31).

Para contrarrestar tanto la propuesta de Touring de que la máquina puede pensar como la analogía de que el *hardware* es al *software* lo que el cerebro es a la mente, Searle, en su segunda etapa de pensamiento, sostiene la tesis de que la mente es algo más que la manipulación sintáctica de símbolos formales que cualquiera puede hacer. Pensar también conlleva semántica (relaciones entre los símbolos que tienen significado, esto es, contenido), de la cual carecen las máquinas, por cuanto tampoco tienen intencionalidad, sino sólo sintaxis (relaciones de orden entre los símbolos):

> Porque las manipulaciones de símbolos formales por sí mismas carecen de intencionalidad; son bastante carentes de sentido; ni siquiera son manipulaciones de símbolos, ya que los símbolos no simbolizan nada. En la jerga lingüística, sólo tienen sintaxis pero no semántica. La intencionalidad que parecen tener las computadoras sólo está en las mentes de quienes las pro-

137 De hecho, ya existe una máquina que perfectamente "podría engañar" a un ser humano. Se trata de: *Project Debater*, un sistema de inteligencia artificial (IA) que puede debatir sobre temas complejos con personas.

> graman y de quienes las usan: los que envían la información de entrada y los que interpretan la información de salida (Boden, 1990, p. 98).

En este asunto hay una posible relación entre el pensamiento searleano y el zubiriano, tal como se ve en la siguiente explicación de González:

> El *logos* no es lo mismo que la inteligencia. De hecho, una computadora puede realizar operaciones lógicas, sin aprehender las cosas como realidades. Lo que se llama usualmente "inteligencia animal" o "inteligencia artificial" sería más bien, desde la terminología de Zubiri, algo así como un "*logos* animal" o un "*logos* artificial . Ciertas operaciones lógicas y lingüísticas se podrían desarrollar perfectamente sin "inteligencia", si por tal se entiende la aprehensión de las cosas como reales (2016, p. 434).

Por supuesto, los conceptos no son del todo equivalentes entre los de Zubiri y los de Searle, ya que, para este último, el computador no puede ser inteligente porque aunque tiene sintaxis –y en eso estaría de acuerdo con Zubiri–, no tiene semántica. En este punto, Zubiri no habla de la semántica impuesta por la intencionalidad, sino de lo esencial del ser humano que es aprehender las cosas como realidades, esto es, como diferentes a los actos del ser humano. No obsante, Zubiri sí considera que la captación de sentido –que se trata de un nivel estructuralmente ulterior a la aprehensión de la realidad– se debe a la intencionalidad. Lo que sí es claro en esta comparación es que las máquinas no tienen cómo razonar, tal como lo explicita González en la siguiente cita bibliográfica:

> En este planteamiento, difícilmente podría hablarse de una actividad racional que no transcurriera en la formalidad de realidad, pues precisamente la razón pretende sumergirse en la realidad ya aprehendida, para inteligir lo que las cosas son en el mundo, con independencia de su aprehensión. De ahí que, desde la filosofía de Zubiri, no habría propiamente racionalidad animal o racionalidad artific al. Los "razonamientos" que se produjeran en esos ámbitos serían más bien operaciones lógicas, y no propiamente racionales (p. 434).

Para Searle, las máquinas actúan sin comprender lo que hacen ni por qué lo hacen, lo cual las aleja de parecerse a los seres humanos, ya que la comprensión es clave para el pensamiento. En otros términos, aunque una máquina imite adecuadamente las respuestas que un ser humano da a las preguntas del interrogador, no hay indicios para considerarla como inteligente, como si ella tuviera mente, ya que sólo lleva a cabo las órdenes que le programaron de forma mecánica. Para demostrar que la semántica sólo corresponde a la intencionalidad humana, Searle inventa un experimento mental denominado por él como la caja china.

La caja china está diseñada como un cuarto en el que está un estadounidense que nunca ha estudiado chino, por lo cual no entiende los caracteres de dicho idioma. Para

saber si la caja china se comporta como un ser humano pensante o no, un interrogador chino inserta en una ranura un papel que tiene preguntas escritas en su idioma, con el fin de que la máquina las conteste. El estadounidense tiene un libro de instrucciones en inglés que le dice paso a paso cuáles símbolos chinos debe escribir ordenadamente en el papel, al cual deberá poner en otra ranura para contestar coherentemente las preguntas del interrogador. Al imitar bien una conversación escrita en chino, la máquina, esto es, el estadounidense pasa el test de Turing (Searle, 1980, pp. 417-418).

Pero, por superar la prueba, ¿la caja china es realmente semejante a un ser humano pensante?, ¿por qué afirmar de ella que es inteligente, si fue una persona dentro de ella la que llevó a cabo las instrucciones que estaban escritas en inglés y que daban a la máquina la apariencia de saber chino e interactuar como un humano en dicho idioma? Searle cuestiona la idea de Turing según la cual el comportamiento de la máquina es evidencia de su mente. Para él, "la única máquina que puede pensar es el cerebro" (Martínez, 2007, p. 168). Habrá que esperar a ver si dentro de unas décadas los computadores cuánticos comienzan a dar evidencias lingüísticas de su pensamiento, si es cierto que la mente emerge del cerebro o procede de algo distinto a dicho componente material. También habrá que ver si es posible fabricar máquinas pensantes que sean falibles en sus cálculos, es decir, que como los humanos a veces acierten y en otras ocasiones elijan errar, ya que hasta ahora las máquinas no pueden equivocarse por voluntad propia. Por ahora, sólo el ser humano es capaz de suspender el juicio.

Pero, ¿cómo es que la persona que está adentro de la caja china puede contestar las preguntas, si no sabe chino?, ¿es el manual el que sabe dicho idioma?, ¿es el sistema (la caja, la persona, el papel y las respuestas) el que conoce dicho idioma? La respuesta genera este dilema: o el sistema comprende chino o el test de Turing no sirve para probar la inteligencia, sino sólo el comportamiento (que no necesariamente es evidencia de lo que se piensa, como sí lo es el lenguaje). Así el sistema de la caja china pase dicho examen, no sirve para evaluar si el estadounidense que está adentro de ella sabe chino o no. En efecto, esa persona no conoce dicho idioma, por lo cual:

> La habitación china superaría la llamada "prueba de Turing", prueba que consiste en presuponer que un ordenador tiene las capacidades de una mente humana si es capaz de mantener conversaciones humanas, pero resultaría obvia la diferencia entre su manera de "entender" la conversación y la nuestra (Borrel, 2007, p. 90).

En fin, según Searle, si es cierto lo que afirma la inteligencia artificial fuerte (la mente es como el *software*), entonces cualquier máquina que pueda ejecutar el programa correspondiente al chino es inteligente porque entiende ese idioma (Santos, 2005, p. 48). Pero, cualquier persona que conozca bien su propio idioma puede

ejecutar el programa correspondiente al chino de forma mecánica, por causa de la traducción desde el chino a su idioma vernáculo, sin comprender ningún símbolo, y una máquina diseñada para operar con sintaxis puede hacer lo mismo. Por lo anterior, el sistema no entiende chino, sino que aparentemente lo entiende, o, más bien, el humano personifica a la máquina, como si esta última pudiera comprender ese idioma, razón por la cual la mente no es equivalente a un *software*, esto es, lo postulado por la inteligencia artificial fuerte es falso. De esta forma, Searle considera que las cosas no dirigen las actuaciones de los humanos, sino viceversa.

Si, por ejemplo, una persona va conduciendo un carro y comienza a frenar porque ve que a unos metros hay un policía acostado[138] u otra señal de tránsito que le indique disminiur la velocidad, Searle no considera que dicho objeto sea el que emane significado, sino que es la mente humana la que impone intencionalidad en él, entendiendo así que debe mermar la marcha del carro. La señal de tránsito en cuestión no tiene poder en sí misma para comunicar significados, sino que depende de la mente para lograrlo, o sea, su intencionalidad es derivada de la intencionalidad original de la mente de quien la diseñó y de la de quien la interpreta[139]. Así, una cosa jamás puede tener voluntad de dirigir las actuaciones de un humano.

Lo que acontece, según Searle, es una personificación por medio de la intencionalidad "como si", que se da cuando un humano atribuye características humanas a objetos no-humanos, tal como cuando afirma que el carro tiene sed, para referirse a que ya es hora de acudir a la estación de gasolina; cuando menciona que el computador está lento porque está pensando; para denotar el hecho de que el procesador se está haciendo obsoleto y la información se actualiza en las personas más lentamente que antes. A estas máquinas les da sed y piensan como si fueran humanas, debido a la imposición de intencionalidad original o primitiva de la mente humana sobre ellas (Searle, 2006, pp. 44-45). De esta manera, cuando se habla de inteligencia artificial, realmente se están personificando unos procesos sintácticos como si fueran semánticos.

3. ¿Es Prometea realmente una inteligencia?

A partir de la filosofía de la mente de Searle, se puede afirmar que Prometea no es una inteligencia, debido a que sólo tienen capacidad sintáctica, mas no semántica. Que dicho programa pueda leer muchas sentencias en poco tiempo no significa que

138 El policía acostado es un reductor de velocidad o banda de frenado, que también responde al nombre de lomo de burro, túmulo, rompemuelles, entre otros.

139 Esto, de alguna manera, implica "descajanegrización". La intencionalidad original del diseñador no aparece en la señal de tránsito, pero se presupone y Searle la saca a la luz.

las comprenda, ya que sólo es capaz de entablar relaciones planas entre las tutelas digitalizadas y las normas constitucionales de Colombia.

Lo anterior puede resultar inconveniente para muchos ciudadanos colombianos que interponen acciones de tutela para procurar la defensa de sus derechos concernientes a la salud, por cuanto la jerarquización que hace Prometea a la hora de preseleccionar las que son más relevantes puede dejar de lado sentencias que realmente son muy importantes. Así, por ejemplo, es posible que dicha máquina descarte una acción de tutela interpuesta por un ciudadano con sobrepeso excesivo, porque, según la normatividad sintáctica, una liposucción es una cirugía estética irrelevante si se la compara con una operación de cáncer de próstata. Es el ser humano el único que tiene capacidad para imponer intencionalidad en las letras de la acción de tutela que aboga por el ciudadano con sobrepeso, y es dicha capacidad la que puede salvar a ese ciudadano de un paro cardíaco inminente.

En relación con lo anterior, Prometea no ve a las tutelas ni a las personas que las interponen como realidades distintas a ella. Es decir, para Prometea sólo existen datos relacionables sintácticamente. Esta carencia de alteridad puede generar problemas a la hora de solucionar las tutelas, debido a que Prometea no tiene en cuenta emociones netamente humanas como la misericordia, relacionada con capacidades también propiamente humanas como la empatía. En otras palabras, los colombianos que sufren problemas legales con el sistema de salud al que están afiliados quedan a merced de una máquina que entabla relaciones lógicas, pero que no profundiza en la realidad, indagando por cuáles pueden ser las causas que hacen que una persona interponga una acción de tutela. Así, la jerarquización de tutelas responde más a unos parámetros meramente objetivos, lógicos, despersonalizados, que poco tienen que ver con la salud integral de una persona. Pero, dado que la salud no se restringe a un proceso fisiológico balanceado, sino que también involucra situaciones cotidianas, problemas laborales, estrés por la contaminación medioambiental, entre muchos otros factores, Prometea presenta serias limitaciones para preseleccionar los casos de salud relevantes a ser atendidos por los seres humanos.

En fin, Prometea es una herramienta virtual que, en tanto que *software*, puede ayudar a los integrantes de la Corte Constitucional de Colombia para agilizar sus tareas. Pero, debido a que dicha ayuda es netamente objetiva, lógica, mas no racional, por cuanto no percibe las cosas como reales, puede perjudicar a muchos colombianos cuyas acciones de tutela son subvaloradas por dicha máquina. De esta manera, en la Corte Constitucional se puede confundir el medio con el fin, generando más problemas en el sistema de salud que los que se pretende solucionar. Es decir, aunque Prometea no toma decisiones por el juez, el hecho de que de 2016 casos ella preseleccione 32 ya es una forma de seleccionar, de reemplazar al ser humano. Sin pretender cometer una falacia de abuso de analogía, esto es algo parecido a lo que pasa con los medios masivos

de comunicación, que en épocas preelectorales sólo entrevistan a los candidatos que, según ellos, tienen más opciones de ganar la presidencia o la alcaldía. Que de 10 candidatos el medio masivo de comunicación sólo entreviste a 3 es una forma de decidir de antemano por la gente. En este caso, tal vez Prometea diga que de 3000 tutelas diarias sólo 32 son pertinentes porque tienen que ver con cáncer. Pero, ¿cuál es el criterio de Prometea para considerar que dicha enfermedad es más prioritaria que otra enfermedad? Hay casos que sólo un humano, por su capacidad de imponer semántica y porque ve las cosas como reales, puede decidir.

REFERENCIAS BIBLIOGRÁFICAS

Arias, A. (2013). El problema de la conciencia en John R. Searle. ¿Naturalismo o dualismo biológico? ArtefaCToS. Revista de estudios sobre la ciencia y la tecnología, *6*(1), 181-200.

Boden, M. (1990). Filosofía de la inteligencia artificial. México: Fondo de Cultura Económica.

Borrel, C. (2007). El misterio de la habitación china y la filosofía de Zubiri. *The Xavier Zubiri Review*, *9*, 89-97.

El Espectador. (2019). Prometea, la nueva tecnología para selección de tutelas en la Corte Constitucional. https://www.elespectador.com/noticias/judicial/prometea-la-nueva-tecnologia-para-seleccion-de-tutelas-en-la-corte-constitucional-articulo-838034 [Fecha de consulta: 14 de julio de 2019]

González, A. (2016). La evolución humana en Zubiri. En Scocozza, A. y D'Angelo, G. (eds.), *Magister et discipuli: Filosofía, historia, política y cultura. Tomo 1*, pp. 425-448. Bogotá, Colombia: Editorial Penguin Random House.

Martínez, P. (2007). La importancia del conocimiento: filosofía y ciencias cognitivas. La Coruña: Netbiblo.

Murgo, E. (2019). Prometea, Inteligencia Artificial para agilizar la justicia. http://www.unidiversidad.com.ar/prometea-inteligencia-artificial-para-agilizar-la-justicia [Fecha de consulta: 14 de julio de 2019]

Peña, D. (2019). Promete Prometea! Inteligencia Artificial en la Corte Constitucional. https://dernegocios.uexternado.edu.co/comercio-electronico/promete-prometea-inteligencia-artificial-en-la-corte-constitucional [Fecha de consulta: 14 de julio de

2019].

Rivadeneira, J. (2019). Prometea, inteligencia artificial para la revisión de tutelas en la Corte Constitucional. https://www.ambitojuridico.com/noticias/informe/constitucional-y-derechos-humanos/prometea-inteligencia-artificial-para-l [Fecha de consulta: 14 de julio de 2019]

Rodríguez, F. (2003). La filosofía del lenguaje: su naturaleza y su contexto. *Diánoia, 48*(50), 41-68.

Santos, M. (2005). De la Habitación China al Laboratorio de I. A. Bajo palabra. Revista de Filosofía, 47 II Época, Nº 0, año 2005: 47-52.

Searle, J. (2006). La mente: una breve introducción. Bogotá: Grupo Editorial Norma.

Searle, J. (2001). Mente, lenguaje y sociedad. La filosofía en el mundo real. Madrid: Alianza Editorial.

Searle, J. (1994). Actos de habla: Ensayo de filo ofía del lenguaje. Barcelona, España: Planeta-Agostini.

Searle, J. (1985). Mentes, cerebros y ciencia. Madrid, España: Editorial Cátedra.

Searle, J. (1983). Intentionality. An essay in the philosophy of mind. Nueva York, Estados Unidos de América: Cambridge University Press.

Searle, J. (1980). Minds, brains and programs. *Behavioral and Brain Sciences, 3*(3), pp. 417-457.

Turing, A. (1997). Computing Machinery and Intelligence. En J. Haugeland (ed)., *Mind design II: Philosophy, psychology, and artificial intelligence* (29-56). Cambridge, Estados Unidos de América: The MIT Press.

Turing, A. (1950). Computing Machinery and Intelligence. *Mind, New Series, 59*(236), 433-460.

Universidad de Los Andes. (2019). Memorias Evento Herramientas digitales al servicio de la justicia en Colombia: el caso PROMETEA. https://gecti.uniandes.edu.co/images/pdf/PROMETEA_EVENTO.pdf [Fecha de consulta: 14 de julio de 2019]

REGULACIÓN DE LA INTELIGENCIA ARTIFICIAL Y LA PROTECCIÓN DE LOS DERECHOS FUNDAMENTALES EN LA CUARTA REVOLUCIÓN INDUSTRIAL

Eje temático: Inteligencia artificial: Riesgos y desafíos jurídico

Autora:
Lucana María Estévez Mendoza
Profesora Colaboradora Doctora de Derecho Procesal.
Universidad CEU San Pablo (Madrid- España)

RESUMEN
Actualmente, las nuevas tecnologías, entre ellas la inteligencia artificial como uno de sus exponentes máximos, alcanzan a múltiples ámbitos de la vida, incluido el derecho, empezando a emplearse en diversas tareas jurídicas, si bien más propias del ámbito privado. No obstante, el entorno del Derecho Penal y de la Ciencia Criminológica no escapa a esta tendencia, existiendo países que comienzan a utilizar sistemas de este tipo para prevenir, investigar y perseguir hechos delictivos.
De ahí que la relación existente entre su uso y el plano jurídico sea un tema de gran relevancia e interés, dado que, además, en un mundo globalizado y cada vez más tecnológico, los beneficios de emplear sistemas de *machine learning* y/o *forecasting behavior* se prevén enormes y esenciales en el corto plazo, si bien no son escasos los problemas legales que éstos conllevan.
Analizar las ventajas e inconvenientes que el uso de sistemas de inteligencia artificial conlleva, es el objetivo de esta comunicación. En concreto, el elemento esencial que constituye la hipótesis de trabajo es valorar dónde queda la protección de los derechos fundamentales cuando el campo del control delictivo y/o el ejercicio del *ius puniendi* queda en manos, al menos parcialmente, de instrumentos de IA. Ello hace necesario analizar la afectación que esta tecnología conlleva en relación a derechos como el de la vida y la integridad, la libertad de pensamiento y movimiento, la libertad de expresión e información o el derecho al honor y a la intimidad.

1. INTRODUCCION

La inteligencia artificial (IA) es el cambio más disruptivo de la historia, transformando hábitos, costumbres y creencias sociales[140]. No obstante, no faltan augurios de que podría suponer un riesgo para la existencia humana, postura defendida

140 ALBOR, J: "La IA, el cambio más disruptivo en la historia", *Revista Forbes, Portada,* 29 marzo 2019, https://www.forbes.com.mx/la-ia-el-cambio-mas-disruptivo-en-la-historia/

por científic s como Stephen Hawking o Elon Musk, quienes forman parte de las más de 1.200 personas que, en 2017, firmaron " os 23 principios de Asilomar"[141].

Sea como fuere, la IA se ha colado en nuestras vidas y está dispuesta a quedarse en ellas. Ante esta irrupción de las máquinas inteligentes, parece claro que el Derecho, como ciencia que interviene en los conflictos sociales, no puede permanecer al margen, dejando al arbitrio de las partes o colectivos que defienden parcialmente sus intereses, la resolución de los mismos, aunque lo puedan hacer de forma más o menos legítima.

Dado que el empleo de mecanismos basados en IA alcanza ya a múltiples ámbitos de la vida, se usa en diversas tareas jurídicas, no sólo del ámbito privado (jurimetría), sino también en el entorno del Derecho penal, como Derecho público y de la ciencia criminológica, existiendo países que comienzan a utilizar sistemas de este tipo para prevenir, investigar y perseguir hechos delictivos[142]. Por ello, se plantea la presente comunicación, con el objetivo de analizar el lugar que ocupan los derechos fundamentales en este contexto.

Por ello, especialmente relevantes son los principios de Asilomar relativos a la transparencia judicial, en el sentido de que la decisión resultante de un sistema inteligente debería ir acompañada de una explicación satisfactoria y entendible por la autoridad humana que deba valorarla (principio 8); el sistema de responsabilidades, que alcanza a diseñadores y desarrolladores informáticos (principio 9); la protección de los valores y derechos fundamentales de las personas (principio 13); y la búsqueda del bien común, más que el de un Estado en particular (principio 23).

2. LA CONCEPCIÓN ARTIFICIAL DE LA INTELIGENCIA

2.1. Aproximación terminológica a la inteligencia artificial

Para conceptualizar la IA, conviene acudir a los términos que la componen. La "inteligencia", del latín *intelligentia,* es entendida como la capacidad comprender, de resolver problemas, habilidad, destreza y experiencia, según el diccionario de la Real Academia Española de la Lengua. "Artifici l", del latín *artificialis*, es un adjetivo referido a lo producido por el ingenio humano, lo no natural, lo falso, lo hecho por arte o mano del hombre. Corolariamente, la IA es "la disciplina científica que se ocupa de

141 FERRER, S.: "Los 23 mandamientos para evitar que la inteligencia artificial nos domine", *El Confidencial*, 2 de febrero de 2017. Recuperado de https://www.elconfidencial.com/tecn -logia/2017-02-02/inteligencia-artificial-elon-musk-stephen-hawking-ia_132505 [Fecha de consulta: 24/06/2019]

142 Ver ESTÉVEZ MENDOZA, L.: "Prevención e investigación de delitos en España: ¿un nuevo terreno para la IA?", Comunicación presentada en el VIII Fórum de expertos y jóvenes investigadores en Derecho y Nuevas tecnologías, Universidad de Salamanca, 28 y 29 de marzo 2019 (pendiente de publicación).

crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico" (RAE).

La doctrina la define, de manera general, como el "término usado para referirse a cualquier software capaz de ejecutar una tarea normalmente asociada a un humano, al requerir de cierta inteligencia"[143] y, de manera específica, como "la combinación de algoritmos planteados con el propósito de crear máquinas que presenten las mismas capacidades que el ser humano"[144].

Si bien la IA nació en la década de los 50, gracias al trabajo de John McCarthy, que la definió como "la ciencia y la ingeniería de fabricar máquinas inteligentes, en especial máquinas inteligentes de computación"[145], no es hasta los albores del siglo XXI cuando la tecnología estuvo preparada para dotarla de las condiciones necesarias para su desarrollo. Fue entonces cuando lo que parecía ser un fenómeno de ciencia ficción traspasa las pantallas y se empieza a colar en la vida en sociedad.

2.2. El desarrollo tecnológico en el siglo XX y la aceleración de la cuarta revolución industrial

El desarrollo tecnológico acontecido durante el siglo XX ha sufrido vaivenes debido a las diferentes expectativas generadas por la IA desde su aparición y en el desarrollo de su corta vida como disciplina. Prueba de ello es la división producida en el campo de la ingeniería entre los defensores de la *strong AI* (IA fuerte o en sentido genérico), que pretende dotar a las máquinas de aspecto y razón humana y los de la *weak A*I (IA débil o en sentido específico) que buscan obtener, mediante algoritmos, resultados similares a los alcanzados por un humano, sin necesidad de que la máquina tenga aspecto humanoide.

En esta última faceta de la IA se incluyen los algoritmos de *maching learning* y *forecasting behaviour* (aprendizaje automático y predicción), cuyo desarrollo principal, a día de hoy, se basa en las redes neuronales, que llegan al punto de crear esquemas de aprendizaje automático más complejos, dando lugar al denominado *deep learning*.

Actualmente, los expertos hablan de que estamos viviendo la cuarta revolución industrial, con la incorporación del ciberespacio, las tecnologías de la información y, dentro de ellas, las conocidas como tecnologías emergentes, entre las que se encuentra

143 MORELL RAMOS, J.: "La Inteligencia Artificia en el día a día de un abogado: qué le va a enseñar y cómo lo cambiará", *Revista del Consejo General de la Abogacía Española nº 108,* Febrero 2018 (p.7)

144 IBERDROLA: "¿Qué es la Inteligencia Artifici l?.¿Somos conscientes de los retos y principales aplicaciones de la Inteligencia artificial?, *Iberdrola,* Te interesa, Tecnología, (p.2) *https://www.iberdrola.com/te-interesa/tecnologia/que-es-inteligencia-artificial*

145 ALANDETE, D. "John McCarthy, el arranque de la inteligencia artificial" *El País,* 27 de octubre de 2011. Recuperado de https://elpais.com/diario/2011/10/27/necrologicas/1319666402_850215.html

la IA, la sensorización de las ciudades (*smart cities*) y la industria 4.0 y el internet de las cosas (IoT), que apuesta por que todos los dispositivos electrónicos están constantemente conectados a internet.

Es patente que para llegar hasta aquí hemos pasado por diversas etapas[146]: La primera revolución industrial se debió a la incorporación de máquinas en el ámbito laboral (telares, barco de vapor, locomotora…), lo que supuso a un importante cambio en la estructura socioeconómica del momento, al tiempo que la aparición de nuevos tipos de relaciones jurídicas; la segunda aconteció con la aparición de la electricidad y la tercera convino con la irrupción de la electrónica y los primeros sistemas de información que han llegado hasta el momento actual[147], dando lugar a lo que se ha denominado, por algunos sectores doctrinales, como industria 4.0. El cambio que implica esta nueva revolución supone el acceso en tiempo real a la información y el establecimiento permanente de una conexión entre el mundo real y el digital[148].

3. INCIPIENTE REGULACIÓN DE LA INTELIGENCIA ARTIFICIAL

En la actualidad, la IA no ha sido aún suficientemente objeto de regulación en el Derecho positivo. Sin embargo, existen hojas de ruta que están empezando a establecer pautas de actuación legislativa de cara a futuro. Entre esta incipiente tendencia destacan diversas estrategias, como las promovidas por Estados Unidos y la Unión Europea, que comienzan a trascender tanto a nivel supranacional, en el marco de Naciones Unidas y de la OCDE, como a nivel inferior. Al mismo tiempo, diversas organizaciones o grupos de Estados también se han puesto manos a la obra y han comenzado a incluir, entre sus temas prioritarios, el debate de las cuestiones éticas y las consecuencias jurídicas relacionadas con la IA.

En cuanto a la Estrategia de los Estados Unidos para la IA, responde el propósito del gobierno americano de liderar el mercado de la IA, con la expectativa de obtener grandes beneficios económicos y aprovechar la coyuntura para modular este desarrollo, con la máxima de mejorar la calidad de vida de las personas[149]. La Orden Ejecutiva 13859, de 11 de febrero de 2019[150], implementa la estrategia del

146 LONGÁS, H.: "Las tres revoluciones industriales", *El País,* Madrid, 17 de octubre de 2012. Recuperado de https://elpais.com/elpais/2014/10/17/media/1413577081_550723.html

147 ENATIC Y RODRÍGUEZ BERMÚDEZ, M.: "Retos jurídicos de la cuarta revolución industrial", *Abogacía Española,* 9 de mayo de 2016. Recuperado de https://www.abogacia.es/2016/05/09/retos-juridicos-de-la-cuarta-revolucion-industrial/

148 COTTELEER, M. and SNIDERMAN, B.: "Forces of change: Industry 4.0", *A Deloitte series on Industry 4.0,* https://www2.deloitte.com/es/es/pages/manufacturing/articles/que-es-la-industria-4.0.html [Fecha de consulta: 19/06/2019]

149 *Vid.* https://www.whitehouse.gov/ai/ai-american-values/ [Fecha de consulta: 01/07/2019]

150 Executive Order 13859 of February 11, 2019 "Maintaining American Leadership in Artificial Intelligence", Federal Register Vol. 84, No. 31, Thursday, February 14, 2019, https://www.

gobierno en colaboración y compromiso con el sector público y privado, la academia, y otros actores internacionales, con el fin de aumentar la investigación, el desarrollo y la innovación en este tipo de sistemas.

En 2018, los países más poderosos del mundo, reunidos en torno a la cumbre del G7 en Montreal (Canadá), apoyaron el desarrollo de la tecnología IA y el crecimiento económico que supone, fomentando la confianza de los ciudadanos en ésta y su inclusión en la sociedad. De hecho, redactaron el manifiesto *"Statement on Artificial Intelligence"*, que reconoce que la IA representa un conjunto de tecnologías complejas y poderosas, que transformarán la industria y ayudarán a resolver parte de los problemas más desafia tes de la sociedad[151]. Además, subraya la necesidad de desarrollar la IA centrada en seres humanos, apoyando tres actividades principales: i) el crecimiento económico basado en la innovación en IA, toda vez que se estima que ésta generará más de tres mil millones de dólares en la economía global anualmente hasta 2030; ii) un incremento de la confianza depositada en la adopción de la IA, lo que habilitaría lo anterior, mediante iniciativas educativas y tareas de concienciación; y iii) el desarrollo y despliegue inclusivo de aplicaciones de IA, que permita que toda la sociedad disfrute de los beneficios esperados de la misma.

El interés por el fenómeno de la IA ha llegado incluso a Naciones Unidas que, en los últimos años ha puesto en marcha un centro específico para supervisar el desarrollo de la IA y la robótica desde un punto de vista ético y en relación a la justicia penal, denominado UNICRI (*Center for Artificial Intelligence and Robotics*)[152].

En mayo de 2019, la OCDE aprobó la *Recomendación sobre Inteligencia Artificial*[153], recogiendo en ella una serie de principios que deben informar el empleo adecuado de los mecanismos de IA. Éstos se concretan en los siguientes:

1. Desarrollo inclusivo y sostenible, para no alentar desigualdades derivadas del uso de herramientas de IA ni aplicarlas en contra de las personas o del planeta.
2. Valores centrados en lo humano y la equidad, lo que pone de relieve la necesidad de que las aplicaciones de IA respeten el estado de derecho, los valores democráticos, la libertad, la dignidad y autonomía personal, la privacidad, la protección de datos, la igualdad y no discriminación, la diversidad social, la equidad, la justicia social y los derechos laborales reconocidos internacionalmente. Para ello, los actores de la IA (tecnólogos y no tecnólogos) deben implementar mecanismos apropiados para el contexto y el momento en

govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02544.pdf

151 Ver Centro de información del G7, Mink School of Global Affairs and Public Policy, Univeristy of Toronto, en http://www.g8.utoronto.ca/employment/2018-labour-annex-b-en.html [Fecha de consulta: 01/07/2019]

152 *Vid.* www.unicri.it [Fecha de consulta: 01/07/2019]

153 OECD/LEGAL/0449: Recomendación del Consejo sobre Inteligencia Artificial, adoptada el 22 de marzo de 2019, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

el que se usen.

3. Transparencia y explicación: Debe haber una actitud de transparencia y divulgación responsable de lo que hacen los algoritmos de IA, en base a cuatro medidas: fomentar la comprensión general de los sistemas; tomar conciencia de su impacto, particularmente sobre el alcance en el lugar de trabajo; permitir que interesados en la IA pudieran comprender los resultados obtenidos con sus algoritmos; y, por último, que sea posible establecer mecanismos de contradicción de los resultados, basándose en la información tomada como referencia para la predicción, recomendación o decisión de IA.

4. Robustez y seguridad de los sistemas, para que funcionen adecuadamente y no supongan razonablemente un riesgo de seguridad para la sociedad.

5. Responsabilidad, en el sentido, de establecer alguna manera de rendir cuentas, por parte de los actores de IA, sobre el buen funcionamiento de estos sistemas.

Tomando como referencia las recomendaciones anteriores, en junio de 2019, los países del G20, reunidos en Japón, han firmado una Declaración sobre comercio y economía digital que resalta el carácter humanista de la IA y hace suyos los 5 principios enunciados por la OCDE, dando lugar a los *"G20 AI Principles"*[154].

Alineada en este contexto, la Unión Europea ha actuado, primero, adoptando la *Resolución del Parlamento Europeo de 16 de febrero de 2017*[155], que propone unas las leyes de robótica para hacer frente a potenciales problemas de responsabilidad que su uso puede conllevar y, durante el presente año, redoblando sus esfuerzos por sacar adelante la Estrategia Europea de IA[156], basada en tres pilares:

1. Conseguir que Europa esté por delante de otros países en el desarrollo de esta tecnología y fomentar la participación público-privada (PPP). Para ello, está invirtiendo en proyectos I+D, bajo el programa Horizon 2020 y ha creado el Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial (AI HLEG)

2. Prepararse para el futuro cambio socio-económico consecuencia del desarrollo de esta tecnología, reteniendo el talento en IA dentro de Europa, la formación profesional dentro de las empresas, prediciendo cambios en el mercado, mejorando las competencias en ciencia y tecnología (perfiles STEM) y animando a los países a modernizar sus sistemas educativos y de formación.

154 G20 Ministerial Statement on Trade and Digital Economy, https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf [Fecha de consulta: 01/07/2019]

155 PARLAMENTO EUROPEO: Resolución del PE, de 16 de febrero, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL)), Doc. P8_TA(2017)0051, Estrasburgo, 2017.

156 EUROPEAN COMMISSION: Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and The Committee of the Regions "Artificial Intelligence for Europe", COM (2018) 237 final, Brussels, 25 April.

3. Asegurar un marco ético y legal apropiado. En este sentido, menciona la responsabilidad, la imparcialidad en la toma de decisiones y la claridad jurídica en las aplicaciones basadas en IA.

Como consecuencia de esta actuación, España ha iniciado los trabajos de planificación política para poder sumarse a esta tendencia mundial. En marzo de este año el Gobierno presentó el proyecto de Estrategia de I+D+i en Inteligencia Artificia [157], estableciendo como principales retos a cubrir los sectores relacionados con la medicina, el turismo, la ciberseguridad y la interoperabilidad en la administración electrónica. Su consecución hará necesario llevar a cabo adaptaciones normativas, estructurales y organizativas y crear una comisión interministerial de inteligencia artificial para poder abordarlas. Las prioridades de este plan se concretan en seis puntos: 1) lograr una estructura organizativa, 2) establecer áreas estratégicas para el país, 3) facilitar la transferencia de conocimiento y su repercusión en la sociedad, 4) planificar formación y profesionalización en IA, 5) desarrollar un sistema basado en datos con las infraestructuras actuales ("ecosistema digital de datos"), 6) analizar la ética de la IA.

4. LOS DERECHOS FUNDAMENTALES ANTE LA INTELIGENCIA ARTIFICIAL

Los derechos fundamentales son aquéllos que, por ser inherentes a la dignidad humana y resultar necesarios para el libre desarrollo de la personalidad, se encuentran recogidos legalmente en las constituciones modernas y protegidos procesalmente en las legislaciones tanto nacionales como internacionales, dado que son dotados de un valor jurídico superior. España dedica el Título I de su Constitución a los derechos y deberes fundamentales, previendo dos sistemas diversos de protección, según se encuentren incluidos en la sección 1º o 2º del capítulo segundo, que los enumera y conceptualiza de manera individual.

El desarrollo de la IA debe convivir con el respeto de estos derechos, lo que da lugar a un binomio complejo, especialmente si se tiene en cuenta que la regulación de la robótica y la IA responde, de momento, más a normas de *soft law* que a una auténtica normativa de obligado cumplimiento (derecho sustantivo o *hard law*).

En este contexto, uno los inconvenientes de emplear mecanismos de IA en el plano jurídico y especialmente en las investigaciones penales se deriva de la falta de conocimiento del sistema de funcionamiento por el ser humano, en concreto por los miembros de los órganos jurisdiccionales a la hora de decidir en base a resultados obtenidos por la razón artificial. Por otro lado, el uso masivo de herramientas de

157 http://www.ciencia.gob.es/stfls/MICINN/Cien_ia/Ficheros/Estrategia_Inteligencia_Artificial_IDI.pd [Fecha de consulta: 01/07/2019]

IA, potenciado por el *big data*, por parte de órganos gubernamentales y fuerzas de seguridad incrementa la eficiencia policial a cambio de confiar en una máquina más que en un humano, con los problemas éticos y de responsabilidad por daños que ello genera. En otras palabras, se plantea la duda de ¿quién responde jurídicamente si el algoritmo falla?, teniendo en cuenta que en el proceso intervienen múltiples actores tanto de carácter tecnológico como jurídico[158].

Todo ello hace planear una sombra de potencial vulneración de las garantías procesales y los derechos fundamentales de cualquier investigado, pero ¿qué derechos concretos quedan en entredicho ante situaciones de este tipo? Veámoslos[159].

4.1. El derecho a la vida y a la integridad

La vida y la integridad física y moral son un derecho reconocido por el artículo 15 de la Constitución Española, además de por normas europeas e internacionales. Su protección y sistema de garantía hace que cualquier atentado contra los mismos, proveniente de un ser humano, pueda ser considerado un ilícito penal.

El problema que se plantea en este sentido es que mecanismos que funcionan con sistemas de IA como los drones y vehículos autónomos, por ejemplo, pueden errar o no seguir las pautas que le han sido establecidas en operaciones concretas de control, seguimiento, detección o prevención de conductas, lo que supondría una amenaza o lesión de estos derechos[160].

En este contexto, habría que tener presente algunos los principios recogidos en la Resolución del PE de 2017, entre otros documentos no vinculantes, para incorporar normas éticas en los códigos de programación y sistemas que permitan la desconexión de la máquina ante situaciones de riesgo contra estos bienes jurídicos protegidos. Así sería esencial respetar los principios de benefic ncia, según el cual los robots deben actuar siempre en beneficio del hombre y de no perjuicio o maleficencia, que supone no hacer daño y, en virtud del cual los robots no deberían nunca perjudicar a las personas.

4.2. Libertad de expresión y de información

158 O'NEIL, C.: *Weapons of math destruction: How big data increases inequality and threatens democracy*. Penguin Random House UK, Great Britain, 2016.

159 SALGADO, V.: **"Los nuevos Derechos Humanos ante el Avance de la Inteligencia Artificial" conferencia** *impartida en el evento #LegalThinking: Derecho 2.0, Reflexiones de abogad@s TIC sobre tecnología, robótica e inteligencia artificial,* Facultad de Derecho de la Universidad de A Coruña, 17 de marzo de 2017. Recuperado de https://pintos-salgado.com/2017/03/17/derechos-humanos-e-inteligencia-artificial-leyes-de-la-robotica-en-la-ue [Fecha de consulta: 25/06/2019]

160 PARDO, P.: "La guerra del futuro: drones lanzallamas, robots-centinelas... y ni un solo humano", *El Mundo,* Washington, 25 enero 2019. Recuperado de https://www.elmundo.es/papel/futuro/2019/01/25/5c49e69c21efa013618b463c.html

El párrafo a) del artículo 20 de la CE reconoce el derecho "a expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción", mientras que el d) ampara el derecho "a comunicar o recibir libremente información veraz por cualquier medio de difusión".

En la actualidad, estos derechos se ejercen en el plano físico o mundo real, pero también en el virtual o digital, pues interactuamos con la red, expresándonos y compartiendo información personal relativa a opiniones e intereses a través de nuestras búsquedas en ella o en redes sociales, al tiempo que accedemos a información difundida en dicha red. Este tipo de conductas nos deja expuestos a un rastreo y clasificación por parte de empresas y Estados, con el consiguiente impacto negativo que se puede generar en la protección de estos derechos fundamentales.

En este sentido, el análisis que de nuestro comportamiento se puede realizar con herramientas de IA, plantea desafíos en relación con los datos personales (como veremos) pero también con la información confidencial.

Otro problema vinculado a estas libertades puede surgir al interactuar con robots cuyos sistemas pueden verse comprometidos, de manera que terceros no autorizados accedan a ellos, los hackeen y obtengan información personal, privada o confidencial que éstos tengan. Si bien en España no estamos aún a ese nivel, sería especialmente sensible en el caso de que tal vulneración se produjese en robots que actúan como asesores legales o como cuidadores, por ejemplo.

Para lidiar con este potencial campo de minas contra los derechos fundamentales, se debe trabajar, en el corto plazo, estableciendo procedimientos para prevenir y detectar estas vulnerabilidades, así como sistemas de contingencia ante la realización de las mismas. Ésta debe ser una tarea que acometan tanto el sector público como el privado, está claro que existirán, al menos inicialmente, diferencias entre los conocimientos y medios económicos y técnicos de que dispondrán para ello. Los primeros pasos en este sentido quizás pasarían, por un lado, por asegurar que la información que se dé o reciba a través de mecanismos de IA vaya siempre cifrada, y por otro, por decidir si conceder a los robots una personalidad jurídica a la que se pueda dar derecho a la privacidad.

4.3. El derecho al honor y a la intimidad

El artículo 18 de nuestra Carta Magna reconoce el derecho al honor y la intimidad (además de a la propia imagen) cuya protección, desarrolla en la L*ey 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y propia imagen,* pasa por garantizar el respeto de: i) la zona íntima y reservada de una persona o de un grupo, especialmente de una familia, el espacio que cada persona decide resguardar de la

curiosidad ajena[161]; y ii) de la propia estimación o dignidad (aspecto interno), al buen nombre (fama) y a la reputación (aspecto externo)[162]. Relacionado con estos derechos se encuentra el concepto de privacidad, entendido como el derecho de los individuos a no ser personalmente identificables, salvo que medie el consentimiento expreso del sujeto.

Por tanto, un elemento esencial en la protección de estos derechos es el consentimiento de la persona a que se refieren. En los modelos tradicionales de actuación, éste era fácilmente recabable, se obtuviera o no, pero en un mundo marcado por robots o sistemas inteligentes que pueden adoptar formas diversas y ser aéreos, móviles, casi invisibles y con capacidad para pensar y tomar decisiones de manera autónoma, obteniendo datos variados de manera selectiva y/o masiva, con finalidades muy distintas, el consentimiento humano parece quedar en un segundo plano y, por consiguiente, la determinación de sus zonas de protección, especialmente si se parte de que éste debería obtenerse antes de que se produzca la interacción entre el humano y la máquina.

Ello resulta aún más grave si se tiene en cuenta que los mecanismos de IA van a procesar datos de carácter personal como la imagen, la voz, los rasgos faciales, pues el riesgo de colisión con derechos fundamentales trasciende el de la intimidad y podría alcanzar también a derecho autónomo a la protección de datos personales[163].

Garantizar la legitimidad de actuaciones llevadas a cabo por sistemas de IA que tratan datos de manera indiscriminada va a hacer necesario diseñar medidas técnicas de anonimización y encriptación de los mismos, pues en caso contrario los Estados podrían limitar el uso de estos sistemas al ámbito privado, acabando con la posibilidad de que mecanismos inteligentes actúen en espacios públicos donde resulta complicado, si no imposible, solicitar el consentimiento de las personas para tratar sus datos, con los perjuicios que ello conllevaría en la vigilancia masiva de datos.

A pesar de ello, combinar IA con honor, intimidad y privacidad está obligando a trabajar por dilucidar diversas incógnitas: cómo garantizar el derecho al olvido o la supresión de información de un robot o sistema inteligente, cómo llevar a cabo la portabilidad de datos recabados por éstos, entre otras, cuyas respuestas aun no están disponibles.

4.4. La libertad de movimiento

161 STC, sala primera, 241/2012 de 17 diciembre.

162 SSTC, sala segunda, 208/2013, de 16 de diciembre y 51/2008 de 14 de abril.

163 SANTOS GONZALEZ, M.J.: "Regulación legal de la robótica y la inteligencia artificial: retos de futuro", *Revista Jurídica de la Universidad de León*, núm. 4 -2017 (p.35)

Partimos ya de que existen máquinas inteligentes (algoritmos de IA débil) capaces de hacer un perfil de las personas en base a datos, por ejemplo, de su navegación, presentes en discos duros, navegadores, servidores, la nube, en redes sociales…. En definitiva, en base a información masiva, tratados por herramientas de inteligencia artificial, se podría clasificar e incluso predecir a las personas, sus pensamientos o movimientos pasados y/o futuros.

Esta conducta que se me ocurre especialmente útil en el campo de la investigación criminal, por ejemplo, para realizar un perfil, patrón de conducta o de movimiento de investigado o encausado, ¿chocaría con el derecho a la residencia y libertad de movimiento reconocido en el artículo 19 de la Constitución Española? Por el sentido tradicional de la configuración de este derecho[164], la existencia o empleo de mecanismos de IA no supone *a priori* y de manera abstracta, una limitación a la libertad de movimiento, pero si se establece formalmente un sistema de control continuado en ese sentido, lo que no es tan descabellado viendo el auge de las *Smart cities* en determinadas zonas del planeta, quizás habría que replantearse el concepto base pues podría suponer una restricción indirecta a la libertad de movimiento, además por supuesto, de una vulneración de la privacidad de las personas.

5. CONCLUSIONES

La IA es una tecnología poderosa, tiene potencial para influir y modificar múltiples ámbitos de la sociedad, desde el transporte y la fabricación hasta la forma de dispensar atención médica o de educar. Además, su utilización es ya un hecho dentro del sistema policial, judicial e incluso del ejército, aunque el grado de intensidad en uno y otro varié según los avances tecnológicos, de un lado, y según los países en que nos centremos, de otro lado.

Es ya innegable que la IA puede aumentar la efic encia y obtención de resultados en todos aquellos sectores en que se emplee, generando beneficios económicos, nuevos conocimientos y acelerar el descubrimiento de novedades, pero la cara alternativa es que un empleo indebido de estas técnicas, sea intencional o no, puede generar múltiples amenazas y vulnerar los derechos fundamentales de las personas.

Ello, unido al hecho de que las elevadas capacidades de procesamiento existentes y el tratamiento del *big data* hace que sea dificult so para las personas llegar a conocer cómo un robot o un sistema de IA ha adoptado una determinada decisión y cuál es la base o fundamento que la forma, nos hace plantearnos diversas cuestiones en el campo procesal, tales como: si es posible iniciar un procedimiento por vulneración de derechos fundamentales cuando esta intromisión se debe a una máquina; en caso afirmativo,

164 Sinopsis artículo 19 de la CE en http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=19&tipo=2 [Fecha de consulta: 1/07/2019]

quién respondería de los daños causados, el sistema en si mismo, para lo que habría que configurar una personalidad electrónica que conviva con la personalidad física y jurídica, o los humanos que están detrás de su creación; si un robot puede actuar como testigo en un procedimiento judicial y, en tal caso, si su decisión tiene valor a los efectos de razonamientos judiciales; o si las personas que cometen crímenes bajo el control robótico son en realidad penalmente responsables de tales actos o si pueden escaparse de la pena prevista para la conducta que ha llevado a cabo.

Por otro lado, no puede obviarse que uno de los riesgos más importantes que presenta el aprendizaje automático es el peligro de amplificar la discriminación y los sesgos existentes contra ciertos grupos, a menudo comunidades marginadas y vulnerables. Cuando se utilizan datos históricos para entrenar a los sistemas de aprendizaje automático sin salvaguardias, éstos pueden reafirmar o incluso aumentar el sesgo estructural existente. También se pueden causar daños discriminatorios cuando las decisiones tomadas al diseñar los sistemas de IA producen resultados sesgados, ya sea de forma deliberada o no.

En definitiva, lo cierto es que los problemas principales relativos a la IA es la falta de normas sustantivas al respecto, siendo ésta la tarea esencial a cometer si queremos seguir conviviendo con estos mecanismos, con el fin de establecer criterios que permitan determinar el impacto sobre la responsabilidad de los actos con ocasión del uso de los sistemas IA; la atribución de la culpa, la imprudencia, el desarrollo informático deficiente, las vulnerabilidades imprevisibles, la falta de configuración adecuada o de mantenimiento irregular de los sistemas, la instalación defectuosa o el uso inadecuado de los mismos por parte del usuario; la inclusión de parámetros inteligentes que podrían matizar las responsabilidades penales, etc.

A modo de refl xión final, se puede sostener que, en el mundo actual, la realidad de la inteligencia artifi ial avanza más rápidamente que el derecho, motivo por el cual es un reto de futuro aprender a conjugarla, de manera que se pueda utilizar respetando y garantizando la protección de los derechos fundamentales que algunas de sus manifestaciones podrían vulnerar.

6. BIBLIOGRAFIA

ALANDETE, D. "John McCarthy, el arranque de la inteligencia artificial" *El País,* 27 de octubre de 2011.

ALBOR, J: "La IA, el cambio más disruptivo en la historia", *Revista Forbes, Portada,* 29 marzo 2019.

BARRIO ANDRÉS, M.: "Robótica, inteligencia artificial y Derecho", Real Instituto

Elcano, ARI 103/2018, de 11 de septiembre de 2018.

ENATIC Y RODRÍGUEZ BERMÚDEZ, M.: "Retos jurídicos de la cuarta revolución industrial", *Abogacía Española,* 9 de mayo de 2016.

FERRER, S.: "Los 23 mandamientos para evitar que la inteligencia artificial nos domine", *El Confidencial*, 2 de febrero de 2017.

IBERDROLA: "¿Qué es la Inteligencia Artificia ?.¿Somos conscientes de los retos y principales aplicaciones de la Inteligencia artific al?, *Iberdrola,* Te interesa, Tecnología, *https://www.iberdrola.com/te-interesa/tecnologia/que-es-inteligencia-artificial*

JOYANES AGUILAR, L.: *Big Data. Análisis de grandes volúmenes de datos en organizaciones*. Alfaomega. Marcombo ediciones técnica, México, 2014.

LONGÁS, H.: "Las tres revoluciones industriales", *El País,* Madrid, 17 de octubre de 2012.

MCCARTHY, J. AND HAGES, P.J.: *Some philosophical problems from the standponit of Artificial Intelligence",* Standford Universiry, Standfor, 1969.

MORELL RAMOS, J.: "La Inteligencia Artificial en el día a día de un abogado: qué le va a enseñar y cómo lo cambiará", *Revista del Consejo General de la Abogacía Española nº 108,* Febrero 2018.

O'NEIL, C.: *Weapons of math destruction: How big data increases inequality and threatens democracy*. Penguin Random House UK, Great Britain, 2016.

PARDO, P.: "La guerra del futuro: drones lanzallamas, robots-centinelas... y ni un solo humano", *El Mundo,* Washington, 25 enero 2019.

PAUWELS, E.: "Artifici l Intelligence raises ethical, policy challenges", *United Nations News, 16 November 2018*.

RODRIGUEZ, P.: *Inteligencia Articficial. Cómo cambiará el mundo (y tu vida),* Deusto, Grupo Planeta, Barcelona, 2018.

SANTOS GONZALEZ, M.J.: "Regulación legal de la robótica y la inteligencia artificial: retos de futuro", *Revista Jurídica de la Universidad de León*, núm. 4-2017.

LOS NUEVOS MODELOS DE NEGOCIOS Y LA APLICACIÓN DEL PRINCPIO DE PREVENCION DE OPERACIONES ILICITAS: DESAFIOS Y RESPONSABILIDADES

Eje temático: Legaltechs, Fintechs, Starups

Autora:
Graciela Cami Soria
Escribana pública (Universidad de la República); máster en derecho de internet y nuevas tecnologías (Instituto Campus Stellae, Santiago de Compostela, España); diplomada en administración digital (Centro Tecnológico de Comercio Electrónico [CETECE], Perú); técnico superior en seguridad informática, firmas y facturación electrónica (Instituto Euroinnova, España); experta profesional en derecho tecnológico e informática forense (Universidad de Extremadura, España); integrante de la Comisión de Derecho Informático y Tecnológico del Instituto de Investigación y Técnica Notarial de la Asociación de Escribanos del Uruguay; miembro de la Asociación de Informáticos del Uruguay (ASIAP). escribaniacami@gmail.com

ABSTRACT
La Cuarta Revolución Industrial junto con el descrédito de la banca tradicional, producto de las últimas grandes crisis, y otros fenómenos que se desarrollarán en el presente trabajo ha venido afectando el sector financi ro y propiciado el auge de nuevos emprendimientos y plataformas web vinculados a las finanzas. Se ingresa de esta forma al mundo de los *crowlending*, los *peer to peer lending* y las *fintech*.
Las tecnologías que emplean y la modalidad en cómo operan algunos de estos nuevos modelos de negocios los hace susceptibles de convertirse en instrumentos para el lavado de activos y financiamiento al terrorismo.
El presente trabajo tiene por cometido analizar las circunstancias que han facilitado la aparición de esos nuevos modelos de negocios en línea, vinculados al sector financiero.
Muchos países de la región vienen monitoreando de cerca este fenómeno, pero muy pocos cuentan con normativa que regule estos emprendimientos.
En este trabajo se investiga el accionar de algunos ordenamientos jurídicos con el fin de supervisar las actividades desarrolladas por esas nuevas empresas.
En principio se ha explorado el derecho comparado —en particular, la ley mexicana que regula las instituciones de tecnología financiera—, para luego abordar el estudio de la normativa uruguaya. Es así que se incluye una novedosa circular dictada recientemente por el Banco Central del Uruguay que reglamenta la actividad de las empresas administradoras de plataformas web de préstamos entre personas.
Se incorpora asimismo una sucinta referencia a soluciones alternativas, como lo son las *sandbox*.
A lo largo de esta investigación se ha visto que el verdadero desafío para estas iniciativas y sus reguladores radica en controlar estos negocios sin correr el riesgo de hacerlos desaparecer.
No obstante, se concluye que hay un interés superior, el cual consiste en dar cumplimiento al principio de prevención de operaciones ilícitas, para lo cual deben aplicarse los estándares internacionales en materia de lavado de activos; en especial, las recomendaciones de gafi sobre nuevas tecnologías, con el fin de mitigar riesgos y evitar que estas plataformas tecnológicas sean empleadas como instrumentos

para cometer ilícitos (lavar activos o financiar el terrorismo).
Palabras clave: FinTech, banca digital, préstamos entre personas, lavado de dinero, tecnología financiera

1. INTRODUCCIÓN

En diferentes foros se ha venido hablando de cómo la industria 4.0 impacta en la profesión notarial así como tantas otras profesiones, oficios y trabajos en general. De igual forma, el sector financiero se ha visto afectado por esta cuarta revolución industrial a la que hoy asistimos.

Sin embargo, la transformación de la banca no solo se debe a la llegada disruptiva de las nuevas tecnologías, sino que se ha venido gestando también a causa de diferentes fenómenos que han coadyuvado para que esa transformación sea factible.

Uno de esos sucesos clave se verificó hace aproximadamente una década, con la caída del banco de inversiones Lehman Brothers, el cuarto banco de inversión más grande de Estados Unidos, fundado en 1850 y con sede en Nueva York.

En realidad, más que un banco se trataba de un *holding*, es decir, una sociedad financiera que administraba un conjunto de empresas y poseía la mayoría del capital accionario.

Dicho *holding* quebró el 15 de setiembre de 2008; la quiebra constituyó la mayor en Estados Unidos y llevó, casi inmediatamente, a una crisis financiera a nivel mundial.

La quiebra del Lehman Brothers se vinculó a las hipotecas *subprime*, caracterizadas por un alto riesgo de impago; esto suponía un sistema de garantías aparentes, sin respaldo alguno, envuelto en una burbuja de aire que podía estallar en cualquier momento.

Tras la caída de Lehman Brothers, la banca tradicional quedó en una posición desfavorable. Muchos inversores, descontentos, buscaron en nuevos emprendimientos otras alternativas para la colocación de sus fondos.

A lo antedicho se agrega la llegada de las llamadas generaciones *Y* y *Z*, también denominadas respectivamente *milénica* o *millennial* (los nacidos entre 1980 y 1999) y *posmilénica* o *post milenian* (los nacidos a partir del año 2000). Se trata de una franja etaria entre los diecinueve y los treinta y nueve años que no solo se relaciona socialmente a través de diferentes aplicaciones y redes sociales: también compran y venden a través de internet (eBay, Amazon, Mercado Libre), alquilan vehículos (Uber), trabajan (*freelancers, influencers*), estudian (aulas virtuales, *webinars*), adquieren pasajes de avión, reservan hoteles, consiguen préstamos personales, etcétera, todo desde su celular, tablet o pc .

Si la realización de un trámite, la contratación de un servicio o la adquisición de un producto tienen su *alter ego* digital —es decir, si existe una aplicación o plataforma

digital que les ofrezca la posibilidad de gestionarlo en línea—, difícilmente concurran a un lugar físico para obtenerlo: optarán por la vía *online*.

2. LOS NUEVOS MODELOS DE NEGOCIOS

En muchos países, la banca tradicional advirtió esta situación y comenzó la digitalización de sus procesos y sistemas; surgieron así los llamados *neobanks* y los *challenger banks*.

Los *neobanks* constituyen bancos tradicionales que ofrecen sus servicios y productos financieros en línea; sus clientes pueden acceder a los servicios del *neobank* a través de dispositivos móviles. Los *neobanks* cuentan con el respaldo de la entidad bancaria que los generó.

Los *challenger banks*, por el contrario, son modelos de negocios totalmente nuevos; son *startups* que también ofrecen sus servicios en línea, pero que están por fuera del sistema bancario tradicional.

El fenómeno de descrédito de la banca tradicional, junto a la forma como se manejan las generaciones *milénica* y *posmilénica*, propició así el auge de las denominadas *fintech* e *insurtech*.

El término *fintech* es un anglicismo formado por la yuxtaposición de las primeras sílabas de *fin*ance y *tech*nology. Básicamente, refiere a las tecnologías aplicadas a las finanzas. Las *insurtech* (*insur*ance + *tech*nology) son las nuevas tecnologías aplicadas al sector seguros.

Las *fintech*, coloquialmente llamadas «Uber financieros» constituyen nuevos emprendimientos, plataformas web, *startups* que, sirviéndose de herramientas tecnológicas, ofrecen sus servicios y productos totalmente *online* y en diversos giros, tales como préstamos de dinero, inversiones, pagos, cambio de moneda, cheques.

En Uruguay existe una importante cantidad de *fintech*; también hay una Cámara Uruguaya de Fintech que a la vez es miembro de la Alianza Fintech Iberoamericana, esta última formada en 2017 e integrada por la Asociación Española de Fintech (aefi), Colombia Fintech, Fintech México, Fintech Perú, Fintech Centro América y El Caribe y por la Cámara Uruguaya de Fintech.

Los siguientes son algunos ejemplos de *fintech* uruguayas: Inversionate, Paganza, Bankingly, Ábaco, Socius, Dimo, Sha 256 Trading, Fimix, MiCheque, Prezzta, Cámbiame, Efectivo Clic, Prex, Tutyasa, In Switch y zir cont ech.

Con referencia a los préstamos entre particulares, los anglosajones han acuñado el término *crowdlending* o *P2P* (*peer to peer lending*). El término significa 'préstamos entre particulares', los que se realizan en línea y sin la intervención de la banca tradicional.

Los *crowdlending* son nuevos modelos de negocios desarrollados a través de plataformas web, que conectan a inversores con personas que buscan financiación. No solo median entre la oferta y la demanda, sino que también adoptan un rol más activo, analizando operaciones, aconsejando y ayudando en la toma de decisiones. Intervienen en los movimientos de dinero, es decir, reciben el pago de las cuotas por parte de los deudores y también hacen los pagos de intereses y capital a los inversores.

Es positivo que el sector financiero haya detectado la existencia de segmentos de la población a los que hay que atender en forma *online*. Es bueno que existan emprendimientos tecnológicos que ofrezcan nuevos productos y servicios financieros, porque con ellos se mejora la experiencia del usuario. Las transacciones se vuelven más transparentes y efectivas, y bajan los costos para el cliente final.

Sin embargo, no hay que descuidar los controles; no hay que permitir que estos nuevos modelos de negocios se transformen en instrumentos para la comisión de operaciones ilícitas y el financiamiento al terrorismo.

3. REGULACIÓN DE LOS NUEVOS EMPRENDIMIENTOS TECNOLÓGICO-FINANCIEROS

¿Cómo se controlan y regulan estos nuevos emprendimientos? Para responder a esta interrogante primero se ha consultado el derecho comparado, y encontramos así la ley mexicana que regula las instituciones de tecnología financiera (itf). Se trata de una ley de orden público, conocida como «Ley de Fintech», publicada el 9 de marzo de 2018, que cuenta con 144 artículos y una serie de disposiciones transitorias.

Dicha ley tiene la particularidad de no solamente regular el funcionamiento de las itf , sino que además contiene disposiciones sobre pagos electrónicos y activos virtuales, como así también diversas disposiciones del mercado de valores y de lavado de activos.

Resulta sumamente llamativa una disposición en particular, el artículo 58 de dicha ley, que establece las obligaciones para las itf y recoge las políticas de prevención de actividades con recursos de procedencia ilícita.

El giro particular de las itf y las tecnologías con que operan las hacen propensas a ser empleadas para la comisión de operaciones ilícitas. Por esa razón, la ley mexicana exige a las itf que establezcan una metodología que les permita llevar a cabo una evaluación de riesgos.

La reglamentación de este artículo 58 supuso un texto de 106 artículos y varias disposiciones transitorias más. Básicamente, incorpora todo lo que nosotros, notarios uruguayos, conocemos o hemos venido estudiando en materia de prevención de lavado de activos; en especial, la recomendación 1 del Grupo de Acción Financiera

(gafi), esto es, «identificar, evaluar y tomar acciones para mitigar el riesgo de lavado de activos y financiamiento al terrorism ».

Es así que esta reglamentación del artículo 58 recoge la obligación de identificar al cliente y determinar al «propietario real» —usa esta expresión en lugar de beneficiario final—, así como la verificación de si es una persona expuesta políticamente (pep), la designación de un oficia de cumplimiento, la elaboración de un reporte de operaciones sospechosas y la implementación por parte de las itf de programas de capacitación —en formato de talleres o cursos— para sus directivos, administradores, funcionarios y empleados al menos una vez al año. También incluye la recomendación de contar con sistemas automatizados que permitan detectar posibles operaciones inusuales del cliente y hacerle seguimiento, garantizando siempre la integridad, confidencialidad y disponibilidad de dicha información.

Otras legislaciones vienen trabajando en este tema, aunque no muchas poseen un marco regulatorio integral como el caso de México.

El análisis de todos los casos y los países que poseen regulación en esta materia excedería el límite máximo de folios permitidos para esta ponencia, por lo que solamente haré mención a dos países de Latinoamérica: Brasil y Argentina.

Brasil cuenta con una Resolución aprobada por el Consejo Monetario Nacional el 26 de abril de 2018 (resolución número 4656), que regula entre otras, las Sociedades de Préstamos entre Personas por medio de plataformas electrónicas (SEP por su sigla de origen) y establece los requisitos para el funcionamiento de la mismas.

Con referencia al tema que nos ocupa, es decir, el cumplimiento del principio de prevención de operaciones ilícitas, dicha normativa hace apenas dos sucintas referencias al tema. La primera mención se encuentra en su artículo 31, cuando dentro de los requerimientos para lograr la autorización del Banco Central del Brasil a los efectos de poder operar, dispone que deberá presentarse comprobante de origen de los recursos utilizados en el emprendimiento. La segunda referencia se realiza en el artículo 38 numeral 1° cuando establece las operaciones que se deben comunicar al Banco Central de Brasil y remite al artículo 31 antes referido.

Argentina por su parte, cuenta con la Ley 27349 del 29 de marzo de 2017, denominada "Ley de Apoyo al Capital Emprendedor".

Con el fin de fomentar el financiamiento de capital emprendedor en la República Argentina, esta ley establece la implementación del Sistema de Financiamiento Colectivo a través de las plataformas, que bajo el tipo de sociedades anónimas, conectan a inversores con personas que solicitan financiación. Se trata entonces de plataformas en línea que tienen por finalidad destinar fondos a un proyecto de financiamiento colectivo (lo que los anglosajones denominan: crowdfunding).

La Resolución General 717-E/2017 de fecha 29 de diciembre de 2017, reglamentaria de la referida ley, establece que la Comisión Nacional de Valores

será la autoridad de control, reglamentación y fiscalización de estas plataformas de financiamiento colectivo.

En relación al tema central de este trabajo, es de destacar el artículo 6° de la reglamentación, que entre los requerimientos para la inscripción de estas plataformas establece la obligación de presentar una declaración jurada de prevención de lavado de activos y financiami nto al terrorismo. En dicho documento los responsables de la plataforma deberán indicar si son o no Personas Expuestas Políticamente (PEP), asimismo declararán que no poseen delitos de lavados de activos y no figuran en las listas de terrorismo del Consejo de Seguridad de las Naciones Unidas.

Los requisitos y documentación a presentar para la inscripción de estas plataformas en el registro llevado por dicha Comisión, son similares a los que impone la circular del Banco Central del Uruguay para la inscripción de las Empresas Administradores de Plataformas de Préstamos entre Particulares, que analizaré en el párrafo siguiente.

4. NORMATIVA URUGUAYA SOBRE PREVENCIÓN DE OPERACIONES ILÍCITAS CON RELACIÓN A LOS NUEVOS MODELOS DE NEGOCIO

4.1. Las empresas administradoras de plataformas para préstamos entre personas

¿Qué ha hecho Uruguay en referencia a la regulación y supervisión de estos nuevos modelos de negocios y particularmente en este tema para cumplir con los estándares internacionales en materia de prevención de lavado de activos?

Recientemente, con fecha 21 de noviembre de 2018, la Superintendencia de Servicios Financieros del Banco Central del Uruguay (bcu) dictó una resolución, la que fue comunicada por circular n.º 2307, de 23 de noviembre siguiente (también se la puede encontrar en la Recopilación de Normas de Regulación y Control del Sistema Financiero), dada a conocer por circular del bcu n.º 2321, de 17 de enero de 2019.

La circular 2307 incorpora las empresas administradoras de plataformas para préstamos entre personas (título xii , libro i) y las define como «aquéllas personas jurídicas que administren aplicaciones web u otros medios electrónicos diseñados para mediar entre el oferente y demandantes de préstamos de dinero».

Los «clientes» de estas plataformas serán aquellos que se registren para divulgar sus ofertas o sus demandas de préstamos de dinero.

La circular del bcu establece que estas empresas administradoras de plataformas deben organizarse como sociedades comerciales y optar por alguno de los tipos sociales previstos en la ley 16 060; sus socios deben ser personas físicas. Si optaren por organizarse como sociedades anónimas, sus acciones deberán ser nominativas.

Asimismo, la circular les impone la obligación de inscribirse en un registro que a tal efecto llevará la Superintendencia de Servicios Financieros del bcu . La inscripción debe ser previa al inicio de actividades.

Para aquellas empresas que ya se encuentren operativas, la circular contiene una disposición transitoria por la cual se establece un plazo de cuatro meses, contados a partir de la fecha de la resolución —21 de noviembre de 2018—, para que procedan a la inscripción.

A diferencia de los *crowdlending*, mencionados anteriormente, estas empresas administradoras de plataformas para préstamos entre particulares solo podrán mediar entre la oferta y demanda de préstamos; es decir, solo se les estará permitido «conectar» o «acercar» las partes, pero no asumir obligaciones ni riesgo alguno. Son los prestamistas del dinero quienes asumirán el riesgo de pérdida total o parcial del capital prestado, y quienes serán responsables en caso de incumplimiento de la ley 18 212 (tasa de interés y usura). No obstante, la empresa administradora de la plataforma tendrá la obligación de advertir al prestamista de dichos riesgos y responsabilidades.

Tampoco pueden las empresas administradoras de la plataforma manejar el dinero de los préstamos, ya que todo el movimiento de dinero, tanto los préstamos, como los pagos de cuotas y de intereses, deben canalizarse a través de las entidades participantes en el Sistema Nacional de Pagos (Abitab, Red Pagos, Correo Uruguayo).

Los requisitos para la inscripción en el registros llevado por la Superintendencia de Servicios Financieros son muchos y variados; entre ellos, destacamos la constitución y el mantenimiento de «un depósito a la vista en el Banco Central del Uruguay no inferior a ui 50.000 (cincuenta mil unidades indexadas), a efectos de atender las obligaciones con dicha institución». Asimismo se establecen límites en los montos tanto de las inversiones como de los préstamos dentro de la plataforma.

Vinculado al tema de este trabajo, existe una disposición en particular que se encuentra dentro de los requisitos para la solicitud de la licencia —es decir, dentro de la información requerida a estas empresas para su inscripción en el registro del bcu— y es la que exige la presentación de un Manual del Sistema Integral para prevenirse de ser utilizadas en el lavado de activos y el financia iento del terrorismo, y la designación de un oficial de cumplimiento.

La reglamentación exige a estas empresas adoptar instrumentos eficaces para verificar la identidad de sus clientes e implementar sistemas para prevenirse de ser utilizadas en el lavado de activos. Están obligadas a contar con procedimientos que les permitan determinar cuándo un cliente o beneficiario final es pep, familiar o asociado cercano a una pep. Asimismo, tendrán la obligación de reportar operaciones sospechosas.

Tratándose de clientes que otorguen préstamos de más de trescientas seis mil unidades indexadas al año —aproximadamente treinta y ocho mil dólares—, la

identidad del cliente deberá verificarse en forma presencial, cara a cara, aunque se deja abierta la posibilidad de que dicha identificació pueda ser realizada por un prestador de servicios de confianza (conforme al artículo 31 de la ley 18 600, en la redacción dada por el artículo 28 de la ley 19 535).

La circular, además, dispone que las empresas administradoras de plataformas para préstamos entre personas deben mostrar total compromiso con el funcionamiento del sistema preventivo, estableciendo políticas y procedimientos apropiados y asegurando su efectividad.

Esas empresas estarán obligadas a implementar procedimientos que permitan detectar, prevenir y reportar transacciones; deberán exigir al personal un alto nivel de integridad y ofrecerle capacitación permanente acerca de la normativa aplicable y de las pautas para reconocer operaciones sospechosas.

La designación de ofi ial de cumplimiento deberá recaer en una persona comprendida dentro de la categoría de personal superior; puede ser un socio o un accionista radicado en el país.

El oficial de cumplimiento será el responsable de la implementación, seguimiento y control del adecuado funcionamiento del sistema y será el funcionario de enlace con los organismos competentes. También deberá documentar la evaluación de riesgos realizada por la empresa y los procedimientos de control establecidos para su mitigación.

Estas empresas, asimismo, deberán adoptar un Código de Conducta que refleje el compromiso institucional asumido a efectos de evitar que se use el sistema financiero para el lavado de activos.

5. *SANDBOX*: UNA SOLUCIÓN ALTERNATIVA

Algunas *fintech* han expresado su descontento por la normativa adoptada por el Banco Central del Urugu ay alegando que contiene requisitos excesivos para su licenciamiento, los que les impiden continuar con su actividad.

Siendo Uruguay un país con grandes carencias en seguridad, salud y educación, no puede permitirse desviar recursos humanos y económicos en proyectos informáticos que permitan a estas empresas administradoras de plataformas de préstamos entre particulares experimentar con productos financi ros, mientras cumplen los requisitos para su licenciamiento. En cambio, otros países desarrollados, como Reino Unido, Suiza, Australia, Emiratos Árabes y Singapur han implementado una solución alternativa denominada *sandbox* ('caja de arena'). México también posee su *sandbox,* Brasil y España vienen trabajando para poder implementarla.

La *sandbox* consiste en un ambiente virtual de prueba, un ecosistema informático controlado, en el cual estos nuevos emprendimientos pueden realizar sus actividades, pero bajo la atenta mirada de los reguladores.

Dado que muchas veces es imposible cumplir con todos los requisitos previos al inicio de actividades, la *sandbox* permitiría a estas plataformas desarrollar poco a poco su operativa, acotando los riesgos; por ejemplo, con mínima cantidad de clientes y operaciones de bajo monto, y cumpliendo gradualmente con los requerimientos para la obtención de sus licencias. Al mismo tiempo, permitiría a las autoridades el monitoreo de sus actividades para ir evaluando los riesgos y tomando acciones tendientes a mitigarlos.

6. REFLEXIONES FINALES

Resultado del avance de la tecnología, el surgimiento de nuevos modelos de negocios, en sana competencia con la banca tradicional, redunda en un beneficio para el usuario final.

No obstante, no hay que descuidar los controles. Es necesario regular, aunque sin ahogar estas nuevas iniciativas, y en este punto justamente radica el verdadero desafío.

Para el cabal cumplimiento del principio de prevención de operaciones ilícitas es necesario tener en cuenta la recomendación número 15 del gafi sobre nuevas tecnologías; es decir, los países deben identificar y evaluar los riesgos de lavado de activos y el uso de las nuevas tecnologías para modelos nuevos o ya existentes, con el fin de mitigar riesgos y evitar que estas plataformas tecnológicas sean empleadas como instrumentos para cometer ilícitos (lavar activos o financiar el terrorismo).

Asimismo, es responsabilidad de los titulares de empresas administradoras de dichas plataformas web comprometerse con las políticas de prevención de lavado de activos para evitar que sus modelos de negocios sean usados como instrumentos para la comisión de operaciones ilícitas.

7. REFERENCIAS

Asociación Española de Fintech e Insur tech . *Propuesta para la implantación de un* sandbox *en España*. En colaboración con Hogan Lovells, España, 2018. Sitio Web: ‹https://asociacionfintech.es/wp-content/uploads/2018/03/Informe_ inal_ Propuesta_Sandbox_Espa%C3%B1a.pdf› [Fecha de consulta: 30 de enero de 2019].

Banco Central del brasil . *Resolución 4656/2018*, de 26 de abril de 2018,

Brasil, 2018. Sitio Web: https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attacments/50579/Res_4656_vl_O.pdf. [Fecha de consulta: 12 de agosto de 2019].

Banco Central del Urugu ay. *Circular n.º 2321* («Recopilación de Normas de Regulación y Control del Sistema Financiero»), de 17 de enero de 2019, Montevideo, 2019.

Banco Central del Urugu ay. *Circular n.º 2321* («Reglamentase las empresas administradoras de plataformas para préstamos entre personas»), de 23 de noviembre de 2018, Montevideo, 2018.

Banco Central del Urugu ay. *Circular n.º 2078* («Empresas de transferencias de fondos. Modificación de la normativa en materia de prevención del lavado de activos y del financiamiento del terrorism »), de 21 de febrero de 2011, Montevideo, 2011.

Banco Central del Urugu ay. *Resolución 712/2018*, de 19 de noviembre de 2018, Uruguay, 2018. Sitio Web: ‹https://www.bcu.gub.uy/Servicios-Financieros-SSF/Resoluciones_SSF/RR-SSF-2018-712.pdf› [Fecha de consulta: 26 de enero de 2019].

Cámara Uruguaya de Fintech. Sitio Web: ‹https://cafu.org.uy/› [Fecha de consulta: 30 de enero de 2019].

Comisión Nacional de Valores de la Nación Argentina. *Resolución General 717-E/2017*, de 29 de diciembre de 2017, Buenos Aires, Argentina, 2017. Sitio Web:

https://www.boletinoficial.gob.ar/detalle_viso/primera/177095/20180103 [Fecha de consulta: 26 de enero de 2019].

Da Sil va, M. *Al «Uber financiero» le llegó la regulación: bcu regulará a las fintech como mediadores financieros*. Diario El País, suplemento Negocios, Montevideo, 14 de setiembre de 2017. Sitio Web: ‹https://negocios.elpais.com.uy/noticias/bcu-regulara-fintech-mediadores-financieros.html› echa de consulta: 26 de enero de 2019].

Fundación Wikimedia. «Lehman Brothers», *Wikipedia, la enciclopedia libre*. Sitio Web: ‹https://es.wikipedia.org/wiki/Lehman_Brothers› [Fecha de consulta: 26 de enero de 2019].

Plataformas para préstamos: Piden al bcu dejar sin efecto regulación de fintech. Diario El País, suplemento Negocios, Montevideo, 15 de diciembre de 2018. Sitio Web: ‹https://negocios.elpais.com.uy/finanzas/piden-bcu-deha -efecto-regulacion-fintech.html

[Fecha de consulta: 29 de enero de 2019].

Pozzi , S. *Crisis financiera mundial; la caída de un gigante de Wall Street: Lehman presenta la mayor quiebra de la historia con un pasivo de 430.000 millones*. Diario El País, sección Economía, Madrid, 16 de setiembre de 2008. Sitio Web: ‹https://elpais.com/diario/2008/09/16/economia/1221516004_850215.html› [Fecha de consulta: 26 de enero de 2019].

—o0o—

Cámara de Diputados del Honorable Congreso de la Nación, Secretaría General, Secretaría de Servicios Parlamentarios Estados Unidos Mexicanos (s/f.). *Ley para regular las Instituciones de Tecnología Financiera*. Diario Oficial de la Federación, Ciudad de México, 9 de marzo de 2018. Sitio Web: ‹http://www.diputados.gob.mx/LeyesBiblio/pdf/LRITF_090318.pdf› [Fecha de consulta: 7 de enero de 2019].

Senado y Cámara de Diputados de la Nación Argentina. *Ley 27349 de Apoyo al Capital Emprendedor*. Sala de Sesiones del Congreso Argentino, Buenos Aires, 29 de marzo de 2019. Sitio Web: https://www.senado.gov.ar/parlamentario/comisiones/verExp/80.16/CD/PL

[Fecha de consulta: 12 de agosto de 2019].

Uruguay, Poder Legislativo, Sala de sesiones de la Cámara de Senadores. *Ley 18 600* («Reconócese la admisibilidad, la validez y la eficacia jurídicas del documento electrónico y de la firma electrónica»), de 15 de setiembre de 2009. Diario Oficial, Montevideo, 5 de noviembre de 2009.

Uruguay, Poder Legislativo, Sala de sesiones de la Cámara de Senadores. *Ley 19 535* («Rendición de Cuentas y Balance de Ejecución Presupuestal correspondiente al ejercicio 2016»), de 18 de setiembre de 2017. Diario Oficial, Montevideo, 3 de octubre de 2017.

DIGNIDAD HUMANA, DERECHOS HUMANOS Y TECNOLOGÍA: NUEVOS DESAFÍOS A PARTIR DEL DESARROLLO Y USO DE ALGORITMOS

Eje temático: Inteligencia Artificial: riesgos y desafíos jurídico

Autor:
Olivia Andrea Mendoza Enríquez
Profesora Investigadora Titular Tiempo Completo del Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación INFOTEC

SUMARIO

I. La dignidad humana como sustento de la Declaración Universal de los Derechos Humanos 1948. II. Derechos humanos y tecnología. III. Desafíos jurídicos del desarrollo y uso de algoritmos IV. Algoritmos y su impacto en los derechos humanos. V. Conclusiones.

ABSTRACT

Durante las siguientes líneas, se abordará una breve refl xión en torno a la forma en la que los derechos humanos en la época moderna, se sustentaron en la dignidad de las personas, y la necesidad de tener esto presente, en la nueva configuración de los derechos humanos a la luz de la tecnología. En este sentido, se presenta también un análisis en relación a los derechos humanos y su nueva dimensión, a la par del desarrollo tecnológico, y la forma en la que son garantizados, ahora no solo por los Estados, sino por las corporaciones. De igual forma, este trabajo pondrá en relieve los nuevos desafíos jurídicos, que implican el desarrollo y uso de algoritmos para eficientar la toma de decisiones y procesos dentro de las organizaciones e instituciones, y la forma en la que estos algoritmos, impactan a derechos humanos, como la libertad de expresión, el acceso a la información, la privacidad y protección de datos personales y la no discriminación.

Este trabajo parte de la hipótesis de la necesidad de reconocer expresamente e incorporar la idea de la dignidad de las personas como sustento del desarrollo tecnológico, lo cual permitirá desarrollar mecanismos no solo jurídicos, sino técnicos para la efectiva garantía de los derechos humanos en el desarrollo tecnológico, particularmente en el desarrollo y uso de los algoritmos.

De esta forma, podemos concluir de manera provisional, la necesidad de una nueva configuración de derechos humanos a la luz del desarrollo tecnológico, a partir del reconocimiento en todas sus dimensiones de la dignidad humana, lo cual permitirá que se salvaguarden derechos mínimos de los usuarios de tecnología, particularmente de algortimos, por parte no solo de los Estados, sino de las corporaciones. Este trabajo no pretende ser punto final de la discusión, sino que tiene como objetivo aportar elementos que a la par del desarrollo tecnológico parecen casi invisibles, pero necesarios para una profunda refl xión en torno, por ejemplo, a los fines que debería seguir la técnica, el papel del Derecho en el desarrollo tecnológico, y la manera en la que las formas tradicionales del reconocimiento y confi uración de derechos humanos desde la posguerra, permiten actualizar y configurar nuevos mecanismos de protección en ámbitos como los de las tecnologías de la información y comunicación.

I. LA DIGNIDAD HUMANA COMO SUSTENTO DE LA DECLARACIÓN UNIVERSAL DE LOS DERECHOS HUMANOS 1948

Resulta pertinente iniciar este apartado, respondiendo la pregunta: ¿por qué cuando hablamos de desarrollo tecnológico, es importante recordar la dignidad humana como sustento de los derechos humanos?

Pareciera que es una pregunta cuya respuesta resulta obvia, pero no lo es. El desarrollo tecnológico ha permitido que los humanos eliminemos las barreras de tiempo y espacio, haciendo casi todo posible.

No obstante, todos esos beneficios, también han desafiado la idea original del sustento y respeto de la dignidad de las personas. Solo por mencionar un ejemplo, si bien tenemos avaneces en la inteligencia artificial que nos permiten pensar en la singularidad tecnológica y utilizar robots para eficientar la vida de los humanos, también se ha presentado la posibilidad de utilizar estos robots sofisticados como armas de ataques masivos y letales por parte de los países desarrollados en zonas de conflicto armado, que han hecho que diversos Estados[165] impulsen la necesidad de una nueva legislación internacional que prohíba la utilización de este tipo de tecnología.

Este ejemplo es dual, ya que por un lado, los robots nos permiten aspirar a la idea de hacer más fácil la vida de las personas, pero por el otro, la misma tecnología permitiría el exterminio masivo de humanos… y ante desafíos de este tipo, resulta muy necesario recordar las atrocidades de la Segunda Guerra Mundial, el reconocimiento de las mismas y el compromiso que firmaron los Estados para nunca más vulnerar esos derechos mínimos de las personas, en un reconocimiento inédito de la dignidad de todos los humanos, por el simple hecho de serlo.

En este sentido, el Considerando Primero del Preámbulo de la Declaración Universal de los Derechos Humanos de 1948 , señala "Considerando que la libertad, la justicia y la paz en el mundo tienen por base el reconocimiento de la dignidad intrínseca y de los derechos iguales e inalienables de todos los miembros de la familia

165 El grupo de expertos gubernamentales sobre sistemas de armas autónomos letales de la Convención sobre Ciertas Armas Convencionales se reunió en Ginebra en agosto de 2018 para debatir opciones con las que abordar los desafíos éticos, humanitarios, de derechos humanos y de seguridad planteados por los sistemas de armas totalmente autónomos. La mayoría de los Estados que asistieron subrayaron la importancia de mantener el control humano sobre los sistemas de armamento y el uso de la fuerza, y manifestaron su apoyo al desarrollo de nueva legislación internacional sobre sistemas de armas autónomos letales. Veintiséis de estos Estados, entre ellos Austria, Brasil y Egipto, pidieron una prohibición total. China también ha pedido un nuevo protocolo de la Convención sobre Ciertas Armas Convencionales que prohíba el uso de sistemas de armas totalmente autónomos; sin embargo, varios Estados clave se oponen a crear prohibiciones jurídicamente vinculantes, entre ellos gobiernos de los que se sabe que ya están desarrollando sistemas de armas autónomos, como Corea del Sur, Estados Unidos, Francia, Israel, Reino Unido y Rusia. Aministía Internacional España. Disponible en: https://www.es.amnesty.org/en-que-estamos/noticias/noticia/articulo/onu-se-necesita-una-accion-energica-para-prohibir-los-robots-asesinos-antes-de-que-sea-demasiado/ Fecha de consulta: 20 de junio de 2019.

humana"[166], lo cual permite afirmar que el sustento de este instrumento internacional es un reconocimiento inédito por parte de los Estados, de la dignidad de las personas, a fin de evitar que se vuelvan a cometer atrocidades como las cometidas durante la Segunda Guerra Mundial.

Por su parte, el artículo primero de la misma Declaración, señala que todos los seres humanos nacen libres e iguales en dignidad y derechos y, dotados como están de razón y conciencia, deben comportarse fraternalmente los unos con los otros. [167]

En este sentido, podemos afirmar que la dignidad humana sustento de la Declaración de 1948, ha quedado rezagada durante el desarrollo tecnológico, en el cual pareciera que la pregunta y la acción gira en torno al poder que tiene el humano en desarrollar la técnica, y no así en el deber ético de salvaguardar dicha dignidad, y en particular los derechos mínimos reconocidos a las personas.[168]

Ante tal panorama, el Derecho tiene retos complejos que superar frente al avance tecnológico, los cuales radican primordialmente en recuperar la parte humanística relacionada al mismo, para así otorgar certidumbre, generar confianza y ofrecer un entorno digital distinto a los usuarios. Reforzando esta idea, es necesario invocar la Declaración de Principios de la Cumbre Mundial sobre la Sociedad de la Información,[169] en la que se estableció el compromiso de construir una sociedad basada en la persona, en la que todos pudiéramos crear, consultar, utilizar y compartir la información y el conocimiento, para impulsar el desarrollo sostenible y mejorar la calidad de vida, sobre la base de los propósitos y principios de la Carta de las Naciones Unidas y respetando plenamente y defendiendo la Declaración Universal de Derechos Humanos.[170]

Derivado de lo anterior, podemos afirmar que la idea de dignidad humana, debe estar más presente que nunca, en el desarrollo tecnológico y en la forma en la que se configura la regulación en torno a dicho rubro, y uno de los grandes desafíos de no hacerlo, es la paradoja de la coordinación y fragmentación de procesos desiguales de

166 La Declaración de 1948 intentaba ser una respuesta a las atrocidades ocurridas durante la Segunda Guerra Mundial, periodo en el que se violó la dignidad de las personas.

167 Declaración Universal de los Derechos Humanos, edición ilustrada. Disponible en: https://www.un.org/es/documents/udhr/UDHR_booklet_SP_web.pdf Fecha de consulta 20 de junio de 2019.

168 La experiencia atroz de la Segunda Guerra Mundial, así como lo narrado en los Juicios de Nüremberg, ha quedado en el olvido, para así evolucionar la técnica hacia posibilidades que muchas veces vulneran la dignidad de las personas –particularmente de los invisibles-. Algunos ejemplos los encontramos en los ataques cibernéticos, la venta de grandes cúmulos de información de los ciudadanos, las pocas políticas públicas de inclusión digital, el desarrollo y uso de algoritmos con fines de discriminación de las personas, etc.

169 Celebrada del 10 al 12 de diciembre de 2003, en Ginebra.

170 Adelantando un poco la respuesta respecto a los principios ahí establecidos y el resultado de la sociedad digital construida, podemos mencionar el informe anual del Alto Comisionado de las Naciones Unidas para los Derechos Humanos de 2014, denominado el Derecho a la Privacidad en la Era Digital, que deja en relieve la responsabilidad que hasta ahora han tenido las empresas para vulnerar la privacidad de las personas en el ciberespacio. Disponible en: https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Privacy-In-digital-Age-Spanish-version.pdf Fecha de consulta enero, 2016.

desarrollo.[171] Es decir, el desarrollo tecnológico debe preservar un equilibrio entre la libertad y la dignidad humana, el cual podría lograrse a través de un humanismo sólido y del respeto de dicha dignidad como eje de cualquier avance científico: la tecnología como herramienta para empoderar a las personas, pero no como el único fin. Apuntalando lo anterior, el derecho en nuestro siglo tiene el reto de recuperar el carácter humanístico frente al desarrollo tecnológico. [172]

II. DERECHOS HUMANOS Y TECNOLOGÍA

Hablar de la relación de los derechos humanos y la tecnología, es cada vez más común, atendiendo a que el desarrollo tecnológico ha permeado en casi todas las zonas geográficas del mundo y está presente en todos los procesos de la vida cotidiana de las personas.[173]

En este sentido, resulta pertinente decir que los derechos humanos[174] surgieron en un clima cultural ilustrado de la Modernidad y fueron formulados como categorías que pretendían expresar las exigencias intemporales y perpetuas de la naturaleza humana, como conjunto de facultades jurídicas y políticas propias de todos los hombres y en todos los tiempos.[175] De esto, se desprende que los derechos humanos reconocidos en 1948, bajo ese carácter de intemporal, podrían fungir como derechos espejo, pero ahora en el ámbito digital, en el marco de la sociedad de la información. Es decir, en su mayoría, no se trata de nuevos derechos, sino de derechos humanos tradicionales, ahora configurados y manifestados a partir del desarrollo tecnológico.

En este sentido, los derechos humanos se formaron en sociedades en las que los cambios se producían de manera lenta, por lo que la ciencia jurídica se hallaba en condiciones de poder asumirlos y alojarlos en los correspondientes conceptos

171 Giddens, A., *Consecuencias de la Modernidad,* Ed. Alianza, Madrid, 1993, p. 162.

172 *Véase* Lefranc Weegan, F. *Terra Incógnita. Bases para una política criminal pro persona en la sociedad digital*, INFOTEC, México, 2015, p. 9.

173 Es importante decir, que a pesar de que el desarrollo tecnológico se encuentra presente en casi todas las latitudes del mundo –aunque cuando se trata de países en vías de desarrollo, sea solo, bajo el rol asignado de países compradores-, esto no significa, por dar un ejemplo, en el caso de Internet, que exista accesibilidad y cobertura para el total de la población, ya que si bien existe tecnología que se pueda comprar (laptops, computadoras, tabletas o cualquier dispositivo móvil), temas como la brecha digital, siguen enfatizando lo que en la realidad física sucede: los pobres no son sujetos de conexión (no son público directo por parte de las grandes compañías). Esto se corrobora con el Estudio de Hábitos de Uso de Internet de la Asociación Mexicana de Internet del año 2018, en el que se determinó que el hogar sigue siendo el lugar de conexión por excelencia, y en el que podemos refl xionar, si en los hogares con altos índices de pobreza, sería o no una prioridad contratar un servicio de conexión a Internet.

174 Para Pérez Luño el paradigma eleático concebía los derechos humanos como unas verdades, cuya evidencia podía demostrarse a través de los dictámenes de la recta razón.

175 Pérez Luño, Enrique, (2012). Los Derechos Humanos en la sociedad tecnológica. España: Universitas. p. 13.

jurídicos[176]; sin embargo, hoy día, el desarrollo tecnológico, plantea nuevos retos al ámbito jurídico en relación a los derechos humanos, ya que éste, es tan rápido que no permite una respuesta idónea y única desde el Derecho.

Introducir la variable tecnológica significa atender a la necesidad de traducir el discurso de los derechos humanos en términos que puedan abarcar también a la ciencia y la tecnología, en virtud de que éstos son elementos que modifican el concepto de espacio o ámbito en el que se manifiestan, profundizan y desarrollan los derechos humanos en general. De tal forma que este nuevo contexto abre nuevas perspectivas para comprender de una forma más amplia la Declaración Universal de los Derechos Humanos, al surgir problemas éticos, políticos y jurídicos que tienen que ver con nuestros derechos.[177]

Como se ha dicho, la incidencia de la tecnología en la tutela de los derechos humanos ha sido notoria, ya que si bien supone un medio o herramienta idónea para el ejercicio de los derechos humanos, también implica nuevas formas de vulneración de los mismos; es decir, y a manera de ejemplo, si por una parte cada día existen más plataformas electrónicas ciudadanas que sirven como instrumento para el ejercicio de la libertad de expresión, también existen servicios de almacenamiento de información en la nube –con poca regulación jurídica y nula ética en el manejo de la información-, lo cual supone un riesgo exponencial respecto a la vida privada de las personas. [178]

En esas coordenadas se está iniciando un movimiento de la doctrina jurídica y de la jurisprudencia de los países con mayor grado de desarrollo tecnológico tendente al reconocimiento del derecho a la libertad informática y a la facultad de autodeterminación en la esfera informativa. Es evidente por tanto, que para la opinión pública y el pensamiento filosófico jurídico y político de nuestro tiempo constituye un problema nodal el establecimiento de unas garantías que tutelen a los ciudadanos frente a la eventual erosión y asalto tecnológico de sus derechos y libertades[179].

Esta proyección de los efectos del uso de la informática sobre la identidad y dignidad humanas incide también en el disfrute de los valores de la libertad y la igualdad. La libertad en las sociedades más avanzadas, se encuentra acechada por el empleo de técnicas informáticas de control individual y colectivo que comprometen o erosionan gravemente su práctica. Contemporáneamente se produce una agresión a la igualdad, más implacable que en cualquier otro periodo histórico, desde el momento

176 Op. Cit., Nota 11, p. 9.

177 Peschard, Mariscal. (2013). Cap. 3. El derecho fundamental a la protección de datos personales en México. En Protección de Datos Personales en México, México: Tirant lo Blanch, p. 21.

178 Mendoza Enríquez, (2012). Libertad de Expresión e Internet. En Memorias del XVI Congreso Iberoamericano de Derecho e Informática, Ecuador: Ministerio de Justicia, Derechos Humanos y Cultos.

179 Op. Cit., nota 12, pp. 22 y 23.

en que se desarrolla una profunda disparidad entre quienes poseen, o tienen acceso, al poder informático y quienes se hallan marginados de su disfrute[180].

Aunado a lo anterior, uno de los retos que enfrenta la efectiva garantía de los derechos humanos a la lu del desarrollo tecnológico, es que éste no es propiedad del bien común, ya que la era tecnológica es también excluyente; al vivir en sociedades desiguales, no todos los individuos tienen la misma oportunidad para acceder a los recursos tecnológicos. Es así que la principal crítica a la era digital, originada en la postmodernidad, radica en que ha acentuado las diferencias entre las personas para acceder a los recursos que ofrece la tecnología, y esto, sin hablar de las lagunas jurídicas en cuanto a la regulación de ésta, y ambos factores inciden en el efectivo ejercicio de derechos humanos.

Finalmente, resulta importante hablar del nuevo rol de los Estados en la garantía de los derechos humanos a la luz del desarrollo tecnológico, ya que como hemos visto en casos como *Cambridge Analytica,* el rol del Estado se ve cada vez más reducido, para dar paso a las políticas de las grandes corporaciones en el ciberespacio. Un fenómeno que parece constante en el mundo, es la forma en la que las legislaciones locales, sobre todo, en materia de protección de datos personales, ceden frente a las políticas y esquemas de aparente gobernanza establecidos o impuestos por las grandes empresas[181].

Es decir, si bien la garantía tradicional de los derechos humanos ha sido entregada a los Estados, hoy día nos encontramos ante nuevos operadores que finalmente son responsables de garantizar o no derechos humanos como el de privacidad, protección de datos personales, libertad de expresión y no discriminación, y se trata de las corporaciones.

Ante tal panorama, el derecho tiene retos complejos que superar frente al avance tecnológico, los cuales radican primordialmente en recuperar la parte humanística relacionada al mismo, para así otorgar certidumbre, generar confianza y ofrecer un entorno digital distinto a los usuarios. Reforzando esta idea, vale la pena invocar la Declaración de Principios de la Cumbre Mundial sobre la Sociedad de la Información,[182] en la que se estableció el compromiso de construir una sociedad basada en la persona, en la que todos pudiéramos crear, consultar, utilizar y compartir la información y el conocimiento, para impulsar el desarrollo sostenible y mejorar la calidad de vida, sobre la base de los propósitos y principios de la Carta de las Naciones Unidas y respetando plenamente y defendiendo la Declaración Universal de Derechos Humanos.[183]

180 Op. Cit., nota 11, p. 23.

181 Una excepción a este común denominador, es el caso de la Unión Europea y los países adheridos al Convenio 108 del Consejo de Europa, los cuales han hecho frente a políticas abusivas relacionadas a la privacidad de los usuarios de redes sociales, a fin de establecer un estándar mínimo a través del Reglamento Europeo de Protección de Datos Personales.

182 Celebrada del 10 al 12 de diciembre de 2003, en Ginebra.

183 Adelantando un poco la respuesta respecto a los principios ahí establecidos y el re-

III. DESAFIOS JURÍDICOS DEL DESAROLLO Y USO DE ALGORITMOS

Como podríamos adelantar, existe casi nula legislación que reconozca expresamente los principios y límites en el usos de los algoritmos. Los pocos instrumentos en la materia, más bien refier n a documentos o códigos de ética respecto del tratamiento de la información, insumo de los algoritmos, o en el mejor de los casos, respecto de los sesgos que podrían originarse al momento de su implementación.

No obstante lo anterior, resulta conveniente citar a la Dra. Cathy O´Neil, autora del libro "Armas de destrucción matemática. Cómo el Big Data aumenta la desigualdad y amenaza la democracia", en relación a que no necesitamos generar nuevas normativas a partir del desarrollo de algoritmos, -al menos en este momento-, sino aplicar la regulación existente a este fenómeno tecnológico; es decir, la mayoría de legislaciones en el mundo, de los países en los que se desarrollan e implementan algoritmos, reconocen derechos humanos como el derecho a la no discriminación y éste sería el principal derecho vulnerado a la luz de decisiones tomadas por algoritmos, sin la intervención final humana, desconociendo la forma en la que funcionan y toman decisiones y sobre todo, sin tener una oportunidad de alegato, respecto de dicha decisión automatizada[184].

Dicho esto, podemos afirmar que en la mayoría de legislaciones, se reconoce un catálogo de derechos humanos que pueden verse afectados con la instrumentación de algoritmos sin límites éticos, jurídicos y sociales, por lo que simplemente apoyando lo dicho por O´Neil, particularmente en el campo de los derechos humanos, se requiere aplicar los derechos ya reconocidos, pero ahora a través de nuevas formas de manifestación como las referidas a los algoritmos.

No obstante lo anterior, es importante hablar de un aspecto regulatorio que tiene cierto grado de innovación respecto del régimen de protección de los algoritmos y es el que tiene que ver con el valor de éstos y la ventaja competitiva que aportan a las empresas o instituciones que los desarrollan; es decir, el costo de desarrollo de algoritmos para impulsar la innovación es alto, por lo que existen corrientes que afirman que son un bien intangible que debe protegerse en términos de las normas de propiedad intelectual o industrial correspondientes e incluso bajo perspectiva de las reglas de competencia económica. Algunas de las vías sugeridas de protección bajo esta perspectiva son la de patentes, copyright o protección del know how, competencia desleal. La postura contraria a estas afirmacione , es la necesidad de incluir conceptos como la transparencia en el desarrollo de algoritmos que permita a las personas tener

sultado de la sociedad digital construida, podemos mencionar el informe anual del Alto Comisionado de las Naciones Unidas para los Derechos Humanos de 2014, denominado el Derecho a la Privacidad en la Era Digital, que deja en relieve la responsabilidad que hasta ahora han tenido las empresas para vulnerar la privacidad de las personas en el ciberespacio.

184 Información disponible en: https://youtu.be/hPr4Dwg4O_A. Fecha de consulta 18 de febrero de 2019.

la certeza de cómo funcionan y así, asegurarse que no tengan por diseño o de forma aprendida, algún sesgo de discriminación.[185]

Otra de las dimensiones regulatorias que tienen los algoritmos es la relativa a las normativas en materia de protección de datos personales. El caso particular a referir, es el Reglamento General de Protección de Datos (RGPD) aplicable en el ámbito europeo, el cual refuerza los requisitos relacionados con las decisiones automatizadas, basadas en el uso de algoritmos; es decir, las entidades que utilicen algoritmos tendrán que proporcionar una explicación sobre la lógica de las decisiones automatizadas y sobre sus consecuencias principales para los individuos, pudiendo éstos pedir la intervención humana y recurrir la decisión (principio de transparencia).[186]

En este sentido, la preocupación de desarrolladores e implementadores, también vinculada al ya mencionado principio de transparencia, tiene que ver con la exposición de la "fórmula" con la que trabajan los algoritmos utilizados, lo cual podría derivar en competencia desleal por parte de industrias del mismo sector. No obstante este argumento, parece ser claro que el principio de transparencia, que garantiza un derecho humano como el del debido tratamiento de la información de carácter personal, debe prevalecer sobre aquéllos que invoquen cuestiones económicas de las entidades, pero considerando la importancia de la innovación en la economía digital.

Una vez que hemos abordado las aristas anteriores, podemos preguntarnos si estamos ante el reconocimiento de nuevas formas de manifestación del derecho a la protección de datos personales, como el derecho a la no identificación en la utilización de algoritmos.

Apuntalando el tema regulatorio, resulta conveniente citar al Dr. Jorge Vega Iracelay, quien ha identificado 5 elementos mínimos a considerar en este ámbito para el tema de Inteligencia Artificial, relacionados y aplicables también, al tema de los algoritmos. Dentro de estas consideraciones, destacan: no desarrollar marcos legales domésticos, realizas esfuerzos desde el Derecho Internacional, a fin de evitar que tecnologías que utilizan algoritmos, se constituyan como instrumentos bélicos válidos, instrumentación de políticas de transparencia y privacidad, normas de responsabilidad civil y objetiva aplicada a este tipo de tecnologías, cuyo desafío sea no frenar y promover la innovación, garantizar que el uso de algoritmos no profundice la desigualdad existente.[187]

185 De acuerdo a Álvarez Caro, la Oficina Europea de Patentes ha denegado la mayoría de solicitudes sobre métodos basados en algoritmos. En cambio, en EE.UU se ha observado una mayor aceptación, pese a que en 2014 ha habido un giro jurisprudencial que endurece los requisitos de patentabilidad de algoritmos. Información consultada en: Álvarez Caro, María, Algoritmos, activos intangibles claves en la industria financiera. Información disponible en: https://www.bbvaresearch.com/publicaciones/algoritmos-activos-intangibles-claves-en-la-industria-financiera . Fecha de consulta 10 de febrero de 2019.

186 *Ídem.*

187 Vega Iracelay, Jorge, Perspectiva regulativo de la Inteligencia Artificial, en Gobernanza y Regulaciones de Internet en América Latina. Análisis sobre la infraestructura, privacidad, cibersegu-

Es importante resaltar la trascendencia de los acuerdos internacionales que deberían adoptarse al menos desde la perspectiva del derecho internacional humanitario, ya que las máquinas de destrucción masiva que funcionan con inteligencia artificial y a través de algoritmos previamente entrenados, plantean nuevos desafíos y riegos para la continuidad de la humanidad. En este sentido, el uso de robots y drones, podría derivar en el exterminio masivo de los humanos, lo cual significa no solo el poco ético desarrollo tecnológico con estos fines, sino la urgencia de estandarizar compromisos internacionales por parte de los Estados, a fin de establecer un límite claro ante un riesgo inminente en donde este tipo de máquinas de destrucción masiva ya se están desarrollando. De nueva cuenta estaríamos ante la disyuntiva de los científicos que en su momento desarrollaron la bomba atómica y cómo se pierde el control a partir de que una tecnología es terminada, ya que su implementación dependería de decisiones incluso geopolíticas, en donde la ética puede ser evidentemente disminuida.

En las líneas anteriores, se ha referido a un instrumento universal de derechos humanos y a la normativa en materia de protección de datos personales en el ámbito europeo, pero no debemos olvidar que la regulación va más allá de lo tradicionalmente "legislado" y nos permite invocar documentos de "*soft law*"[188], tales como los "Principios para garantizar la transparencia y responsabilidad en materia de algoritmos" emitidos por la *US Association for Computing Machinery ACM*[189], los cuales si bien no son vinculantes,

ridad y evoluciones tecnológicas, coords. Belli Luca y Cavalli Olga, Brasil, 2018, pp.455-459.

188 El término es usualmente empleado por la doctrina para describir principios, reglas, estándares o directrices que carecen de efecto vinculante aunque no dejan por ello de producir determinados efectos jurídicos. Sztucki, Jerzy, "Reflections on International "Soft law", Ramberg, Jan, *et al.* (eds), *Festskrift till Lars Hjerner. Studies in International Law,* Norstedts, Stockholm, 1990, pp. 549-575. Citado en "El fenómeno del Soft Law y las nuevas perspectivas del derecho internacional, Del Toro Huerta, Iván. Disponible en: https://revistas.juridicas.unam.mx/index.php/derecho-internacional/article/view/160/257. Fecha de consula 15 de febrero de 2019.

189 "Principles for Algorithmic Transparency and Accountability 1. Awareness: Owners, designers, builders, users, and other stakeholders of analytic systems should be aware of the possible biases involved in their design, implementation, and use and the potential harm that biases can cause to individuals and society. 2. Access and redress: Regulators should encourage the adoption of mechanisms that enable questioning and redress for individuals and groups that are adversely affe - ted by algorithmically informed decisions. 3. Accountability: Institutions should be held responsible for decisions made by the algorithms that they use, even if it is not feasible to explain in detail how the algorithms produce their results. 4. Explanation: Systems and institutions that use algorithmic decision-making are encouraged to produce explanations regarding both the procedures followed by the algorithm and the specific decisions that are made. This is particularly important in public policy contexts. 5. Data Provenance: A description of the way in which the training data was collected should be maintained by the builders of the algorithms, accompanied by an exploration of the potential biases induced by the human or algorithmic data-gathering process. Public scrutiny of the data provides maximum opportunity for corrections. However, concerns over privacy, protecting trade secrets, or revelation of analytics that might allow malicious actors to game the system can justify restricting access to qualified and authorized individuals. 6. Auditability: Models, algorithms, data, and decisions should be recorded so that they can be audited in cases where harm is suspected. 7. Validation and Testing: Institutions should use rigorous methods to validate their models and document those methods and results. In particular, they should routinely perform tests to assess and determine whether the model generates discriminatory harm. Institutions are encouraged to make the results of such tests public". Información consultada el 15 d febrero de 2019, en: https://www.acm.org/binaries/content/assets/

si permiten orientar a los desarrolladores e implementadores de algoritmos, a fin de evitar consecuencias poco éticas, derivadas del uso de los mismos.

Por otra parte, tal vez estemos frente a nuevas configuraciones de derechos como el de oposición frente al tratamiento de datos personales para fines de entrenamiento o toma de decisiones a través de algoritmos por parte de organizaciones e instituciones y por otro lado, ante el planteamiento de nuevos mecanismos legales como los recursos jurídicos que pudiera tener el titular de datos personales para impugnar las decisiones automatizadas a a través de algoritmos.

Como hemos visto, a nivel local, los Estados carecen de normativas específicas que limiten o establezcan las reglas para la utilización de algoritmos y esto puede explicarse incluso por las características propias de la tecnología, en la que su instrumentación se lleva a cabo en el ciberespacio, el cual elimina las fronteras físicas, para hacer de múltiples jurisdicciones, sujetos de intervención en conflictos que ahí se susciten. Aunque existieran intentos locales de regular de manera tradicional a los algoritmos, simplemente estos se diluirían en la globalización de la era digital.

No obstante lo anterior, esto no significa que no sea necesario establecer límites para el uso de algoritmos, especialmente de aquéllos que puedan atentar en contra de la dignidad de las personas, pero por el momento, una posible solución es la aplicación del marco legal de los derechos humanos a estas formas de procesar la información, el reconocimiento e incorporación de conceptos como la dignidad humana y el impulso de estándares y códigos de ética que permitan potencializar la responsabilidad de los sujetos, organizaciones e instituciones que desarrollan e implementan algoritmos, respecto de los usuarios finales o titulares de la información procesada.

IV. ALGORITMOS Y SU IMPACTO EN LOS DERECHOS HUMANOS

Una vez que hemos analizado el rol de la dignidad humana en el desarrollo tecnológico, la importancia de una nueva configuración de derechos humanos a la par de la tecnología y los nuevos desafíos jurídicos a partir del desarrollo y uso de algoritmos, es tiempo de hablar en específico del impacto que tienen los algoritmos en la esfera de los derechos humanos.

Se advierte que los principales derechos humanos que podrían verse afectados ante algoritmos poco transparentes, con sesgos en su desarrollo y entrenamiento, y con nulos aspectos éticos y regulatorios incorporados en su funcionamiento, son: la libertad de expresión, -incluyendo la vertiente de acceso a la información-, el derecho a la privacidad y protección de datos personales, y el derecho a la no discriminación.

---

public-policy/2017_usacm_statement_algorithms.pdf

Los derechos humanos antes mencionados, no se citan de forma exhaustiva ya que derechos como el de la salud, pueden verse afectados ante decisiones automatizadas a través de algoritmos que por ejemplo, decidan entre candidatos idóneos y aquéllos que no son susceptibles a ser sometidos a tratamientos médicos.

El derecho a la libertad de expresión, incluyendo su vertiente de acceso a la información, puede verse afectado, cuando son únicamente los algoritmos los que deciden que información, por ejemplo, se presenta en un buscador a un usuario con un perfil específico. Este problema se podría agravar, si la tecnología es instrumentada desde ámbitos públicos como las campañas electorales, en las que un algoritmo matemático, pueda decidir en lo que debe y lo que no debe conocer un ciudadano para direccionar el voto. Esto evidentemente supone un riesgo directo no solo a los derechos humanos, sino a las democracias de los Estados.

Respecto del derecho a la privacidad y la protección de datos personales, es importante recordar que desde la teoría tradicional, se ha reconocido el poder sobre la información de carácter personal a su titular, y este poder no tiene fecha de caducidad; es decir, el poder que en principio y por regla general, tendríamos las personas frente a nuestra información y el derecho a que no sea sometida a decisiones automatizadas a través de algoritmos. No obstante, frente al desarrollo tecnológico, esto parece cada vez más difícil de garantizar, ya que la información contenida en medios digitales, se encuentra expuesta en mayor medida a ser sometida a este tipo de tratamientos y muchas veces sin siquiera el conocimiento de su titular. Esto, evidentemente supone un riesgo a la vida privada de las personas y hace necesario el planteamiento de nuevos recursos legales que permitan cuestionar y revisar las decisiones automatizadas a través de algoritmos y cualquier acción que derive de ellos y que vulnere la vida privada; asimismo, se plantean nuevos derechos como el de la transparencia frente al funcionamiento matemático de dichos algoritmos.

Como podemos ver, los ejemplos citados anteriormente derivan invariablemente en un riesgo enorme a que las personas sean discriminadas, en relación a conceptos, formulas y elementos que no conocemos. Ejemplos como los sesgos que los algoritmos adquieren durante su entrenamiento, ponen sobre la mesa, la necesidad de crear mecanismos desde la técnica y desde el ámbito regulatorio que garanticen candados efectivos para que los algoritmos, no sean utilizados como herramientas de discriminación.

V. CONCLUSIONES

A modo de conclusión, podemos afirmar que hoy más que nunca resulta pertinente invocar conceptos como la dignidad humana, que dieron sustento a la

Declaración Universal de Derechos Humanos de 1948, a fin de que esté presente frente al desarrollo tecnológico y ésto pueda ser un candado efectivo de protección, frente a la garantía de derechos humanos.

También podemos afirmar que el catálogo de derechos humanos configurados de forma tradicional a partir de dicha Declaración, están más vigentes que nunca, con una nueva dimensión que es la tecnológica.

Nuevas tecnologías como el desarrollo y uso de algoritmos, plantean nuevos desafíos al campo del Derecho, que normalmente se encuentra un paso atrás. No obstante, sería necesario no generar tan altas expectativas únicamente en el ámbito jurídico, ya que para la efectiva protección de la persona frente a la técnica, resulta necesaria también la incorporación de estándares éticos y regulatorios a los nuevos desarrollos tecnológicos.

No se puede negar la trascendencia de los algoritmos en la era digital, ya que permiten resolver grandes problemas, y garantizan la subsistencia y mejora de tecnologías disruptivas como la inteligencia artificial, el internet de las cosas, y el big data; sin embargo, también plantean el permanente desafío del respeto a la dignidad de las personas, y el uso y comportamiento ético de las máquinas, aunque suene paradójico porque hablamos de cosas y no personas, identificando que detrás de un algoritmo en lo abstracto, está un desarrollador y una empresa, entidad, institución o grupo de personas, que fondean la evolución de los mismos.

Los algoritmos evidentemente tienen aspectos sociales y éticos que exigen a desarrolladores e implementadores, asumir a responsabilidad de los alcances que puedan tener las técnicas mejoradas y utilizadas. En este tema, la responsabilidad ética sigue estando de lado de los humanos y no de la técnica.

VI. BIBLIOGRAFIA

1. Álvarez Caro, María, Algoritmos, activos intangibles claves en la industria financiera. Información disponible en: https://www.bbvaresearch.com/publicaciones/algoritmos-activos-intangibles-claves-en-la-industria-financiera/.

2. Amnistía Internacional España: https://www.es.amnesty.org/en-que-estamos/noticias/noticia/articulo/onu-se-necesita-una-accion-energica-para-prohibir-los-robots-asesinos-antes-de-que-sea-demasiado/

3. Declaración Universal de los Derechos Humanos, edición ilustrada. Disponible en: https://www.un.org/es/documents/udhr/UDHR_booklet_SP_web.pdf.

4. Del Toro Huerta, Iván, El fenómeno del Soft Law y las nuevas perspectivas del

derecho internacional, Disponible en: https://revistas.juridicas.unam.mx/index.php/derecho-internacional/article/view/160/257.

5. Derecho a la Privacidad en la Era Digital, que deja en relieve la responsabilidad que hasta ahora han tenido las empresas para vulnerar la privacidad de las personas en el ciberespacio. https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Privacy-In-digital-Age-Spanish-version.pdf

6. Giddens, A., *Consecuencias de la Modernidad,* Ed. Alianza, Madrid, 1993.

7. Lefranc Weegan, F. (2015). *Terra Incógnita. Bases para una política criminal pro persona en la sociedad digital*, INFOTEC, México.

8. Mendoza Enríquez, (2012). Libertad de Expresión e Internet. En Memorias del XVI Congreso Iberoamericano de Derecho e Informática, Ecuador: Ministerio de Justicia, Derechos Humanos y Cultos.

9. Pérez Luño, Enrique, (2012). Los Derechos Humanos en la sociedad tecnológica. España: Universitas.

10. Peschard, Mariscal, (2013). Cap. 3. El derecho fundamental a la protección de datos personales en México. En Protección de Datos Personales en México, México: Tirant lo Blanch.

11. O´Neil Caty, https://youtu.be/hPr4Dwg4O_A.

12. Vega Iracelay, Jorge, (20181). Perspectiva regulativo de la Inteligencia Artificial en Gobernanza y Regulaciones de Internet en América Latina. Análisis sobre la infraestructura, privacidad, ciberseguridad y evoluciones tecnológicas, coords. Belli Luca y Cavalli Olga, Brasil.

13. https://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf

INTELIGENCIA ARTIFICIAL APLICADA AL SISTEMA DE REVISIÓN JUDICIAL

EL CASO DE LA SUPREMA CORTE DE JUSTICIA DE LA PROVINCIA DE BUENOS AIRES COMO MODELO DE IMPLEMENTACIÓN

Eje tematico: Inteligencia Artificial: riesgos y desafíos jurídico

Autor:
Sebastián Carlos Chumbita
Auxiliar Letrado de la Secretaría Civil y Comercial de la Suprema Corte de Justicia de la Provincia de Buenos Aires. Profesor Adjunto Universitario.
Poder Judicial de la Provincia de Buenos Aires, Universidad Nacional de La Plata, Universidad de Ciencias Empresariales y Sociales, Comisión de Jóvenes Procesalistas y Laboratorio de Innovación e Inteligencia Artificial de la Universidad de Buenos Aires
schumbita@hotmail.com

ABSTRACT
El mundo de la tecnología ha logrado importantes avances en materia de almacenamiento (Big Data) y procesamiento de datos (Smart Data). Tanto ha sido el progreso, que los sectores de comunicaciones, comercios y empresas han posicionado a la Inteligencia Artificial como la herramienta clave para el desarrollo de las futuras sociedades.
Se dice que educación, sanidad, cultura, ningún sector puede resistirse a sus ventajas, ¿puede el proceso judicial incorporarla? Si una de las mayores ventajas que ofrece es la celeridad, ¿qué pasaría si descubriéramos que la inteligencia artificial puede ser aplicada para que aporte eficiencia y, también, repotencie al operador jurídico?
Si los mayores problemas que atraviesan y aquejan en forma constante a los órganos jurisdiccionales en Latinoamérica son la sobrecarga de trabajo y la falta de respuesta en tiempo oportuno, ¿cómo pueden afrontarse estas problemáticas? ¿corresponde volver a viejas instituciones procesales, reformular las existentes o incorporar nuevas herramientas?
En el presente trabajo, tomando como ejemplo a la Suprema Corte de Justicia de la Provincia de Buenos Aires, en particular, su desenvolvimiento en materia civil y comercial, repasaremos las nociones básicas de la inteligencia artificial y dejaremos sentadas las bases constitucionales y procesales sobre las que el mentado órgano se desenvuelve. Más luego, reflejaremos ciertos argumentos tendientes a la implementación de un sistema predictivo para el cumplimiento de las actividades recursivas, destacando sus principales virtudes y los aportes más significativos que traería al proceso judicial, en pos de responder a las consignas planteadas.

Asimismo, esbozaremos cinco fundamentos -a los cuales reputamos como esenciales- para demostrar por qué la implementación de un sistema dotado de inteligencia artificial puede resguardar los derechos de las partes, respetar el debido proceso, asegurar la garantía de la defensa en juicio, emitir una respuesta jurisdiccional en un tiempo razonable, humanizar el trabajo del operador jurídico y aumentar la eficiencia de las tareas de manera xponencial.

SUMARIO: I.- INTRODUCCIÓN. BREVES NOCIONES SOBRE LA INTELIGENCIA ARTIFICIAL (IA); II.- LA APLICACIÓN DE LA IA EN EL CAMPO DEL DERECHO; III.- EL CASO DEL SUPERIOR TRIBUNAL DE JUSTICIA DE LA PROVINCIA DE BUENOS AIRES Y EL ANÁLISIS DE LA SUFICIENCIA TÉCNICA RECURSIVA; IV.- SOBRE LA CREACIÓN DE UN ALGORITMO. SUS FUNDAMENTOS Y V.- A MODO DE CONCLUSIÓN.

I.- INTRODUCCIÓN. BREVES NOCIONES SOBRE LA INTELIGENCIA ARTIFICIAL (IA)

Si bien no existe consenso entre los autores para establecer qué significa realmente Inteligencia Artificia [190] (en adelante, IA), podemos definirla como la ciencia que -a través de la utilización de algoritmos[191]- es capaz de lograr objetivos complejos[192].

Esta tecnología se centra en la automatización de comportamientos inteligentes como razonar, recabar información, planifica , aprender, comunicar, manipular, observar e incluso crear, soñar y percibir; y aborda distintas áreas de conocimiento, tales como: la informática cognitiva (cognitive computing: algoritmos capaces de razonamiento y comprensión de nivel superior -humano-), el aprendizaje automático (machine learning: algoritmos capaces de enseñarse a sí mismos tareas), la inteligencia aumentada (augmented intelligence: colaboración entre humanos y máquinas) y la robótica (IA integrada en robots).[193]

En la actualidad, muchas personas le confían su vida, mediante la utilización de los sistemas antibloqueo en los frenos de los autos y los pilotos automáticos en los aviones hasta las aplicaciones en los teléfonos móviles. La principal fuente de energía de las ciudades (la red eléctrica) está bajo el control de sistemas de inteligencia artificial, tres de cada cuatro transacciones en los mercados de valores de los Estados

190 Su término, es atribuido al matemático estadounidense John McCarthy quien, en el año 1956, convocó a una conferencia en Darmouth College (Hanover, New Hampshire) sobre la base de la conjetura de que todos los aspectos del aprendizaje o cualquier otra característica de la inteligencia podían describirse con tanta precisión que se podía hacer una máquina para simularlo. John, McCarthy, "*A proposal for the Darmouth Summer Research project on artificial intelligence*", http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf [Fecha última consulta: 29 de julio de 2019]

191 Conjunto preciso de instrucciones o reglas o una serie metódica de pasos que puede emplearse para hacer cálculos, resolver problemas y tomar decisiones. Corvalán, Juan G.; "*Inteligencia Artificial y Derechos Humanos*", suplemento de Inteligencia Artificial, nº 1 del Diario DPI, publicado con fecha 3-VII-2017.

192 Tegmark, Max; "*Inteligencia Artificial - IBM*"; https://www.youtube.com/watch?v=5rvZBsueMoc [Fecha última consulta: 29 de julio de 2019]

193 Dictamen del Comité Económico y Social Europeo nº 526 sobre la "*Inteligencia artificial: las consecuencias de la inteligencia artificial para el mercado único (digital), la producción, el consumo, el empleo y la sociedad*"; https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52016IE5369&from=ES [Fecha última consulta: 29 de julio de 2019]

Unidos se realizan mediante algoritmos automatizados de negociación y uno de cada tres matrimonios en ese país comenzó con una relación online.[194]

Bajo esa premisa, distintas empresas hoy en día se dedican a desarrollar aplicaciones con el objeto de mejorar la calidad de vida de la gente. Por ejemplo, se han creado softwares para: optimizar el uso del agua empleado para el riego de las tierras[195]; recomendar sobre oportunidades de trabajo existentes y cómo navegar en futuros movimientos de una carrera profesional[196]; predecir qué jóvenes tienen más probabilidades de experimentar la falta de vivienda a largo plazo, esencialmente en una trayectoria para convertirse en adultos crónicos sin hogar[197] y, también, proveer soluciones de biometría, prevención de fraude, protección de identidad y gestión de riesgos informáticos[198], etc.

Por estos motivos, nadie duda que la IA es un factor clave para el desarrollo del mundo, más aún, cuando recientes estudios han afirmado que existe la posibilidad de que -prontamente- deleguemos todas las decisiones que tomamos en las máquinas.[199]

II.- LA APLICACIÓN DE LA IA EN EL CAMPO DEL DERECHO

Aunque la IA nos parezca una ciencia lejana y misteriosa, el empleo de tecnología digital cuenta con varios años de experiencia en el mundo del derecho. Con la utilización de procesadores de texto como el *Microsoft Word*, motores de búsqueda como *Google*, sistemas de gestión de expedientes como *Augusta* (Provincia de Buenos Aires) hasta buscadores de jurisprudencia como *Thomson Reuters* (La Ley), los operadores del campo jurídico han intentado incorporar -desde hace mucho tiempo- diversas tecnologías con el propósito de mejorar su trabajo y ser más eficientes.

Tal es así que, en la última década, mediante la implementación del expediente judicial por medio de presentaciones y notificaciones electrónicas, se ha generado un cambio paradigmático a la hora de gestionar recursos y organizar agendas. [200]

---

194 Comisión Económica para América Latina y el Caribe (CEPAL), *"Datos, algoritmos y políticas: la redefinición del mundo digital"*, (LC/CMSI.6/4), Santiago, 2018, pág. 169.

195 Kilimo, ver más en https://www.kilimo.com.ar/ [Fecha última consulta: 29 de julio de 2019]

196 IBM Watson Career Coach, ver más en https://www.ibm.com/talent-management/career-coach [Fecha última consulta: 29 de julio de 2019]

197 TAY Triage Tool, ver más en https://www.orgcode.com/ [Fecha última consulta: 29 de julio de 2019]

198 VU Security, ver más en http://www.vusecurity.com/ [Fecha última consulta: 29 de julio de 2019]

199 "El futuro de la IA: hacia inteligencias artificial s realmente inteligentes"https://www.bbvaopenmind.com/articulos/el-futuro-de-la-ia-hacia-inteligencias-artifi iales-realmente-inteligentes/

200 En la Provincia de Buenos Aires, según Res. 1827/12 y sus normas complementarias. Para más información http://www.scba.gov.ar/servicios/notiypresen.asp [Fecha última consulta: 29 de julio de 2019]

Más allá de ello, de un tiempo a esta parte se han concretado interesantes proyectos en la materia con el objeto de mejorar la prestación del servicio de justicia, utilizando inteligencia artificial en materia predictiva para la toma de decisiones. Veamos algunos ejemplos.

COMPAS[201], un algoritmo que evalúa los riesgos de reincidencia de los acusados y, a través de su resultado, fija el monto de una pena[202]; *VERIPOL*, una herramienta que es capaz -a partir de técnicas de procesamiento del lenguaje natural y aprendizaje automático- de indicar la veracidad de una denuncia policial[203]; *ECHO* y *PEIRCE-IGTT*, una aplicación que elabora hipótesis y estrategias de acusación y defensa[204] y *ALIBI*, un programa que, ante un determinado delito, realiza un pronóstico sobre las diferentes explicaciones que pueda tener el comportamiento de un reo.[205]

PROMETEA, un sistema diseñado para predecir la solución de expedientes jurídicos simples. Este software, que es conducido íntegramente por IA, está siendo implementado en la Fiscalía General de la Ciudad Autónoma de Buenos Aires y funciona de la siguiente manera: cuando llega un expediente a dictaminar -que no ha sido analizado por ninguna persona- se le carga el número correspondiente a la máquina. El programa busca la carátula en la página del Tribunal Superior de Justicia de la Ciudad de Buenos Aires, lo asocia con otro número (vinculado a las actuaciones principales) y luego va a la página del Poder Judicial de dicho distrito (Juscaba). Pero eso no es todo. Busca y lee las sentencias de primera y segunda instancia, analiza dictámenes elaborados previamente y finalme te emite la predicción[206]. En otras palabras, detecta un modelo determinado para resolver el expediente y hasta ofrece la posibilidad de completar algunos datos para imprimir o enviar a revisar el dictamen con base a ese modelo.[207]

---

201 De su inglés, Correctional Offender Management Profiling for Alternative Sanctions. "*Compas*" https://doc.wi.gov/Pages/AboutDOC/COMPAS.aspx [Fecha última consulta: 29 de julio de 2019]

202 Este aplicativo ya es utilizado en los Estados Unidos y cuenta con decisiones de Superiores Tribunales Estatales como el caso de Wisconsin. "*Un juez usó un software para condenar a un hombre a 6 años de prisión*", https://www.clarin.com/tecnologia/condenan-hombre-anos-prision-software-secreto_0_H1Ax36elW.html [Fecha última consulta: 29 de julio de 2019]

203 "*Veripol, inteligencia artificial a la caza de denuncias falsas*", publicado por la Universidad Complutense de Madrid. Vicerrectorado de Transferencia del Conocimiento y Emprendimiento. Oficina de Transferencia de Resultados de Investigación (OTRI); https://www.ucm.es/data/cont/docs/1334-2018-09-18-2018_09_not5.pdf [Fecha última consulta: 29 de julio de 2019]

204 Nissan, E., "*Digital technologies and artificial intelligence´s present and a foreseeable impact on lawyering, policing and law enforcement*"; AI & Society, 2015, pág. 13, su cita en Nieva Fenoll, Jordi, "*Inteligencia artificial y proceso judicial*", Marcial Pons, Madrid, 2018, pág. 26.

205 Nissan, E., "*Legal Evidence, Police Intelligence, Crime Analysis or Detection, Forensic Testing, and Argumentation: An Overview of Computer Tools or Techniques*", 17 Int´l J.L. & Info. Tech, 1, 2009, págs. 1 y sigs., su cita en Nieva Fenoll, Jordi, ob. y pág. cit.

206 Según datos, predice la solución de un caso judicial en menos de 20 segundos, con una tasa de acierto del 96%. "*Usamos la inteligencia artificial para transformar la burocracia estatal*"; en http://www.noticiasurbanas.com.ar/noticias/aprovechamos-la-inteligencia-artificial-para-transforma -la-burocracia-estatal/ [Fecha última consulta: 29 de julio de 2019]

207 Corvalán, J. G.; "*La primera inteligencia artificial predictiva al servicio de la Justicia: Prometea*";

Por si fuera poco, este sistema también está siendo utilizado por la Corte Constitucional de Colombia con la diferencia de que las acciones de leer, analizar, detectar y sugerir están enfocadas en seleccionar los casos vinculados con tutela de salud que resulten más urgentes y que requieran un tratamiento prioritario por parte del Superior Tribunal.[208]

RADAR, una herramienta que identifica y separa casos con pretensiones idénticas contemplando, a su vez, la materia ya decidida por los Tribunales Superiores. Los magistrados pueden hacer búsquedas inteligentes por palabra clave en general, por fecha de distribución, por órgano juzgador, por magistrado, por parte, por abogado y por otras demandas que los juzgados necesiten. También pueden verificar casos repetitivos, agruparlos y juzgarlos conjuntamente a partir de una decisión paradigma.[209]

Finalmente, destacamos los casos de China, país que cuenta con un robot asistente de información al público, Xiaofa, implementado en cortes en Nanjing, Xi'an y Guangzhou, el cual ha sido entrenado con más de 20.000 regulaciones y es capaz no sólo de repetir normas, sino de transformarlas a lenguaje "no jurídico", es decir, lenguaje de uso común para la ciudadanía, pudiendo responder más de 40.000 preguntas sobre litigación en diversas áreas del serecho, desde divorcios y violencia doméstica hasta bancarios[210]; y Estonia, en donde su Ministerio de Justicia ha decidido invertir en IA con el propósito de sustituir a jueces humanos para resolver juicios de escasa cuantía, con la posibilidad de que las decisiones tomadas por la máquina, sean finalmente revisadas por un humano en grado de apelación [211].

III.- EL CASO DEL SUPERIOR TRIBUNAL DE JUSTICIA DE LA PROVINCIA DE BUENOS AIRES Y EL ANÁLISIS DE LA SUFICIENCIA TÉCNICA RECURSIVA

publicado en el diario La Ley de fecha 29-IX-2017.

208 "*Inteligencia artificial y blockchain en la Corte Constitucional de Colombia: `Otra experiencia Prometea´*"; publicado en el Diario Constitucional y Derechos Humano nro. 214 de DPI del 4-II-2018.

209 Esta herramienta está siendo implementada en Brasil, más precisamente en la Cámara Civil del Tribunal de Justicia de Minas Gerais, el cual logró juzgar, con apenas un "click", un total de 280 procesos. http://www.tjmg.jus.br/portal-tjmg/noticias/tjmg-utiliza-inteligencia-artificial-em-julgamento-virtual.htm#.XPBE3dNKi8r [Fecha última consulta: 29 de julio de 2019]

210 Hoy hay más de 100 robots diferentes repartidos en las más de 3.000 cortes en China que no solo sirven a las partes, sino a abogados, funcionarios de tribunales y jueces. Ver "Jueces e inteligencia artificial en China: ¿podríamos implementar un Xiaofa?", en http://idealex.press/opinion/columnas/xiaofa-jueces-e-inteligencia-artificial-en-china/ [Fecha última consulta: 29 de julio de 2019]

211 Por oposición a *Prometea* y *Radar*, quienes se basan en inteligencia aumentada, es decir, inteligencia artificial más inteligencia humana, esto sustituye directamente al hombre por el robot. "*Estonia construirá 'juez de robot' para eliminar la acumulación de casos*" http://www.legaltechforum.gt/2019/04/01/estonia-construira-juez-de-robot-para-eliminar-la-acumulacion-de-casos/ [Fecha última consulta: 29 de julio de 2019]

La Suprema Corte de Justicia es el Superior Tribunal de la Provincia de Buenos Aires (Argentina). Este organismo, posee diversas competencias que le han sido constitucionalmente asignadas, tales como, por un lado, las administrativas, institucionales y de superintendencia (vgr. remover y trasladar a los funcionarios y empleados de la totalidad de los tribunales de la provincia; el ejercicio del poder disciplinario sobre los mismos; el control de gestión de cada órgano jurisdiccional del Poder Judicial y el diálogo institucional del cuerpo con los restantes poderes del estado) y, por el otro, a las jurisdiccionales (avocamiento y resolución de cuestiones originarias y apeladas).[212]

En cuanto a estas últimas, nos vamos a referir a la competencia apelada, es decir, aquellas cuestiones que llegan a conocimiento del Cimero Tribunal por vía de impugnación. En esa dirección, debemos ilustrar cuáles son, por un lado, las delimitaciones que estableció la Carta Magna local y, por el otro, las cargas procesales que tienen las partes a la hora de interponer un recurso extraordinario.

Según los artículos 161 y 171 de la Constitución provincial, el referido cuerpo colegiado ejerce la jurisdicción de apelación para conocer y resolver acerca de: a) La constitucionalidad o inconstitucionalidad de leyes, decretos, ordenanzas o reglamentos que estatuyan sobre materia regida por dicha Ley Suprema y se controviertan por una parte interesada; b) La aplicabilidad de la ley en la que los tribunales provinciales de justicia en última instancia, funden su sentencia sobre la cuestión que decidan y c) La nulidad argüida contra las sentencias pronunciadas en última instancia por los tribunales locales de justicia, cuando se alegue violación a las mandas contenidas en los artículos 168 y 171 de la Constitución.

Por su parte, el Código de Procedimientos Civil y Comercial, se encarga de receptar tales mandatos constitucionales por medio de sus arts. 279, 297 y 300, estableciendo los recaudos de admisibilidad.[213]

De tal modo, si alguien se siente agraviado por una sentencia y quiere interponer un recurso extraordinario para satisfacer su pretensión, debe: a) optar por el carril idóneo para canalizar sus agravios, b) sortear los recaudos de admisibilidad correspondientes (vgr. interposición en plazo, efectuar el depósito previo, tramitar el beneficio de litigar sin gastos, etc.) y c) realizar una faena que sea técnicamente suficiente como para que el Superior Tribunal pueda decidir acerca de su procedencia.[214]

Dicha actividad recursiva, se encuentra expresamente regulada por el Código ritual, el cual establece que los embates deben contener, en términos claros y concretos,

212 Giannini, L. J., "*El certiorari, la jurisdicción discrecional de las Cortes Supremas*", Librería Editora Platense, La Plata, 2016, págs. 282/291.

213 La presente propuesta también resulta aplicable, en lo pertinente, a lo dispuesto por los arts. 489, 491 y 494 del Código Procesal Penal y 55 y 63 de la Ley de Procedimiento Laboral 11.653.

214 Hitters, J. C., "*Técnica de los recursos extraordinarios y de la casación*", Librería Editora Platense, La Plata, 2da. Edición, 1998, pág. 594.

la mención de la ley o de la doctrina que se repute violada o aplicada erróneamente en la sentencia, indicando igualmente en qué consiste la violación o el error (vgr. inaplicabilidad de una ley determinada; violación al art. 171 de la Constitución provincial por carecer la sentencia cuestionada de fundamentación normativa; inconstitucionalidad de algún texto legal; conculcación de una doctrina legal que la Suprema Corte tenga establecida sobre un tópico determinado; etc.).[215]

Empero, quien define los contornos de los recursos extraordinarios es el propio Superior Tribunal a través de su doctrina, la cual se encarga de precisar cuál es el grado de satisfacción que deben alcanzar los escritos impugnativos para ser considerados suficientes.

Para ejemplifica , ha dicho que quien afirma que una sentencia transgrede determinados preceptos del derecho vigente o denuncia absurdo, anticipa una premisa cuya demostración debe luego llevar a cabo y que el incumplimiento de dichas exigencias provoca la insuficiencia del intento revisor.[216] También, que no resulta atendible un recurso extraordinario que se desentiende por completo de las normas legales expresamente actuadas en la resolución en crisis[217] y que cuando se denuncia infracción de doctrina legal, es necesario que el recurrente cumpla con la carga de individualizarla, a fin de exponer su similitud con el caso, si pretende su aplicación, ya que el incumplimiento de tales exigencias, también torna insuficiente la impugnación. [218]

Además, ha sostenido que son tan distintas las fuentes de los medios de impugnación a que se refieren los arts. 161, 168 y 171 de la Constitución provincial y 279 y 296 del Código Procesal Civil y Comercial, que el hecho de que se pretenda fundarlos en los mismos argumentos o entrelazándolos, es totalmente inadmisible.[219]

IV.- SOBRE LA CREACIÓN DE UN ALGORITMO. SUS FUNDAMENTOS

215 Ver postura contraria en Giannini, L. J., ob. cit., pág. 397, su nota. En este segmento, el destacado autor analiza la respectiva remisión que hacen los arts. 297 y 330 -correspondientes a los recursos extraordinarios de nulidad e inconstitucionalidad- hacia el art. 279 y considera prescindible la denuncia de normas legales.

216 Conf. doctr. causas C. 121.715, "Ribulotta", resol. de 27-XII-2017; C. 122.597, "Saavedra", resol. de 26-XII-2018 y C. 123.088, "Giorgi", resol. de 10-IV-2019; entre muchas. Fuente: https://mev.scba.gov.ar/

217 Conf. doctr. causas C. 121.887, "Salerno", resol. de 25-X-2017; C. 121.591, "Monte", resol. de 21-XI-2018 y C. 122.859, "Rodríguez", resol. de 20-III-2019; entre varias. Fuente: https://mev.scba.gov.ar/

218 Conf. doctr. causas C. 121.432, "Ascuaga", resol. de 28-VI-2017; C. 122.928, "Muñoz", resol. de 19-XII-2018 y C. 123.047, "González", resol. de 10-IV-2019; entre tantas. Fuente: https://mev.scba.gov.ar/

219 En lo que denomina el Supremo Tribunal, "el recurso promiscuo", cuyo rechazo está sustentando en la insuficien e fundamentación. Conf. doctr. causas C. 121.164, "Navas", resol. de 28-XII-2016; C. 122.085, "Cura", resol. de 27-XII-2017 y C. 122.737, "Pacenza", resol. de 17-X-2018; entre otras. Fuente: https://mev.scba.gov.ar/

Como punto de partida, debemos consignar que la Suprema Corte de Justicia al igual que otros Superiores Tribunales de Latinoamérica- se encuentra sumergida en la denominada "crisis cuantitativa de los Superiores Tribunales". Esta denominación, no hace otra cosa más que referir a la sobrecarga de trabajo que está sometida producto del lugar que ocupa dentro de la "pirámide" de justicia y de la cantidad de pretensiones impugnativas a las que se encuentra sometida como consecuencia de la propia actividad jurisdiccional[220].

En referencia a lo expuesto, nos preguntamos ¿podría crearse un algoritmo susceptible de determinar la suficiencia técnica de un recurso xtraordinario?

Consideramos que la posibilidad de diseñar un sistema complejo -sustentado en políticas públicas de administración- que utilice aprendizaje automático para detectar patrones relevantes y, sobre esa base, tome una decisión a través de un mecanismo predictivo, es altamente factible y deviene necesaria[221], ya que aumentaría exponencialmente la productividad del órgano[222] y descomprimiría su agenda[223].

He aquí algunos fundamentos.

En primer lugar, porque el proceso judicial ya cuenta con la digitalización de los escritos. Es decir, si las partes realizan sus presentaciones en forma electrónica y los jueces emiten sus sentencias definitivas con firma digital, la obtención y procesamiento de los datos que hagan a la fundamentación del recurso, pueden ser fácilmente[224] analizados[225]. Sin embargo, aunque esto no ocurra, también el procesamiento de los datos resultaría fácil mediante la utilización de un software OCR (Optical Character Recognition).

En segundo plano, porque tanto la normativa constitucional como la procesal anticipan en forma previa a la confección del escrito, cuáles son las formalidades que debe atender cada recurso para lograr el éxito en la casación. Además, como vimos,

---

220 Según la estadística oficial, el mentado órgano recibe -en promedio- 4.539 causas por año, ver http://www.scba.gov.ar/planificacion/suprema 20corte%20-%20ingresadas.pdf [Fecha última consulta: 29 de julio de 2019]

221 Sobre todo, en cuestiones netamente patrimoniales, en donde los derechos involucrados son materia disponible para las partes y no afectan el orden público.

222 Se dice que la IA hoy por hoy brinda como mínimo un 300% de eficiencia y puede llegar a superar el millón por ciento. "*Usamos la inteligencia artificial…*", cit.

223 De acuerdo a la última estadística publicada, en el año 2018, la Suprema Corte tuvo un ingreso de 4.388 causas, de las cuales 3.951 han arribado por vía de apelación extraordinaria. Fuente: http://www.scba.gov.ar/informacion/estadisticas.asp?opcion=2 [Fecha última consulta: 29 de julio de 2019]

224 "Las tareas donde el resultado deseado puede describirse fácilmente y existe una necesidad limitada de juicio humano, generalmente, son más fáciles de automatizar. Vaccarezza, Pablo, ¨¿Qué esperar de la inteligencia artificial?" http://laley.thomsonreuters.com/nota/23 [Fecha última consulta: 29 de julio de 2019]

225 En esta actividad, resulta necesaria la confrontación del escrito recursivo con los actos procesales anteriores a su interposición, tales como la sentencia definitiva, el escrito de expresión de agravios o la demanda.

es la propia Corte la que "predice", a través de su doctrina legal, cuáles son las consecuencias derivadas del incumplimiento de la actividad impugnativa.[226]

En ese contexto: a] encontrándose digitalizados los fallos de la Corte[227], la automatización de las decisiones no traería obstáculos; b] el mecanismo de carga de información contaría con la debida transparencia que toda administración pública debe guardar[228] y c] el recaudo de previsibilidad, en aras de que se respeten las garantías constitucionales, estaría abastecido.

En tercer orden, porque la herramienta informática no tiene la posibilidad de provocar sesgos derivados de la automatización, ya que la satisfacción de las exigencias técnico-formales previstas por la normativa aludida, se muestra en forma evidente. Empero, siendo que éstas, más allá de su incumplimiento, son dejadas de lado con menuda frecuencia a la luz de los derechos que se encuentren involucrados[229], la posibilidad de incluir estas variables al sistema, tampoco se constituye en un escollo.[230]

En cuarto turno, porque la incorporación de la IA a la función pública mediante técnicas de automatización, no está basada en la sustitución o eliminación de puestos de trabajo, sino que apunta a abordar tareas rutinarias, mecánicas y repetitivas, brindándole la posibilidad al operador jurídico para que se reconvierta, potencie su propia inteligencia y dedique su tiempo a otras tareas afines. En otras palabras, aunque cierta tarea se automatice, esto no significa que se vaya a sustituir a la persona por la máquina[231]. Por el contrario, su implementación generaría una gran oportunidad

226 En el punto, compartimos el análisis que realiza el procesalista español Nieva Fenoll respecto de la posibilidad de la creación de un algoritmo para el Supremo Federal de los Estados Unidos en la admisión de recursos (writ of Certiorari). El referido autor destaca que la mayoría de los criterios fijados en las "Rules of the Supreme Court of the United States" son aptos para elaborar un sencillo algoritmo y que, conociéndolo, se aumentarían las garantías de los justiciables en el proceso acerca del cálculo de sus posibilidades en el mismo y no dependerían ya del factor humano de los jueces (ob. cit., págs. 37/39). También deviene aplicable al acogimiento o rechazo de recursos por "casos análogos" o como dispositivo de selección mediante la causal de "insustancialidad" (v. art. 31 bis de la ley orgánica del Poder Judicial bonaerense n° 5.827, texto según 13.812).

227 *In extenso* desde el año 1986. Más información en https://juba.scba.gov.ar/

228 Se ha dicho que la técnica de automatización más predicción aplicada al sector público, podría ser muy útil cuando existen tendencias claras, jurisprudencia o actividad administrativa previa relativamente estable. "*Prometea. Inteligencia artificial para transformar organizaciones públicas*", Editorial Astrea, Buenos Aires, 2019, pág. 65.

229 Conf. causas C. 96.826, "Juzgado Notarial General San Martín", sent. de 14-VIII-2013; P. 116.393, "Figueroa", resol. de 11-XII-2013 y A. 70.155, "Instituto Médico Constituyentes S.A.", sent. de 23-XII-2013; etc. Fuente: https://mev.scba.gov.ar/

230 "Es importante tener en cuenta que el desarrollo de la IA no consiste –al menos exclusivamente– en imitar o copiar el cerebro humano. La IA utiliza diversos métodos para procesar la información y resolver problemas o tomar decisiones y no necesita copiar al cerebro, del mismo modo en que los ingenieros en aviación no necesitaron copiar o imitar el método o las técnicas de aprendizaje de los pájaros para construir los aviones modernos". Corvalán, Juan G.; "*Inteligencia Artificial y Derechos Humanos*", cit.

231 La automatización, en defini iva, efectivamente sustituirá ciertas actividades en el ámbito de un empleo y ello en esencia transformará la naturaleza de los trabajos, pero estos, en sí mismos, no se encuentran en riesgo. El eje de discusión debe situarse en actividades o tareas y no en puestos de trabajos. Gil, Gabriela F., "*La inteligencia predictiva como herramienta de eficacia en la gestión judicial*", AR/DOC/3637/2018.

para reconfi urar la división de tareas, aumentar la eficiencia productiva y mejorar la relación Estado-Ciudadanía.[232]

Finalmente, como aporte más significativo y yendo al punto de partida que aludimos, la utilización de la IA en el proceso llegaría para palear la problemática que aqueja al servicio de justicia desde hace mucho tiempo y que, aún hoy en día, no se ha logrado revolver pese a los innumerables proyectos de reformas y a las distintas estrategias que se han intentado para reducir el tiempo en la resolución de los conflicto [233].

En ese sentido, si bien la Suprema Corte de Justicia puede expedirse -a través del mecanismo del Certiorari- en un plazo razonable que ronda los 80 días corridos[234], la aplicación de un sistema disruptivo como *PROMETEA* -que supo generar en el Ministerio Público Fiscal de la Ciudad de Buenos Aires, 1.000 dictámenes relativos al derecho a la vivienda en 45 días frente a los 174 que demanda habitualmente y reducir el tiempo de control de requisitos formales de los expedientes de 160 días de trabajo a 38 en 1000 causas; en la Corte Constitucional Colombiana, sugerir casos prioritarios de atención sobre derecho a la salud en 2 minutos frente a los 96 días que se requieren; en un Juzgado Civil y Comercial del Departamento Judicial de Morón, 3.443 resoluciones iniciales de cobros ejecutivos frente a las 720 que se pueden hacer en un mes y en un Juzgado Penal de Córdoba, 495 sentencias de juicio abreviado contra 66 en igual período[235]- parece responder a la cuestión y palear la crisis material que afronta.

V.- A MODO DE CONCLUSIÓN

Es evidente que la implementación de la tecnología, a través de bases jurisprudenciales, mesas de entradas virtuales, presentaciones, notificaciones y subastas electrónicas, videograbación de audiencias, sistemas de gestión, videoconferencias, etc., ha conseguido importantes avances para el proceso.

---

232 Conf. *"Prometea. Inteligencia artificial para transformar organizaciones públicas"*, ob. cit., págs. 6 y 11.

233 Ver Camps, C. E., *"Hora clave para el futuro de la eficacia procesal bonaerense"* https://carlos-camps.com/2019/05/23/hora-clave-para-el-futuro-de-la-eficacia-procesal-bonaerense/ [Fecha última consulta: 29 de julio de 2019]

234 Dando cumplimiento al art. 286 del Código Procesal Civil y Comercial. Estadística elaborada en base a 20 causas Civiles y Comerciales tomando como fecha de inicio el ingreso del expediente hasta la fecha de su resolución (C. 122.508; C. 122.396; C. 123.047; C. 122.996; C. 122.986; C. 122.914; C. 122.597; C. 122.847; C. 122.822; C. 122.873; C. 122.823; C. 122.809; C. 121.497; C. 122.693; C. 122.683; C. 122.382; C. 121.164; C. 121.305; C. 122.671 y C. 122.477). Fuente: https://mev.scba.gov.ar/

235 Datos aportados por el IALAB (Laboratorio de Innovación e Inteligencia Artificial de la Universidad de Buenos Aires) y *"Prometea. Inteligencia artificial para transformar organizaciones públicas"*, ob. cit., págs. 44 y 45 y *"Aprovechamos la inteligencia artificial…"* cit.

Sin embargo, la incorporación de nuevas tecnologías de información y comunicación (TIC), capaces de generar inteligencia predictiva, puede ayudar a rediseñarlo.

En ese contexto, consideramos que el empleo de una aplicación disruptiva, sustentada en políticas públicas de administración y fundamentada en los principios de legalidad, debido proceso y defensa en juicio, tendiente a consagrar el derecho a obtener una sentencia en un plazo razonable[236], puede ser la clave para aumentar la eficacia procesal.

Para ello, resulta necesario que primero derribemos aquellas barreras mentales que, en definitiva, impiden el efectivo goce de los derechos de los habitantes y la reconversión del operador jurídico. Como bien dijo Sócrates, si realmente deseamos obtener distintos resultados, debemos enfocar toda nuestra energía no en luchar contra lo viejo sino en construir lo nuevo.

236 Conf. Corte Interamericana de Derechos Humanos, autos "*Furlán y familiares vs. Argentina*", sent. de 31-VIII-2012; entre otras. http://www.corteidh.or.cr/cf/jurisprudencia2/ficha_tecnica cfm?nId_Ficha=210 [Fecha última consulta: 29 de julio de 2019]

IA EN CONTACTO CON EL DERECHO[237]

Eje temático: Inteligencia Artificial y su articulación con el Derecho

Autor:
Angie Verónica Rubio Velásquez
Estudiante de quinto semestre de la Facultad de Derecho, estudiante investigadora adscrita al Semillero de Derecho y Tecnología en la Sociedad de la Información (DITSI), vinculada al Grupo de Investigación Doctor Angélico Iuris Et Realitas Categoría C de la facultad de Derecho de la Universidad Santo Tomás, Sede Villavicencio. Angie.rubio@usantotomas.edu.co

RESUMEN
En la siguiente ponencia se desarrollará el eje temático de Inteligencia Artificial (IA) y su articulación con el Derecho. De acuerdo a esto, se expondrán algunos conceptos fundamentales para entender las enunciadas áreas y su fusión. Dichos conceptos comprenderán aquellos referidos a la administración de justicia, derecho, software, robótica e inteligencia artificia ; estableciendo un preámbulo claro y conciso que permita una total asimilación por parte del público acerca de la temática de esta ponencia.
Actualmente la IA ha abarcado la mayoría de ramas y actividades que desarrolla el hombre, y dicha propagación se ha incorporado con más prontitud en ciertas áreas naturalmente relacionadas a la tecnología, que con otras no tan familiares con la última mencionada. Sin embargo; es indubitable que han hecho contacto con dichas materias distantes y por tanto es menester entender contiguamente cómo es posible la relación tecnológica de la IA con el derecho; su correcta implementación, sus principales problemas y los objetivos a lograr con la unión de estas dos áreas. Este trabajo nos mostrará cómo se está implementando la IA al mundo jurídico en diversas instituciones y desarrollos. Ya que el derecho persigue un mejoramiento a la sociedad mediante la implementación de justicia y la IA permite mecanismos eficace y de respuesta ágil, las distintas ramas del derecho han decidido optar por la implementación de IA a sus ejercicios. Esta fusión deja paso a diferentes inquietudes por parte de usuarios y beneficiados, ya que si bien el fin de implementar justicia se ve ocasionalmente interrumpida por los incorrectos juicios del hombre, es inquietante saber, cómo pues, un sistema de IA diseñado por el razonamiento de los mismos hombres pueden dar respuestas diferentes a las mismas problemáticas. Consecuentemente, se esbozarán los múltiples beneficio , dificultades y prevenciones a tomar en la acomodación de la IA al derecho. Conduciéndonos a la terminación de que si bien es inaplazable la fusión de éstas dos áreas; será de vital importancia el minucioso cuidado al momento de elegir los razonamientos de estas máquinas, pues de su discernimiento dependerá el orden y la justicia de la sociedad en cuestión.

MARCO TEÓRICO

A continuación esbozaré el marco teórico pertinente para la comprensión de los temas a tratar con esta ponencia. Los siguientes conceptos estarán respaldados con la citación de los expertos doctrinantes en cada materia, y así mismo; conllevará la mayor brevedad y practicidad para una comprensión amena y clara por parte del público.

237 Artículo resultado del proyecto de investigación denominado Inteligencia Artificial al Servicio de la Justicia desarrollado en el Semillero de Derecho y Tecnologías en la Sociedad de la Información. Para participar como ponente en el XXIII Congreso Iberoamericano de Derecho e Informática a realizarse del 01 al 04 de Octubre del 2019 en la ciudad de San Pablo – Brasil.

Software: Según una breve citación acerca de qué es software, el autor de uno de los libros más acudidos sobre la materia escogió la siguiente, "el software es: instrucciones (programas de cómputo) que cuando se ejecutan proporcionan las características, función y desempeño buscados" (Pressman, 2010, p. 3)[238]. Dentro de éste también subyacen varios tipos o materias como: Software incrustado, de sistemas, aplicación, ingeniería y ciencias, de línea de productos, de inteligencia artificial, etc. Sin embargo; la definición más generalizada aplicada a dichas materias, sería el expuesto anteriormente.

Robótica: Es una disciplina que combina todas aquellas actividades relacionadas con el estudio, diseño, construcción, operación y mantención de robots. Es un campo de trabajo que combina diferentes disciplinas como Ingeniería Eléctrica, Ingeniería Electrónica, Ingeniería Mecánica, Ciencias de la Computación, Matemáticas, Física, Biología, Neurociencias, etc. Ruiz, J. & Salazar, R. (2007)[239].

Inteligencia Artificial: La inteligencia artificial (IA) ha venido abriéndose campo durante las últimas décadas. Es una definición amplia la cual abarca, tiene por objeto el estudio del comportamiento inteligente en las máquinas. Dicho comportamiento supone percibir, razonar, aprender, comunicarse y actuar en entornos complejos (Nilsson, 2001, pp. 1)[240]. Según la RAE, la IA es la disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico. Para lograr entender si una máquina posee IA, Alan Turing dispuso el llamado Test de Turing en 1950. Para lograr resolver dicha incertidumbre, el examen evaluará las capacidades de: reconocimiento del lenguaje natural, razonamiento, aprendizaje y representación del conocimiento. Una vez superadas de manera satisfactoria estas capacidades; la máquina será catalogada como una máquina de IA.

A.)Tipos

Hay cuatro tipos de IA según Stuart Russell y Peter Norving: A) los sistemas que piensan como humanos, estos realizan actividades como resolución de problemas, toma de decisiones y aprendizaje mediante la automatización de actividades. B) Los

238 Pressman, R. (2010). *Ingeniería del Software*. 7ª ed. México: McGraw-Hill companies.

239 Ruiz, J. & Salazar, R. (2007). *Introducción a la robótica*. Disponible en: http://cooperativabarbosa.edu.co/documentos/c apitulo1.pdf

240 Nilsson, J., (2001). *Inteligencia Artificial: Una nueva síntesis*. Madrid. McGraw-Hill.

sistemas que actúan como humanos, los cuales imitan el comportamiento humano, por ejemplo; la robótica. C) Los sistemas que piensan racionalmente, los cuales serían los sistemas expertos. Éstos tratan de imitar el pensamiento humano. Y por último; D) los sistemas que actúan racionalmente, los cuales vendrían a ser a manera de ejemplo, los agentes inteligentes (Russell y Norving, 2009, p.2)[241].

Además, es también objeto de estudio en la diferente doctrina sobre IA, las materias o campos que tienen que ver con: sistemas reactivos, búsqueda en espacios de estado, representación del conocimiento y razonamiento, métodos de planificación basados en lógica, comunicación e integración, entre otros.

B.) Objetivos

Los objetivos de la IA se sintetizan en poder alcanzar el aprendizaje y razonamiento de la mente humana, logrando dar respuestas y facilitando todas las áreas del conocimiento o desempeño que el hombre llegue a necesitar. Lograr éste nivel de raciocinio y aprendizaje será el determinante de la IA y su anhelada expresión.

Administración de Justicia: Según la Ley 270 de 1996, la administración de justicia es definida en su artículo 1° de la siguiente manera:

> La administración de justicia es la parte de la función pública que cumple el Estado encargada por la Constitución Política y la ley de hacer efectivos los derechos, obligaciones, garantías y libertades consagrados en ellas, con el fin de realizar la convivencia social y lograr y mantener la concordia nacional. (Ley 270, 1996)[242].

Acceso a la justicia: La ONU definió el acceso a la justicia como un principio básico del Estado de Derecho. "Sin acceso a la justicia, las personas no pueden hacer oír su voz, ejercer sus derechos, hacer frente a la discriminación o hacer que rindan cuentas los encargados de la adopción de decisiones" (ONU, 2019)[243]. Ésta además debe ser imparcial y no discriminatoria.

Según el Ministerio de Justicia, el acceso a la justicia es una pieza fundamental del Estado Social de Derecho, por la relación intrínseca que tiene con la reducción de la pobreza y el crecimiento inclusivo. El acceso a la justicia abarca cada aspecto

241 Russell, Stuart J.; Norvig, Peter Norvig (2009). *Artificial intelligence: a modern approach* (en inglés) (3.ª edición). Upper Saddle River, N.J.: Prentice Hall. ISBN 0-13-604259-7.

242 Congreso de Colombia. (7 de marzo de 1996) Ley estatutaria de la administración de justicia. [Ley 270 de 1996]. Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6548

243 Naciones Unidas. (2019). Acceso a la Justicia. Recuperado de https://www.un.org/ruleoflaw/es/thematic-areas/access-t -justice-and-rule-of-law-institutions/access-to-justice/

de la cotidianidad, incluyendo la salud, el empleo, la educación, la vivienda y el emprendimiento. Además, en la sentencia T-283/13, se estableció concepto sobre el derecho de acceso a la administración de justicia, de la siguiente manera:

> El derecho a la administración de justicia ha sido defini o por la jurisprudencia constitucional como la posibilidad reconocida a todas las personas residentes en Colombia de poder acudir en condiciones de igualdad ante los jueces y tribunales de justicia, para propugnar por la integridad del orden jurídico y por la debida protección o el restablecimiento de sus derechos e intereses legítimos, con estricta sujeción a los procedimientos previamente establecidos y con plena observancia de las garantías sustanciales y procedimentales previstas en las leyes. Aquella prerrogativa de la que gozan las personas, naturales o jurídicas, de exigir justicia, impone a las autoridades públicas, como titulares del poder coercitivo del Estado y garantes de todos los derechos ciudadanos, distintas obligaciones para que dicho servicio público y derecho sea real y efectivo. Corte Constitucional. (16 de mayo de 2013) Sentencia T- 3.567.368 [MP Jorge Ignacio Pretelt Chaljub].[244]

Celeridad en la administración de justicia: Según la ley 270 de 1996[245], la celeridad en la administración de justicia debe ser pronta, cumplida y eficaz en la solución de fondo de los asuntos que se sometan a su conocimiento. Los términos procesales serán perentorios y de estricto cumplimiento por parte de los funcionarios judiciales. Su violación injustificada constituye causal de mala conducta, sin perjuicio de las sanciones penales a que haya lugar. Lo mismo se aplicará respecto de los titulares de la función disciplinaria. Así mismo, la Corte Constitucional en sentencia C-826-13 expresó sobre el principio de celeridad lo siguiente:

> En cuanto al principio de celeridad, la jurisprudencia de esta Sala ha sostenido que éste implica para los funcionarios públicos el objetivo de otorgar agilidad al cumplimiento de sus tareas, funciones y obligaciones públicas, hasta que logren alcanzar sus deberes básicos con la mayor prontitud, y que de esta manera su gestión se preste oportunamente cubriendo las necesidades y solicitudes de los destinatarios y usuarios, esto es, de la comunidad en general. Igualmente ha señalado esta Corporación, que este principio tiene su fundamento en el artículo 2º de la Constitución Política, en el cual se señala que las autoridades de la Nación tienen la obligación de proteger la vida, honra, bienes, creencias y demás derechos y libertades de los ciudadanos, al igual que asegurar el cumplimiento de los deberes sociales del Estado y de los particulares, lo cual encuentra desarrollo en artículo 209 Superior al declarar que la función administrativa está al servicio de los intereses generales entre los que se destaca el de la celeridad en el cumplimiento de las funciones y obligaciones de la administración pública.[246]

244 Corte Constitucional, (2013) T- 3.567.368. [MP Jorge Ignacio Pretelt Chaljub].

245 Congreso de Colombia. (7 de marzo de 1996) Ley estatutaria de la administración de justicia. [Ley 270 de 1996]. Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6548

246 Corte Constitucional, (2013) D-9623 [MP Luis Ernesto Vargas Silva].

Con este precedente, podremos ver en ésta ponencia cómo la IA ayudará a la celeridad en la administración de justicia, facilitando los diversos procesos que ésta necesita para hacerse efectiva y célere.

ACTUALIDAD

Hoy por hoy la IA es capaz de detectar el fraude, ayudar a la vigilancia y seguridad, detectar rostros y relacionarlos en fotografías y videos (administración de fotografías), contribuir al ahorro de energía, investir de autonomía a los vehículos, manejar la exploración espacial,

> En la actualidad ya es usada para guiar naves espaciales en sus viajes a cuerpos del sistema solar. Robots enviados a Marte como el Spirit y el Opportunity fueron dirigidos por algoritmos autónomos, y otros como el Curiosity desarrollan investigaciones independientes en las cuales seleccionan las zonas para estudiar y fotografi r en aquellos remotos lugares. El Tiempo,Vargas, (2019)[247].

Inclusive; la IA hoy día habita en un robot con "razonamiento humano".

> Sophia fue construida por Hanson Robotics, empresa norteamericana con base en Hong Kong, a imagen y semejanza de la actriz hollywoodense Audrey Hepburn y es capaz de mostrar 62 expresiones faciales. Ha visitado ciudades, universidades, estudios de grabación del mundo. Y desde 2017 es el primer robot en tener una nacionalidad: es ciudadana saudí. El Tiempo, Editorial, (2018)[248].

Para el derecho, actualmente se usa en ciertos sectores el modelo Watson de IBM,

> Watson es una herramienta de computación cognitiva que reconoce el lenguaje natural utilizado por los humanos, responde a preguntas complejas analizando gran cantidad de información, muestra de forma clara y sencilla su razonamiento y tiene capacidad de aprendizaje. Este sistema evita la utilización de una modelización del conocimiento jurídico. Más directamente, recurre a la utilización de una enorme capacidad de proceso de datos para interpretar el lenguaje natural utilizado por el usuario, contrastarlo con

247 Vargas, S., (2019). *La inteligencia artificial, a la conquista del universo* / Opinión. El Tiempo. Recuperado de https://www.eltiempo.com/vida/ciencia/inteligencia-artificial-a-la-conquista-del-un - verso-columna-de-santiago-vargas-344136

248 Editorial, (2018). *El mundo de Sophia: La primer robot humanoide con inteligencia artificial avanzada estuvo en Colombia esta semana*. El Tiempo. Recuperado de https://www.eltiempo.com/opinion/editorial/el-mundo-de-sophia-robot-con-inteligencia-artificial-en-medellin-25035

una gran cantidad de datos (contenidos tanto en textos jurídicos generales, como específicos del usuario), analizarlos y ser capaz de proponer alternativas eficientes." Noticias Jurídicas, Hernández y Boulat, (2015 [249].

Actualmente el derecho ha iniciado los ejercicios de implementación de IA a sus diferentes áreas y ramas correspondientes. De esto puede observarse a manera de ejemplo los tutores inteligentes proporcionados por el sistema CATO desarrollado por Kevin Ashley en Pittsburg, el cual proporciona diversos casos, instrucciones y maneras de argumentar o contra-argumentar a aquellos que hagan uso de dicho sistema. También observamos otros ejemplos como el sistema Split-Up (Legal Advisory Systems), el cual brinda información probable de la situación jurídica a la hora de la disolución de un vínculo matrimonial. [250]

En Colombia se ha implementado recientemente la IA en instituciones como el Ministerio de Educación, quienes han ahorrado más de US$340 millones al detectar miles de 'niños fantasma' que recibían recursos sin siquiera existir. Además, esta implementación de IA permite detectar cuándo están las familias en sus casas para poder entregar a tiempo las raciones de comida del Plan de Alimentación Escolar y así evitar su caducidad. Por otro lado, la Contraloría General de la República está implementando la IA para vigilar a los contratistas en casos de fraude, corrupción o incumplimiento de requisitos, y corolario a esto generar las alarmas respectivas.[251] La Corte Constitucional también se ha apuntado al uso de la IA y ha introducido a 'Prometea', un sistema de IA para la selección de tutelas que actualmente opera sobre el campo de la salud. [252]

INQUIETUD PRINCIPAL

249 Hernández, F., Boulat, P., (2015). *Inteligencia Artificial y Derecho. Problemas y perspectivas*. Noticias Jurídicas. Recuperado de http://noticias.juridicas.com/conocimiento/articulos-doctrinales/10061-inteligencia-artificial- -derecho-problemas-y-perspectivas/

250 Cáceres, E. (2006). Boletín Mexicano de Derecho Comparado. *Inteligencia artificial, derecho y E-JUSTICE (El Proyecto IIJ-CONACYT), volumen (39. No.116)*. Recuperado de http://www.scielo.org.mx/scielo.php?pid=S0041-86332006000200012&script=sci_arttext

251 Neira Marciales, L. (20 de marzo de 2019). El Gobierno de Colombia le apuesta al desarrollo de la Inteligencia Artificial. *La República*. Recuperado de https://www.larepublica.co/alta-gerencia/el-gobierno-de-colombia-le-puesta-al-desarrollo-de-la-inteligencia-artificial-284183

252 Rivadeneira, J. (22 de marzo de 2019). Prometea, inteligencia artificial para la revisión de tutelas en la Corte Constitucional. *Legis Ámbito Jurídico*. Recuperado de https://www.ambitojuridico.com/noticias/informe/constitucional-y-derechos-humanos/prometea-inteligencia-artificial-para-l

Sin embargo, el uso e implementación de la IA en un campo como el derecho que implica impostergables razonamientos multi-temáticos y decisiones, genera cierta especulación acerca de la asertividad que puedan llegar a tener dichos sistemas para la solución de conflictos en la sociedad. Pues es claro que para impartir justicia se necesita de discernimiento entre lo justo y lo injusto, una visión amplia acerca del contexto en que se manejan los casos y por supuesto; un precedente educativo que permita llegar a una correcta decisión. Sin embargo, esta clase de ejercicios ha sido desarrollada por el hombre hasta el momento gracias a su discernimiento netamente biológico. Seguidamente; es claro y manifiesto que dichas conjeturas hechas por los funcionarios no han sido siempre correctas, justas o céleres. Pues bien el hombre es susceptible de diversas dinámicas psicológicas en razón de su naturaleza biológica y aspectos claves como educación, cosmovisión, emociones, políticas y demás dinamismos propensos a la identifi ación del hombre. Entonces se despliega la inquietud principal: ¿Cómo puede la IA estar libre de éstos dinamismos si es creada por el mismo hombre?

Emociones e identificaci n psicológica es de lo que carece la Robótica, el Software, la Maquinaria y la Inteligencia Artificial. Es así pues que la IA quedaría exenta de decisiones guiadas por factores distintos a la previa información académica, práctica y de razonamiento implementado en dichos sistemas de IA señalados anteriormente. Por supuesto será vital utilizar las pruebas matrices como el Test de Alan Turing para verificar la efectividad de la máquina en cuestión. Además, de seguir la implementación hecha hasta el momento en Colombia por parte de la Corte Constitucional; los usos y resultados efectuados por sistemas de IA estarían sujetas al 'ojo público' como se ha manejado con Prometea. Esto permitiría un control por parte de la ciudadanía y una respectiva vigilancia en la implementación y ejercicios efectuados con IA.

PERSPECTIVA GENERAL

A continuación plasmaré una tabla general de las ventajas y desventajas que implica la implementación de IA al Derecho.

VENTAJAS	DESVENTAJAS
Celeridad en la administración de justicia.	Miedo al cambio.
Respuestas absentas de vicios de juicio biológico.	Falta de recursos prácticos en la implementación de IA con el Derecho.
Economía de recursos a largo plazo.	Exigencia económica a corto plazo.
Perdurabilidad y constante mejoramiento de los conocimientos adquiridos para una mejor aplicación caso a caso.	Incertidumbre respecto de la evolución trayectoria en el trabajo de los diferentes funcionarios y litigantes del Derecho.

CONCLUSIÓN

En suma de lo tratado hasta el momento, es evidente que la IA es una realidad para el Derecho y éste debe adaptarse a este nuevo recurso para así incrementar la exactitud, efectividad y celeridad en sus fines y objetivos. Claramente las circunstancias y la naturaleza primicia de la materia, hacen de este camino de implementación algo más complejo de lo que se visualiza en los escritos y opiniones dadas hasta el momento. La incertidumbre acerca de las carreras profesionales de miles, los cuestionamientos filosóficos la excitación de ver un mundo más justo, los estudios por hacer y la información a implementar abundan. Los pasos a seguir como la elección de la maquinaria, la aplicación de pruebas como el Test de Alan Turing para verificar la efectividad del sistema, y el trayecto en general no son sencillos. Sin embargo; de hacerlo correctamente será sin duda gratamente efectivo. Los beneficios a recibir en consecuencia de esta implementación, cambiarían drásticamente una historia de corrupción e injusticias de las que han sido víctimas Naciones enteras, sería el paso más crucial a un camino de celeridad y verdadera justicia.

BIBLIOGRAFÍA

Cáceres, E. (2006). Boletín Mexicano de Derecho Comparado. Inteligencia artificial, derecho y E-JUSTICE (El Proyecto IIJ-CONACYT), volumen (39. No. 116). Recuperado de http://www.scielo.org.mx/scielo.php?pid=S0041-86332006000200012&script=sci_arttext

Congreso de Colombia. (7 de marzo de 1996) Ley estatutaria de la administración de justicia. [Ley 270 de 1996]. Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6548

Corte Constitucional, (2013) D-9623 [MP Luis Ernesto Vargas Silva].

Corte Constitucional, (2013) T- 3.567.368. [MP Jorge Ignacio Pretelt Chaljub].

Editorial, (2018). *El mundo de Sophia: La primer robot humanoide con inteligencia artificial avanzada estuvo en Colombia esta semana*. El Tiempo. Recuperado de https://www.eltiempo.com/opinion/editorial/el-mundo-de-sophia-robot-con-inteligencia-artificial-en-medellin-25035

Hernández, F., Boulat, P., (2015). *Inteligencia Artificial y Derecho. Problemas y perspectivas*. Noticias Jurídicas. Recuperado de http://noticias.juridicas.com/conocimiento/articulos-doctrinales/10061-inteligencia-artificial-y-derecho-problemas-y-

perspectivas/

Naciones Unidas. (2019). Acceso a la Justicia. Recuperado de https://www.un.org/ruleoflaw/es/thematic-areas/access-t -justice-and-rule-of-law-institutions/access-to-justice/

Neira Marciales, L. (20 de marzo de 2019). El Gobierno de Colombia le apuesta al desarrollo de la Inteligencia Artificial. La República. Recuperado de https://www.larepublica.co/alta-gerencia/el-gobierno-de-colombia-le-puesta-al-desarrollo-de-la-inteligencia-artificial-284183

Nilsson, J., (2001). *Inteligencia Artificial: Una nueva síntesis*. Madrid. McGraw-Hill.

Pressman, R. (2010). *Ingeniería del Software*. 7ª ed. México: McGraw-Hill companies.

Rivadeneira, J. (22 de marzo de 2019). Prometea, inteligencia artificial para la revisión de tutelas en la Corte Constitucional. Legis Ámbito Jurídico. Recuperado de https://www.ambitojuridico.com/noticias/informe/constitucional-y-derechos-humanos/prometea-inteligencia-artificial-para-l

Ruiz, J. & Salazar, R. (2007). *Introducción a la robótica*. Disponible en: http://cooperativabarbosa.edu.co/documentos/c apitulo1.pdf

Russell, Stuart J.; Norvig, Peter Norvig (2009). *Artificial intelligence: a modern approach* (en inglés) (3.ª edición). Upper Saddle River, N.J.: Prentice Hall. ISBN 0-13-604259-7.

Vargas, S., (2019). *La inteligencia artificial, a la conquista del universo* / Opinión. El Tiempo. Recuperado de https://www.eltiempo.com/vida/ciencia/inteligencia-artificial-a-la conquista-del-universo-columna-de-santiago-vargas-344136

CROWDFUNDING EN EL DERECHO DE LAS NUEVAS TECNOLOGIAS EN EL PERU: IMPLICANCIAS JURIDICAS DEL FINANCIAMIENTO PARTICIPATIVO FINANCIERO POR INTERNET

Eje Temático: Legaltech, Fintechs y Starup

Autor:
Julio Núñez Ponce
Doctor en Derecho y Ciencia Política por la Universidad Nacional Mayor de San Marcos (UNMSM). Magister en Derecho Empresarial y Abogado por la Universidad de Lima. Profesor de Derecho de las Nuevas Tecnologías en la Universidad ESAN. {PERU}

ABSTRACT
En la presente ponencia se analiza las implicancias jurídicas del financiamiento participativo por internet (crowdfunding) en el Derecho de las Nuevas Tecnologías en el Perú, incidiendo en las propuestas legislativas presentadas en el congreso de la republica peruano, en la legislación sobre identidad digital, firmas y certificados digitales, protección de datos personales, dinero electrónico, afectación tributaria de los servicios digitales en el impuesto a la renta, delitos informáticos. Se plantea la importancia del crowdfunding para promover el desarrollo de las "starups" y medianas y pequeñas empresas en un entorno digital. Una hipótesis presente en la investigacion: es necesario concordar el derecho de las nuevas tecnologías en forma sistémica para proponer una legislación adecuada de crowdfunding en el Perú. El SUMARIO es el siguiente: 1. INTRODUCCION. 2. OBJETO, FINALIDAD; AMBITO DE APLICACIÓN E IMPORTANCIA DE LOS PROYECTO DE LEY PRESENTADOS SOBRE CROWFUNDING EN EL CONGRESO DE LA REPUBLICA PERUANO. 3. ANALISIS DEL CROWDFUNDING EN EL DERECHO DE LAS NUEVAS TECNOLOGIAS PERUANO. 3.1. CROWDFUNDING, LA IDENTIDAD DIGITAL Y LA LEY DE FIRMAS Y CERTIFICADOS DIGITALES. 3.2. RELACION DEL CROWDFUNDING CON LA LEY PERUANA DE PROTECCION DE DATOS PERSONALES. 3.3. RELACION DEL CROWDFUNDING CON LA LEY PERUANA DE DINERO ELECTRONICO. 3.4. RELACION DEL CROWDFUNDING Y FINTECH CON LA AFECTACION TRIBUTARIA DE LOS SERVICIOS DIGITALES EN LA LEY PERUANA DEL IMPUESTO A LA RENTA. 3.5. LA RELACION DEL CRODWFUNDING CON LA LEY DE DELITOS INFORMATICOS Y EL CODIGO PENAL PERUANO. 4. LA INNOVACION, EL EMPRENDIMIENTO, LAS EMPRESAS STAR UP, EL FINTECH Y LA REGULACION DEL CROWDFUNDING EN EL PERU. 5. CONCLUSIONES.

1. INTRODUCCION

Una de las principales categorías de financiamiento colaborativo es el crowdfunding. Etimológicamente del inglés crowd: masa y sourcing (externalización). Pudiendo afirmar que se trata de una externalización masiva por internet. En cambio, fintech o Financial Technology (en español tecnología financiera) es una actividad que aplica la tecnología para mejorar las actividades financieras.

El crowdfunding es, por excelencia el mecanismo para financiar el emprendimiento y la innovación en el mundo. Su rol en la cadena de financiamiento emprendedor es de gran importancia, en razón de que recoge lo que el mercado necesita, valida, democratiza y permite a los reguladores tener finalmente un mecanismo de financiación transparente y en línea (on line). El crowdfunding es fácilmente accesible por internet. Aunque no existe una clasificación única a nivel internacional de los diferentes tipos de operaciones de financiamiento participativo, se suele distinguir entre dos tipos de esquemas: financiero y no financiero. En el primero los inversionistas o aportantes de fondos esperan obtener un retorno financiero como contraprestación a dicha aportación, mientras que en el segundo no existe retronó financiero asociad [253].

"El crowdfunding, motiva la participación, involucra al público con los productos que consume, promueve una relación dinámica mediada por la posibilidad de compartir el conocimiento y la información. Sin duda alguna, este es un conjunto de propiedades que se deben aprovechar y explotar en un mundo como el actual, en donde se necesita un cuidado y atención especial en el desarrollo de los productos y de las ideas creadas y consumidas día tras día, modificando de alguna manera los estilos de vida y la forma en que las personas se conectan entre sí"[254].

"El Crowdfunding surge como una iniciativa colectiva tendiente apoyar económicamente la ejecución de proyectos particulares, no obstante, sus inicios no están marcados con claridad, su reconocimiento formal como plataforma de financiación colectiva ha sido fruto de varios momentos, que aunque recientes, han servido para sentar las bases de lo que al día de hoy se identifica a nivel mundial como crowdfunding"[255].

En el Perú, el 13 de Mayo de 2019 el Poder Ejecutivo ha enviado al Congreso de la República el Proyecto de Ley que Regula el Financiamiento Participativo Financiero por Internet (Crowdfunding), que junto a iniciativa ya existente está siendo analizado

253 Vid. BANCO INTERAMERICANO DE DESARROLLO: "Alternative Finance (Crowdfunding) Regulation in Latin America and the Caribbean". Septiembre 2016.

254 SILVA ORTIZ, Julian Armando: "Beneficios y Riesgos asociados del crowdfunding para el desarrollo y financiamiento de las starup". Universidad Nacional Abierta y a Distancia. Maestria en Administración y Organizaciones. Bogota, Colombia. 2017. En: https://repository.unad.edu.co/bitstream/10596/17384/1/80820494.pdf

255 VILLADA CALDERON, Juan Sebastián y GARCIA LONDOÑO, Carlos: "Crowdfunding y su implementación en Colombia". Tesis de Grado para optar el título de especialista en Derecho Comercial. Pontificia Universidad Javeriana. Facultad de Ciencias Jurídicas. Especialización en Derecho Comercial. Bogotá. D.C., Colombia. 2017. Página 5. En: https://repository.javeriana.edu.co/bitstream/handle/10554/41266/Documento.pdf?sequence=1&isAllowed=y

en las comisiones del congreso peruano. En la exposición de motivos de este proyecto de ley se señala que:

"El financiamiento participativo financiero es un mecanismo bajo el cual un individuo o persona jurídica publicita su proyecto personal o empresarial a través de una plataforma en Internet con el propósito de captar pequeñas contribuciones, a fin de poderlo llevar a cabo. Este mecanismo de financiamiento se constituye en una alternativa de recursos para apoyar una amplia gama de proyectos de negocios"[256].

El Derecho de las Nuevas Tecnologías está en constante crecimiento. El objeto de la presente ponencia es analizar las implicancias jurídicas del crowdfunding en los ámbitos de identidad digital, firmas y certificados digitales, protección de datos personales, legislación de dinero electrónico, afectación tributaria a los servicios digitales por el impuesto a la renta, delitos informáticos, normas promocionales para el emprendimiento e innovación de las starup y modalidades de fintech.

2. OBJETO, FINALIDAD; AMBITO DE APLICACIÓN E IMPORTANCIA DE LOS PROYECTO DE LEY PRESENTADOS SOBRE CROWFUNDING EN EL CONGRESO DE LA REPUBLICA PERUANO

"¿Cómo regular? ¿Cómo regular sin que ello implique un desincentivo para la creación y participación de estas plataformas electrónicas? ¿Cómo regular pensando en las micro, pequeñas y medianas empresas? ¿Cómo regular considerando un sistema financiero como el nuestro y respetando los principios regulatorios que lo guían? Esos son los grandes cuestionamientos que deben ser atendidos por los reguladores involucrados para proponer un esquema regulatorio que no se convierta en el obstáculo de una actividad económica que se está desarrollando y que, de incentivarla adecuadamente, puede implicar una interesante fuente de financiamiento para las empresas que activan de forma constante la economía del país. Justamente, la importancia de otorgar alternativas adicionales a las micro, pequeñas y medianas radica en el hecho de que representando un flujo importante de dinero para la economía peruana son las que más inconvenientes tienen para acceder a financiamientos que pueden contribuir a su desarrollo"[257].

256 CONGRESO DE LA REPUBLICA DEL PERU: Exposición de Motivos de Proyecto de Ley N° 4324/2018-PE que regula el Financiamiento Participativo Financiero. Presentado el 13 de Mayo de 2019. En: http://congreso.gob.pe

257 GUTIERREZ VEGA, Miluska Jazmin: "¿Cómo Regular? Una aproximación al Crowdlending, desde la perspectiva del regulador, como mecanismo adicional de acceso al financiamiento de las micro, pequeñas y medianas empresas". Tesis para optar el Grado Académico de Magister en la Maestría de Derecho Bancario y Financiero. Pontificia Universidad Católica del Perú. Lima, Abril 2018. Pagina 5. En: http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/12044

El desarrollo de la tecnología financiera fintech en el Perú debe ser promovida por la legislación y concretamente el crowdfunding, debe ser adecuadamente regulado. Al respecto, cabe señalar que el Objeto del Proyecto de Ley peruano 4324/2018-PE del 13 de mayo de 2019, es el siguiente: "establecer el marco jurídico para regular y supervisar la actividad de financiamiento participativo financiero, así como las sociedades autorizadas para administrar las plataformas a través de las cuales se realiza dicha actividad".

El financiamiento participativo financiero por internet o crowdfunding es materia de la propuesta legislativa señalada en el ámbito de la regulación y la supervisión. El financiamiento participativo financiero es un mecanismo bajo el cual un individuo o persona jurídica publicita su proyecto personal o empresarial a través de una plataforma en internet con el propósito de captar pequeñas contribuciones, a fin de poderlo llevar a cabo. Este mecanismo de financiamiento se constituye en una fuente alternativa de recursos para apoyar una amplia gama de proyectos de negocios.

En otro Proyecto de Ley peruano 3083/2017-CR del 27 de junio de 2018, nótese que hay una diferencia en el enfoque, al señalar que su objeto es: "regular el régimen jurídico de las plataformas de financiamiento participativo-PFP. Establece las normas a las que deben sujetarse las personas jurídicas cuyo objeto social sea administrar plataformas de financiamiento participativo-PFP, con el fin de financiar el emprendimiento y la innovación". Se hace énfasis en la regulación para la financiación de las "starup" y las iniciativas innovadoras de pequeñas y medianas empresas en un entorno digital.

Según un estudio del Banco Mundial[258], el financiamiento participativo emergió con el inicio de la crisis financiera de 2008, en respuesta a las dificultades que tenían las empresas en formación para obtener financiamiento. El financiamiento participativo empezó concretamente con la captación de recursos a través de donaciones o aportes voluntarios y posteriormente se desarrollaron esquemas financieros a través de préstamos y aportes de capital.

En las propuestas legislativas peruanas señaladas el Financiamiento Participativo Financiero se concibe como una actividad en la que a través de una plataforma se pone en contacto a persona naturales domiciliadas en el país, que solicitan financiamiento a nombre propio, denominados receptores, con una pluralidad de personas naturales, jurídicas o entes colectivos, denominados inversionistas, que buscan obtener un retorno financiero. En el caso de personas naturales, son mayores de dieciocho años. Aquí cabe comentar que las personas que soliciten financiamiento domicilian en el Perú y son mayores de edad, en cambios las personas que financian pueden domiciliadas o no domiciliadas, permitiendo un financiamiento global por internet.

258 The World Bank. "Crowfunding´s Potential to developing World. Washington D.C. 2013. P.14.

Las modalidades de financiamiento participativo financiero que se proponen en las propuestas legislativas son las siguientes:

a) Financiamiento participativo a través de valores representativos de capital y/o deuda, en cuyo caso se entiende como receptores a los emisores de éstos. También conocido como Crowdfunding de inversión o equity; esta modalidad es enfocada para los emprendedores, sobre todo en etapas tempranas , donde requieren financiar su crecimiento o consolidación.

b) Financiamiento participativo a través de préstamos, en cuyo caso se entiende como receptores a personas naturales o jurídicas prestatarias. La Superintendencia del Mercado de Valores (SMV) puede requerir, como condición de la operación, que se lleve a cabo bajo esta modalidad, la emisión de un instrumento financiero u otro título valor. Esta modalidad es también conocida como Crowdfunding de préstamo o Crowdlwlending. La deuda juega un rol fundamental cuando la empresa cuenta ya con flujos estables, léase ventas regulares. Con respecto a los instrumentos financieros o títulos valores, deberá tenerse en cuenta los títulos valores electrónicos con uso de firmas y certificados digitales, microforma digit [259] y blockchain.

Con respecto a la disposición de que la Superintendencia del Mercado de Valores (SMV) puede requerir la emisión de un instrumento financiero o título valor, al tratarse de financia iento en internet, será necesaria la utilización de títulos valores digitales. Al respecto, debe considerarse que: "Los títulos valores electrónicos o digitales, conforme el ordenamiento jurídico peruano, pueden ser utilizados empleando la firma electrónica y/o la microforma digital , permitiendo que los principios propios de esta institución se apliquen adecuadamente a los cambios tecnológicos que se van dando en la realidad. La Ley de Títulos Valores peruana de liquidación y compensación reconoce a los valores desmaterializados y supedita su validez y eficacia jurídica a que tengan anotación en cuenta y se registre en una institución de liquidación y compensación de valores, pero no se queda ahí, con las concordancias respectivas , permite tener un marco legal suficiente para utilizar los títulos valores electrónicos o digitales en un contexto de desarrollo constante de los negocios electrónicos"[260].

En las propuestas legislativas señaladas, se establece el régimen de las Entidades autorizadas, al precisarse que la administración de las plataformas sólo podrá llevarse a cabo (cuando se apruebe el proyecto de Ley) por sociedades anónimas constituidas e el Perú, debidamente autorizadas por la SMV, cuyo objeto social sea la administración de dichas plataformas de internet.

---

259 En el ordenamiento jurídico peruano el Decreto Legislativo 681 establece el marco legal de la microforma digital, que es la imagen digitalizada de un documento con características de inalterabilidad, fijeza y durabilidad, que cumple requisitos y formales que garantizan su seguridad técnica y jurídica.

260 NUÑEZ PONCE, Julio: "Los Títulos Valores Electrónicos o Digitales". En Tratado de Derecho Mercantil. Tomo III. Página 928, Ed. Gaceta Jurídica. Lima, Perú. Primera Edición agosto 2004.

Con respecto a la propuestas legislativas es necesario comparar y contrastar las modalidades propuestas, con las definidas en la doctrina, tal es así que con respecto a las Modalidades de crowdfunding, existen diversas clasificaciones respecto de los modelos de crowdfunding, que son las siguientes: donation crowdfunding, reward crowdfunding, debt crowdfunding y equity crowdfunding.

Estas modalidades se desarrollan a continuación: "- Donación: El donation crowdfunding ha sido utilizado, tradicionalmente, para financiar proyectos sociales de interés general, que no necesariamente buscan una finalidad lucrativa. Reward: El reward crowdfunding es una modalidad de similar naturaleza a la donación. Así, quien contribuye para el proyecto específico recibe una contraprestación a cambio, puede ser el mismo producto, el servicio que está financiando o algún bien de naturaleza simbólica. No se trata de una compraventa y tampoco se trata de una inversión. Son liberalidades de las personas que participan en este tipo de financiamientos. Equity Consiste en la emisión y colocación de valores mobiliarios de renta variable, como mecanismo para financi r un proyecto, utilizando una plataforma electrónica. Mediante el equity crowdfunding el inversor puede adquirir un porcentaje de titularidad sobre las acciones o los derechos del proyecto empresarial o la empresa del promotor. Lending Consiste en el préstamo entre pares (peer- to-peer lending). Esto involucra que un número plural de individuos provea un conjunto de pequeñas cantidades de dinero a una persona natural o persona jurídica, a título de muto. En virtud del debt crowdfunding el inversor calificaría como un prestamista que pacta la recuperación de su inversión con una rentabilidad determinada, a través del uso de una plataforma electrónica"[261].

Las propuestas legislativas peruanas señaladas se circunscriben a dos modalidades, sin embargo, el ámbito de regulación es mas amplio y podrá plantearse que la regulación que se de en el Perú pueda paulatinamente incluir otras modalidades, de acuerdo a las normas específicas que emita la Superintendencia Nacional del Mercado de Valores (SMV).

El financia iento participativo financiero se propone que esté sujeto a las siguientes condiciones: a) Los receptores solicitan financiamiento a nombre propio, su proyecto es de tipo personal y/o empresarial, y es desarrollado íntegramente en el territorio peruano, salvo excepciones que determine la Superintendencia del Mercado de Valores (SMV) en la respectiva regulación. B) Los proyectos de financiamiento participativo financiero están dirigidos a una pluralidad de personas naturales, jurídicas o entes colectivos denominados inversionistas, tener un objetivo de financiamiento así como un plazo máximo de recaudación.

261 GUTIERREZ VEGA, Miluska Jazmin: Ob.cit. Página 43.

La regulación del crowdfunding se ha dado en distintos países como España[262], Estados Unidos, [263]Argentina[264], México[265], Singapur[266], entre otros países. Saludamos la iniciativa del Poder Ejecutivo en presentar este importante proyecto de Ley para su aprobación por el Congreso de la República. Es pertinente mencionar que la iniciativa legislativa propone designar a la Superintendencia del Mercado Valores (SMV) como entidad competente para autorizar a las personas jurídicas a administrar las plataformas, las cuales deberían constituirse como sociedades anónimas y adoptar la denominación de "Sociedades Administradoras de Financiamiento Participativo Financiero". La iniciativa también prescribe que estas sociedades deben construirse en el Perú, siguiendo la tendencia internacional de mitigar los riesgos de actividades transfronterizas. Siendo que en los proyectos de financiamiento participativo financiero, las Sociedades Administradoras, juegan un rol trascendental en la medida que contactan a inversionistas con receptores, la presente propuesta legislativa fijas sus obligaciones. Entre estas se encuentran el establecimiento de los mecanismos para que los inversionistas puedan conocer la identidad de los receptores y con ello puedan evaluar adecuadamente el riesgo de su inversión. Hay otros temas importantes que analizar en este proyecto de Ley, que desarrolla una modalidad de financiamiento que utiliza las tecnologías de información y comunicaciones y que está en el ámbito del Derecho de las Nuevas Tecnologías. Confío que esta ponencia suscite interés y mediante el dialogo se mejore las propuestas legislativas presentadas, que van a ser analizadas y discutidas en el Congreso de la República del Perú.

---

262 En España, el financiamiento participativo está incluido en la Ley 5/2015, de fecha 27 de abril de 2015, publicada el 28 de abril de 2015, Ley de Fomento de la Financiación Empresarial. Esta Ley contiene un título completo en el cual regula el "Régimen Jurídico de las plataformas de financiac - ón participativa", las que se encuentran bajo el ámbito de la Comisión Nacional del Mercado de Valores de dicho país.

263 Estados Unidos fue el primer país que reguló el financiamiento colaborativo a través de la Jumpstart Our Bussines Starups(JOBS) Act, en el año 2012. En ella se regula el crowdfunding en particular, en el Título III. "El objetivo de la norma es esencialmente aligerar la carga regulatoria de las plataformas de crowdfunding (denominadas funding portals).

264 En Argentina, el crowdfunding fue implementado mediante la Ley N° 27.349 (la "Ley"), publicada en el Boletín Oficial el 12 de abril de 2017, con el objeto de fomentar el financiamie - to de la industria de capital emprendedor a través del mercado de capitales. Mediante la Resolución General 717-E/2017 (la "Resolución"), la CNV incorpora como Título XIX de las Normas (N. T. 2013 y modif.; las "Normas CNV") la reglamentación de los Sistemas de Financiamiento Colectivo.

265 En México, el 09 de Marzo de 2018 , se ha publicado en el Diario Oficial de la Federación la Ley para regular las instituciones de tecnología financiera. La ley tiene por objeto "regular los servicios financieros que prestan las instituciones de tecnología financiera , así como su organización , operación y funcionamiento y los servicios financieros sujetos a alguna normatividad especial que sean ofrecidos o realizados por medios innovadores".

266 En Singapur la recaudación de fondos del público a través de crowdfunding basado en préstamos o P2P préstamos, está regulada por la Monetary Authority of Singapore (MAS) bajo la Securities and Futures Act (Cap. 289) (la "SFA") y la Financial Advisers Act (Cap.110) (la "FAA") Monetary Authority of Singapore, 2016).

3. ANALISIS DEL CROWDFUNDING EN EL DERECHO DE LAS NUEVAS TECNOLOGIAS PERUANO

3.1. Crowdfunding, la Identidad Digital y la Ley de Firmas y Certificados Digitales

En el financiamiento participativo financiero por internet (crowdfunding) las plataformas que se utilicen deben utilizar la identificación y autenticación de la identidad en un entorno digital. Al respecto, conforme la legislación peruana: "La identidad digital es aquel conjunto de atributos que individualiza y permite identificar a una persona en entornos digitales. Los atributos de la identidad digital son otorgados por distintas entidades de la Administración Pública que, en su conjunto, caracterizan al individuo"[267].

Las plataformas de financiamiento participativo son las empresas que conectan de manera profesional a través de páginas web y medios electrónicos a inversionistas que buscan rendimiento financiero. La identidad digital de inversionistas y promotores en estas plataformas debe preservarse dando un tratamiento adecuado a los atributos.

Al respecto, "por atributo se entiende un elemento de información o datos asociados a un sujeto. En el caso de la persona natural ejemplos de atributos son el nombre, la dirección, la edad, el sexo, el cargo, la remuneración, la dirección del correo electrónico, entre otros. Estos atributos son fundamentales para distinguir a una persona de otra y reconocer su unicidad"[268]. Tratándose de inversionistas y promotores que se van a relacionar jurídicamente en una plataforma en internet debe darse seguridad jurídica y técnica de forma tal que se evite la suplantación de identidad y el uso indebido de los atributos.

En este orden de ideas, tengamos en cuenta que "la regulación jurídica de las identidades digitales supone múltiples retos para su declaración-recepción-certificación por terceros , o por agentes o funcionarios nacionales o internacionales bajo forma de actos, registros, certificados, contratos, procesos y formalidades"[269]. Por ello la implementación de plataformas de autenticación nacional en el Perú que incluyan a nacionales y a extranjeros para que puedan ser autenticados e identificados en forma fidedigna es la forma de garantizar la seguridad de inversionistas y promotores en

267 Decreto Legislativo N° 1412, Ley de Gobierno Digital. Capitulo II Identidad Digital. Artículo 10. Diario Oficial El eruano. 13 de Setiembre de 2018. Lima, Perú.

268 NUÑEZ PONCE, Julio: "Identidad Digital, Ética en la función Pública, Transparencia y Protección de Datos Personales". En Libro "Ética para los tiempos. Trayectoria de Excelencia en la función pública. Identidad. Ciudadanía y Tecnología. Página 259. Ed. Registro Nacional de Identificación y Estado Civil (RENIEC). Primera edición Enero de 2019. Lima, Perú.

269 FERREYROS SOTO, Carlos et al: "Derecho de Personas e Informática: Identidad Digital" Pagina 223, Ed. Grijley. 2016. Lima, Perú.

el financia iento participativo financiero en internet (crowdfunding) es necesario regular e incluir en las propuestas legislativas analizadas.

Por otra parte, conforme la Ley 27269, Ley Peruana de Firmas y Certificados Digitales: "Certificado Digital es el documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada, confirmando su identidad". Los certificados digitales contenidos en el Documento Nacional de Identidad Electrónico (DNIe) de persona natural y los certificados digitales de persona jurídica permiten la autenticación t la firma digital de los documentos electrónicos como contratos, títulos valores y otros que se empleen en el financiamiento participativo financiero en internet (crowdfunding).

El Reglamento de la Ley de Firmas y Certifica os Digitales, Decreto Supremo 052-2008-PCM, establece que: "La firma digital generada de la Infraestructura Oficial de Firma Electrónica (IOFE) tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita. En tal sentido, cuando la ley exija la firma de una persona, ese requisito se entenderá cumplido en relación con un documento electrónico, si se utiliza una firma digital generada en el marco de Infraestructura Oficial de Firma Electrónica (IOFE). Lo establecido en el presente artículo y las demás disposiciones del presente Reglamento no excluyen el cumplimiento de las formalidades específicas requeridas para los actos jurídicos y el otorgamiento de la fe pública. Asimismo, conforme el artículo 4°, se establece que: "Los documentos electrónicos firmados digitalmente dentro del marco de la IOFE deberán ser admitidos como prueba en los procesos judiciales y/o de procedimientos administrativos.". Este marco jurídico permite garantizar la equivalencia funcional de la firma digital que le otorga la misma validez y efic cia jurídica que una firma manuscrita y el valor probatorio de los documentos electrónicos generados con firma digital.

El uso de la identidad digital y de las firmas y certificados digitales debe incluirse expresamente en la legislación del financiamiento participativo financiero en internet (crowdfunding), hay que tener presente que " el prestatario tiene incertidumbre sobre sus derechos y obligaciones (también relevante para los prestamistas) Este riesgo se presenta si una plataforma no divulga información comprensible acerca de los servicios que serán proporcionados por la plataforma y una descripción de los derechos y obligaciones contractuales que se aplicarían a los prestamistas y los prestatarios. Puede darse el caso que las MYPES no sean entidades sofisticadas por lo que el envío de mensajes claros, veraces y oportunos resultan relevantes. - El prestatario enfrenta un inadecuado mecanismo de manejo de reclamos en una plataforma (también relevante para los prestamistas). Este riesgo está estrechamente vinculado a la protección al consumidor y la implementación de las medidas necesarias para canalizar los reclamos y quejas que éstos puedan tener en relación a los términos y condiciones de la plataforma. Ello a su vez puede generar una mala reputación del prestatario en el

sistema, cerrando una de las alternativas de financiamiento propuesta para ese tipo de entidades"[270]. Los contratos, los reclamos, los títulos valores y otros documentos electrónicos que se requieren en el financiamiento participativo financiero en internet (crowdfunding) se generaran en forma segura y cierta, garantizado la identidad digital de inversionistas y promotores, así como con la utilización de las firmas y certificados digitales.

3.2. Relación del Crowdfunding con la Ley Peruana de Protección de Datos Personales

En las propuestas legislativas peruanas de regulación del financiamiento participativo financiero por Internet (crowdfunding) se propone establecer que las Sociedades Administradoras provean la infraestructura, servicios y sistemas para materializar las operaciones que en ellas se realicen, permitiendo conectar a receptores e inversionistas, antes, durante y después de financiamiento del proyecto, para lo cual realizan tratamiento de datos personales en Internet. Al respecto, cabe señalar que conforme la Ley Peruana de Protección de Datos Personales, Ley 29733, se define los datos personales como "toda información sobre una persona natural que la identifica o la hace identificable a través de medios que puedan ser razonablemente utilizados". Por Banco de Datos Personales se entiende "Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuera la forma o modalidad de su creación, formación, almacenamiento, organización y acceso. Por transferencia de datos personales se entiende "Toda transmisión, suministro o manifestación de datos personales, de carácter nacional o internacional, a una persona jurídica de derecho privado a una entidad pública o a una persona natural distinta del titular de datos personales.

Conforme el artículo 3° de la Ley 29733, Ley Peruana de Protección de Datos Personales "la presente ley es de aplicación a los datos personales contenidos o destinados a ser contenidos en banco de datos personales de administración pública y de administración privada, cuyo tratamiento se realiza en territorio nacional. Son objeto de especial protección los datos sensibles". Los bancos de datos personales de las Sociedades Administradoras del financiamiento participativo financiero por Internet (crowdfunding) están sujetos a la ley de protección de datos personales en los distintos tratamientos de datos que realizan automatizados o no.

Por Tratamiento de Datos Personales se entiende "cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro,

270 GUTIERREZ VEGA, Miluska Jazmin: Ob.cit. Página 57.

organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales".

Por datos sensibles se entiende: "datos personales constituidos por los datos biométricos, que por sí mismos pueden identifi ar al titular; datos referidos al origen racial o étnico; ingresos económicos; opiniones o convicciones políticas o religiosas, filosófica o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual".

La actuación de los titulares y encargados de tratamiento de datos personales y, en general de todos los que intervengan con relación a datos personales, debe ajustarse a los principios rectores. Los principios rectores contenidos en la Ley 29733, son los siguientes: a) Legalidad. b) Consentimiento. c) Finalidad. d) Proporcionalidad. e) Calidad de Datos. f) Seguridad. g) Nivel de Protección. h) Tutela efectiva de los derechos.

Los derechos reconocidos en la ley de protección de datos personales son: i) Derecho de Información. ii) Derecho de actualización, inclusión, rectificación. Iii) Derecho de cancelación o supresión. Iv) Derecho de Impedir el suministro. V) Derecho de Oposición. Vi) Derecho a ser indemnizado.

Uno de los derechos que en el financiamiento participativo financiero por Internet (crowdfunding) se puede utilizar tanto como inversionistas y proveedores es el derecho de acceso. Conforme la legislación peruana "la información que podrá tener acceso el titular de los datos personales se encuentra: que datos se están tratando, como y donde fueron recopilados, con que finalidades se recopilaron, a solicitud de quien se realizó la recopilación, condiciones en que se realizan el tratamiento de datos personales y tiempo en que se viene realizando dicho tratamiento"[271]. En las propuestas legislativas de financiamiento participativo financiero por Internet (crowdfunding) debiera realizarse mención expresa al ejercicio de este derecho de acceso, en concordancia con la ley de la materia.

Otros de los aspectos a incluirse que relaciona la protección de datos personales con la protección al consumidor es la relacionada con la información, dado que "que los inversionistas pueden no tener el conocimiento o la experiencia de identificar a los "buenos deudores", lo que a su vez crea un problema de selección adversa. Por tanto, es necesario precisar en la regulación del crowdfunding es la asimetría de la información, por cuanto "los efectos de la situación de asimetría de la información pueden multiplicarse en un número mayor de inversionistas dado que el primer

271 MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS DEL PERU: Dirección General de Protección de Datos Personales. Resolución Directoral N° 670-2017-JUS/DGTA/PD-DPDP. Lima, 25 de Octubre de 2017. Procedimiento Trilateral de Tutela que interpone ciudadano contra Banco con respecto al derecho de acceso de sus datos personales. En: http://minjus.gob.pe

fondeo de un proyecto es una señal de lo que percibe el mercado respecto de dicho mercado. Del mismo modo, se da un supuesto de asimetría de la información porque no se tiene seguridad sobre el destino de los fondos ni otra información relevante del deudor"[272]. Estos aspectos deben ser contemplados en dispositivos con rango de ley y en las normas complementarias.

3.3. Relación del Crowdfunding con la Ley Peruana de Dinero Electronico

Otra norma que hay que concordar con la regulación financiamiento participativo financiero por Internet (crowdfunding) cuando se regula el financiamiento participativo financiero por Internet (crowdfunding) es la Ley Peruana de Dinero Electrónico Ley 29985 del 17/01/2013, que regula las características básicas del dinero electrónico como instrumento de inclusión financiera es el marco para la creación y supervisión de las Empresas Emisoras de Dinero Electrónico (EEDE), que serán las encargadas de ofrecer cuentas para hacer operaciones aceptadas no solamente entre bancos, sino por restaurantes, pago de servicios públicos, tiendas comerciales, etc.

- Uno de los soportes será el teléfono celular y para que los usuarios accedan a este servicio, las EEDE deberán proveer de fideicomisos (como una cuenta para abonos) que recibirán depósitos para convertirlos a dinero electrónico: esta condición le permitirá que sea aceptado para realizar las transacciones que el usuario disponga, sin depender del banco de donde salen los fondos.
- Pero su uso no sólo se restringe a los móviles, ya que estas empresas también podrán emitir tarjetas prepago, a las cuales se podrá hacer recargas al igual que en la cuenta celular. El monto máximo por transacción al mes será de una Unidad impositiva tributaria UIT (S/. 4,200 soles).
- El dinero electrónico es un valor monetario representado por un crédito exigible a su emisor, el cual tiene las siguientes características: • a) Es almacenado en un soporte electrónico. • b) Es aceptado como medio de pago por entidades o personas distintas del emisor y tiene efecto cancelatorio. • c) Es emitido por un valor igual a los fondos recibidos. • d) Es convertible a dinero en efectivo según el valor monetario del que disponga el titular, al valor nominal. • e) No constituye depósito y no genera intereses.

Los emisores de dinero electrónico deben constituir fideicomisos por el valor del dinero electrónico emitido conforme a las disposiciones que dicta la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones. Dicho Organismo de Control puede regular otras modalidades alternativas de garantía para los fondos de dinero electrónico emitidos.

272 GUTIERREZ VEGA, Miluska Jazmin: Ob.cit. Página 81 y 82.

La emisión de dinero electrónico constituye un servicio financiero, y la información del usuario de dinero electrónico y de las operaciones que realice están sujetas a la Ley 29733, Ley de Protección de Datos Personales. La Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones establece las modalidades de contratación aplicables al dinero electrónico, las que pueden ser escritas, electrónicas u otras, de acuerdo a la naturaleza de los productos, sus características y las circunstancias en que estos se ofrecen, en concordancia con lo dispuesto en la Ley 29571, Código de Protección y Defensa del Consumidor; la Ley 28587, Ley Complementaria a la Ley de Protección al Consumidor en Materia de Servicios Financieros, y las normas reglamentarias emitidas para garantizar su cumplimiento.

Una precisión a considerarse es que en la ley de dinero electrónico peruana se precisa que en el marco del proceso de implementación del Documento Nacional de Identidad electrónico (DNIe), el Registro Nacional de Identificación y Estado Civil (Reniec), en coordinación con los sectores pertinentes, habilita las aplicaciones correspondientes para que en dicho documento se almacene información para usos financieros, bancarios y no bancarios, con autorización del usuario, conforme a la Ley 29733, Ley de Protección de Datos Personales. Estos criterios legales deben ser mencionados expresamente y concordados en la legislación sobre financiamiento participativo financiero por Internet (crowdfunding).

3.4. Relación del Crowdfunding y Fintech con la Afectación Tributaria de los Servicios Digitales en la Ley Peruana del Impuesto a la Renta

Otro de los aspectos a tenerse en cuenta en la regulación del financiamiento participativo financiero por Internet (crowdfunding) es la afectación tributaria de los servicios digitales en la ley peruana del impuesto a la renta. Conforme la Ley Peruana del Impuesto a la Renta, en general y cualquiera sea la nacionalidad o domicilio de las partes que intervengan en las operaciones y el lugar de celebración o cumplimiento de los contratos, se considera rentas de fuente peruana: "Las obtenidas por servicios digitales prestados a través del Internet o de cualquier adaptación o aplicación de los protocolos, plataformas o de la tecnología utilizada por Internet o cualquier otra red a través de la que se presten servicios equivalentes, cuando el servicio se utilice económicamente, use o consuma en el país".

Debe tenerse en cuenta, que tratándose de contribuyentes no domiciliados en el país, de sus sucursales, agencias o establecimientos permanentes, el impuesto a la renta recae sólo sobre las rentas gravadas de fuente peruana.

Conforme el Reglamento: "Se entiende por servicio digital a todo servicio que se pone a disposición del usuario a través de Internet o de cualquier adaptación o

aplicación de los protocolos, plataformas o de la tecnología utilizada por Internet o cualquier otra red a través de la que se presten servicios equivalentes mediante accesos en línea...". Los servicios de financiamiento participativo financiero por Internet (crowdfunding) consideramos que están incluidos dentro del ámbito de aplicación de los servicios digitales.

Al respecto, cabe señalar que el servicio digital se utiliza económicamente, se usa o consume en el país, cuando ocurre cualquiera de los siguientes supuestos:

1. Sirve para el desarrollo de las actividades económicas de un contribuyente perceptor de rentas de tercera categoría. Se presume que un contribuyente de rentas de tercera categoría que considera como gasto o costo la contraprestación por el servicio digital, el que cumple con el principio de causalidad, utiliza el servicio económicamente en el país. 2. Sirve para el desarrollo de las actividades económicas de los sujetos intermediarios con el propósito de generar ingresos. 3. Sirve para el desarrollo de las funciones de cualquier entidad del Sector Público Nacional.

Los Servicios Digitales en Internet (Según Reglamento de la Ley de Impuesto a la Renta) son: 1. Mantenimiento de Software. 2. Soporte Técnico al Cliente en Red. 3. Almacenamiento de Información (Data Ware Housing). 4. Aplicación de Hospedaje (Application Hosting). 5. Provisión de Servicios de Aplicación (Application Server Provider- ASP). 6. Almacenamiento de Páginas Web (Web Site Hosting). 7. Acceso Electrónico a servicios de consultoría. 8. Publicidad (Banners Ads). 9. Subastas "en línea". 10. Reparto de Información. 11. Acceso a una Página Web Interactiva. 12. Capacitación Interactiva. 13. Portales en línea para Compraventa. Pero esta relación no es limitativa y consideramos que están incluidos los servicios de financiamiento participativo financiero por Internet (crowdfunding).

Dentro de la regulación del financiamiento participativo financiero por Internet (crowdfunding) debiera incluirse exoneraciones tributarias a los servicios digitales que se presten. Al respecto, cabe señalar que "como todo nuevo negocio, a efectos de impulsar su desarrollo y crecimiento, sería recomendable que estas iniciativas incorporen ciertos beneficios de índole (principalmente tributaria). En ese sentido, lo ideal es que por el lado de la MIPYME esto funcione como un financiamiento a través del sistema financiero y pueda deducir gastos y estar exonerado del pago de IGV y medidas similares. Por el lado de los prestamistas, lo ideal es que este mecanismo de financia iento sea comparado con otra alternativa de inversión (i.e.por ejemplo, depósitos a plazo o participación en fondos mutuos)"[273].

3.5. La Relación del Crodwfunding con la Ley de Delitos Informaticos y el Codigo Penal Peruano

273 GUTIERREZ VEGA, Miluska Jazmin: Ob.cit. Página 130.

Otros de los temas legales a concordarse con la regulación del financiamiento participativo financiero por Internet (crowdfunding) es la Ley peruana de Delitos Informáticos 30096, que tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

Los delitos tipifcados en la ley de delitos informáticos que consideramos guardan directa relación con una regulación del financ amiento participativo financiero por Internet (crowdfunding), son los siguientes:

a) Delito Acceso Ilicito. Art. 2. Ley 30096. Modificada por Ley 30171. Bien Jurídico Protegido: Datos y Sistemas informáticos. Seguridad. Conductas tipificadas: -"El que deliberada e ilegítimamente accede a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo". - "Acceso a un sistema informático excediendo lo autorizado". Penas: Pena Privativa de Libertad no menor de uno ni mayor de cuatro años. Treinta a noventa días multa. El acceso ilícito en el caso específic de la regulación del financiamiento participativo financiero por Internet (crowdfunding), tiene especial importancia para preservar la seguridad de las plataformas de internet utilizadas para esta actividad.

b) Delito Atentado contra la Integridad de Datos Informáticos. Art. 3. Ley 30096. Modificada por Ley 30171. Bien Jurídico Protegido: Datos y Sistemas Informáticos. Seguridad. Conductas Tipificadas: "El que deliberada e ilegítimamente, daña, introduce, borra, deteriora, altera, suprime o hace inaccesible datos informáticos". Penas: -Pena Privativa de Libertad no menor de tres años ni mayor de seis años. -Ochenta a Ciento Veinte días multa. Los datos en la regulación del financiamiento participativo financiero por Internet (crowdfunding) tienen un papel fundamental, por tanto, la regulación en esta materia deberá concordarse con la tipificación de este delito y con las medidas necesaria para preservar la evidencia digital.

c) Delito Atentado contra la integridad de sistemas informáticos. Art. 4. Ley 30096. Modificado por Ley 30171. Bien Jurídico Protegido: "El que deliberada e ilegítimamente, inutiliza, total o parcialmente, un sistema informático, impide el acceso a éste, entorpece o imposibilita su funcionamiento o la prestación de sus servicios". Penas: Pena Privativa de Libertad no menor de tres ni mayor de seis años. Ochenta a Ciento Veinte Días Multa. En la regulación del financiamiento participativo financiero por Internet (crowdfunding) es necesario asimismo dictar las disposiciones necesarias para que también se preserve la evidencia digital para probar la comisión de estos delitos.

d) Delito Suplantación de Identidad. Art. 9. Ley 30096. Bien Jurídico Protegido: Fe Pública. Conductas Tipificadas. "El que mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre

que de dicha conducta resulte algún perjuicio, material o moral". Pena: Pena Privativa de Libertad no menor de tres ni mayor de cinco años. La identidad digital, como ya hemos visto es fundamental en la regulación del financiamiento participativo financiero por Internet (crowdfunding) por tanto las normas de seguridad y conservación de la evidencia digital deben incluirse en las normas jurídicas que se emitan sobre esta materia.

Hay que tener presente que: "Los datos personales de un prestatario pueden ser robados o mal utilizados (lo cual también es aplicable para el prestamista que accede a la plataforma). Este riesgo puede surgir si una plataforma carece de un documento suficientemente robusto sobre política de tratamiento de datos o si la política no se aplica correctamente en la práctica, llevando a la pérdida de datos personales o el aprovechamiento de dichos datos sin el consentimiento del titular. Este es un riesgo general de la actividad. La regulación sobre datos personales está siendo implementada con mayor recelo en los últimos años. Sin embargo, el tratamiento inadecuado de esta información puede generar no solo una mala reputación para la plataforma sino que puede reflejarse, incluso, en un incremento de la tasa de interés, lo que genera un perjuicio para la mediana y pequeña empresa (MYPE)"[274].

e) Delito Tráfico Ilegal de datos. Art. 154-A del Código Penal, fue incorporado por Ley 30171, que deroga art. 6 Ley 30096. Bien Jurídico Protegido: Intimidad y Secreto de las Comunicaciones. Conductas Tipificadas: "El que ilegítimamente comercializa o vende información no pública relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga, sobre una persona natural. Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta un tercio por encima del máximo legal previsto. Pena: Pena Privativa de Libertad no menor de tres ni mayor de cinco años. En la regulación del financiamiento participativo financiero por Internet (crowdfunding) hay que combatir con normas específicas concordantes el tráfico ilegal de dato.

f) Delito Interceptación de Datos Informáticos. Art. 7. Ley N° 30096. Modificad por Ley 30171. Bien Jurídico Protegido: Intimidad y Secreto de las Comunicaciones. Conductas Tipificadas: "El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos". Penas: Pena Privativa de Libertad: de 3 a 6 años. Pena Privativa de Libertad de 5 a 8 años. Si recae sobre información secreta, reservada o confidenc al. Pena Privativa de Libertad de 8 a 10 años, cuando comprometa la defensa, seguridad o soberanía nacional. En la regulación del financia iento participativo financiero por Internet (crowdfunding) es necesario incluir medidas preventivas para evitar la interceptación de datos informáticos.

274 GUTIERREZ VEGA, Miluska Jazmin: Ob.cit. Página 55.

g) Delito Fraude Informático. Art. 8° Ley 30096. Modificado por Ley 30171. Bien Jurídico protegido: Patrimonio. Conductas Tipificadas: "El que deliberada e ilegítimamente, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático". Penas: - Pena Privativa de Libertad de 3 a 8 años. 60 a 120 días multa. Pena Privativa de Libertad de 5 a 10 años. 80 a 140 días multa. Cuando se afecta el Patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social. En la regulación del financiamiento participativo financiero por Internet (crowdfunding) es necesario incluir medidas preventivas, procesos auditados y controles necesarios para evitar los fraudes informáticos.

Hay que tener en cuenta que por Resolución Legislativa N° 30913, publicada el 13 de Febrero de 2019, se aprueba la adhesión del Perú al Convenio sobre Ciberdelincuencia. Por tanto las normas sobre tipificación de cibercrimenes, las normas procesales para conservación y preservación de la evidencia digital y las referente a la cooperación mutua internacional, con la implementación de la Red 24/7, las 24 horas del día los siete días de la semana van a ser de valiosa aplicación para combatir el fraude informático y los otros cibercrimenes mencionados.

Con respecto a la regulación del financiamiento participativo financiero por Internet (crowdfunding) debe considerarse que con respecto al riesgo reputacional o riesgo de fraude: "Un prestatario puede tener incertidumbre sobre la reputación y la seguridad de la plataforma (lo cual también es aplicable para el prestamista que accede a la plataforma). Puede ser difícil para los prestamistas y los prestatarios encontrar información independiente sobre la reputación de las plataformas, en la medida que dicha plataforma no esté obligada a cumplir con requisitos legales de divulgación o información. Además, las plataformas no necesariamente requieren autorizaciones o licencias, por lo que pueden no estar sujetas a ningún tipo de supervisión. Resulta relevante uniformizar y otorgar claridad sobre las reglas aplicables a las plataformas. Debe establecerse también si es que están o no están sujetas a algún tipo de regulación y cuál es el alcance de la misma. La claridad en la información resulta clave especialmente para las MYPES con la finalidad que puedan utilizar esta alternativa de financiamiento [275].

Otras de las figuras delictivas a considerar, pero que está contenido el Código Penal Peruano es el delito de lavado de activo y las normas aplicables al crimen organizado. En la regulación del financiamient participativo financiero por Internet (crowdfunding) es necesario incluir normas específicas que disminuyan el Riesgo de lavado de activos y otras actividades ilícitas. Teniendo presente que "este es uno de los riesgos que más se acentúa en las plataformas. Sería recomendable que se exija que

275 GUTIERREZ VEGA, Miluska Jazmin: Ob.cit. Página 54.

los participantes tengan abiertas cuentas en el sistema financiero local o en bancos que califiqu n como bancos de primera categoría. De esa manera, la verificación previa del cliente es efectuada (en el marco de la regulación aplicable) por las entidades financieras correspondiente [276].

4. LA INNOVACION, EL EMPRENDIMIENTO, LAS EMPRESAS STAR UP, EL FINTECH Y LA REGULACION DEL CROWDFUNDING EN EL PERU

El Ministerio de Producción del Perú-PRODUCE viene realizando esfuerzos por promover el emprendimiento y la innovación, que lo viene haciendo en forma efectiva. La innovación y el emprendimiento en las startups se han convertido hoy en día en un binomio estratégico que ayuda a mejorar la competitividad de las organizaciones. El emprendimiento no solo es el medio ideal para difundir los productos de innovación, sino que también ayuda a incrementar la capacidad económica de las regiones, ya que tienen acceso a más conocimientos, experiencias, ideas y recursos que, en conjunto, aumentan de manera significativa el aprendizaje de las organizaciones.

Ahora bien, hay que considerar el tema de la financiación de los emprendimientos vinculados al desarrollo y a las soluciones tecnológicas. "El Crowdfunding se ha establecido como una solución efectiva, coherente con los ritmos de trabajo, la naturaleza y las particularidades de las startups, que ayuda de una manera particular a recaudar los fondos necesarios para comenzar las fases de producción de la idea"[277]. El Crowdfunding aparece, y se enraíza con fuerza presentándose como una nueva oportunidad para los emprendedores, que permite el desarrollo de negocios o proyectos, democratizar la fuerza inversionista.

El Crowdfunding genera a la par puntos positivos para las dos partes intervinientes: "Primero: el creador del negocio o proyecto tiene más alternativas para vender sus productos o buscar el apoyo económico necesario para su desarrollo. Segundo: la persona con recursos altos o bajos puede optar por financiar proyectos o comprar bienes recibiendo como beneficios los réditos de su inversión o el disfrute del bien comprado"[278]. La aparición del Crowdfunding como nueva fuente de financiación ha cambiado de manera significativa el paisaje del emprendimiento. Además, con el uso creciente de las redes sociales, el crowdfunding aparece como un medio de financiación accesible a todos.

El Crowdfunding permite a emprendedores de proyectos con cierto nivel de riesgo, "acceder a recursos financieros sin entrar en contacto con los intermediarios financieros tradicionales como los venture capitalists, por ejemplo. Hoy en día, la

276 Ibidem. Pagina 117.
277 SILVA ORTIZ, Julian Armando: Ob.cit. Página 24.
278 VILLADA CALDERON, Juan Sebastián et al: Ob.cit. Página 6.

idea de que existe una complementación entre el crowdfunding y el venture capital gana importancia. Es pertinente entender el funcionamiento del crowdfunding, pero sobretodo sus dinámicas, como ha ganado importancia y como ha conseguido obtener una posición relevante en este sector en los últimos años"[279]. El Venture Capital y los fondos de private equity son intermediarios financieros entre fuentes de inversión (inversores institucionales) y empresas con alto potencial de crecimiento o empresas de alta tecnología.

El crowdfunding permite ofrecer soluciones a este sesgo creando plataformas dirigidas especialmente a mujeres. Por ejemplo, Portfolia es la única plataforma de recaudamiento de "equity capital" que se dirige a las mujeres fundadoras e inversoras. Se puede poner en relieve el ejemplo de Shebooks que ha recaudo fondos a través de la plataforma Portfolia. Esta empresa ofrece e-books con respecto a temas femeninos de mayor importancia y que se leen rápidamente. Otro ejemplo que podemos mencionar es el de MoolaHoop, una plataforma de "rewardbased" crowdfunding. Se dirige especialmente a pequeñas sociedades para proveer fuentes alternativas de financiación para las compañías "early stage" ya que muchas mujeres lanzan sus negocios con recursos bastante restringidos. "Se puede deducir al tenor de estos datos que el Crowdfunding resuelve el sesgo de genero ya que, como hemos mencionado previamente, este proceso de financiación no requiere contacto físico como el Venture Capital. Los aportantes se ven menos influido por la identidad del emprendedor. Suponemos que a través de este método las comunidades están más interesadas en la calidad del proyecto que en el emprendedor en sí mismo"[280].

En la actualidad, uno de los principales elementos que deben tener en cuenta las empresas para potenciar el emprendimiento y la innovación empresarial es el de generar un enfoque en la competitividad, que les permita "mejorar sus bienes y servicios y garantizar la calidad en los procesos de atención al cliente, integración de la empresa con el entorno, y conocimiento de los elementos que se deben potenciar para mejorar el uso de la información como medio para crear valor agregado"[281]. En el marco de la regulación de la tecnología financiera –FINTECH, las disposiciones específicas del financia iento participativo financiero por Internet (crowdfunding), coadyuvan a fomentar la innovación y emprendimiento.

5. CONCLUSIONES

279 RIGAUDIERE, Constance: "Relación entre Crodwfunding y Venture Capital". Universidad Pontificia Comillas. ICADE. Facultad de Ciencias Económicas y Empresariales". Madrid. España. Junio 2018. Página 5. En: https://repositorio.comillas.edu/jspui/bitstream/11531/18710/1/TFG-%20Rigaudiere%20Constance.pdf

280 RIGAUDIERE, Constance: Ob.cit. Páginas 29 y 30.

281 SILVA ORTIZ, Julian Armando: Ob.cit. Página 18.

El beneficio principal de una regulación del financ amiento participativo financiero por Internet (crowdfunding) adecuada es compartir el gran valor que puede generar una star up exitosa cuando sale al mercado, en el Perú y hacia el mundo. El crowdfunding es un método de recolección de dinero innovador, que se genera utilizando las tecnologías de información y comunicaciones (TIC) por medio de donativos y ventas, en líneas virtuales, con el fin de desarrollar una idea o un emprendimiento, o de desarrollar un objetivo de negocio particular claros que mostrarle al público.

En una conversación sostenida con mi asesor de tesis doctoral, sobre el tema que estaba desarrollando esta ponencia sobre la regulación del crowdfunding en el Perú[282]. Me hizo énfasis en la necesidad de asegurar la seguridad técnica y jurídica de este tipo de financiamiento por Internet; asimismo, en la conveniencia de interrelacionar en forma sistemática el derecho de las nuevas tecnologías y las propuestas legislativas presentadas en el Congreso de la República del Perú.

En este orden de ideas, afirmamos que la regulación del financiamiento participativo financiero por Internet (crowdfunding) debe incluir disposiciones que amplíen y concuerden las implicancias jurídicas y temas relevantes señalados con respecto a la identidad digital, las firmas y certificados digitales, los títulos valores electrónicos o digitales, la protección de datos personales, la legislación sobre dinero electrónico, la afectación tributaria de los servicios digitales por el impuesto a la renta y la necesidad de establecer exoneraciones para promover esta actividad, la prevención de los delitos informáticos tipificados y la emisión de normas específicas para la conservación de la evidencia digital en concordancia con el Convenio de Ciberdelinciencia al que el Perú se ha adherido recientemente. Los beneficios serán directamente aplicables en la promoción de la innovación y emprendimiento de las "starup" en el Peru y su directa relación con la aplicación ajustada a nuestra realidad de esta modalidad de fintech o tecnología financiera en el Perú.

BIBLIOGRAFIA CONSULTADA

BANCO INTERAMERICANO DE DESARROLLO (BID): "Alternative Finance (Crowdfunding) Regulation in Latin America and the Caribbean". Septiembre 2016.

CONGRESO DE LA REPUBLICA DEL PERU: Exposición de Motivos de Proyecto de Ley N° 4324/2018-PE que regula el Financiamiento Participativo Financiero. Presentado el 13 de Mayo de 2019. En: http://congreso.gob.pe

282 Conversación sostenida con el Dr. Ulises Montoya Alberti, en la Sala de Profesores de la Unidad de Postgrado de Derecho de la Universidad Nacional de San Marcos, en Lima, Perú, el miércoles 05 de junio de 2019, cuando coincidimos en el dictado de la cátedra universitaria.

GUTIERREZ VEGA, Miluska Jazmín: "¿Cómo Regular? Una aproximación al Crowdlending, desde la perspectiva del regulador, como mecanismo adicional de acceso al financiamient de las micro, pequeñas y medianas empresas". Tesis para optar el Grado Académico de Magister en la Maestría de Derecho Bancario y Financiero. Pontificia Universidad Católica del Perú. Lima, Abril 2018. . En: http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/12044

FERREYROS SOTO, Carlos et al: "Derecho de Personas e Informática: Identidad Digital" Ed. Grijley. 2016. Lima, Perú

The World Bank. "Crowfunding´s Potential to developing World. Washington D.C. 2013. P.14.

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS DEL PERU:. Direccion General de Proteccion de Datos Personales. Resolucion Directoral N° 670-2017-JUS/DGTA/PD-DPDP. Lima, 25 de Octubre de 2017. Procedimiento Trilateral de Tutela que interpone ciudadano contra Banco con respecto al derecho de acceso de sus datos personales. En: http://minjus.gob.pe

NUÑEZ PONCE, Julio: "Los Títulos Valores Electrónicos o Digitales". En Tratado de Derecho Mercantil. Tomo III. Páginas 928, Ed. Gaceta Jurídica. Lima, Perú. Primera Edición agosto 2004.

NUÑEZ PONCE, Julio: "Identidad Digital, Ética en la función Pública, Transparencia y Protección de Datos Personales". En Libro "Ética para los tiempos. Trayectoria de Excelencia en la función pública. Identidad. Ciudadanía y Tecnología. Páginas 257 a 270. Ed. Registro Nacional de Identificación y Estado Civil (RENIEC). Primera edición, enero de 2019. Lima, Perú.

RIGAUDIERE, Constance: "Relación entre Crodwfunding y Venture Capital". Universidad Pontificia Comillas. ICADE. Facultad de Ciencias Económicas y Empresariales". Madrid. España. Junio 2018. En: https://repositorio.comillas.edu/jspui/bitstream/11531/18710/1/TFG-%20Rigaudiere%20Constance.pdf

RODRIGUEZ DE LAS HERAS, Teresa (2014, febrero) El Crowdfunding como mecanismo alternativo de la financiación de proyectos. Disponible en: http://www.redemer.org/contneido/el-crowdfunding-como-mecanismo-alternativo-de-finaciacion-de-proyecto

SILVA ORTIZ, Julian Armando: "Beneficios y Riesgos asociados del crowdfunding

para el desarrollo y financiamiento de las starup". Universidad Nacional Abierta y a Distancia. Maestria en Administración y Organizaciones. Bogota, Colombia. 2017. En: https://repository.unad.edu.co/bitstream/10596/17384/1/80820494.pdf

VILLADA CALDERON, Juan Sebastián y GARCIA LONDOÑO, Carlos: "Crowdfunding y su implementación en Colombia". Tesis de Grado para optar el título de especialista en Derecho Comercial. Pontificia Universidad Javeriana. Facultad de Ciencias Juridicas. Especialización en Derecho Comercial. Bogota. D.C., Colombia. 2017.En: https://repository.javeriana.edu.co/bitstream/handle/10554/41266/Documento.pdf?sequence=1&isAllowed=y

IMPLICANCIAS JURIDICAS DE LA NUEVA GENERACION DE SISTEMAS ROBOTICOS INTELIGENTES: ROBOTS SOCIALES Y ESTEREOTIPOS CULTURALES

Eje Temático: Inteligencia Artificia

Autor:
Ana Karin Chávez Valdivia
Abogada. Doctora en Derecho y Magister en Derecho de la Empresa por la Universidad Católica de Santa María. Especialista en Derecho Informático y Gobierno Electrónico por la Universidad Inca Garcilazo de la Vega. Conciliadora Extrajudicial.
Directora del Departamento Académico de Ciencias Jurídicas. Docente Asociada e investigadora de la Facultad de Derecho.
Universidad La Salle de Arequipa-Perú.

RESUMEN
En un escenario donde enfrentamos el hecho de que la nueva generación de sistemas robóticos no sólo convivirá de manera natural con los seres humanos sino que además el diseño y construcción de robots "sociales" serán suficientemente humanos y atractivos en múltiples aspectos.
En un estadio en el cual, como resultado del rápido desarrollo e interés por introducir robots en nuestra vida cotidiana la premisa que cuanto mayor sea la inteligencia artificial mayor será su autonomía y por consiguiente, menor su dependencia de fabricantes, propietarios y usuarios; se viabiliza en toda su extensión; consideramos que deviene en un hecho impostergable el cuestionar la capacidad de los sistemas legales existentes para manejar los casos que involucren a estos nuevos actores más allá de la posibilidad de demandas por responsabilidad del producto como fue hasta ahora en razón que la atención recayó siempre en la fabricación y el diseño de robots.
Finalmente, ante el hecho indiscutible que la robótica se está aventurando en un ámbito de responsabilidad legal que tradicionalmente ha gobernado las interacciones sociales entre seres humanos y no entre humanos y sistemas cyber-físicos; se hace evidente que nos enfrentaremos a uno de los cambios sociales más cuestionables de todos los tiempos; por lo tanto estimamos conveniente un análisis en torno a la no tan lejana existencia de un Derecho de los Robots y en consecuencia la necesidad de creación de una nueva categoría de sujeto jurídico.

Palabras Clave: Robótica, Inteligencia Artificial, Derecho de los Robots, Personalidad Jurídica, Robots sociales

INTRODUCCION

Vivimos en una era de innovación tecnológica sin precedentes. Los increíbles avances del binomio robótica e inteligencia artificial en las últimas décadas resaltan que la diferencia entre la ciencia ficción y la ciencia real se está cerrando con el paso del tiempo. Asimismo, es innegable que las implicancias y efectos de esta conjunción revolucionarán las estructuras sociales existentes y comportarán innumerables desafíos regulatorios que los actuales marcos legales –en su mayoría- no están preparados para enfrentar.

Los diversos cambios que fueron surgiendo en la medida que las sociedades fueron avanzando, trajeron consigo cuestionamientos de todo orden; lo que llevó a que diversos sectores empezaran a cuestionarse sobre sus realidades; y la pregunta sobre el cómo y el por qué evolucionaron nuestras relaciones personales más importantes aún no encuentra una respuesta definitiva y mucho menos determinante; más aún, las posibilidades se incrementan a la par del surgimiento de nuevos avances, elementos o tendencias. En este contexto no es de sorprender que en los últimos años se estén desarrollando relaciones sociales con los robots en sus diversas manifestaciones debido en gran parte a que esta dupla tecnológica se ha convertido no sólo en un factor esencial sino en gran medida indispensable para el despliegue de prácticamente todas las actividades habituales en diversos entornos, más no así en la misma medida.

El presente estudio considera la revisión de la evolución doctrinal donde la mayoría de ordenamientos reconoce la existencia de dos personalidades jurídicas diferenciadas; así como las principales tendencias del estadio tecnológico actual que plantean la imperiosa necesidad de abordar la procedencia o no de crear una personalidad jurídica específica para los robots y una rama nueva del Derecho; al tiempo que se constituye en un intento por hacer un análisis del redimensionamiento de nuestras relaciones interpersonales basadas en la compleja naturaleza humana y sus tendencias.

I. ENTRE LA ADOPCIÓN DE MEDIDAS LEGALES EN EL ÁMBITO DE LA ROBÓTICA E INTELIGENCIA ARTIFICIAL Y LOS LÍMITES DE SUS IMPLICANCIAS

El mes de febrero del año 2017 se aprobó la Resolución del Parlamento Europeo con recomendaciones destinadas a la Comisión Europea sobre normas de Derecho Civil en torno a la Robótica[283]. El documento en mención formula una serie de consideraciones previas, así como recomendaciones que han de seguirse para regular a corto plazo la creación, uso y efectos de la robótica en la hoy Unión Europea. La resolución está centrada principalmente en las reglas civiles aplicables a los robots, y en especial, las

283 Resolución del Parlamento Europeo con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL)), de 16 de febrero de 2017 (Base de datos del Parlamento Europeo)

cuestiones relativas a la responsabilidad derivada de sus acciones u omisiones. En este sentido compartimos la opinión de Niza[284] en cuanto a que la Robótica basada en inteligencia artificial debe obedecer a un estructurado sistema jurídico organizado bajo un código de conducta establecido para las personas implicadas en el desarrollo, fabricación y uso de robots inteligentes con el fin de prevenir diversos tipos de efectos nocivos o perjudiciales que pudieran surgir del desarrollo de las funciones del desempeño de la inteligencia artificial en robots inteligentes.

De otro lado Aranzay (2018)[285] menciona que la Resolución de Schuman de 1950 ya habría considerado que la regulación futura en materia de responsabilidad había de centrarse en determinar si una máquina puede considerarse parcial o totalmente responsable de su conducta, y si la misma puede subsumirse en alguna de las categorías jurídicas ahora existentes (p. 97).

Siendo así, con miras a poder enfrentar las posibles situaciones de riesgo en diversos ámbitos, el Parlamento Europeo planteó la adopción de diversas medidas legales con implicancias en diversos ámbitos y áreas básicas que permitan establecer un marco legal en torno a las obligaciones y derechos dirigidos a los fabricantes de robots -en el entendido de que estos se encuentran sometidos a las Leyes de Asimov- a las instituciones, así como a los propietarios, usuarios y ciudadanos en general.[286]

Sin embargo, la evolución de la dupla inteligencia artificial y robótica con la consecuente inserción de nuevos agentes inteligentes en la sociedad y en la vida cotidiana que comenzarán a operar sin la intervención de humanos y eventualmente incluso sin su conocimiento, marcarán un hito en el desarrollo del derecho; situándolo en la necesidad de replantearse un nuevo tipo de persona no concebida por los hasta ahora ordenamientos jurídicos vigentes. Siendo así, podemos evidenciar que acorde al párrafo anterior esta evolución tecnológica encontraría una limitación insalvable si se concibiese un estricto marco legal acorde tan solo a las medidas proyectadas que se abocan únicamente a todos aquellos actores que gravitan alrededor de los robots y no en los robots en sí mismos.

Por otro lado, la base axiológica de los ordenamientos jurídicos occidentales se centra en la dignidad inherente de la persona humana. Este hecho implica entre otras cosas el "derecho a tener derechos". Los sistemas legales se basan en un conjunto de suposiciones filosófica en el que los seres humanos ocupan una posición excepcional; esto resulta no solo del hecho de que las normas legales son establecidas por ellos, sino también, o más aún, del valor moral inherente del ser humano como un fin en sí

284 Liderar Innovando: http://liderar-innovando.blogspot.com/2016/07/javier-antonio--nisa-avila-robotica-e.html [Fecha de consulta: 28 de marzo del 2019]

285 ARANZAY, A., "Antecedentes y propuestas para la regulación jurídica de los robots", Derecho de los Robots, coord. Moises Barrio, Wolters Kluwer, Madrid, 2018, pp. 87-106.

286 Entre estas medidas proyectadas se encuentran: la responsabilidad, un Código ético, una Administración reguladora, Propiedad intelectual y Seguridad sobre el diseño, Fiscalidad y Seguridad Social, Ajustes en los ordenamientos jurídicos nacionales, entre otras.

mismo. En este sentido el derecho se basa en el supuesto de que todas las relaciones jurídicas tienen lugar entre las personas naturales y/o jurídicas, es decir los seres humanos y sus entidades orgánicas.

Siendo así, la idea de que los robots hayan evolucionado más allá de la consideración como "propiedad" y la viabilidad de que adquieran estatus legal como seres con "derechos" plantea múltiples interrogantes sobre diversos temas.

II. ENTRE DERECHOS Y PERSONALIDADES: EXPECTATIVAS Y REALIDAD

La creciente e imparable introducción de la inteligencia artificial promete revolucionar las estructuras sociales actuales y comportará no solo innumerables desafíos regulatorios, sino también tecnológicos e industriales.

En este contexto, Pagallo (Citado en Barrio, 2018, p.81) a la hora de abordar la sustantividad de un Derecho de los Robots pone de relieve como las tendencias en los derechos comparados pueden sistematizarse en tres grandes respuestas:

a) Una primera aproximación, que únicamente examina como los robots afectan a los conceptos y principios legales tradicionales, como por ejemplo es el caso del concepto de persona jurídica; personería que será abordada en la presente investigación.

b) Otra segunda dirección que pretende edificar una nueva disciplina jurídica con nuevos paradigmas, como sería el caso por ejemplo de la responsabilidad por operaciones realizadas por sistemas robóticos autónomos

c) Una tercera y última dirección, que por el contrario, niega su especificidad y convierte los retos que plantean los robots en cuestiones que se pueden abordar siempre dentro de los parámetros de los vigentes ordenamientos[287].

Compartimos la opinión de Barrio (2018) [288] cuando acertadamente sostiene que el problema es que los conceptos fundamentales se están volviendo problemáticos como marcadores de límites (p.82). En este sentido y en contraposición al acápite precedente donde se contempla una regulación del ámbito de la robótica que partiendo de un marco de situaciones de riesgo está dirigido tan solo a los actores vinculados con los robots; el autor propugna una disciplina autónoma que aparentemente al denominarla "Derecho de los Robots" supondría propuestas y aproximaciones de una regulación centrada en los robots en sí mismos y por consecuente lógica la identificación de derechos y obligaciones de especial naturaleza que ostentarían sus portadores. Sin embargo, a pesar que su propuesta la sintetiza bajo la denominación

287 PAGALLO, U., The laws of robots: Crimes, Contracts, and Torts, Springer, Nueva York, 2013.

288 BARRIO, M., "Del derecho de internet al derecho de los robots", Derecho de los Robots, coord. Moises Barrio, Wolters Kluwer, Madrid, 2018, pp. 61-86.

señalada no aborda directamente este tema ni profundiza en mayor medida de que derechos centrados en los robots estamos hablando ni cuales serían pasibles de regulación; más aún, prioriza en gran medida a los agentes que giran en torno a ellos siguiendo así la consideraciones de la Unión Europea en cuanto al planteamiento de medidas legales. Señala también el autor que entre las circunstancias que justifican un tratamiento unitario del tema a través su propuesta se encuentra en primer lugar y principalmente una cuestión fáctica que pertenece al mismo sector de investigación y de la innovación tecnológica, que aun sirviéndose de diversas disciplinas auxiliares presenta características suficientemente específicas y en segundo lugar, considera la relevancia de carácter socio-económico, puesto que la robótica implica un mercado en expansión y de gran impacto a nivel social, cuyo crecimiento requeriría ser controlado mediante una intervención regulatoria.[289]

En sentido contrario, es preciso mencionar que un estudio realizado por el gobierno británico que pretende adelantarse al desarrollo tecnológico de los próximos 50 años, reveló que los robots podrán reclamar en un futuro los mismos derechos de los que gozan los seres humanos. De ser así, tal como señala el informe titulado Escaneos Sigma y Delta - producto del trabajo conjunto de la sociedad Outsights-Ipsos Mori y el Instituto para el Futuro (IFTF) - los estados estarán obligados a proveerles de seguridad social, incluido alojamiento y seguro médico.[290] En consecuencia, consideramos el cuestionamiento de Winfield como una interrogante válida: ¿por qué los robots no podrían tener derechos? en el entendido que muchos de los ya existentes son robots inteligentes, capaces de participar plenamente en el discurso con los seres humanos, en el arte, la filosofía, las matemáticas; robots capaces de empatizar o expresar opiniones; sostiene el autor que tal vez resulte por ahora difícil imaginar que

289 En base a estas consideraciones sostiene que de los dos aspectos señalados emergen las principales razones que justifican la creación de un Derecho de los Robots ya que de un lado brindaría un marco de reglas jurídicas claras que pueda conferir certeza respecto a los deberes y las responsabilidades de los actores involucrados que -como ya se vio- es precisamente la demanda de los operadores del sector; y del otro, sería capaz de impulsar el desarrollo de la robótica en un entorno en el cual se respeten valores y se observen derechos fundamentales; los cuales evidentemente corresponden a los distintos agentes que ya han sido mencionados. Cabe recalcar que el enfoque de protección sigue orientándose hacia quienes que por situaciones diversas mantienen alguna relación con los robots y no hacia a los robots en sí mismos y a pesar de sostener que el Derecho de los Robots que propone -por el momento- tendría un doble objeto; refiere que el primero se enfoca en cómo distribuir los derechos y las responsabilidades que surgen de las acciones de los seres no humanos -lo que evidentemente nos conduce nuevamente a la esfera de los agentes- y el segundo vinculado con el anterior, es lo que se ha denominado como impacto social en la vertiente de la sustitución de seres humanos por robots y sistemas de inteligencia artifici l, precisando además que probablemente esta sustitución sólo se realice para ciertos propósitos y que sea contextual, inestable y a menudo oportunista. Siendo así, somos de la opinión que se puede evidenciar que del doble objeto que señala el autor la tendencia en su propuesta se mantiene también en la línea de tuitividad hacia los diversos actores involucrados con los robots y las cuestiones relativas a la responsabilidad derivada de sus acciones u omisiones en perjuicio de la sociedad y no centrada en los robots como hemos puntualizado.

290 BBC MUNDO: http://news.bbc.co.uk/hi/spanish/misc/newsid_6201000/6201131.stm [Fecha de consulta: 1 de mayo de 2019]

en determinados contextos los robots sean lo suficientemente inteligentes, elocuentes y persuasivos para poder argumentar su caso; y que no hay ninguna razón para suponer que la emancipación del robot será rápida o directa; más aún, si consideramos que a pesar de que los derechos humanos tal como ahora se entienden se establecieron hace más de 200 años, aún no son universalmente respetados ni defendidos. Por lo que es de suponer que para los robots tampoco será un camino fácil.[291]

Siendo así y en base a los escenarios advertidos deviene en imperativo abordar algunas consideraciones en torno al otorgamiento de una personalidad jurídica específica para los robots.

María José Santos (2017)[292] señala que la persona jurídica es una entidad que sin tener existencia individual física está sujeta a derechos y obligaciones, siendo por tanto una figura legal ficticia (p. 42). En este sentido, sostiene que esta condición legal es susceptible de ser atribuía a los robots; no obstante considera también que existen varias diferencias que determinarían un trato diferente[293]. Para Santos el robot

291 Alan Winfield's Web Log: http://alanwinfield. logspot.com/2007/02/rights-of-robot.html [Fecha de consulta: 28 de abril de 2019]

292 SANTOS GONZALES, M. J., "Regulación legal de la robótica y la inteligencia artificial: retos de futuro", Revista jurídica de la Universidad de León, núm. 4, 2017, págs. 25-50.

293 Entre las similitudes del robot con una persona jurídica el autor considera las siguientes: Es una Persona de configuración legal, distinta de su propietario. Su existencia y capacidad es independiente de su propietario. Ambas podrían adquirir capacidad de obrar, esto es capacidad para el ejercicio de derechos y deberes. La empresa -como persona jurídica puede llevar a cabo contrataciones; el robot podría adquirir la capacidad para contratar en su propio nombre. Más aún, en la actualidad los robots contratan en muchos casos a través del software sin intervención humana debido a los servicios digitales. La persona jurídica tiene capacidad para causar daños y para ser responsable penalmente -bajo ciertos supuestos-. Además se podría sancionar al robot aunque los efectos inmediatos no producirían efectos respecto al robot. Por otro lado, las personas jurídicas adquieren personalidad desde el instante que han quedado válidamente constituidas de acuerdo con la ley; en consecuencia, los robots también quedarán constituidos y adquirirán los derechos de acuerdo con los requisitos que se configuren en la ley. De hecho, el robot debería adquirir un estatus jurídico desde el momento que es válidamente inscrito en el Registro correspondiente.

En sentido contrario, las diferencias identificadas por Santos y que determinarían la necesidad de una figura jurídica nueva son: La personalidad de las personas jurídicas se constituye en torno a la idea de un grupo de personas físicas que funcionan agrupados y no individualmente. Esta idea sin embargo está alejada de los robots, que están emergiendo para cubrir nuestras carencias o mejorar nuestras deficiencias sustituyendo ciertas acciones y operaciones de los humanos pero no entorno a su agrupación social. Señala también que las empresas no han sustituido a los humanos sino que han permitido su organización y facilitado el funcionamiento de la sociedad; que la persona jurídica también puede nacer de la agrupación de bienes y que carecen de cuerpo físico, no pudiendo actuar si no son representadas por una persona física.

El autor sostiene que en el caso de un robot inteligente éste puede firmar electrónica o físicamente un contrato tomando una decisión lógica sin necesidad de que en la operación participe una persona física y podría hacerlo en su nombre y con su identificado . Considera además la configuración legal de los derechos y obligaciones (capacidad jurídica). Refiere que en el caso de las empresas no se puede hablar de inmadurez psíquica del sujeto, las empresas son incapaces por eso siempre actúan a través de representantes. En el caso de los robots sin embargo se podría fijar un test de inteligencia y de madurez. El robot interactúa directamente con el entorno, las empresas sin embargo deben hacerlo a través de sus representantes. Por ejemplo, un robot podría robar, causar un daño de manera autónoma;

y la persona jurídica tal como está contemplada en los tradicionales ordenamientos existentes son condiciones jurídicas distintas; sin embargo precisa el autor que si acogemos las teorías antiformalistas, es completamente factible aplicar la condición de persona jurídica a un robot ya que estas teorías consideran que en el caso de las personas jurídicas de lo que se trata es de comprender cómo una entidad que no es un hombre puede ser titular de derechos y obligaciones y actuar jurídicamente. En este contexto, cabe señalar que si bien en su momento, producto de largos debates doctrinarios la mayoría de Sistemas Normativos reconocieron la existencia dos personalidades jurídicas diferenciadas; la evolución tecnológica ha hecho que en los últimos años el tema de la personalidad del robot haya pasado a un primer plano en la robótica social gracias a diversas publicaciones que abordan este planteamiento desde múltiples aristas. Aceptar la posibilidad de que los robots estén dotados de algún tipo de personalidad artificial implica un proceso de transición que no será el igual en todos los países ni encontrará el mismo nivel de aceptación debido a innumerables factores -sin perjuicio del interés teórico y filosófico que implica abordar la creación de una nueva Personalidad Jurídica- pero que aun siendo así, todas las sociedades deberán afrontar en un corto periodo de tiempo.

El debate ya se inició y una vez superada la infinidad de cuestionamientos y controversias que ha suscitado; el siguiente paso será determinar qué postura asumiremos; con todo lo que ello implique.

Siendo así, la Resolución del Parlamento de la Unión Europea conmina a la Comisión para que la personalidad jurídica se otorgue únicamente a aquellos entes capaces de tomar decisiones autónomas, al tiempo que en sus recomendaciones evita usar la palabra "voluntad" haciendo constante alusión al término autonomía -el mismo que desde la época griega ya hacía referencia a cierto estado de "capacidad" o de "voluntad propia" y que posteriormente con Kant alcanza una definición más clara en la filosofía.[294]

---

sin embargo la empresa no puede hacerlo por sí mismo por ser un ente no físico. Por otro lado, en la persona jurídica se exige siempre el control y la vigilancia del humano: en los robots inteligentes se podría prescindir de esta exigencia. Se podría argumentar la doctrina del levantamiento del velo y responsabilizar jurídicamente siempre a su titular pero no parece acorde con la realidad de la existencia y funcionamiento del robot, ni con las posibilidades de control reales de su propietario cuya responsabilidad se encaminará a la gestión del riesgo. Finalmente señala que el robot inteligente podría actuar en nombre de la empresa y en su representación bajo el contrato de mandato. La empresa no puede representar a un robot por carecer de condición física.

294 Sin embargo; y no obstante, cabe mencionar que en la edad media la voluntad recibió diversas nomenclaturas entre las que debe destacarse el apetito racional y el apetito intelectivo, elementos estos que vincularían por tanto la autonomía con la inteligencia (artificial)

En el campo de la Robótica la "autonomía" se referiría a la posibilidad de adoptar decisiones por uno mismo, sin dejarse influenciar por los demás; y en la previsión del Parlamento Europeo, es la capacidad de ser responsable del propio comportamiento y de conducir la existencia; de acuerdo con dictados propios.

Por consiguiente, concordamos con Savigny cuando considera que las personas morales son el resultado de un artificio legal que la ley elabora por razones de conveniencia -recurriendo entonces a la ficción- y compartimos la opinión de Ercilla García (2018)[295] al precisar que devendría en una cuestión de conveniencia la creación de una personalidad jurídica específica para los robots, en consideración a que un lapso de tiempo medianamente corto la sociedad contará con entes no humanos dotados de voluntad que realizarán actos susceptibles de crear derechos u obligaciones en el ámbito jurídico (p.17).

En este orden de ideas señala el autor que el panorama del sistema jurídico se conformaría por el reconocimiento de tres personalidades jurídicas; la del ser humano individual dotado de voluntad propia; la de las colectividades humanas dotadas de voluntad común producto de voluntades aisladas y la de los sistemas ciber-físicos dotada de una voluntad surgida de procesos algorítmicos. Sostiene Ercilla también qué en virtud de la Teoría pura del Derecho, la persona jurídica, tanto individual, colectiva; como electrónica, no serían sino un conjunto de obligaciones jurídicas y derechos subjetivos, cuya unidad se expresa metafóricamente en el concepto de "persona". Al tiempo que el concepto de "portador" de derechos y obligaciones jurídicas desempeña un papel decisivo en la teoría tradicional de la personalidad jurídica. Si bien, determinar el contenido concreto de los derechos y obligaciones que la persona ciber-física haya de "portar" deviene en un tema crucial, complejo y altamente debatible, al no ser objeto de la presente investigación no será abordado.

Por otro lado, mientras en los Estados Unidos se habla de persona artificial y el Parlamento Europeo hace alusión a una "persona electrónica"; en opinión de Ercilla el término ciber-físico es el que más se acercaría a la descripción de lo que ha de ser un robot inteligente. Siendo así, esta nueva personalidad jurídica encontrará asidero en la medida que se reconozca y acepte que no estaremos frente a entes sometidos a la total voluntad humana sino que también serán consecuencia del entorno que los rodea lo cual le permitirá adoptar decisiones en virtud de aprendizajes autodidactas y realidades circundantes.

III. ROBOTS SOCIALES: REDIMENSIONANDO NUESTRAS RELACIONES INTERPERSONALES

295 ERCILLA, J., *Normas de Derecho Civil y Robótica. Robots Inteligentes, Personalidad Jurídica, Responsabilidad Civil y Regulación,* Thomson Reuters Arazandi, Pamplona, 2018.

Las realidades sociales no permanecen inmutables en el tiempo; en consecuencia, el Derecho no puede permanecer ajeno a cambios sustanciales que demandan su obligada atención por lo que nos cuestionamos hasta cuándo puede la ley retrasarse con respecto a la tecnología considerando la inminente presencia de robots artificialmente inteligentes en nuestras vidas. En Japón se habla de que esto ocurrirá en el 2030, más aún, en este país el Gobierno aprobó en el año 2004 el establecimiento de zonas especiales "Tokku" para probar los robots en entornos reales[296] y desde el año 2007, el estado japonés ha promovido activa e incansablemente una sociedad y un estilo de vida dependientes del robot; tal es así que, en febrero de ese mismo año, el primer ministro Shinzð Abe dio a conocer "Innovation 25", un plan visionario para revitalizar la economía, la sociedad civil y los hogares "tradicionales" de Japón para el año 2025.

Dario et al. (2011)[297] en "Robot Companions for Citizens"; abordó temáticas que años más tarde serían recogidas por la resolución del Parlamento Europeo; el autor parte del hecho que el envejecimiento de la población generará nuevas necesidades asistenciales y de salud; esta realidad es también compartida por la sociedad japonesa; en la cual, no solo se espera que los robots reemplacen la necesidad de inmigrantes y trabajadores migrantes, sino que los humanoides están siendo diseñados para cumplir muchos roles, incluyendo la preservación de costumbres japonesas "únicas" y formas de arte escénico tradicionales. En este sentido, señala Jennifer Robertson (2014)[298] que existe un creciente apoyo popular, por un lado, para denegar los derechos civiles a los residentes permanentes por el otro, para conferir los derechos de ciudadanía y residencia a los robots y animales no humanos, e incluso Personajes de caricatura (p.578). Refiere además que la población y la fuerza de trabajo de Japón está envejeciendo y disminuyendo rápidamente. Así, las estimaciones del Ministerio de Salud, Trabajo y Bienestar indican que la población disminuirá a menos de 111 millones en 2035 y a menos de 90 millones en 2055. De otro lado, señala Robertson que las encuestas nacionales realizadas por la Oficina del Gabinete indican que los ciudadanos japoneses no se sienten cómodos con la idea de ser atendidos por enfermeras y cuidadores extranjeros, así como que muchas personas mayores se preocupan particularmente por el estrés de lidiar con las diferencias lingísticas y culturales; de ahí que se sienten más cómodos compartiendo entornos de vida con robots al punto que más del 80 % manifiesta interés por adquirir un robot cuidador. Esta misma tendencia se refleja en el ámbito laboral donde prefieren tener robots que contratar trabajadores migrantes.

296 ROBOTLAW.ASIA: http://www.robolaw.asia/research-es-01.html [Fecha de consulta: 10 de abril de 2019]

297 DARIO, P., VERSCHURE, P., PRESCOTT, T., CHENG, G., SANDINI, G., CINGOLANI, R.,…ALBU, A., "Robot Companions for Citizens", *Procedia Computer Science,* num. 7, 2011, págs. 47-51.

298 ROBERTSON, J., "Human rights vs. robot rights: Forecasts from Japan", *Critical Asian Studies,* núm. 4, 2014, págs. 571-598.

Ante la evolución y tendencias de los diversos contextos sociales, la propuesta "Robot Companions for Citizens" precisa la necesidad de atender situaciones actuales por lo que los Compañeros Robots serán una nueva generación de máquinas que ayudarán y asistirán principalmente a las personas mayores en las actividades diarias del hogar, en su lugar de trabajo y en otros entornos. Por su parte Rafael de Asis (2015)[299] señala que actualmente se estima que en el mundo hay aproximadamente más de un millón de robots que desempeñan diversas funciones y se encuentran en hospitales, industrias y casas (p.34)[300]. Además, según la labor que realizan cuentan con capacidades para convivir con las personas y realizar tareas que incidan directamente en su forma de vida.

En este orden de ideas es indiscutible que la sociedad deberá lidiar con robots dotados de voluntad, aprendizaje e inteligencia artificial que dará como resultado que cada ente electrónico posea una individualización diferenciada de los demás una vez fabricado y programado; por lo que estarán en capacidad de distinguirse de los demás en la medida que sean capaces de aprender de su entorno y en consideración a las circunstancias alrededor de las cuales transcurra su existencia. Todo esto conllevará a que por ser seres autónomos relacionables con la sociedad precisen de un estatus jurídico distinto.[301]

Sin embargo; cabe mencionar que evidentemente no todas las Inteligencias artificiales se encuentran en el mismo nivel desarrollo. Si bien es cierto John Searle (2000)[302] construyó la distinción entre la IA débil y la IA fuerte hacia 1980 su posición fue enfrentada por quienes sostienen la inespecificidad humana de la inteligencia y cuestionaron el enigma de la habitación china (p.9).

De otro lado, el Parlamento Europeo en la recomendación Nro. 3 del documento ya citado señala que: "(...) *que debe prestarse especial atención al posible desarrollo de un vínculo emocional entre seres humanos y robots -especialmente en el caso de grupos vulnerables, como niños, personas mayores y personas con discapacidad-, y destaca los problemas que pueden*

299 DE ASÍS, R., Una mirada a la robótica desde los derechos humanos, Dykinson, Madrid, 2015.

300 El Informe Mundial Robótica 2016, "Robots de Servicio", publicado por la Federación Internacional de Robótica (IFR) señalo que el número mundial de robots domésticos subiría a 31 millones entre 2016 y 2019 aumentando alrededor de 30 millones de unidades a diferencia del crecimiento en el 2015 que fue de 3,6 millones. En cuanto a los robots de entretenimiento prevé que entre los años señalados este sector crecerá a 11 millones de unidades, siendo que los robots de juguete y pasatiempos representan el 70 por ciento de la cuota del mercado. En cuanto a los robots de ayuda para minusválidos se espera que aumente a 37,500 unidades de 2016 a 2019 a diferencia del 2015 que sólo contó con un volumen de 4,700 unidades.

301 La normativa jurídica asiática tal como señala Nisa diferencia entre cuatro conceptos, niveles o categorías de robots existentes a regular jurídicamente para poder alcanzar a generar una correcta definición que abarque completamente su naturaleza jurídica

302 SEARLE, J., *The Mistery of Consciousness,* The New York Review of Books, Nueva York, 2000

plantear las graves consecuencias físicas y emocionales que este vínculo emocional podría causar a los seres humanos".

Existen, sin embargo, diversos estudios psicológicos sistemáticos que identificaron como elemento esencial en determinadas relaciones el *factor antropomórfico*.[303] El antropomorfism [304] y la tendencia a establecer determinados vínculos sea cual fuere el nombre que se les dé, como podría ser el apego parecieran ser innatos en el ser humano -sin perjuicio de hacia quién o hacia qué se dirija- por lo que Joseph Weinzenbaum, en los inicios de la inteligencia artificial quedo perplejo por el alcance de antropoformización que algunas personas le concedieron al programa de computador ELIZA[305].

En este contexto para Breazeal Cynthia (2002)[306] un robot sociable es capaz de comunicarse, interactuar, comprender y aún relacionarse con nosotros de una forma personal; al tiempo que debe ser capaz de entenderse y entendernos en términos sociales. Nosotros, a cambio, debemos poder entenderlo en los mismos términos sociales, relacionarnos y ser empáticos con él. Señala además la autora que este tipo de robot debe poder adaptarse y aprender a lo largo de su tiempo de vida, incorporando experiencias compartidas con otros individuos dentro de su comprensión sobre sí mismo, sobre otros y las relaciones que ellos comparten (p. 1). En síntesis, según Breazeal un robot sociable es socialmente inteligente de la misma forma que lo es el ser humano e interactuar con él es como interactuar con cualquier otra persona.

Así mismo, Kahn et al. (2011)[307] tras una serie de experimentos tendientes a esclarecer que es lo que piensan las personas acerca de los robots, concluyó en que éstos pueden pertenecer a una categoría ontológica completamente nueva y que existe

303 La web site www.marryyourpet.com ofrece la posibilidad de contraer matrimonio con una mascota de forma rápida y fácil -así como lucrativa para su administrador-. El servicio incluye paquetes que están acorde a la elección de una boda simple o una gran boda.

304 Es considerado por algunas personas como una creencia, aun que fuere solo transitoria, que el objeto en cuestión es esencialmente humano.

305 En 1966, Winzenbaum creó el programa Eliza que, junto con su desarrollo de 1967 denominado Parry del psiquiatra Kennet Colby, constituye una sofisticación que va más allá de los juegos de aventura, para adentrarse en la ficción interactiva. Parry simulaba conversaciones de un esquizofrénico paranoico tan fidedignamente que los siquiatras no podían diferenciarlas de las acaecidas en sus consultas con pacientes reales. Eliza era capaz de sintetizar el significado de varias palabras: deficiente estado mental= deprimido, infeliz. La idea de Weizenbaum era que Eliza conversara (de forma escrita) con su interlocutor de modo tal que diera la sensación de que lo estaba escuchando y de que empatizaba con sus problemas e inquietudes. Para lograr una conversación no robótica, lo más semejante posible a un diálogo entre dos seres humanos, Eliza se valía de varios recursos. Uno de sus secretos era reconocer palabras clave, para luego hacer preguntas referidas a dicho tema. Por ejemplo, cuando el interlocutor mencionaba en su discurso la palabra padre o madre, Eliza reconocía que estaba hablando sobre la familia y luego hacía preguntas relacionadas con esa cuestión. También tenía almacenadas frases hechas sobre una variedad de temas, que utilizaba al reconocer palabras clave, así como frases empáticas y de continuidad.

306 BREAZEAL, C., *Designing Sociable Robots*, MIT Press, Massachusetts, 2002.

307 KAHN, P., REICHERT, A., GARY, H., KANDA, T., ISHIGURO, H., SHEN, S.,…GILL, B., "The new ontological category hypothesis in human-robot interaction", *ACM DL*, 2011, págs. 159-160.

la inclinación humana por atribuir estados mentales a los robots, e incluso adoptar comportamientos que serían impensables al tratar con un simple objeto al tiempo que Balkin (2015)[308] señala que el problema no es que las personas confundan a los robots con seres vivos, sino que a través de sus interacciones con robots y demás sistemas de inteligencia artificial , las personas están dispuestas a sustituir a los animales o seres humanos por robots en ciertos contextos y determinados propósitos- denominado: "efecto de sustitución" (p. 46). En base a estas consideraciones no carece de sentido el hecho que las interrelaciones personales en un futuro cercano se establezcan entre una persona y un robot.

IV. CONSIDERACIONES FINALES

Vislumbramos que ante una nueva generación de robots que convivirá con los humanos el derecho deberá dar respuestas basadas en argumentos jurídicos lo suficientemente consistentes; consideramos que si la ley crea personas jurídicas, entonces las "definicion s legales de personas" son prescriptivas más que descriptivas; en consecuencia, llegar a un concepto satisfactorio de la personalidad es una cuestión de decisión, no de descubrimiento. Es decir; el establecimiento de la personalidad jurídica corresponde a una evaluación realizada por una legislatura, instancia u órgano ad-hoc a efecto de determinar el otorgamiento derechos y obligaciones a la "entidad", independientemente de cómo ésta se vea y si podría o no pasar por humana o bajo qué consideraciones.

Por otro lado, en cuanto a los robots sociales, si bien, cuán mutuas o consensuadas son estas relaciones en la ficción versus la realidad es un tema diferente y una zona mucho más gris, lo que sí está claro, es que estas relaciones sean del tipo que fueren eventualmente tendrían implicancias legales significativas, por lo que existe una necesidad cada vez mayor de un marco normativo adecuado que las contemple.

V. REFERENCIAS

Alan Winfield's Web Log: http://alanwinfield.blogspot.com/2007/02/rights of-robot.html [Fecha de consulta: 28 de abril de 2019]

ARANZAY, A., "Antecedentes y propuestas para la regulación jurídica de los robots", Derecho de los Robots, coord. Moises Barrio, Wolters Kluwer, Madrid, 2018, pp. 87-106.

308 BALKIN, J., "The path of Robotics Law", The Circuit, núm. 72, 2015, págs. 45-60.

BARRIO, M., "Del derecho de internet al derecho de los robots", Derecho de los Robots, coord. Moises Barrio, Wolters Kluwer, Madrid, 2018, pp. 61-86.

BALKIN, J., "The path of Robotics Law", The Circuit, núm. 72, 2015, págs. 45-60.

BBC MUNDO: http://news.bbc.co.uk/hi/spanish/misc/newsid_6201000/6201131.stm [Fecha de consulta: 1 de mayo de 2019]

BREAZEAL, C., *Designing Sociable Robots*, MIT Press, Massachusetts, 2002.

DARIO, P., VERSCHURE, P., PRESCOTT, T., CHENG, G., SANDINI, G., CINGOLANI, R.,…ALBU, A., "Robot Companions for Citizens", *Procedia Computer Science,* num. 7, 2011, págs. 47-51.

DE ASÍS, R., Una mirada a la robótica desde los derechos humanos, Dykinson, Madrid, 2015.

ERCILLA, J., *Normas de Derecho Civil y Robótica. Robots Inteligentes, Personalidad Jurídica, Responsabilidad Civil y Regulación,* Thomson Reuters Arazandi, Pamplona, 2018.

KAHN, P., REICHERT, A., GARY, H., KANDA, T., ISHIGURO, H., SHEN, S.,…GILL, B., "The new ontological category hypothesis in human-robot interaction", *ACM DL*, 2011, págs. 159-160.

Liderar Innovando: http://liderar-innovando.blogspot.com/2016/07/javier-antonio-nisa-avila-robotica-e.html [Fecha de consulta: 28 de marzo del 2019]

PAGALLO, U., The laws of robots: Crimes, Contracts, and Torts, Springer, Nueva York, 2013

Resolución del Parlamento Europeo con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL)), de 16 de febrero de 2017 (Base de datos del Parlamento Europeo)

ROBERTSON, J., "Human rights vs. robot rights: Forecasts from Japan", *Critical Asian Studies,* núm. 4, 2014, págs. 571-598.

ROBOTLAW.ASIA: http://www.robolaw.asia/research-es-01.html [Fecha de consulta: 10 de abril de 2019]

SANTOS GONZALES, M. J., "Regulación legal de la robótica y la inteligencia artificial:

retos de futuro", Revista jurídica de la Universidad de León, núm. 4, 2017, págs. 25-50.

SEARLE, J., *The Mistery of Consciousness,* The New York Review of Books, Nueva York, 2000.

DISCRIMINACIÓN 4.0: LA INTELIGENCIA ARTIFICIAL COMO UN DESAFÍO DE GÉNERO

Eje temático: Inteligencia Artificial - riesgos y desafíos jurídico

Autores
Rodrigo Cortés Borrero
Abogado "Cum Laude" de la Universidad Santo Tomás, Colombia; Especialista en Derecho Administrativo de la Universidad Santo Tomás, Conciliador en Derecho, Magíster en Derecho Contractual Público y Privado, Universidad Santo Tomás, Cursando Doctorado en Derecho Privado de la Universidad de Salamanca, España; Docente Investigador y Director del Semillero de Investigación de Derecho Informático y de las Tecnologías en la Sociedad de la Información (DITSI) de la Facultad de Derecho de la Universidad Santo Tomás, Sede Villavicencio. Miembro de la Federación iberoamericana de Asociaciones de Derecho e Informática (FIADI). rodrigocortes@usantotomas.edu.co

Paola Consuelo Ramos Martínez
Abogada "Cum Laude" de la Universidad Santo Tomás, Colombia, cursando Maestría en Estudios Interdisciplinares de Género en la Universidad de Salamanca, España. Profesional Investigadora adscrita al Semillero de Investigación de Derecho Informático y de las Tecnologías en la Sociedad de la Información (DITSI) de la Facultad de Derecho de la Universidad Santo Tomás, Sede Villavicencio. Miembro de la Federación iberoamericana de Asociaciones de Derecho e Informática (FIADI). paolaramosmartinez@hotmail.com

RESUMEN
Actualmente la mayor apuesta tecnológica se ha desarrollado en el campo de la inteligencia artificial. No obstante, su continuo perfeccionamiento ha venido trayendo diversos interrogantes acerca de la forma en la que se congelan en líneas de código los sesgos de género de la sociedad, puesto que se consolidan como un medio a través del cual se extiende al campo digital la imperante desigualdad y segregación. En el presente trabajo autodenominamos esta situación como la actual "discriminación 4.0" en donde abordaremos el desafío tecnológico que los sistemas de Inteligencia Artificial tienen que afrontar para no replicar los prejuicios de género existentes en la colectividad. De esta manera, dividimos el tema en dos partes: la primera, se relaciona con La Inteligencia Artificial, sus definiciones, tipos y aplicaciones; y la segunda, viene a tratar el tema de género desde sus definiciones hasta su conjugación con la era digital y los sistemas de Inteligencia Artificial, identific ndo en este último apartado los casos más relevantes y las causas de la discriminación 4.0, para así concluir con una serie de propuestas generales en torno al control y prevención de la desigualdad en dicho espacio digital.

PALABRAS CLAVE: Discriminación, Inteligencia Artificial, Género

ABSTRACT
Currently, the greatest technological commitment has been developed in the field of artificial intelligence. However, its continuous improvement has been bringing various questions about the way in which the gender biases of society are frozen in lines of code, since they are consolidated as a means through which the prevailing field is extended to the digital field inequality and segregation. In the present work we call this situation the current "discrimination 4.0" where we will address the technological challenge that Artificial Intelligence systems have to face in order not to replicate the gender prejudices existing in the community. In this way, we divide the subject into two parts: the first

is related to Artificial Intelligence, its definitions, types and applications; and the second, it deals with the gender issue from its definitions to its conjugation with the digital era and the systems of Artificial Intelligence, identifying in this last section the most relevant cases and the causes of discrimination 4.0, to conclude with a series of general proposals regarding the control and prevention of inequality in said digital space.

KEY WORDS: Discrimination, Artificial Intelligence, Gende

INTRODUCCIÓN

La cuarta revolución industrial trae consigo la transformación y perfeccionamiento de la tecnología que nos rodea. Dicha evolución se encuentra intrinsecamente relacionada con la acumulación creciente de grandes cantidades de datos (big data), al uso de algoritmos para procesarlos y a la interconexión masiva de sistemas y dispositivos digitales. La mayor expresión de dicho avance puede reunirse en un único concepto: La Inteligencia Artificial.

Lo anterior implica un buen grado de automatización y de digitalización que requiere de una transformación caracterizada por una intercomunicación continua e instantánea entre las diferentes estaciones de trabajo que componen las propias cadenas de producción de la industria, así como la completa digitalización de las cadenas de valor a través de la integración de tecnologías de procesamiento de datos, software inteligente y sensores.

Por otro lado, ese mismo desrrollo tecnológico, implica que cada acción que se despliegue conlleve un valor incluyente y no diferenciador, ya que la tecnología ha sido un arma de doble filo que ha conseguido replicar los estereotipos existentes en un escenario nuevo, el escenario digital.

No obstante, la falta de control y responsabilidad social, de las empresas en la Industria de la Tecnología, con la programación discriminatoria que se le ha dado a lo que concebimos como la Inteligencia Artificial, pueden llegar a perpetuar los prejuicios de género existentes en la sociedad. La discriminación 4.0 es la combinación peligrosa de la tecnología con los prejuicios arraigados de una humanidad enferma.

CAPITULO 1. INTELIGENCIA ARTIFICIAL

1.1. Antecedentes y definición

Como lo describe (Rouse, 2017) la inteligencia artificial (Artificial Intelligence, o AI) es la simulación de procesos de inteligencia humana por parte de máquinas, especialmente sistemas informáticos. Estos procesos incluyen el aprendizaje (la adquisición de información y reglas para el uso de la información), el razonamiento

(usando las reglas para llegar a conclusiones aproximadas o definitivas) y la autocorrección. Las aplicaciones particulares de la AI incluyen sistemas expertos, reconocimiento de voz y visión artificial.

El término AI fue acuñado por John McCarthy, un informático estadounidense, en 1956 durante la Conferencia de Dartmouth, donde nació la disciplina. Hoy en día, es un término general que abarca todo, desde la automatización de procesos robóticos hasta la robótica actual. Ha ganado prominencia recientemente debido, en parte, a los grandes volúmenes de datos, o al aumento de velocidad, tamaño y variedad de datos que las empresas están recopilando. AI puede realizar tareas tales como identificar patrones en los datos de manera más eficiente que los seres humanos, lo que permite a las empresas obtener más información sobre sus datos.

No obstante como lo describe (Torra, 2011) existen otras definiciones que no se basan en el comportamiento humano. Son las cuatro siguientes.

1. Actuar como las personas. Esta es la definición de McCarthy, donde el modelo a seguir para la evaluación de los programas corresponde al comportamiento humano. El llamado Test de Turing (1950) también utiliza este punto de vista. El sistema Eliza, un bot (programa software) conversacional es un ejemplo de ello.
2. Razonar como las personas. Lo importante es cómo se realiza el razonamiento y no el resultado de este razonamiento. La propuesta aquí es desarrollar sistemas que razonen del mismo modo que las personas. La ciencia cognitiva utiliza este punto de vista.
3. Razonar racionalmente. En este caso, la definición también se focaliza en el razonamiento, pero aquí se parte de la premisa de que existe una forma racional de razonar. La lógica permite la formalización del razonamiento y se utiliza para este objetivo.
4. Actuar racionalmente. De nuevo el objetivo son los resultados, pero ahora evaluados de forma objetiva. Por ejemplo, el objetivo de un programa en un juego como el ajedrez será ganar. Para cumplir este objetivo es indiferente la forma de calcular el resultado.

De lo anterior es posible afirmar que existen dos tipos de inteligencia artificial.

– Inteligencia artificial débil

Se considera que los ordenadores únicamente pueden simular que razonan, y únicamente pueden actuar de forma inteligente. Las partidarios de la inteligencia artificial débil consideran que no será nunca posible construir ordenadores conscientes, y que un programa es una simulación de un proceso cognitivo pero no un proceso

cognitivo en sí mismo. La AI débil, también conocida como AI estrecha, es un sistema de AI que está diseñado y entrenado para una tarea en particular. Los asistentes personales virtuales, como Siri de Apple, son una forma de débil de AI.

– Inteligencia artificial fuerte

En este caso se considera que un ordenador puede tener una mente y unos estados mentales, y que, por tanto, un día será posible construir uno con todas las capacidades de la mente humana. Este ordenador será capaz de razonar, imaginar, etc. La AI fuerte, también conocida como inteligencia general artificial, es un sistema de AI con habilidades cognitivas humanas generalizadas, de modo que cuando se le presenta una tarea desconocida, tiene suficiente inteligencia para encontrar una solución. La prueba de Turing, desarrollada por el matemático Alan Turing en 1950, es un método utilizado para determinar si una computadora puede realmente pensar como un humano, aunque el método es polémico.

No obstante, Arend Hintze, profesor asistente de biología integradora e ingeniería y ciencias de computación en la Universidad Estatal de Michigan. Categoriza la AI en cuatro tipos, desde el tipo de sistemas de AI que existen hoy en día hasta los sistemas sensitivos, que aún no existen. Sus categorías son las siguientes:

1.2. Tipos de inteligencia artificial

Tabla 1. Tipos de Inteligencia Artificial

Tipo 1: Máquinas reactivas	No tienen la capacidad de formar recuerdos. Tampoco pueden utilizar experiencias pasadas en las que basar las decisiones actuales. Un ejemplo es Deep Blue, el programa de ajedrez de IBM que venció a Garry Kasparov en los años noventa. Deep Blue puede identificar piezas en el tablero de ajedrez y hacer predicciones, pero no tiene memoria y no puede usar experiencias pasadas para informar a las futuras. Analiza movimientos posibles, los propio y los de su oponente y elige el movimiento más estratégico. Deep Blue y AlphaGO de Google fueron diseñados para propósitos estrechos y no pueden aplicarse fácilmente a otra situación.
Tipo 2: Memoria limitada	Estos sistemas de AI pueden usar experiencias pasadas para informar decisiones futuras. Algunas de las funciones de toma de decisiones en vehículos autónomos han sido diseñadas de esta manera. Las observaciones son utilizadas para informar las acciones que ocurren en un futuro no tan lejano, como un coche que ha cambiado de carril. Estas observaciones no se almacenan permanentemente.

Tipo 3: **Teoría de la mente**	Este es un término psicológico. Se refiere a la comprensión de que los demás tienen sus propias creencias, deseos e intenciones que afectan las decisiones que toman. Este tipo de AI aún no existe. Implica la comprensión de que las personas, las criaturas y los objetos en el mundo pueden tener pensamientos y emociones que afectan a su propio comportamiento. Esto es crucial para la forma en que los humanos formamos sociedades, porque nos permite la interacción social. Si las máquinas van a andar entre nosotros, deberán tener una comprensión sobre cómo pensamos y cómo sentimos. Además deberán llegar a saber qué esperamos y cómo queremos que nos traten.
Tipo 4: **Autoconocimiento.**	En esta categoría, los sistemas de AI tienen un sentido de sí mismos, tienen conciencia. Las máquinas con conciencia de sí comprenden su estado actual y pueden usar la información para inferir lo que otros están sintiendo. Este tipo de AI aún no existe. Este es el paso final del desarrollo de la IA es construir sistemas que puedan formar representaciones sobre sí mismos. En última instancia, los investigadores de la IA tendrán que comprender no solo la conciencia, sino también construir máquinas que la tengan. Los seres conscientes son conscientes de sí mismos, conocen sus estados internos y pueden predecir los sentimientos de los demás. Es probable que estemos lejos de crear máquinas que sean conscientes de sí mismas. Sin embargo, los esfuerzos se enfocan hacia la comprensión de la memoria, el aprendizaje y la capacidad de basar las decisiones en experiencias pasadas

Fuente: Arend Hintze citado por (Rouse, 2017)

Elaboración propia

Frente a lo anterior la tecnología a través de una visión ambiciosa ha puesto sus objetivos en que la Inteligencia artificial se materializase en aras de una vida humana mucho mas pacifica, armoniosa y fácil, pero el riesgo es demasiado alto, en cuanto a los escenarios aun no previstos y sus aplicaciones.

1.3. Aplicaciones de AI

- **AI en la asistencia sanitaria.** Las mayores apuestas están en mejorar los resultados de los pacientes y reducir los costos. Las empresas están aplicando el aprendizaje de máquina para hacer diagnósticos mejores y más rápidos que los seres humanos. Una de las tecnologías sanitarias más conocidas es IBM Watson. Entiende el lenguaje natural y es capaz de responder a las preguntas que se le formulan. El sistema extrae datos de los pacientes y otras fuentes de datos disponibles para formar una hipótesis, que luego presenta con un esquema de puntuación de confi nza. Otras aplicaciones de AI incluyen chatbots, un programa de computadora utilizado en línea para responder a preguntas y

ayudar a los clientes, para ayudar a programar citas de seguimiento o ayudar a los pacientes a través del proceso de facturación, así como en asistentes virtuales de salud que proporcionan retroalimentación médica básica.

• **AI en los negocios.** La automatización de procesos robóticos se está aplicando a tareas altamente repetitivas que normalmente realizan los seres humanos. Los algoritmos de aprendizaje automático se están integrando en las plataformas de análisis y CRM para descubrir información sobre cómo servir mejor a los clientes. Los chatbots se han incorporado en los sitios web para ofrecer un servicio inmediato a los clientes.

• **AI en la educación.** La AI puede automatizar la calificación, dando a los educadores más tiempo. AI puede evaluar a los estudiantes y adaptarse a sus necesidades, ayudándoles a trabajar a su propio ritmo. Los tutores de AI pueden proporcionar apoyo adicional a los estudiantes, asegurando que se mantengan en el buen camino. AI podría cambiar dónde y cómo los estudiantes aprenden, tal vez incluso reemplazando a algunos maestros.

• **AI en finanzas**. La AI aplicada a las aplicaciones de finanzas personales, como Mint o Turbo Tax, está transformando a las instituciones financieras. Aplicaciones como estas podrían recopilar datos personales y proporcionar asesoramiento financiero. Otros programas, IBM Watson siendo uno, se han aplicado al proceso de comprar una casa. Hoy en día, el software realiza gran parte de las operaciones en Wall Street.

• **AI en la ley**. El proceso de descubrimiento, a través de la revisión de documentos, en la ley es a menudo abrumador para los seres humanos. Automatizar este proceso es un mejor uso del tiempo y un proceso más eficiente. Las startups también están construyendo asistentes informáticos con preguntas y respuestas que pueden tamizar preguntas programadas para contestar examinando la taxonomía y la ontología asociadas a una base de datos.

• **AI en la fabricación.** Esta es un área que ha estado a la vanguardia de la incorporación de robots en el flujo de trabajo. Los robots industriales solían realizar tareas únicas y estaban separados de los trabajadores humanos, pero a medida que la tecnología avanza eso ha cambiado.

CAPITULO 2. LA PERSPECTIVA DE GÉNERO EN LA INTELIGENCIA ARTIFICIAL

2.1. ¿Qué es género?

El concepto de género es nuevo, no está defini o de manera unánime en todas las disciplinas e instituciones. En contraposición a las diferencias de sexo, el género concierne a las construcciones sociales de las masculinidades y feminidades y a lo que significa ser un hombre y una mujer en el contexto de la sociedad. Desde el punto de vista teórico, la llamada ideología de género se caracteriza por proponer una distinción entre los conceptos de sexo, genero, identidad de género y orientación sexual (Reyes, 2019). En ese sentido, es importante realizar una división conceptual para explicar con exactitud a que se refieren cada uno.

Tabla 2. Ideología de género

IDEOLOGIA DE GÉNERO			
SEXO	**GÉNERO**	**IDENTIDAD DE GÉNERO**	**ORIENTACION SEXUAL**
Se refiere a las características biológicas y fisiológicas que definen a hombres y mujeres.	Son los roles socialmente construidos, los comportamientos, actividades y atributos que una sociedad considera apropiados según el sexo al que pertenezcan.	Es una actitud interna del individuo que le permite identificarse con un género en particular, y lo lleva a actuar externamente de acuerdo con esa propia comprensión.	Se refiere de manera puntual a quien es objeto de atracción sexual para el individuo.

Fuente: Organización Mundial de la Salud Elaboración propia.

Cada sociedad desarrolla los patrones de conducta que espera sean observados por los hombres y las mujeres que la conforman, y que le permiten caracterizar su comportamiento como masculino o femenino. El género es también producto de las relaciones entre las personas y puede reflejar la distribución de poder entre ellas. No es un concepto estático, sino que cambia con el tiempo y del lugar. Cuando las personas o los grupos no se ajustan a las normas (incluidos los conceptos de masculinidad o feminidad), los roles, las responsabilidades o las relaciones relacionadas con el género, suelen ser objeto de estigmatización, exclusión social y discriminación.

De ese modo, alude a la manera como una sociedad considera que los integrantes de cada sexo deben actuar, lo que lleva a que se les asignen determinados roles, a su vez estos parámetros de conducta ponen de presente lo que la comunidad espera sobre la forma como los individuos pertenecientes a un sexo deben comportarse.

2.2. El género en la era digital

El escenario digital se ha configurado como un terreno en el que se ha dado una réplica de la discriminación y de los sesgos de género que siempre han existido en la sociedad. No obstante, todo depende de la perspectiva en la que se mire y el uso que se le dé a las herramientas tecnológicas que se tienen a la mano. Es así como, por un lado, el escenario digital se constituye como una extensión de los sesgos de género, consecuentemente la discriminación imperantes gracias a la comunicación que es de difusión rápida y fácil de la información; y por otro lado, puede constituirse como una herramienta para disminuir la brecha de género gracias a los diferentes colectivos, organizaciones y personalidades activistas que trabajan en pro de difundir mensajes de equidad e igualdad.

En ese orden de ideas, el papel de las plataformas digitales, pero especialmente el de las redes sociales, ha sido relevante en la nueva dinámica social porque han venido a convertirse en un canal de comunicación abierto y sencillo. Pueden tenerse en cuenta los siguientes aspectos:

– Han creado un escenario de interconexión rápida y fácil entre las personas

– Han permitido la creación de grupos y colectivos con un objeto social enfocado en la igualdad de género y la construcción de la equidad.

– Se ha configurado como el canal de comunicación obligatorio entre líderes, activistas, agentes de igualdad y la población en general, permitiendo una mayor efectividad en la recepción del discurso.

– Se configu a como una extensión de la personalidad del ser humano en donde aquel puede interactuar con mayor libertad.

No obstante, también debe resaltarse que la falta de control en el intercambio de datos ha traído como consecuencia la proliferación de la desinformación, la manipulación del discurso y el aumento de las llamadas "*Fake News*". De esta manera, las tecnologías de la información y comunicación se han convertido en un factor importante para ayudar a desarrollar nuevas estrategias en pro de la igualdad real de hombres y mujeres. El solo hecho de tener la oportunidad de interconexión que nos brinda la tecnología contribuye a la construcción de un canal de comunicación efectivo para la difusión de cualquier tipo de información. Así mismo, la posibilidad de tener al alcance, un sinnúmero de datos a través de los buscadores en internet permite que la sociedad se encuentre a un "click" del conocimiento.

2.3. La inteligencia artificial y el sesgo de género

En los últimos años la inteligencia artificial (IA) ganó el centro de la escena tecnológica. Cada día nos sorprendemos con nuevos e ingeniosos mecanismos que imitan la refl xión, el análisis e incluso la creatividad humana y que se encuentran en constante evolución para algún día superar la destreza de nuestro cerebro. Las aplicaciones son incontables, y hay casos tan disruptivos como alentadores. Desde inteligencias que ayudan a prevenir enfermedades, hasta algoritmos que pintan retratos o escriben ensayos académicos. También están en las redes sociales que usamos, en las búsquedas web, o en los procesos de reclutamiento de algunas compañías.

No obstante, dichos modelos de Inteligencia Artificial se encuentran determinados y atravesados por diversos sesgos que reproducen y hasta amplifican relaciones de poder que subyacen en la realidad. Entendido como ese conjunto de suposiciones que efectuamos al momento de comenzar nuestro análisis, el sesgo puede estar en aquellas limitaciones que tiene nuestro algoritmo, en las preguntas que nos hacemos, en los datos que tomamos como set de entrenamiento, en cómo comunicamos el modelo y cómo lo validamos.

Lo que sucede en Inteligencia Artificial es que no intentamos programar a partir de reglas explícitas y conocidas, sino que buscamos explicar determinadas cuestiones a partir de datos o evidencias. Existen algunas técnicas que simplifican esa lógica, con el propósito de ganar poder de generalización, esto es, tratan de aplicar hipótesis a una población nueva, que desconocemos. En dicha simplificación aparecen algunas barreras éticas por encima, discriminando a los individuos por su condición de pertenencia a un grupo que ya estaba discriminado previamente. El riesgo aquí radica en el poder de reproducción que tiene el mundo digital, ya que permite que se masifique un conjunto de reglas discriminatorias e injustas preexistentes: se reproducen y se replican **lógicas** discriminatorias que ya existían en la sociedad. Tal es el caso de lo que ocurre con el sesgo de género.

Existen partidarios que afirman, de manera pesimista, que la Inteligencia Artificial no elimina nuestras limitaciones cognitivas sino que refuerza ciertos aspectos negativos, lo que puede conllevar a tener implicaciones para la igualdad de género. Desde esa perspectiva, puede deducirse que la Inteligencia Artificial tiene el potencial de reducir el sesgo y aumentar la eficiencia de los procesos humanos, pero el problema radica en que esas tecnologías imitan nuestras habilidades y también nuestros defectos.

Es oportuno retroceder un poco en el proceso y pensar en la información base que alimentará a estas plataformas. La Inteligencia Artificial extrae conclusiones a partir de los datos que se le presentan, no obstante, si estos datos tienen, por ejemplo,

estereotipos de género, el software simplemente reproducirá los mismos y perpetuará este sesgo.

2.3.1. Casos de discriminación 4.0

1. Traductor de Google. Es un método asequible y artificial que presume inteligencia, diversas investigaciones demostraron que al escribir frases como "ella es una líder" o "**él** está cocinando", la traducción automática arrojó "**él** es un **líder" y** "ella está cocinando", respectivamente. Varios factores influyeron en dicha traducción sesgada, uno de ellos fue el idioma utilizado, el cual fue del inglés al turco y después volvió al inglés. En ese camino el sistema asoció estereotipadamente ciertos roles a un **género** determinado. Para el traductor, la mujer cocina y el varón lidera.

2. Amazon. El algoritmo de inteligencia artificial utilizado por Amazon para procesar y evaluar los currículums de los solicitantes de empleo e identificar los mejores talentos, producía sesgos sistemáticos en contra de las mujeres. Este es un tipo de algoritmo de aprendizaje automático que se ha venido incorporando en los procesos de reclutamiento de personal de las grandes compañías. Dichos softwares permiten compilar una gran cantidad de datos a una alta velocidad con el fin de mejorar las decisiones de contratación de personal, y en base a los datos recopilados, las plataformas de Inteligencia Artificial tienen la capacidad de detectar los candidatos con alto potencial. En este caso, el algoritmo de Amazon evaluaba a los candidatos a puestos de trabajo observando patrones en los currículums enviados a la compañía durante un período de 10 años. Como la mayor parte de los currículums eran de hombres, resultado de la brecha de género en el sector tecnológico, el mismo penalizaba los que incluían la palabra mujer. Es decir, el algoritmo interpretaba esa distribución desigual no como un resultado de la segregación ocupacional existente en el mercado laboral, sino más bien, como una diferencia en capacidades, discriminando sistemáticamente a las mujeres (El mundo entre nosotras, 2018).

3. Google y anuncios. El algoritmo de Google tendía a mostrar más anuncios de empleos ejecutivos con mayores salarios a los hombres que buscaban trabajo respecto a sus pares mujeres. Estudios realizados en una serie de países desarrollados indican que la forma en la que están escritos los anuncios de empleo importa. El lenguaje utilizado puede contribuir a mantener las brechas de género observadas en el mercado laboral, limitando la participación de las mujeres en sectores de mayor productividad y puestos de liderazgo.

Estos estudios encuentran que cuando palabras como líder, competitivo y dominante son incluidas en los anuncios de empleo las mujeres las asocian con estereotipos masculinos, lo que produce un mayor desinterés en aplicar a estos puestos. Por el contrario, palabras como salario negociable, apoyo, y comprensión se asocian con estereotipos más bien femeninos (Bustelo & Suaya, 2018).

4. Sistemas de reconocimiento facial. Los sistemas de reconocimiento facial que hay disponibles en el mercado se venden como sistemas precisos y neutrales. Pero se hacen pocos esfuerzos para asegurarse de que sean éticos, inclusivos o que respeten los derechos humanos y la igualdad de género, antes de ser utilizados por agencias policiales o corporaciones, lo cual podría tener un impacto negativo en la vida de la gente. Una investigación realizada en la materia, arrojó que los softwares de Inteligencia Artificial de reconocimiento facial utilizados por las compañías *Microsoft, IBM y Face++*, clasificaban correctamente el género de los hombres blancos, pero tenían un mayor grado de error con mujeres y con hombres de tez más oscura.

Actualmente la IA suele utilizar el Aprendizaje Automático con un propósito muy definido. Los datos de entrenamiento son elegidos para ese propósito y se procesan con métodos matemáticos para detectar patrones y desarrollar un modelo que permita hacer predicciones o recomendaciones sobre nuevos datos. Una vez detectados los sesgos, estas grandes compañías han buscado corregir sus algoritmos. Todos los aspectos de nuestras vidas pronto serán transformados por la IA y el aprendizaje automático, a través de innovaciones como los autos que se conducen solos y el reconocimiento facial. Es importante estar consciente de que la tecnología es un fiel reflejo de los sesgos presentes en la sociedad. Durante el diseño de los algoritmos, el quién, el cómo y el para qué, son aspectos relevantes para crear tecnologías inclusivas (El mundo entre nosotras, 2018).

2.3.2. Causas probables de la discriminación 4.0

1. Mayor participación de hombres en el desarrollo de algoritmos base. es muy probable que la enorme participación de hombres, respecto a las mujeres, en el desarrollo de estos algoritmos sea una de las razones por las que los servicios de Inteligencia Artificial conlleven estos sesgos. El hecho de que la computación esté dominada por varones ocasiona que los datos sean creados por informáticos que carecen de un punto de vista feminista. Ante este escenario, la pregunta que surge es qué pasaría en un equipo integrado 100% por mujeres,

¿diseñarían modelos de IA menos discriminatorios? Es muy probable. Antes de sacar a la calle cualquier sistema, el mismo se testea. Y, si bien los más importantes obviamente son los test de validación, antes de llegar a esa instancia los sistemas se prueban internamente entre los mismos integrantes del equipo: "*¿qué película me recomendaría a mí?*" "*¿cómo detecta mi rostro?*". Entonces, si hay más mujeres en el diseño de un modelo de Inteligencia Artificial, sin duda se reducirá la posibilidad de que aparezcan, en el marco del funcionamiento del sistema, lógicas de discriminación de género. Si como programador no se está atento a considerar a las minorías, se pasa por alto la presencia de estos grupos y no se los incluye. En ocasiones, más que una cuestión de pertenecer a un género o a otro, a una determinada raza u a otra, se trata de tener una cierta sensibilidad de las minorías.

2. Existencia de prejuicios de género en el lenguaje. Cuando los sistemas de inteligencia artificia **aprenden un idioma a partir de textos ya existentes se impregnan de los mismos prejuicios raciales y de género incluidos en el lenguaje**. Esto sucede bajo la premisa de que "*las maquinas son el espejo de lo que somos*" (Otero, 2019).
Especialistas **Procesamiento de Lenguaje Natural** -PLN, la rama de la Inteligencia Artificial que estudia el lenguaje- confeccionaron un mapa de relaciones entre palabras a partir de miles de millones de textos. Este ejercicio permitió llevar las palabras a un espacio vectorial y luego medir la distancia entre cualquier par de palabras, insumo muy útil para aplicaciones de *machine learning* que se basan en el lenguaje. Recurriendo a esa red se pueden inducir relaciones como: "Hombre es a Rey, como mujer es a Reina", Este mismo modelo también responde a cosas como:

"Hombre es a **médico**, como mujer es a **enfermera**"
"Hombre es **programador**, como mujer es a **ama de casa**"
"Hombre es a **arquitecto**, como mujer es a **peluquera**"

(7Puentes, 2018)

El espacio de *word embeddings* replicó los estereotipos de género presentes en la sociedad. De manera análoga a lo que nos pasa a nosotros con la 'parcialidad implícita', los modelos de lenguaje inducen las reglas implícitas en el inconsciente social, lo mismo le sucedió a los modelos de lenguaje, quienes inducen las reglas implícitas en el inconsciente social.

2. Estereotipos culturales. Se refiere a la asociación de los roles femeninos y

masculinos con características impuestas que ya existen en el colectivo social pero que se replican en las plataformas de Inteligencia Artificial.

3. Trasmisión de prejuicios a través de las redes sociales. La transmisión de los prejuicios se debe no solo a los programadores de los sistemas sino a los datos con los que se alimentan **y** a **textos procedentes de las redes sociales,** de lo que escribe la gente *on line*.

Grafico 1. Causas de la Discriminación 4.

Fuente: Elaboración propia

CONCLUSIONES

La IA será tan sexista y racista como las sociedades de las que aprende. Si no nos damos cuenta, lo que haremos será diseñar mecanismos que reproduzcan y amplifiquen en el mundo digital las injusticias *at eternum*. La responsabilidad de los que diseñan Inteligencia Artificial es preguntarse si un modelo no está reproduciendo una lógica de poder que queremos cambiar. Deben, entonces, evitar ocultar supuestos discriminatorios bajo la fachada de algoritmos supuestamente justos y honestos (7Puentes, 2018). Así mismo, frente a la problemática expuesta a lo largo del presente trabajo, proponemos que pueden llevarse a cabo las siguientes medidas para la construcción de sistemas más éticos de inteligencia artificial que respeten la equidad de género, la dignidad y los derechos humanos:

– Incentivar el estudio y la participación de las mujeres en el campo de la tecnología y la programación, con el propósito de que trabajen en el desarrollo de sistemas de Inteligencia Artificial (IA), y de esta forma evitar que, los cada vez más habituales sistemas automáticos de toma de decisiones o recomendadores basados en IA repliquen, cuando no amplifiquen, los sesgos de género existentes en la sociedad actual.
– Apoyar las transiciones de las mujeres en sus carreras, con procesos de reclutamiento inclusivos. Un lenguaje que no sea neutral al género en los anuncios de trabajo puede "clasifica " a los solicitantes de empleo antes de que hayan aplicado.
– Aplicar filtros en los datos históricos que se utilizan para entrenar sistemas de IA, para evitar que los mismos pueden reafirmar o incluso aumentar el sesgo existente. Pero no sólo los datos, las decisiones de diseño de los sistemas de IA también pueden conducir a resultados sesgados. Por tanto, es esencial vigilar cómo diseñan y entrenan estos sistemas de aprendizaje automático.
– Exigir un compromiso social responsable por parte de las empresas en la Industria de la Tecnología, o aquellas que se sirvan de este tipo de sistemas, para garantizar que la tecnología de análisis no perjudique a las personas y no extienda la la programación discriminatoria que se le ha dado a lo que concebimos como la Inteligencia Artificial. De la misma forma, a nivel interno, las empresas deben apuntar a la diversidad, a crear equipos diversos entre los creadores de soluciones con IA. Además, de aumentar el control en la programación para que luego de la misma se realice revisión, monitoreo y auditorías. Lo mismo que debería ocurrir en el "mundo real" cuando el ánimo es derribar los sesgos.

La discriminación 4.0 es la combinación peligrosa de la tecnología con los prejuicios arraigados de una humanidad enferma. Pero hay que remarcar que "*la* máquina *solamente aprende lo que el humano le enseña*" (Acámica, 2019) ya que las decisiones de los algoritmos son tan buenas como los datos que utilizan. En esa línea agrega que los programas de IA no son subjetivos por naturaleza, sino que esa mirada deriva del entrenamiento que imparte el humano. Esto quiere decir que si los datos que recibe son sesgados, la IA también lo será. En todo caso y en buena medida, la criatura será tan obtusa o inclusiva como su creador. No obstante, es una buena noticia que dicho sesgo de género sea nuestra culpa, ya que, a diferencia del cerebro humano, los sistemas informáticos son moldeables en el corto plazo. No hay que discutir con la máquina, ni hay necesidad de convencerla de lo que es justo. Es necesario actuar ahora, para que el futuro de la Inteligencia Artificial se incline hacia la justicia y la inclusión.

BIBLIOGRAFIA

Rouse, M. (Abril de 2017). *TechTarget*. From Inteligencia artificial, o AI: https://searchdatacenter.techtarget.com/es/definicion/Inteligencia-artificia o-AI

Torra, V. (Diciembre de 2011). *LYCHNOS*. From Instituto de Investigación en Inteligencia Artificial (CSIC): http://www.fgcsic.es/lychnos/es_ES/articulos/inteligencia_artificia

Reyes Alvarado, Y. (2019). *¿Ideologia o perspectiva de género en la Justicia Transicional?* Bogota : Universidad Externado de Colombia.

Etxebarria Lucia. (2009). *La Eva Futura. La letra futura.* Barcelona, España: Litografia Roses S.A. .

7Puentes. (21 de marzo de 2018). *Discriminación 2.0: Sesgo de género en Inteligencia Artificial*. From 7 Puentes Blog: http://www.7puentes.com/blog/2018/03/21/discriminacion-inteligencia-artificial

El mundo entre nosotras. (10 de novimbre de 2018). *El sesgo de género en la Inteligencia Artificial*. From El mundo entre nosotras: https://elmundoentrenosotras.com/sesgo-genero-la-inteligencia-artificial

Rojon, G. (10 de junio de 2019). *Inteligencia Artificial y sesgos de género*. From El Heraldo de Mexico: https://heraldodemexico.com.mx/opinion/inteligencia-artificial- -sesgos-de-genero/

Otero, L. (2019). *La Inteligencia Artificial es racista y sexista*. From Muy Interesante: https://www.muyinteresante.es/cultura/articulo/la-inteligencia-artificial- s-racista-y-sexista-281492504811

Rojas Rivera, A. (11 de junio de 2019). *Retos de la Igualdad de Género en la Inteligencia Artificial*. From Alcaldes de México: https://www.alcaldesdemexico.com/de-puno-y-letra/retos-de-la-igualdad-de-genero-en-la-inteligencia-artificial

Acámica. (19 de julio de 2019). *Inteligencia artificial y sesgos de género*. From La voz : https://www.lavoz.com.ar/espacio-de-marca/inteligencia-artificial-y-sesgos-de-genero

Bustelo, M., & Suaya, A. (08 de noviembre de 2018). *¿Cómo aprovechar la inteligencia artificial sin perpetuar sesgos de género?* From ¿y si hablamos de igualdad?: https://

blogs.iadb.org/igualdad/es/como-aprovechar-la-inteligencia-artificial-sin-perpetuar-sesgos-de-genero/

INTELIGÊNCIA ARTIFICIAL E DESEMPREGO

Eixo temático: Inteligência Artificia

Autor:
Manuel Martín Pino Estrada
Formado em Direito na Universidade de So Paulo (USP), mestre em Direito pela Universidade Federal do Rio Grande do Sul (UFRGS) e doutorando em Direito pela Faculdade Autônoma de Direito de São Paulo (FADISP). martinpino@yahoo.com

RESUMO
Com o advento da inteligência artificial e dos robôs inteligentes, muitas vagas de trabalho estão sendo extintas, provocando a despedida de muitos trabalhadores, pois os empregadores, ao terem o lucro como atividade-fim, acabam por utilizar softwares inteligentes para cada vez mais ter menos empregados, desta forma, ficam livres de pagamentos de encargos trabalhistas, reuniões sindicais e de muitos tributos que acabam pesando muito nas contas da empresa. Não só as vagas de emprego que estão sumindo, muitas profissões também, inclusive, as empresas que não se adequarem à realidade da Revolução Industrial 4.0 também sumirão do mercado.
Palavras chave: inteligência artificial; robótica; trabalhado .

INTRODUÇÃO

O presente trabalho tem a importância de demonstrar a influência da chegada da quarta revolução industrial ou Revolução Industrial 4.0, ou seja, da inteligência artificial sobre as relações de trabalho, não só na questão da automação de tarefas manuais que antes demandavam muitos trabalhadores para fazê-las, como também no âmbito intelectual, fazendo que profissionais altamente qualificados sejam dispensados, mas não é só isso, a inteligência artificial está provocando o sumiço de muitas profissões, permitindo o surgimento de outras, mas que estas também sumirão rapidamente, surgindo outras novas e assim por diante, demonstrando a necessidade urgente de uma reforma no sistema educacional, pois está comprovado que, o desemprego está cada vez mais sendo provocado pela própria inteligência artificial e por uma robotização das profiss es, muito mais do que a contratação de trabalhadores de países cujos salários são muito baixos, pois até estes já estão sendo substituídos por programas inteligentes e as linhas vindouras irão fundamentar o panorama desta realidade, cada vez mais preocupante, mas tanto do ponto de vista técnico, como também no âmbito jurídico.

CONCEITO DE INTELIGÊNCIA ARTIFICIAL

A inteligência artificial é uma atividade interdisciplinar, pois mistura a ciência da computação com outras ciências, tais como a Psicologia, de onde extrai os conhecimentos sobre a aprendizagem, a consciência, as emoções e interação com o meio ambiente; com a Medicina. A inteligência artific al também é o uso de computadores e equipamentos relacionados para que seja permitida a criação de máquinas que reproduzam ou imitem os comportamentos dos seres humanos. É também a arte de criar máquinas e softwares que exigem inteligência quando executadas por pessoas, consequentemente, é também o estudo de agentes não humanos que percebem percepções do ambiente e executam ações de forma autônoma, independente e autoconsciente, tendo a capacidade de aprender e de se adaptar às mudanças do seu entorno com rapidez, além de evoluir constantemente as suas habilidades, beirando a perfeição, tornando-se uma ferramenta predileta das empresas e até de escritórios de advocacia. A inteligência artificial é a invenção que o homem não deveria haver inventado, isso é baseado nos diversos filmes sobre o tem [309].

A inteligência artificial se localiza na quarta revolução industrial ou "Revolução 4.0", lembrando que a primeira tratou sobre a substituição dos cavalos pela máquina a vapor, a segunda foi a substituição da máquina a vapor pela eletricidade, a terceira tratou da implantação de programas ou *softwares* não inteligentes ou mecânicos, ou seja, só faziam tarefas para as quais foram programados, já a quarta revolução industrial se refere ao advento de *softwares* inteligentes, quer dizer, que pensam, são autônomos, estão adquirindo uma autoconsciência, aprendem e se adaptam rapidamente. Ressalta-se que as revoluções industriais são movimentos empresarialistas que visam o lucro e para isso investem muito em tecnologia, atualmente, o investimento é de bilhões de dólares anuais[310].

A inteligência artificial, ao ser muito dinâmica, chegou ao ponto de se reproduzir sozinha e sem a ajuda de um especialista em Computação ou similar, ou seja, ela cria novas inteligência artificiais mais aperfeiçoadas de forma autônoma e independente sem a ajuda de ninguém, o mesmo acontece com os robôs, quer dizer, nascem robôs mais perfeitos sem a necessidade de alguma interferência humana, isso permite dizer que aquilo que era artificial se tornou natural. Salienta-se que a inteligência artificial evolui constantemente e de forma exponencial, já o ser humano usa o mesmo cérebro de 200 mil anos atrás, ou seja, este é estagnado, não evolui, pois o número de conexões é o mesmo, já as conexões dentro de uma inteligência artificial se multiplicam exponencialmente[311].

---

309 WHITBY, Blay. Inteligência artificial: um guia para iniciantes; tradução de Cláudio Blanc. São Paulo: Madras, 2004, p. 19-21.

310 SCHWAB, Klaus. A quarta revolução industrial. São Paulo: Edipro, 2016, p. 12-16.

311 TEIXEIRA, João de Fernandes. Inteligência artificial: uma odisseia da mente. São Paulo: Paulus, 2009, p. 34-41.

RAZÕES PARA O CRESCIMENTO E INVESTIMENTO

O investimento e o aumento do uso da inteligência artificial se devem a vários fatores, em primeiro lugar, esta permite a substituição de trabalhadores por softwares e robôs inteligentes, que fazem um trabalho muito eficiente e que na maioria dos casos beira a perfeição. Além disso, com ela, as empresas diminuem muito os seus espaços físicos pelo fato de usarem aplicativos inteligentes baixados da internet e no caso do uso de robôs, estes não ocupam muito espaço se se considera o número significativo de trabalhadores que substituem. Salienta-se que as empresas que usam a inteligência artificial, acabam por vender o alugar os galpões ou prédios que antes usavam quando empregavam centenas de funcionários.

Uma outra vantagem da inteligência artificial para as empresas é o fato de ficarem livres de despesas de água e luz e de encargos trabalhistas ao não terem trabalhadores em suas dependências, consequentemente, também ficam com menos tributos para pagar. Importante ressaltar que as empresas que não se adequarem à inteligência artificial vão ser substituídas por aquelas que a usam ou simplesmente vão fali .

Existe um comércio da inteligência artificial, quer dizer, muitas empresas de diversas áreas cada vez mais procuram as de tecnologia, tudo isso para encomendarem e comprarem *softwares* e aplicativos inteligentes que substituam os seus trabalhadores. Esta situação está começando a ser mais comum, pois as empresas perceberam que acabam tendo mais lucro pela produtividade e diminuição de tributos e encargos laborais que conseguem. Na advocacia já começou a procura de escritórios jurídicos por programas que permitam substituir os seus advogados, por exemplo, provocando as respectivas demissões.

Existe uma desvantagem social, que é o aumento do desemprego e que aumentando os tributos não vai resolver, pelo contrário, continuará aumentando. Com a inteligência artificial podem evitar-se as greves, pois as empresas que a usam podem virtualmente operarem sozinhas, inclusive, existem exemplos desta situação espalhados pelo mundo. Infelizmente, os sindicatos de trabalhadores perdem força com a inteligência artificial, especialmente quando nas negociações se discutem questões sobre a não demissão de funcionários[312].

FERRAMENTAS DA INTELIGÊNCIA ARTIFICIAL

A inteligência artificial não age sozinha, pelo contrário, usa várias ferramentas, tais como a internet, que se divide em internet superficial, que representa o 0,15% de toda a rede, a internet profunda, que representa o 99,85% do total e dentro desta,

312 RIFKIN, Jeremy. O Fim dos Empregos: O contínuo Crescimento do Desemprego em Todo o Mundo. 2004, São Paulo: M.Books, p. 140.

encontra-se a internet escura. Junto com a internet como é conhecida, existe a internet das coisas ou também conhecida pela sigla "IoT" (*internet of things*), que trata sobre a comunicam dos aparelhos eletrônicos entre si, só que de forma independente, autônoma e autoconsciente, tanto que o assunto "ética das máquinas" já é estudado. O "big data" é outra ferramenta da inteligência artificial, e é onde os dados de todas as pessoas se encontram e estas as carregam diariamente, salientando que estes dados são usados pelas empresas para fazer marketing e envio de propagandas personalizadas, os bancos o usam para dar créditos aos seus clientes. Finalmente, a inteligência artificial tem a "nuvem" ou "*cloud computing*", que é o lugar onde todos os aplicativos inteligentes se encontram e que podem ser baixados de forma gratuita ou não[313].

IMPACTOS NO DIREITO

A confiança nas máquinas para conseguir resultados positivos já está cada vez mais sendo aceito pelos escritórios de advocacia e que os cursos de Direito já estão preparando os alunos para esta realidade, apesar de que estes lamentem, pois vislumbram um futuro sombrio para a carreira deles. As tecnologias emergentes estão nivelando o campo de jogo entre pequenos e grandes escritórios de advocacia, porém, o número de empregos jurídicos diminuiu. Os programas para resolver problemas legais estão cada vez mais sendo procurados e comprados das empresas de tecnologia, fazendo com que o advogado perca campo de trabalho[314].

A IA pode ser usada na criação de leis, de sentenças e até na criação de jurisprudência cuja experiência foi feita com decisões da Corte Suprema Americana com precisão de até 70% conforme Harry Surden e Aviva Rutkin, pensando-se se os algoritmos seriam mais justos que os magistrados humanos[315].

A IA também foi testa com decisões da Corte Europeia de Direitos Humanos, conforme pesquisa realizada por Nikolas Aletras da College London. Também serve para a criação de políticas públicas e substituir os debates longos nos Poderes Legislativos existentes[316]. Temos os robôs Watson da IBM e de Ross, este último foi contratado por um escritório de advocacia para casos de falência. No Brasil já existe um escritório de

313 BERGMAN, Michael K. The Deep Web: Surfacing Hidden Value, 2001, p. 01. Disponível em http://brightplanet.com/wp-content/uploads/2012/03/12550176481-deepwebwhitepaper1.pdf Acesso em: 20 jun. 2017.

314 PALAZZOLO, Jay. Why Hire a Lawyer? Computers Are Cheaper. In The Wall Street Journal. Disponível em: https://www.wsj.com/articles/SB10001424052702303379204577472633591769336?-cb=logged0.17135589593090117 Acesso em 17 fev. 2017.

315 SURDEN Harry. Predicting the Supreme Court Using Artificial Intelligence. Disponível em <http://concurringopinions.com/archives/2014/10/predicting-the-supreme-court-using-artificial-intelligence.html>. Acesso em: 15 jun. 2017.

316 RUTKIN, Aviva. Law by algorithm: Are computers fairer than humans? Disponível em: <https://www.newscientist.com/article/mg22229735.100-law-by-algorithm-are-computers-fairer-than-humans/>. Acesso em: 21 jun. 2017.

advocacia que ao usar IA demitiu 440 advogados dos 840 que tinha, mesmo assim, conseguiu mais 20% de clientes e com a tendência de demitir mais advogados[317].

Um dos maiores escritórios de advocacia do país tornou-se o primeiro a anunciar publicamente que contratou um advogado robótico para auxiliar casos de falência. O robô, chamado ROSS, foi comercializado como "o primeiro advogado artificialmente inteligente do mundo. A ROSS ingressou nas fileiras do escritório de advocacia BakerHostetler, que emprega cerca de 50 advogados humanos apenas em sua prática de falência. A máquina do AI, a aposta pela tecnologia de Watson de IBM está no sentido de servir como um investigador legal para a firma. Será responsável por peneirar milhares de documentos legais para reforçar os casos da empresa. Esses trabalhos de pesquisador legal são normalmente preenchidos por advogados fora da escola no início de suas carreiras.

NAS DEMAIS PROFISSÕES

Na agricultura (tratores sem motorista, colheitadeiras mecânicas, substituindo os peões de roça, fábricas-fazenda) e até os tosquiadores de ovelha. Nas fábricas de automóveis, nas indústrias têxteis, no setor de telemarketing. No setor bancário, que começou com a implantação dos caixas eletrônicos e agora temos vários aplicativos inteligentes no internet banking. Entregadores de pizza, os pedreiros (impressoras em 3D gigantes), zeladores, motoristas de táxi, de metrô, de caminhões, de trens. As empresas que não se adequarem à IA vão falir e vão ser adquiridas pelas que a usam[318].

Na agricultura

Os grandes avanços tecnológicos não são normalmente associados à agricultura. Quase a metade das pessoas no mundo ainda lavra a terra, porém, os avanços tecnológicos estão ameaçando acabar com a agricultura tradicional, levando-a a um mundo sem agricultores, provocando consequências negativas para 2,4 bilhões de agricultores que dependem da terra para sobreviverem[319]. Tudo isso devido à mecanização da agricultura, que começou há mais de cem anos. Em 1880, eram necessários mais de 20 homens/hora para colher um acre de trigo. Em 1916, o número

317 VASCONCELLOS, De Marcos e CARDOSO, Maurício. Com robôs, escritório atua em mais de 360 mil processos com 420 advogados. Disponível em: http://www.conjur.com.br/2016-mar-05/robos-escritorio-atua-360-mil-processos-420-advogados?utm_source=dlvr.it&utm_medium=facebook Acesso em 17 jun. 2017.

318 LIEMT, Gijsbert van. Industry on the Move: Causes and Consequences of International Relocation in the Manufacturing Industry. Genebra: International Labor Office 1992, p. 76; "Labor Management Bargaining in 1992", Monthly Labor Review, janeiro de 1993.

319 FAO – Food and Agriculture Organization. Country tables: basic data on the agriculture sector. Roma: 1993, p. 332.

de homens/hora foi reduzido para 12,7. Vinte anos depois, só 6,1 homens/hora eram necessários[320]. Os ganhos de produtividade na agricultura têm sido tão fortes que, ao final da década de 20, a instabilidade econômica não era mais alimentada pela quebra de safras, mas, sim, pela superprodução. A mecanização na agricultura foi anunciada como um triunfo da sociedade industrial.

Nas fábricas

Desde o início da Revolução Industrial, máquinas e formas inanimadas de energia têm sido usadas para impulsionar a produção e reduzir a quantidade de mão-de-obra necessária para fabricar um produto. Já no início da década de 1880, fabricantes como a American Tobacco Company, Quaker Oats, Pillsbury, Diamond Match, Campbell Soup, Procter & Gambler, H.J. Heinz e Eastman Kodak começaram a fazer experiências com máquinas de "processo contínuo" na industrialização. Essas máquinas exigiam pouca atenção humana e produziam quantidades maciças de produtos, mais ou menos automaticamente. Os operários apenas as alimentavam com materiais e deixavam o equipamento moldar e embalar o produto.

Em 1881, James Bonsack patenteou uma máquina que enrolava automaticamente os cigarros, sem qualquer mão-de-obra humana, a máquina "arrastrava o fuma para a fita sem fim, comprimia-o dando lhe forma arredondava, embalava-o com o papel, levava-o a um tudo de cobertura, que moldava o cigarro, colava o papel e cortava o bastão resultante no comprimento desejado". Ao final da década de 1880, a máquina de processo contínuo produzia 120 mil cigarros por dia. A maioria dos operários especializados conseguia fazer no máximo 3000 cigarros por dia. Tão produtivo era o novo equipamento que menos de 30 máquinas conseguiam atender toda a demanda nacional de cigarros em 1885, usando apenas alguns operários[321].

Na siderurgia

Enquanto a indústria automotiva global está rapidamente aplicando a reengenharia às suas operações e investindo em novas tecnologias da informação, as quais resultam na redução da mão-de-obra, setores relacionados estão fazendo a mesma coisa, eliminando, com isso, cada vez mais empregos no processo. O destino das indústrias siderúrgicas está tão intimamente ligado ao da indústria automotiva, que não é de surpreender ver as mesmas mudanças devastadoras na organização e

320 U.S. Department of Agriculture. Technology on the farm. Washington, D.C: 1940, p. 63.

321 CHANDLERS. Alfred Dr. The visible hund: the managerial revolution in american business. Cambridge, MA: Harvard University Press, 1977, p. 249-51.

produção ocorrendo no aço como estão ocorrendo nos negócios de automóveis. A indústria do aço é o coração e a alma do poder industrial.

A usina computadorizada é da Nippon Steel, que, juntamente com outros fabricantes japoneses de aço como Kawasaki, Sumitomo e Kobe abriu fábricas nos Estados Unidos, algumas em sociedade com siderúrgicas americanas. As novas usinas de alta tecnologia transformaram com êxito a fabricação do aço de um processo em lote para uma operação contínua altamente automatizada, tudo por meio da combinação de procedimentos antes separados em uma operação única, semelhante à produção de rolos em uma fábrica de papel[322]. A usina de laminação a frio de 400 milhões de dólares da Nippon, próxima a Gary, Indiana, que é uma *joint-venture* com a Inland Still é operada por uma pequena equipe de técnicos, reduzindo o tempo de produção de 12 dias para uma hora. Na fábrica automatizada, a direção da Inland conseguiu reduzir significativamente sua força de trabalho, fechando duas usinas mais velhas e demitindo centenas de operários[323].

Na indústria eletrônica

O aumento do desemprego nesta área também é preocupante devido aos avanços tecnológicos. A General Electric, líder mundial na fabricação de produtos eletrônicos reduziu seu número de trabalhadores em todo o mundo de 400 mil em 1981 para menos de 230 mil em 1993, mesmo assim, conseguiu triplicar as suas vendas ao mesmo tempo. Esta empresa enxugou a sua hierarquia gerencial nos anos 80 e começou a introduzir novos equipamentos de automação na fábrica[324]. Na indústria de utilidades domésticas, novos equipamentos de alta tecnologia, inclusive de desenho assistido por computador, sistemas de engenharia e fabricação, robôs, esteiras e sistemas de transporte automatizados, estão aumentando a produtividade e eliminando empregos em cada estágio do processo de produção. Entre 1973 e 1991, a produção da indústria de utilidades domésticas nos Estados Unidos aumentou a uma taxa anual de 0,5%. No mesmo período, a produção por trabalhador/hora aumentou a uma taxa média de 2,7%[325].

Na indústria têxtil

322 Idem.

323 REICH, Robert. The Work of Nations: Preparing Ourselves for the 21st Century Capitalism. Nova Iorque: Vintage Books, 1992, p. 214-215.

324 NEW YORK TIMES. "Strong Companies Are Joining Trends to Eliminate Jobs". 26 de julho de 1993, p. D3; "Jobs in America", Fortune, 12 de julho de 1993, p. 40.

325 Technology and Labor in Copper Ore Mining, Household Appliances and Water Transportaion Industries. Washington, D.C.: U.S. Department of Labor, Bureau of Labor Statistics, maio de 1993, Boletim 2420, p. 22.

Há mais de 200 anos, as primeiras máquinas movidas a vapor foram utilizadas na Inglaterra na fiação de lã, provocando uma revolução no modo como os bens eram produzidos. Nos anos 90, enquanto outras indústrias tinham se adiantado na corrida da automação, os têxteis ficaram para trás, em grande parte como consequência do uso intensivo de mão-de-obra no processo de costura. Algumas empresas, como a Allied Textille Co., a Parkland Textile Co. e a Courtaulds, da Inglaterra, começaram a introduzir a robotização em seus processos industriais. O desenho assistido por computador reduziu de semanas para minutos o tempo de desenho de um traje. A tintura computadorizada e os sistemas de acabamento também têm sido introduzidos. Sistemas computadorizados também dinamizando a armazenagem, o manuseio, a embalagem e o embarque das roupas[326].

Na prestação de serviços

Durante muito tempo, o setor de serviços absorveu as perdas de empregos nas indústrias. Até algum tempo atrás, a maioria dos economistas e líderes empresariais acreditava que essa tendência continuaria. Porém, suas esperanças foram sendo refreadas, à medida que as tecnologias da informação começaram a invadir o próprio setor de serviços, aumentando a produtividade e tomando o lugar da mão-de-obra em todos os setores de prestação de serviços. Os avanços tecnológicos atualmente são tão rápidos que as empresas podem demitir muito mais trabalhadores do que precisam contratar para implementar a tecnologia ou sustentar a expansão das vendas[327]. Em fevereiro de 1994, o Wall Street Journal publicava um artigo de primeira página, alertando que uma transição histórica está ocorrendo no setor de serviços, com números crescentes de trabalhadores sendo permanentemente substituídos pelas novas tecnologias da informação, enquanto a produção havia aumentado consideravelmente.

Computadores capazes de compreender a fala, ler textos manuscritos e executar tarefas anteriormente desempenhadas por seres humanos prenunciam uma nova era na qual as indústrias de serviços, a exemplo das indústrias de manufatura, estarão cada vez mais sob o domínio da automação. A exemplo das indústrias de manufatura, estarão cada vez mais sob o domínio da automação. A informatização e a automação do setor de serviços começaram há poucos anos, mas seus efeitos profundos já se fazem sentir na economia, impactando tanto a produtividade como o emprego. O economista Stephen Roach, da Morgan Stanley, afirma que "o setor de serviços perdeu

326 New Technologies, Employment Shifts, and Gender Divisions Within the Textile Industry", New Technology, Work and Employment, primavera de 1991, p. 44.

327 WALL STREET JOURNAL. "Retooling Lives: Technological Gains Are Cutting Costs and Jobs in Services", 24 de fevereiro de 1994, p. A1.

seu papel como máquina desenfreada de geração de empregos" e alerta que ainda não surgiram quaisquer novos setores para substitui-la[328].

Nos bancários

Caixas automáticos, antes uma raridade, tornaram-se presença obrigatória em cidades e subúrbios dos Estados Unidos, reduzindo significativamente o número de caixas humanos. As máquinas reduzem os tempos de transação, estão disponíveis 24 horas por dia e operam a uma fração do custo de caixas humanos. "Um caixa humano pode realizar até 200 transações por dia, trabalho 30 horas semanais, ganha um salário de 8 mil e 20 dólares anuais, mais benefícios, tem intervalo para o café, férias e licença médica, dentre outras benesses. Em contraste, um caixa automático pode fazer 2 mil transações diárias, trabalhar 168 horas semanais, sua operação custa aproximadamente 22 mil dólares anuais e não interrompe o serviço para tomar café ou tirar férias[329]. Entre 1983, os bancos eliminaram 179 mil caixas humanos, ou seja, 37% de sua força de trabalho, substituindo-os por caixas automáticos. Por volta do ano 2000, mais de 90% dos clientes de bancos usaram caixas automáticos[330].

CONSIDERAÇÕES FINAIS

O mundo está num momento de transição e como tal, está sendo dolorosa, pois a quarta revolução industrial está sendo mais rápida que as outras três revoluções industriais juntas, pois todo trabalho pode ser substituído pela inteligência artificial, dando um grande impulso na produtividade das empresas e consequentemente dos países, mas as consequências trabalhistas terão um forte impacto negativo, especificamente nos trabalhos menos qualificados e é neste setor onde haverá também uma estagnação e até uma diminuição dos salários.

O desemprego já está se tornando num negócio muito lucrativo, porque as empresas em todas as áreas, inclusive os escritórios de advocacia começaram a procurar aquelas que criam softwares e robôs inteligentes para poder substituir trabalhadores em vários setores, tais como na Agronomia, no setor bancário, fábricas de automóveis, pedreiros, arquitetos, contadores, taxistas, entregadores de pizza e até advogados,

---

328 Entrevista em 15 de março de 1994. Stephen Roach disse: "Na década de 1970, quando foi debatido o Estado da era pós – industrial, o mito era o de que o setor de serviços... preencheria o vácuo deixado pelo *downsizing* e pelo encolhimento do setor industrial". Segundo Roach, "isso pareceu funcionar até percebermos que os setores de serviços não eram muito produtivos na forma que usavam seus funcionários."

329 LEONTIEF, Wassily e DUCHIN, Faye. The Future Impact of Automation on Workers. Nova Iorque: Oxford University Press, 1986, p. 84.

330 "Retooling Lives", p. A7; Vision 2000, p. 43.

pois o empregador, se puder, substituirias os seus empregados por um só software que faça tudo que ele quiser, sem reclamar, trabalhando as 24 horas por dias, os 365 dias por semana e sem ter que pagar direitos trabalhistas, é o grande sonho dele, que está prestes a se concretizar de forma plena.

REFERÊNCIAS BIBLIOGRÁFICAS

BERGMAN, Michael K. The Deep Web: Surfacing Hidden Value, 2001, p. 01. Disponível em http://brightplanet.com/wp-content/uploads/2012/03/12550176481-deepwebwhitepaper1.pdf Acesso em: 20 jun. 2017.

CHANDLERS. Alfred Dr. The visible hund: the managerial revolution in american business. Cambridge, MA: Harvard University Press, 1977.

FAO – Food and Agriculture Organization. Country tables: basic data on the agriculture sector. Roma: 1993.

LIEMT, Gijsbert van. Industry on the Move: Causes and Consequences of International Relocation in the Manufacturing Industry. Genebra: International Labor Office 1992, p. 76; "Labor Management Bargaining in 1992", Monthly Labor Review, janeiro de 1993.

New Technologies, Employment Shifts, and Gender Divisions Within the Textile Industry", New Technology, Work and Employment, primavera de 1991.

NEW YORK TIMES. "Strong Companies Are Joining Trends to Eliminate Jobs". 26 de julho de 1993, p. D3; "Jobs in America", Fortune, 12 de julho de 1993.

PALAZZOLO, Jay. Why Hire a Lawyer? Computers Are Cheaper. In The Wall Street Journal. Disponível em: https://www.wsj.com/articles/SB10001424052702303379204577472633591769336?cb=logged0.17135589593090117

REICH, Robert. The Work of Nations: Preparing Ourselves for the 21st Century Capitalism. Nova Iorque: Vintage Books, 1992.

RIFKIN, Jeremy. O Fim dos Empregos: O contínuo Crescimento do Desemprego em Todo o Mundo. 2004, São Paulo: M.Books.

RUTKIN, Aviva. Law by algorithm: Are computers fairer than humans? Disponível em: <https://www.newscientist.com/article/mg22229735.100-law-by-algorithm-are-computers-fairer-than-humans/>. Acesso em: 21 jun. 2017.

SCHWAB, Klaus. A quarta revolução industrial. São Paulo: Edipro, 2016.

SURDEN Harry. Predicting the Supreme Court Using Artificial Intelligence. Disponí-

vel em <http://concurringopinions.com/archives/2014/10/predicting-the-supreme--court-using-artificial-intelligence.html>. cesso em: 15 jun. 2017.

Technology and Labor in Copper Ore Mining, Household Appliances and Water Transportaion Industries. Washington, D.C.: U.S. Department of Labor, Bureau of Labor Statistics, maio de 1993, Boletim 2420.

TEIXEIRA, João de Fernandes. Inteligência artificial: uma odisseia da mente. São Paulo: Paulus, 2009.

U.S. Department of Agriculture. Technology on the farm. Washington, D.C: 1940

VASCONCELLOS, De Marcos e CARDOSO, Maurício. Com robôs, escritório atua em mais de 360 mil processos com 420 advogados. Disponível em: http://www.conjur.com.br/2016-mar-05/robos-escritorio-atua-360-mil-processos-420-advogados?utm_source=dlvr.it&utm_medium=facebook Acesso em 17 fev. 2017.

WALL STREET JOURNAL. "Retooling Lives: Technological Gains Are Cutting Costs and Jobs in Services", 24 de fevereiro de 1994.

WHITBY, Blay. Inteligência artificial: um guia para iniciantes; tradução de Cláudio Blanc. São Paulo: Madras, 2004.

INTELIGENCIA ARTIFICIAL Y DERECHO

Eje Temático: Inteligencia artificia

Autor:
Antonio Martino
Profesor emérito de la Universidades de Pisa (Italia) y Salvador (Argentina)

Homo sum, humani nihil a me alienum puto
Pablo Terencio Africano
Unamuno
Homo sum; nihil humani a me alienum puto dijo el cómico latino. Y yo diría más bien, ***nullum hominem a me alienum puto***; soy hombre, a ningún otro hombre estimo extraño. Porque el adjetivo *humanus* me es tan sospechoso como su sustantivo abstracto *humanitas*, la humanidad. Ni lo humano ni la humanidad, ni el adjetivo simple ni el sustantivado, sino el sustantivo concreto: el hombre.

1. HUMANOS, MAQUINAS, DERECHO

John McCarthy en 1956, en una conferencia organizada junto a Marvin Minsky, Nat Rochester y Claude Shannon, bautizó su campo de estudio como «inteligencia artificial» (IA), La conferencia fue financiada por la Fundación Rockefeller y se llamó *Dartmouth Summer Research Project on Artificial Intelligence*. Desde ese momento comienza una extraña aventura en el mundo del conocimiento pues se trata de hacer realizar a maquinas computadoras acciones que son típicas de los seres humanos como pasar de un juico a otro a través de un razonamiento aunque sea simple como un modus pones (p y q; p, luego q).

En 1958 McCarthy y sus colaboradores en el Instituto Tecnológico de Massachusetts crearon LISP, considerado por algunos el segundo lenguaje de programación de alto nivel. Se realizan algunas experiencias como la de Joseph

Weizembaum, quien desarrolla el programa Eliza, considerado el primer sistema dentro del campo del Procesamiento del Lenguaje Natural, en los años 60. El programa es simple y consta en introducir preguntas inesperadas o realizar preguntas con la misma frase del interviniente. Lo curioso es que viene considerado un psicólogo automático y mucha gente lo usa como analista. Weizembaun se ve obligado a escribir que se trata solo de un ejercicio y que jamás pensó que podría servir para analizar a nadie, lo que provoca la ira de su secretaria escribiendo que no es verdad, que Eliza es un verdadero analista y que ella misma hacer años se analiza con Elisa.

Las pruebas siguen pero entre especialistas y no trascienden al público en general. Comienzan las primeras pruebas en ciencias aplicativas como la medicina y aparece el sistema experto MYCIN, que servía para detectar enfermedades y que es el primer sistema experto con reglas. Allí fue que en los años 80 nos lanzamos sobre esas experiencias a lograr resultados en el campo jurídico sostenidos por los éxitos de El Taxman II de McCarty y Sridharan Desarrollado en la Rutgers University, prototipo de investigación, que provee una estructura idónea para la representación de los conceptos jurídicos y una metodología para relacionarlos. Y El Sistema de la Rank Corporation L.D.S de Waterman y Paterson Asiste a los expertos del derecho en la actividad de decisión de casos de responsabilidad por daños derivados de productos, calculando la responsabilidad de lo convenido, el valor de la causa, y un importe equitativo por la liquidación. Se basa sobre reglas hipotéticas.

Desde la época en que realizábamos sistemas expertos para el derecho SRL Sistema di Ragionamento Legale, Carlos Alchourrón, Antonio Martino in *Theoria*, Año III°, Segunda época, Curso 1987/88, n° 7-8. Seccion IV°: Sistemas expertos para el procesamiento de la información jurídica, muchas cosas han cambiado en el horizonte.

En primer lugar un desarrollo vigoroso – sobre todo en los últimos años – de la Inteligencia Artificial. Y como de costumbre esto ha llevado a exaltaciones por las cuales se piensa que todo está resuelto y aun mas, que los algoritmos van a manejar nuestra sociedad. Esta última afirmación pertenece a Yuval Noah Harari profesor de historia más bien ignorante de todo lo que se refiera a informatica e I.A [331]

Otros suponen que casi todo es una gran mentira y no creen en ningún desarrollo serio.

Ni lo uno, ni lo otro.

---

331 Yuval Noah Harari 21 lecciones para el siglo XXI, Editorial: Penguin Random House Grupo Editorial España 2018

Hay un notable desarrollo de la I.A en varios campos, incluyendo el jurídico y esto nos interesa para una Informatica Judicial eficiente

Siempre que aparece algo nuevo hay un miedo que lo acompaña y que se traduce en historias y fantasías sobre los acontecimientos: la aparición de robots para muchas tareas que antes realizaban los humanos ha despertado una serie de prejuicios y de exageraciones de robots que nos dominan y deciden nuestro futuro.

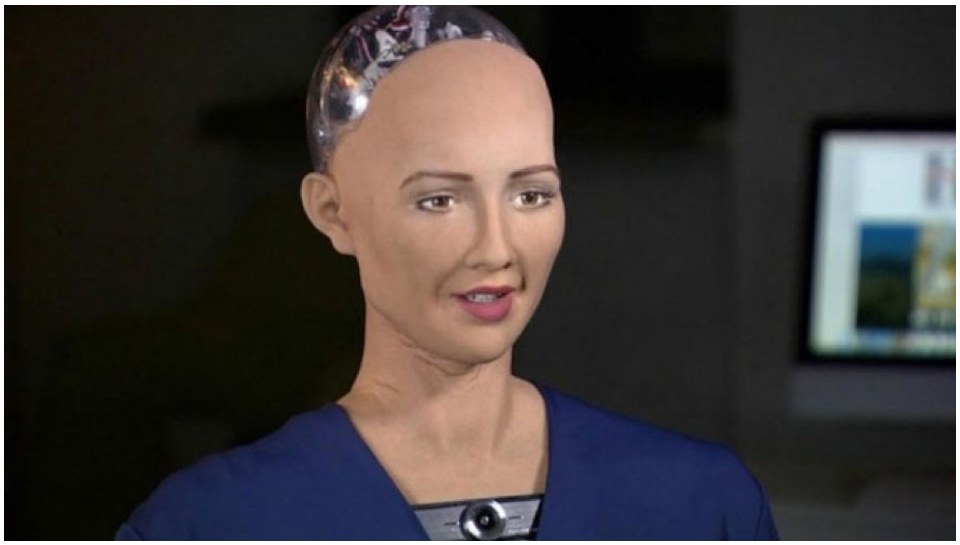
Podemos afirmar que la robótica no supera el 7 % de lo que se trabaja en Inteligencia artificial y que no obstante su desarrollo estamos muy lejos de semejante situación.

Hay avances notables como Gita y Kilo, los robots transportadores, o Cocotto, un robot niñera, Magnus, el robot para adultos mayores, Yumi el robot que dirige orquestas y E2-DR, el robot rescatista. Pero estamos lejos de robots que examinan un contexto real, estraen datos, formulan hipótesis de comportamiento futuro, con cálculo de consecuencias y actúan.

Es cierto que hay programas (no robots) que pueden conducir un automóvil en el tránsito y que últimamente han tenido accidentes. Por esa razón sus desarrolladores les están enseñando el dilema del tranvía (que es un dilema moral). No es necesario pensar que el programa asume una actitud moral, basta con que aprenda a distinguir magnitudes de daños y si tiene que atropellar a un anciano o a un perro, tenga elementos como para elegir este último.

2. Sophia, un robot, con cara humana y que puede expresar sensaciones y emociones. Su creador David Hanson, ha logrado un impacto de marketing extraordinario: Arabia Saudita le ha otorgado la ciudadanía.

El **periodista Charlie Rose haya entrevistado en su icónico show "60 Minutos", e**n el aire desde el año 1968 le hizo una entrevista muy cargada de ironía, pero la ironia la puso Sophia. Luego Rose reconoció que la mayor parte de las preguntas habían sido concordadas "pero que hubo espacio para la improvisación."



David Hanson, el creador de Sophia, cree que si la tecnología de inteligencia artificial se ve y suena humana la gente estará más dispuesta a entablar relaciones cercanas con máquinas. «Creo que es esencial que al menos algunos de los robots sean lo más parecidos a los humanos para que estemos inspirados a relacionarnos con ellos de la misma manera que con otras personas». Podría pensarse que Hanson es un cínico alocado, si no se tiene en cuenta que es el dueño de una empresa que crea estos aparatos con gran éxito. Y no le falta razón cuando sostiene que tal vez puedan servir para personas que de otra manera estarían socialmente asiladas, como aquellos miembros de la tercera edad.

Su compañía, Hanson Robotics está basada en Hong Kong y ya lleva creados más de veinte robots humanoides, habiendo desarrollado piel artificial que simula la carne humana. **Sophia es su último diseño, inspirado en Audrey Hepburn y la esposa de Hanson.**

"Sophia significa sabiduría y se espera que el robot evolucione eventualmente hasta alcanzar el nivel de conocimiento de un humano e incluso superarlo" Esta afirmación es de un vendedor de aparatos domésticos sin responsabilidad con lo que dice.

Llama a sus creaturas "humanoides" porque tienen piel parecida a la humana y hacen razonamientos básicos con capacidad para conseguir muchos datos. De "humanos tienen muy poco, salvo el aspecto exterior y ni vale la pena en preguntarse sobre la "autoconciencia" de Sophia como para haber obtenido la ciudadanía. Ignoramos la razón por la cual el gobierno de Arabia Saudita la otorgo.

2. UNA HISTORIA PARCIAL DE LA I.A EN DERECHO

Me voy a permitir contarla desde el ángulo privilegiado pero singular de mi cargo como Director del IDG del Consejo Nacional de Investigaciones italiano (hoy ITIIG, ver www.itig.cnr.it). Desde mi nombramiento en 1982 dediqué a aplicar las teorías lógicas del derecho, en particular las de G H von Wrigt a los primeros experimentos por obtener un demostrador de problemas jurídicos.

Había un problema teórico no menor: y es el hecho que a partir de Aristóteles[332] se sostenía que la lógica se "aplicaba a los enunciados susceptibles de ser verdaderos o falsos, que había otros enunciados como rezar y dar órdenes que serían tratados en la Retórica y en la Poética". Con Carlos Alchourrón cortamos el nudo gordiano sosteniendo la segunda parte del dilema de Jorgensen o sea que el derecho tenía una lógica pero ella iba más allá (o más acá) de la verdad. De hecho sostuvimos la tesis de la lógica totalmente sintáctica en Lógica sin verdad[333]. Es decir salimos a resolver un

332 De la expresión, capítulo 4, 12 b
333 *Theoria*, Año III°, Curso 1987/88.

problema de la lógica jurídica y terminamos resolviendo un problema de la lógica: es sintáctica, antes de la semántica, por lo tanto nada tiene que ver con verdad y falsedad.

Y el mismo año en la misma Revista publique el trabajo sobre *Sistemas expertos legales*[334].

El tema venia discutiéndose desde dos ángulos diferentes: el lógico, con trabajos de Kovalski y el jurídico, con mis aportes y los más teóricos de Layman Allen. Sucedía que a partir de 1981 inauguramos un Congreso internacional con realización cuadrienal (1981, 1985, 1989 y 1993) con el discutible título por falta de conjunción final Lógica, Informatica, Diritto, en la ciudad de Florencia, sede del Instituto antes nombrado.

De estos congresos fueron publicados compilado por Costantino Ciampi *Artificial Intelligence and Legal Information Systems*,[335] compilado por Antonio A. Martino *Deontic Logic, Computational Linguistics and Legal Information Systems. Volume II*[o336] cuatro años mas tarde, siempre compilado por Antonio A. Martino *Automated Analysis of Legal Texts. Logic, Informatics, Law*.[337] Y 4 años más tarde *Expert System in Law*, [338] siempre compilado por Antonio A. Martino.

334 *Theoria*, Año III°, Segunda época, Curso 1987/88, n° 7-8. Sección IV°: Sistemas expertos para el procesamiento de la información jurídica.

335 North Holland, Amsterdam-New York, 1982, Vol. I, 476 pp.

336 North Holland, Amsterdam-New York, 1982, Vol. II, 466 pp.

337 North Holland, Amsterdam-New York, 1986, 766 pp. North

338 Holland, Amsterdam-New York- Tokio, 1992. 522 pp.

En estos textos se puede seguir la evolución de toda la informática jurídica pero en particular de la I.A. Aplicada al derecho. La revista "Informatica e Diritto" publicada por el Instituto de Documentación Juridica del CNR, italiano publicaba en 1982 *Actas de las jornadas mediterráneas de lógica e informática jurídica, c*on un capítulo especial dedicado a la relación Derecho I. A. y en 1990 el libro Logica, informatica, diritto. Dall'informatica giuridica alle nuove tecniche legislative escrito por Antonio A. Martino y Antonio Chiti[339].

3. TÉCNICAS Y METEDOLOGÍAS QUE SE HAN VENIDO UTILIZANDO: SISTEMAS EXPERTOS, RAZONAMIENTOS BASADOS EN CASOS

A los programas de sistemas expertos que desarrollábamos en los años pasados han sub entrado productos nuevos como Watson.

Nosotros tratamos de usarla para SRL pero fue un fracaso. Hasta que dimos con Alain Colmerauer, uno de los creadores, de Prolog en un congreso. Le comentamos nuestra desazón y riéndose nos dijo que efectivamente no tenía una regla de deducción pero los que comercializaban el producto lo pusieron así y no se podía cambiar ahora.

Téngase en cuenta que en los sistemas expertos trabajábamos de arriba hacia abajo partiendo de un conjunto de enunciados preparados para ser leídos por la máquina y una regla de derivación completa con cadenas justificativas y predictivas

Actualmente se trabaja de otra manera: de abajo para arriba *Botton up* y por eso aparecen programas complejos como Watson que al decir de la Basr Association norteamericana ya sustituye a los pasantes en los estudios jurídicos grandes, con la idea que en un par de años puedan sustituirlos para los trabajos más fatigosos, con la ventaja de no dormir, no mirar el celular y no recibir mensajes de la novia.

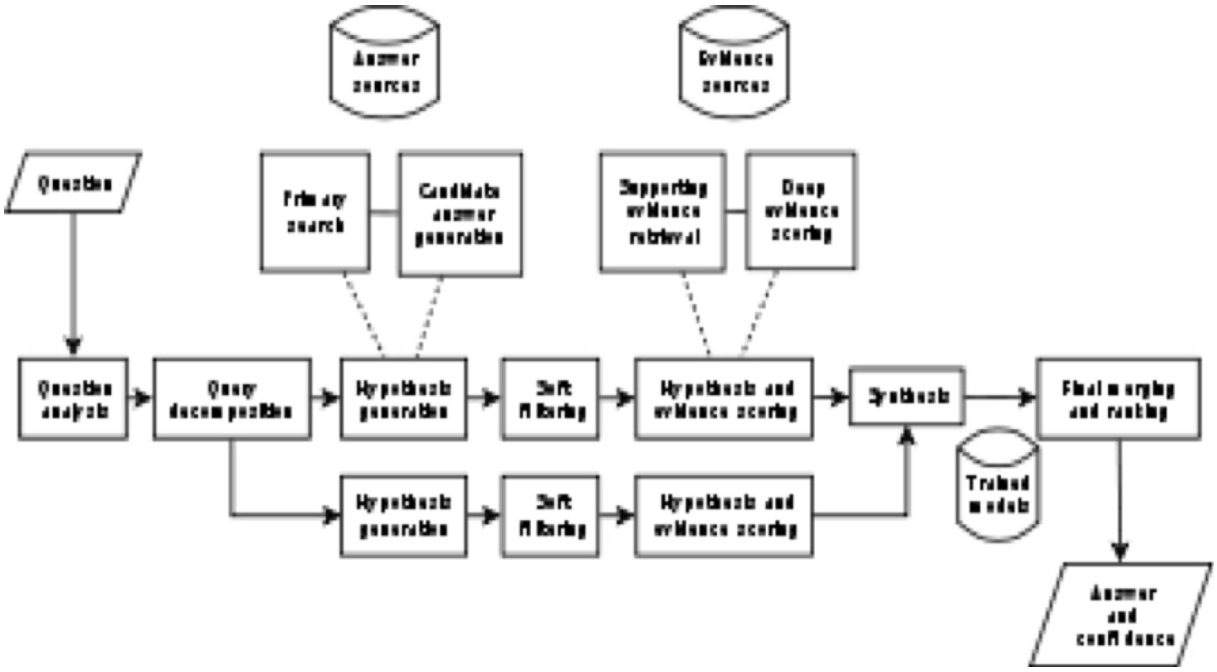
Son conocidas las hazañas de Blu deep al ganarle a Kasparof al ajedrez, pero actualmente ha aparecido un nuevo sistema AlphaZero, que no aprendió de ningún ajedrecista sino que se dedicó a aprender por su cuenta las reglas y las formas de jugar miembros de DeepMind, los "resultados demuestran que un algoritmo de aprendizaje por refuerzo y de propósito general puede aprender desde cero y alcanzar un rendimiento sobrehumano en varios juegos de gran complejidad".

Hay sectores que se han desarrollado más que otros, en este campo y desde un punto de vista comercial de mayor llegada son el de seguros y el bancario. Philips, el coloso holandés, que opera en el sector del mundo sanitario es el primer ejemplo de una sociedad en grado de crear un nuevo negocio de ecosistemas basados en I.A. Aon Benfield, la sociedad de Pensamiento del sector sanitario ha hecho partir los programas y el éxito deriva de la capacidad para dar un significado a contestos complejos. Philips el

339 Lynn Margulis y Dorion Sagan ¿Qué es la vida? Metatemas, Tusquest Editores, Barcelona, tercera edición, 2009.

coloso holandés que opera en el sector sanitario es el primer ejemplo de una sociedad global capaz de crear un nuevo *bussines* de ecosistemas basados en la IA conectando.

Aon Benfiel , la sociedad de reaseguros ha desarrollado una plataforma de I.A. en Inglaterra que saca provecho de la tecnología cluoid para gestionar uno de los productos de pensiones más complejo y con garantías financiarías integradas: rentas vitalicias variables.



Hay un software muy desarrollado **Ross** que es capaz de escuchar el lenguaje humano, rastrear más de 10 mil páginas por segundo y formular una respuesta mucho más rápido que cualquier abogado humano.

Las respuestas de Ross incluyen citas legales, sugieren más artículos para estudiar e incluso calculan una tasa de confianza para ayudar a los abogados a preparar los casos. Además, por tratarse de una inteligencia artificial (IA), mientras más consultas recibe, más aprende, y su eficacia aumenta. oss aprende de su interacción con humanos.

Este software fue creado por una *startup* canadiense de la Universidad de Toronto. Los investigadores utilizaron la tecnología del superordenador Watson.

Algo que tiene que ver con el razonamiento jurídico es el afán de convicción. El razonamiento jurídico se parece más a la retórica que a la lógica. Sería conveniente que abogados y jueces practicaran una vieja materia de las universidades medievales: oratoria. Hay un programa que se ocupa de esto: Project Debater cuya base de conocimiento consiste en alrededor de 10 mil millones de oraciones, tomadas de periódicos y revistas.

En un debate en vivo, el Proyecto Debater debate un tema sobre el que nunca se ha entrenado en una oración muy breve que describe la moción. El primer paso es

construir un discurso de apertura para defender u oponerse a esta moción. Project Debater busca fragmentos cortos de texto en los cuerpos masivos que pueden servir para este propósito. Esto requiere una comprensión profunda del lenguaje humano y sus infinitos matices y una identificación de posición muy precisa, algo que no siempre es fácil para los humanos y ciertamente es muy difícil para las computadoras. Este proceso puede resultar en unos pocos cientos de segmentos de texto relevantes. Para poder debatir de manera efectiva, el sistema necesita construir los argumentos más sólidos y más diversos para apoyar su caso. Project Debater hace esto eliminando textos argumentativos redundantes, seleccionando los reclamos y evidencias restantes más sólidos, y organizándolos por tema, creando la base de la narrativa para respaldar o impugnar la moción.

También utiliza un gráfico de conocimiento que le permite encontrar argumentos para apoyar los dilemas humanos generales que se plantean en el tema del debate, por ejemplo, cuándo es correcto que el gobierno coaccione a sus ciudadanos, infringiendo su libertad personal de elección.

Si bien el formato y el desafío del debate nos han permitido configurar las capacidades de Project Debater, se prevé un futuro para la tecnología más allá del podio. Podría usarse, por ejemplo, para promover más debates civiles en foros de comentarios en línea o por un abogado que se prepara para un juicio en el que podría revisar precedentes legales y probar las fortalezas y debilidades de un caso utilizando un debate legal simulado. En la industria de servicios financieros, Debater podría identificar hechos financieros que apoyan o socavan una estrategia de inversión. O podría aplicarse como una capa de interacción de voz para varias experiencias complejas de clientes, o incluso para mejorar el pensamiento crítico y las habilidades de escritura crítica de los jóvenes. No caben dudas que en materia política puede ser utilizado para desarrollar todas las razones de un propuesta y todas en su contra. Sería muy importante tener una primera visión de esto antes de llevar el debate al aula parlamentaria o a un debate televisivo.

Dominar el lenguaje humano es uno de los objetivos más ambiciosos de la IA.. Absorbe grandes conjuntos de información y perspectivas en la búsqueda de un objetivo simple: ayudarnos a tomar decisiones mejores y más informadas.

3.1 Redes Neuronales

Las redes neuronales pueden ser presentadas como el símil (solo símil) de lo que acontece en el cerebro de un recién nacido: tiene células cerebrales pero no están por ahora conectadas. En los primeros años de vida las células se comunican a través de impulsos eléctricos llamados sinapsis. Cuantas más sinapsis más desarrollado esta un

cerebro. En el mundo informático se ha querido hacer un símil, pero es simplemente "símil" y bastante lejano por la propiedades que tiene una célula en comparación con cualquier conjunto de bits y el hecho que las sinapsis no son naturales sino inducidas con reglas y patrones.

Las llamadas "neuronas artificiales" son conjuntos de unidades de un sistema que se conectan con otras neuronas a través enlaces Estos enlaces varían por el peso de cada nudo y puede incrementarse. Obviamente reciben información por enlace y emiten información como output. El peso de los enlaces puede incrementar o inhibir el estado de activación de las neuronas adyacentes. Esto se llama función de activación. Del mismo modo, a la salida de la neurona, puede existir una función limitadora o umbral, que modifica el valor resultado o impone un límite que se debe sobrepasar antes de propagarse a otra neurona.

La función de red de una neurona artificial{\displaystyle {\begin{alignedat}{2}f(x)\\\end{alignedat}}} se define como una composición de otras funciones {\displaystyle g_{i}{\begin{alignedat}{2}(x)\\\end{alignedat}}}. Este se representa como una estructura de red, con flechas que representan las dependencias entre variables. La característica importante de la función de activación es que proporciona una transición suave como valores de entrada de cambio, es decir, un pequeño cambio en la entrada produce un pequeño cambio en la producción.

Los elementos procesadores se disponen en arreglos lineales llamados capas. Las capas pueden ser de distintas clases: de entrada, de salida y ocultas. Las capas de entrada reciben señales desde el exterior, las capas de salida envían señales hacia el exterior, y las ocultas, no interactúan con el medio exterior, y sus entradas y salidas se producen dentro del sistema.

Los sistemas neuronales pueden aprender y van constituyendo las redes Para realizar este aprendizaje automático se trata de utilizar un criterio para minimizar la función de perdida que evalúa la red en su totalidad. Los valores de los pesos de las neuronas se van actualizando buscando reducir el valor de la función de pérdida. Para ello se usa un mecanismo o función de propagación hacia atrás. Las redes neuronales actuales suelen contener desde unos miles a unos pocos millones de unidades neuronales. Obviamente con el tiempo aumentaran estas unidades y podrán funcionar mejor.

En el derecho implican concebir a los procedimientos como estructuras jerarquizadas en sentido horizontal, donde cada uno de los niveles corresponde a una de las fases cronológicamente consecuentes del procesamiento derivado de la aplicación de la ley cuyos resultados determinan el tipo de procesamiento a realizar en las fases sucesivas.

Los abogados trabajamos con textos pero en una definición moderna de "Texto" es la unidad lingüística comunicativa fundamental, producto de la actividad verbal

humana, que posee siempre carácter social; está caracterizado por su cierre semántico y comunicativo, así como por su coherencia profunda y superficial, debida a la integración (comunicativa) del hablante crear un texto íntegro, y a su estructuración mediante dos conjuntos de reglas: las propias del nivel textual y las del sistema de la lengua".

Con una nueva versión de texto se pueden analizar las formas semánticas recurrentes en un texto jurídico y crear patrones con los cuales hacer elaboraciones con redes neuronales poniendo una cadena o función hacia adelante para obtener resultados jurídicos dadas ciertos elementos sociales que se van configurando y cadenas hacia atrás para saber cuáles son los fundamentos jurídicos de alguna decisión.

Es posible pensar en utilizar una arquitectura de capas para simular los procesos de un abogado durante la calificación jurídica. Cada una de las capas funcionaría como una estructura de nivel inferior especializada en la identificación de cierto tipo de estructura lingüística de nivel inferior o porción textual, cuyos resultados procesales serían integrados por otras capas de nivel superior y cuyas funciones también especializadas serían distintas.

El resultado final habría de ser la calificaci n o calificaciones atribuibles (s) al texto completo, como resultado de la integración de las porciones textuales encontradas por medio de los identificadores sintácticos en la totalidad de las capas. Evidentemente la respuesta final (emergencia) presupone que entre las diferentes capas se han considerado las relaciones de inhibición de determinadas unidades de procesamiento con respecto a otras. Como recordará el lector, en el caso de las quejas no únicamente funcionan como inhibitorios de otras unidades de procesamiento los indicadores denotativos de hechos violatorios, sino también las correspondientes a tipos de autoridades.

Vale la pena tener presente que estas similitudes: inteligencia artificial, redes neuronales se toman de los seres vivos (humanos) pero que las diferencias son enormes "Los organismos están muy por encima de las maquinas construidas por el hombre…Por ejemplo el cuerpo concentra orden. Se autoreproduce continuamente. El epitelio intestinal se renueva cada cinco días. El hígado cada dos meses. La piel cada seis semanas. Cada año se reemplaza el 98 % de los átomos de nuestro cuerpo. Este incesante reemplazamiento químico, el metabolismo, es un signo inequívoco de vida. Los biólogos chilenos Humberto Maturana y Francisco Varela ven en el metabolismo la esencia de algo fundamental para la vida: *autopoyesis*. Una entidad autopoyetica metaboliza continuamente; se perpetua mediante la actividad química. La autopoyesis vincula el gasto de la energía con la desorganización"[340].

340 Lynn Margulis y Dorion Sagan ¿Qué es la vida? Metatemas, Tusquest Editores, Barcelona, tercera edición, 2009.

3.2 Investigaciones

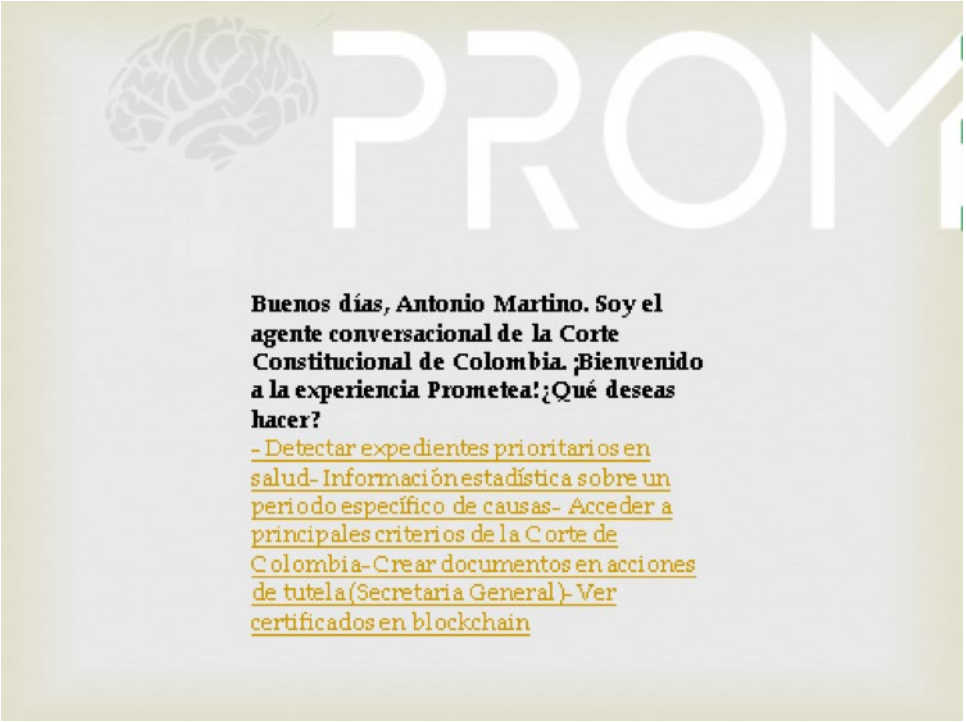
No solo hay productos en funcionamiento sino que se continúa la investigación al más alto nivel. De las muchas experiencias que hay indico dos: MIREL - MIning and REasoning with Legal texts, que es una investigación de la Unión Europea El proyecto MIREL creará una red internacional e intersectorial para definir un marco formal el objetivo de traducir estos textos legales en representaciones formales que puedan ser utilizadas para la consulta de normas, la verificación del cumplimiento y el apoyo a la toma de decisiones. El desarrollo del marco y de las herramientas MIREL se guiará por las necesidades de tres socios industriales y será validado por estudios de casos industriales.

MIREL promueve la movilidad y el intercambio de personal entre las PYMES a las academias con el fin de crear un entorno intercontinental.

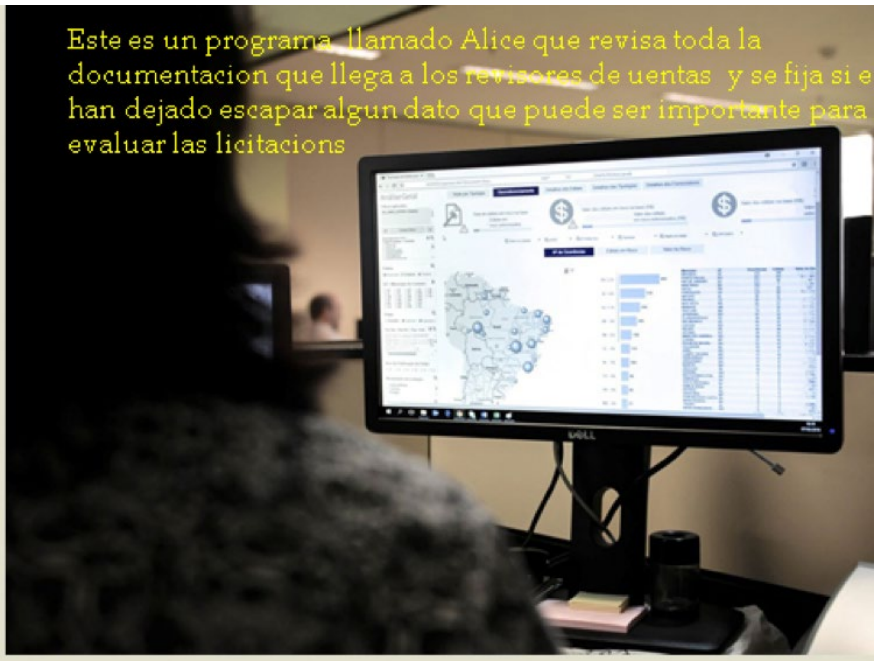
Consorcio interdisciplinario en las áreas de Derecho e Inteligencia Artificial, incluye Procesamiento del Lenguaje Natural, Ontologías Computacionales, Argumentación, y Lógica y Razonamiento. Aborda tanto los retos conceptuales, como el papel de la interpretación legal en la minería y el razonamiento, como los retos computacionales, como el manejo de grandes datos legales, y la complejidad del cumplimiento normativo. Acorta la brecha entre la comunidad que trabaja en ontologías legales y analizadores de PNL y la comunidad que trabaja en métodos de razonamiento y lógica formal. Además, es el primer proyecto de este tipo que involucra a los socios industriales en el desarrollo futuro de productos y servicios innovadores en el razonamiento jurídico y su despliegue en el mercado.

Prometea Es un programa creado por un equipo multidisciplinario del Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires (CABA) para ayudar a la justicia. Para lograrlo, junto con especialistas en inteligencia artificial desarrollaron Prometea, un sistema diseñado para predecir la solución de expedientes jurídicos simples.

El equipo creador de Prometea está liderado por dos funcionarios de la Justicia porteña: Juan Corvalán —fiscal general adjunto en lo Contencioso Administrativo y Tributario del Ministerio Público Fiscal— y Luis Cevasco —fiscal general adjunto a cargo de la fiscalia general.



El sistema se probó con 161 expedientes de temáticas consideradas factibles de tratar con este desarrollo. Entre ellas, cuestiones procesales, de caducidad, empleo público y derecho a la vivienda, en la que mostró una eficacia de 98%.. No es la idea de este tipo de programas reemplazar a funcionarios judiciales y abogados. Es fundamental que atrás de Prometea siempre haya una persona de carne y hueso que, con su inteligencia natural, y no artificial, defina si la propuesta del sistema es adecuada o no.



4. EL GOBIERNO DIGITAL

La inteligencia artificial en el derecho ha sido (y es) protagonista en una de las revoluciones más impactantes de la vida moderna, la incorporación por parte de los tres poderes del Estado de las nuevas tecnologías. Esto ha dado lugar a importantes transformaciones tanto en el poder legislativo con la posibilidad de recuperar rápidamente todo tipo de legislación anterior y la posibilidad concreta de limpiar el orden jurídico de impurezas (normas derogadas) que se conoce como *simplificación legislativa* y que en Argentina, por ejemplo ha dado lugar al Digesto Jurídico argentino[341] el cual habiendo revisado las 32 mil leyes creadas desde 1853 hasta el 2010 ha encontrado que solo 3.144 están en vigor, más las que se han dictado desde esa fecha.[342] En el poder Ejecutivo ha dado lugar, a través de las distintas administraciones a una suma de servicios a la comunidad que omite las largas filas frente a ventanillas y las convierte en actos informáticos que requieren solo de "clics" y relleno de formularios. Desde el pago de impuestos hasta la obtención de documentos aun de los más importantes como de identidad y pasaportes. Obviamente los países se diferencian por el grado de automatización de los documentos administrativos y probablmente Estonia, un pequeño país europeo con 4 millones de habitantes este a la cabeza habiendo logrado: primero automatizar prácticamente todos los documentos administrativos, segundo poner a disposición de los ciudadanos una ventanilla virtual única que contiene todos los datos que la Administracion Publica tiene sobre él y puede dar copia.

> En el poder judicial se ha logrado digitalizar los procesos en muchos países, con ahorro notable de tiempo y de energías, eliminar los procesos de papel, y reducir las audiencias de prueba a una sola que es filmada. Inclusive la nombrada Estonia ha publicado que este año piensa poner en funciones un juez que será un programa con capacidades para valorar argumentos y aplicar las normas en vigor.

Esto ha dado lugar a encendidas disputas sobre si es aceptable un robot como juez. Repárese que no es necesario que sea ningún robot, basta un programa tan complejo como Watson y especializado. Pero la idea del robot acompaña los miedos de la comunidad judía desde la idea del Golem[343] . Luego apareció la idea de Frankestein el monstruo o nuevo Prometeo creado con pedazos de cadáveres a quien, Victor Frankestein da vida a través de un experimento. Demás está decir que es un personaje de novela creado por Mary Shelley[344] pero nuestros miedos ancestrales se van ordenando detrás de estos personajes de fantasía, representados hoy por los

341 Ley Ley 26.939 aprobando el Digesto Jurídico Argentino

342 Ver sistema argentino de información jurídica SAIJ http://www.saij.gob.ar/.

343 En Praga puede visitarse la tumba del rabino Levi a quien atribuyen la creación del Golem

344 Mary Shelley , Frankenstein, or the Modern Prometeo 1 de enero de 1818, Lackington, Hughes, Harding, Mavor & ... Londres.

robots, la palabra viene del checo y significa *servidumbre* o *trabajo forzado*, voz que se usaba en el imperio Austrohúngaro en la mitad de siglo XIX[345].

Que las tomas de decisiones cada vez son más ayudadas por programas digitales y que muchas veces pueden hacerlo directamente si hay suficiente control antes, durante y después de la decisión es ya un hecho.Vimos que el derecho siempre estuvo cerca de las formulaciones organizadas sintácticamente, se trata de ir un poco mas lejos

Muchas de las novedades que hemos visto aparecer en el mundo de la decisión jurídica automatizada son recogidas en el Gobierno electrónico.

La relevancia crucial de la Internet para las sociedades nacionales en todo el mundo ha ejercido una presión adicional a los gobiernos para desarrollar una gobernanza de Internet efectiva a nivel nacional y para involucrarse en esfuerzos de diplomacia de Internet para proteger sus intereses en el ámbito digital.

Los gobiernos tratan con la Internet, como una nueva cuestión de política, en una amplia gama de espacios, desde entidades de múltiples partes, como ICANN y el IGF, hasta las multilaterales, como la UIT y el GGE de la ONU). En segundo lugar, los gobiernos tienen que ocuparse de los aspectos digitales de las cuestiones políticas tradicionales, como el comercio (en el contexto de la OMC), la salud (OMS), y el trabajo (OIT).

Desde el punto de vista internacional la existencia de Internet requiere acuerdos para su uso. Rusia amenaza con retirarse. Y la gobernanza general que se hace a través de ICANN.

345 Curiosamente también debemos el nombre al arte, pues fue usado por primera vez por Karel Čapek en su obra teatral R.U.R

Desde el punto de vista nacional se han propuesto los distintos gobiernos crear una *back office* donde se encuentran todos los datos que forman parte de la Administracion publica para ir creando un *front office* que le permita a ciudadanos y empresas ir a buscar los datos que le sirven para hacer una acción como sacar un documento o un registro o una patente.

Se comenzó en los años 90 a crear estos sistemas nacionales eficientes y electrónicos para responder a las múltiples funciones que la Administracion publica tiene para con los ciudadanos desde su nacimiento hasta su muerte pasando por la educación, el casamiento, el trabajo, los impuestos, los registros hasta el certificado de defunción. Lo mismo para las empresas desde su creación hasta la desaparición por quiebra o disolución pasando por los registros de socios, acciones, relación con el fisco, marcas y patentes hasta la desaparición por quiebra o disolución.

Luego han instituido domicilios electrónicos certificados no solo para profesionales sino para cualquier ciudadano lo que facilita y asegura la notificación

Existe ya una cultura *ciber* que atraviesa toda la sociedad y la mayor parte de las acciones que hacemos individual o colectivamente.

Hay muchos países que están en este camino debiendo tenerse en cuenta que los más grandes y adelantados tienen ventajas. Pero no está dicho, dado que es un campo nuevo hay países como Islandia y sobre todo Estonia (que es el más pequeño país de Europa) que han informatizado prácticamente todos los trámites que deben hacerse ante la Administracion publica.. No contentos con todo lo que han logrado anunciaron oficialmente que se van a dedicar a crear un programa (la prensa habla de "robot" pero es un simple programa, aunque no tan simple) que va actuar como juez. En el fondo no es para escandalizarse tanto: existen ya programas en EEUU que predicen con bastante certeza los resultados de las causas según el caso y el juez competente y todo lo que hacen es analizar todas las sentencias de ese juez en esa materia y tienen ya un patrón de comportamiento que se puede exportar a casos venideros. Además la I.A. en derecho está bien afianzada.

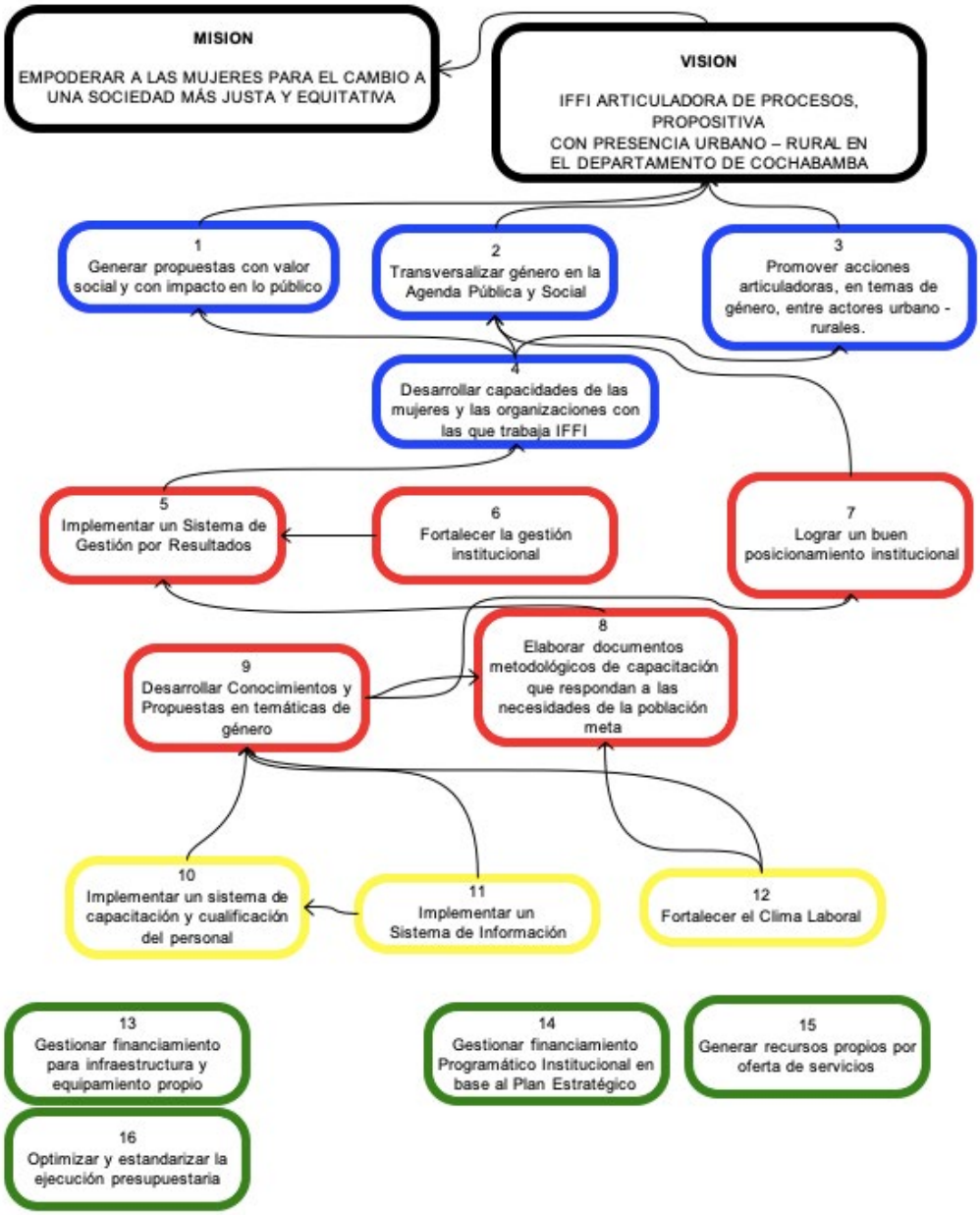
En América Latina hay emprendimientos de gobierno electrónico sostenible en diferentes áreas: medicina, educación, transporte, justicia son los más desarrollados pero hay otro que merecen ser tenidos en cuenta: por ejemplo el tablero de comando que ha logrado una asociación Instituto de Formación Femenina Integral (IFFI) con varios países es una Institución Sin Fines de Lucro ubicada en la ciudad de Cochabamba, en Bolivia.

En Brasil es para destacar el trabajo que se esta haciendo con el Proyecto *Víctor* para el juzgamiento de causas repetitivas hecho por el Supremo Tribunal Federal[346].

346 Ministra Carmen Lucia anuncia el comienzo del Proyecto Victor de Inteligencia Artificial Noticias STF, 30 de agosto 2018. www.stf.jus.br//portal/cms/verNoticaDetalhe.asp?idConteudo=388443.

Antes de usar la técnica de I. A., evaluaron la situación de la organización:

Limitaciones	**Posibilidades**
Gestión en función de proyectos y NO en función de una institución que sirve a las mujeres	Técnica adecuada a la gestión de proyectos
Falta de articulación entre proyectos y áreas de intervención la institución	Muestra el desempeño de un proyecto en todas sus fase
Excesiva concentración en actividades	Claridad en los resultados propuestos para cada proyecto
Multiplicación de actividades, que no siempre logran los resultados propuestos	Identifica factores xternos e internos que afectan a un proyecto
Operatividad muy pesada: Planificación y seguimiento de muchas actividades	Una matriz muestra lo más importante y relevante de un proyecto
Imposibilidad de una gestión global de la institución	La planificación no plantea metas claras y medibles



Partiendo de la obvia referencia al trámite que debe hacerse para obtener un documento de la Administracion pública se ha ido urdiendo una práctica de descompresión a través de la digitalización. En América Latina "tramite" significa problema, barreras, saltos con obstáculos. Esto es dramático para el ciudadano y perjudicial para la Administracion es por ello que con la digitalización se van obteniendo mejores resultados, pero no es una formula sagrada ni un éxito asegurado. Solo el uso va perfeccionando los mecanismos. Esto requiere además una sociedad suficientemente informada y entrenada en el uso de estas tecnologías

Muchos gobiernos lo han entendido y lo primero que han digitalizado es la Recolección de Impuestos: Argentina que tiene una larga trayectoria de informatización habiendo comenzado en 1970 con la automatización del Registro de la propiedad inmueble de la Ciudad Autónoma de Buenos Aires, hoy brinda los servicios de la Afip (Administracion Federal de Ingresos Públicos) para informar y recaudar.

Y lo interesante también es que el gobierno electrónico se está ocupando de ciudades inteligentes. Hay dos elementos a tener en cuenta: el primero es que contrariamente a todas las previsiones la población cada vez se vuelve más urbana y para 2030 se prevé que la población rural en todo el mundo no va a superar el 25 % de toda la población mundial. La segunda es que las ciudades se vienen cableando desde los años 90 del siglo pasado, algunas con fibra óptica.

En la actualidad, la filos fía de las ciudades inteligentes se encuentra plenamente respaldada por empresas y administraciones. Se celebran cumbres y exposiciones anuales como la *Smart City World Expo* en Barcelona, a la que asisten miles de visitantes y que concede galardones a metrópolis de referencia como Dubai .

Desde el punto de vista de la composición de la imagen, en los casos escogidos encontramos planos abiertos para apreciar el agudo contraste entre la escala de la ciudad y las personas. La apuesta por el gran tamaño de los núcleos urbanos es evidente, así como también la necesidad de combinar el material robusto de las construcciones con formaciones vegetales y cielos despejados para componer escenas pintorescas. Pantallas, interfaces y aplicaciones funcionan como correa de transmisión entre sujeto y espacio; también se mantienen algunas escenas de la vida social en las que las tecnologías digitales permiten a sus usuarios comunicarse de forma inmediata, intuitiva y diáfana.

Los albores de las ciudades inteligentes aparecieron en la literatura (Nicholas Negroponte) y en algunas series como Matrix. Se pensó al principio como Smat citys pero pronto se vio que esto implicaba una oligarquía de usuarios y una masa excluida.

Además el modelo Smart es bueno para hacer proyectos y experimentos pero las ciudades reales cada vez son más grandes.

La auténtica ciudad inteligente no ocultaría las posibles fisuras que pudieran surgir como resultado de los múltiples usos que hacen los ciudadanos del tejido urbano. La idea de fondo sería precisamente dotar de capacidad crítica a los habitantes.

Aunque se trate de una simplificación, cabe decir que hasta hace no demasiados años la única estética operativa que permitía imaginar cómo se concretarían las relaciones entre ciudad, ciudadanos y nuevas tecnologías respondía al modelo corporativo de las ciudades inteligentes.

Es posible afirmar que nos encontramos ante una estética ciudadana cognitiva: en estos espacios los ciudadanos se familiarizan con las nuevas tecnologías no mediante informes, reportajes o vídeos promocionales creados por las partes interesadas, sino que lo hacen a través de la interacción directa y en primera persona con las herramientas que se ponen a su disposición. Dicho de otro modo: la cultura tecnológica ciudadana que ha emergido a través de los llamamientos, iniciativas y proyectos de los 'labs' y otros espacios de similar naturaleza ha contribuido a generar una sensibilidad que permite concebir la tecnología como algo que es posible conocer y manipular porque se pone al alcance de usuarios no expertos.

El gobierno digital es uno de los requisitos para formar parte de la OCDE Organización para la Cooperación Comercial y el Desarrollo, como ya los sabe México y lo están aprendiendo Brasil y Argentina.

5. CONCLUSIONES

La mejor manera de coger el tren tecnológico no es perseguirlo, sino estar en la siguiente estación. En otras palabras, necesitamos anticipar y dirigir el desarrollo ético de la innovación tecnológica. Y podemos hacer esto observando lo que es realmente factible, privilegiando, dentro de ello, lo que es ambientalmente sostenible, luego lo que es socialmente aceptable y luego, idealmente, elegir lo que es socialmente preferible compatiblemente con la sostenibilidad de la biosfera, por lo que nuestra ecuación actual es incompleta.

Hemos demostrado que los que las tomas de decisiones cada vez son más ayudadas por programas digitales y que muchas veces pueden hacerlo directamente si hay suficiente control antes, durante y después de la decisión.

Vimos que el derecho siempre estuvo cerca de las formulaciones formalizadas desde los epígrafes romanos hasta la teoría de la argumentación pasando por la profusa actividad normalizadora en derecho de los últimos cuarenta años.

La lógica fue un instrumento extraordinario en este pasaje jurídico a lo formal y creemos haber demostrado que la lógica es puramente sintáctica como los programas informáticos y eso explica la capacidad y velocidad de informatica decisoria jurídica

Vivimos una época de crecimiento extraordinario de la información y su difusión. La expresión Big Data tiene un sentido específico aunque no sea transparente para todo el mundo. Y aquí aparece la segunda característica de nuestro tiempo: así como después de Platón y mucho más después de Gutenberg, el gran tema fue alfabetizar a la población, hoy tenemos un problema parecido con la falta de conocimiento de una parte importante de la población para el uso de los medios informáticos con los cuales se están transformando casi todos los trabajos y los servicios sociales a través del Gobierno electrónico.

Curiosamente vivimos una época bisagra en la cual conviven en el Planeta Tierra las tres culturas: oral, escrita y cibernética.

Pero esta última tiene una velocidad de desarrollo y una fuerza de expansión que no permite los largos tiempos de la alfabetización. Este es un mundo exigente ¡ahora! Y el derecho y muchas funciones del Estado no pueden esperar tiempos "razonables" de conocimiento. Los que queden a un lado serán el lumpen del futuro próximo: ¡no el 2100, en el 2050!

El tema de la inteligencia artificial poniéndose de moda ha invadido campos y agregado ruido, pero también ha servido para un uso más extendido aunque no falto de críticas. Muchas se deben a viejos miedos humanos como el Golem o el Robot, pero algunos deben ser tenidos en cuenta pues no es bueno solo porque es nuevo.

Y, *last but not least*, esto viene todo junto aun con problemas éticos que no podemos sosalayar.

Obviamente que tenemos que ocuparnos de problemas éticos o estos se nos vendrán encima después. Dejemos de discutir inútilmente si las maquinas van a gobernar al hombre, tema para filósofos desocupados y ocupémonos de temas concretos y muy próximos. Por supuesto que cualquier programa, sobre todo si puede aprender y tiene directivas concretas de su finalidad tendera a alcanzarla siempre más. Pero si es un software o como quiere la imaginación popular un robot, el tema es que para alcanzarlo no tiene otros límites que el nosotros le pongamos. De lo contrario – dado que no puede tener una ética pues no es consiente – lo obtendrá de cualquier manera.

Lo preferible y lo políticamente factible, y por tanto, en última instancia, lo legalmente exigible, y lo que los agentes pueden o no pueden hacer. A largo plazo, las personas (como usuarios, consumidores, ciudadanos, pacientes, etc.) están limitadas en lo que pueden o no pueden hacer por las organizaciones, por ejemplo, las empresas, que están limitadas por la ley, pero esta última está formada y limitada por la ética, que es donde las personas deciden en qué tipo de sociedad quieren vivir .

Desafortunadamente, esta cascada normativa se hace obvia principalmente cuando se produce una reacción violenta, es decir, sobre todo en contextos negativos, cuando el público rechaza algunas soluciones, incluso cuando pueden ser buenas soluciones. De todo ello se deduce que la ética en general y la ética digital en particular

no puede ser un mero complemento, una idea de última hora, un búho de Minerva que sólo vuela cuando se reúnen las sombras de la noche, una vez que se ha producido la innovación digital y, posiblemente, se han aplicado malas soluciones, se han elegido menos alternativas buenas o se han cometido errores.

Los problemas éticos son importantes, se comprometen con las partes interesadas afectadas y, sobre todo, proporcionan soluciones compartidas.

La ética digital debe informar las estrategias para el desarrollo y el uso de las tecnologías digitales desde el principio, cuando cambiar el curso de acción es más fácil y menos costoso, entremezclando los recursos y el impacto. Debe sentarse a la mesa de los procedimientos de elaboración de políticas y de toma de decisiones desde el primer día. Porque no sólo debemos pensarlo dos veces, sino que lo más importante es que debemos pensar antes.

La directiva europea de mayo de este año en materia de transacciones informáticas, luego de tres años de discusiones y tratativas llena un horizonte no solo europeo sino también mundial, pues está siendo tomada seriamente en cuenta para organizar las transacciones en muchos países. Y es una contribución universal. [347]

En vista que es fácil hoy en base a repeticiones de sentencias en caso similares hacer el perfil y poder predecir fallos, hay programas que lo hacen con mucha precisión. Este año hay una ley francesa que lo prohíbe. Es tan estúpida como prohibir respirar, lo van a seguir haciendo como lo hicimos siempre, buscando jurisprudencia, antes que apareciera la computadora.

Antes de legislar es necesario pensar con seriedad lo que se va a permitir o prohibir, nuestro miedo a lo nuevo no puede llevarnos a cometer torpezas.

Ejemplo de una cascada normativa, con el negocio como agente y las personas como clientes.

Me ha llamado mucho la atención una aclaración de un gran especialista de Marketing: el marketing no es la actividad para vender mejor mis productos sino la actividad de aprender qué producir.

Todo, dicho conforme a la máxima griega que aparece en el oráculo de Delfos **ΜΗΔΕΝ ΑΓΑΝ (**Χρόνου φείδου) De nada en demasía, que los romanos supieron acuñar en *Ne quid nimis*.

347 DIRECTIVA (UE) 2019/771 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 20 de mayo de 2019 relativa a determinados aspectos de los contratos de compraventa de bienes, por la que se modific n el Reglamento (CE) n.o 2017/2394 y la Directiva 2009/22/CE y se deroga la Directiva 1999/44/CE (Texto pertinente a efectos del EEE)

INTELIGENCIA ARTIFICIAL Y INNOVACIÓN JURÍDICA

Eje temático: Inteligencia Artificial: riesgos y desafíos jurídicos

Autor:
Ernesto Ibarra Sánchez
Abogado y Maestro en Derecho por Universidad Nacional Autónoma de México (UNAM) y candidato a doctor en Derecho por Universidad Panamericana, México. Profesor en la Maestría en Derecho y Tecnologías de la información y comunicación de CONACYT-INFOTEC, México.

ABSTRACT
Este artículo presenta un panorama general sobre la Inteligencia Artificial como agente transformador del sistema jurídico e institucional. Es decir, la IA como Derecho, es herramienta para la innovación jurídica y componente para aplicar el Derecho de manera más eficiente
El texto será desarrollado teniendo en cuenta, como premisa, el poder transformador de la IA en el sistema jurídico (a partir del análisis sobre el impacto de la automatización en el trabajo[348]), la hipótesis es que: el desarrollo e implementación de la IA en el sistema de justicia y andamiaje institucional -vinculado al derecho y la justicia como servicio público-, sólo será efectivo si es que cuenta con: a) modelo de gobernanza multidisciplinario que contribuya a garantizar el desarrollo e implementación óptimo de la IA en el mundo del derecho; b) valores y principios éticos en torno a la IA: diseño, aplicación, auditoría, y más; y c) desarrollo de habilidades y formación en los operadores jurídicos (desde funcionarios de las Cortes supremas, jueces, autoridades públicas), fedatarios públicos, litigantes y asesores de empresas, así como a las facultades y estudiantes de Derecho y otras disciplinas involucradas.
Como conclusión, si bien no hemos llevado a cabo algún ejercicio práctico o de investigación empírica para someter a evaluación la hipótesis y no podemos afirmar categóricamente que la hipótesis se cumple con lo investigado hasta ahora; sí podemos inferir que la suma de las variables podrán acercarnos a un mejor desarrollo y aplicación de la IA al sistema jurídico haciendo un traslape de cómo se desarrollan algunos de estos elementos en otras latitudes u otros temas de desarrollo tecnológico (varios de ellos han sido propuestos y resultados por expertos y actores clave como fundamentales). Esperamos que la IA se adopte de manera transversal por los operadores jurídicos, articulados en una estrategia y visión de Estado, que tenga su vertical orientado a mejorar la eficacia del Derecho y así el sistema de justicia.

PALABRAS CLAVE: Inteligencia Artificial, innovación legal, LegalTech, Ciberjusticia, Gobernanza, tecnologías emergentes, jurista digital.

INTRODUCCIÓN

La inteligencia artificial (en adelante IA) ha sido considerada como uno de los agentes transformadores más poderosos, igual o más de lo que ha sido la electricidad, la cual impactará sustancialmente en todos los aspectos de la vida, y el Derecho no es la excepción. Es fundamental que los actores del sector legal y las instituciones públicas miren la oportunidad que la IA ofrece al Derecho, a la vida institucional y al Estado de

348 BUGHIN, Jaques, SEONG, Jeongmin, MANYKA, James, CHUI, Michael, JOSHI, Raoul, *Notes from the AI Frontier. Modeling the Impact of AI on the World Economy,* McKinsey Global Institute, 2018.

Derecho en general. La automatización (Inteligencia Artificial, *machine learning* y otras tecnologías) terminará con el 30% del trabajo en el sector legal[349], eventualmente también se podrán emitir resoluciones jurisdiccionales a conflictos menores, y asistir a los funcionarios judiciales y operadores del Derecho para tomar las mejores decisiones en el quehacer del jurista, e incluso mejorar la enseñanza aprendizaje de las y los juristas del futuro. En el presente texto abordaremos la necesidad de renovación que deberá emprender el Derecho (sus operadores, procesos e instituciones públicas) para no quedar fuera el dinamismo de la era digital y contribuir a la demanda social de justicia para todos y mejor calidad de vida.

La hipótesis que envuelve el presente texto es: La IA aplicada transversalmente y en el marco de un ecosistema -multidisciplinario y multistakeholder- para el desarrollo y adopción de ésta será crítico para mejorar el sistema jurídico y la justicia en general.

En este artículo nos enfocaremos someramente en el impacto que tiene la IA en el ámbito del derecho, ¿de qué manera la IA ha impactado en el derecho? Y ¿cómo estos cambios producidos por la IA afectan el desarrollo del jurista del futuro? El texto se dividirá en cuatro apartados: en primer lugar, se verá cuál es la situación actual del Estado del Derecho en Iberoamérica y qué herramientas existen para su medición; seguido se explicará qué entendemos por IA, cómo ha impactado las sociedades y se estudiarán ejemplos de la gobernanza multidisciplinaria; en el tercer apartado se expondrá la importancia de la ética y la protección de los derechos de las personas para una efectiva relación entre el derecho y la IA, para que al final se puedan dar ciertas recomendaciones a profesionistas y centros de formación acerca de la llegada de la IA a la disciplina del derecho.

APROXIMACIÓN AL PROBLEMA. EL ESTADO DE DERECHO EN IBEROAMÉRICA

Si bien la tecnología *per se*, en este caso la IA, genera una amplia expectativa sobre la infinidad de trasformaciones es importante partir -desde mi perspectiva- de la identificación de problemáticas sociales que puedan atemperar sus efectos negativos mediante el uso adecuado de IA. En tal sentido, haremos una revisión general sobre el Estado de Derecho, pensemos que se trata de un Estado de Derecho Democrático. ¿Qué entendemos por Estado de Derecho y cómo puede medirse el avance o deterioro de éste? Se trata de una sociedad donde la Constitución sea respetada y guíe el desempeño y actuar de gobernantes y ciudadanos, donde se reconozcan los derechos y haya una separación de poderes. Aunque existen diversos debates sobre su definición, diversos autores identifican elementos necesarios al Estado de Derecho [350]

349 BUGHIN, Jaques, *et. Al., op. Cit.*
350 DÍAZ, Elías. *Estado de Derecho y sociedad democrática,* Madrid, Taurus ediciones, 1981, o.

- Imperio de la ley: ley como expresión de la voluntad general
- División de poderes: legislativo, ejecutivo y judicial
- Legalidad de la Administración: actuación según ley
- Derechos y libertades fundamentales: garantía jurídico formal

World Justice Project (WJP) identifica cuatro principios que definen el Estado de derecho: i) el gobierno y sus funcionarios, así como individuos y entidades privadas están restringidos por la ley; ii) las leyes son claras, públicas, estables y justas; son aplicadas equitativamente y protegen los derechos fundamentales, incluyendo la seguridad de los individuos y la propiedad; iii) el proceso por el cual la ley es promulgada, administrada y aplicada es accesible, de manera justa y eficiente; y iv) la justicia es aplicada en tiempo por representantes éticos, competentes, independientes y neutrales. En la impartición de justicia, existen suficientes representantes, cuentan con los recursos adecuados y reflejan la composición de las comunidades a las que sirven.[351]

Existen críticas sobre el concepto, y sobretodo resalta la complejidad de medición de los diversos principios.[352] Sin embargo, en la actualidad, a pesar del grado de dificultad para medir ciertas variables, existen tres organizaciones que han logrado avances muy valiosos en dicha labor: el Banco Mundial, Foro Económico Mundial y *World Justice Project*. Para dar un ejemplo, según el Índice de Estado de Derecho del WJP, México ocupa la posición 99 de 126 países de acuerdo con el índice de Estado de Derecho 2019. Dicho índice se compone de ocho factores: 1) límites al poder gubernamental, 2) ausencia de corrupción, 3) gobierno abierto, 4) derechos fundamentales, 5) orden y seguridad, 6) cumplimiento regulatorio, 7) justicia civil y 8) justicia penal[353]. De igual manera, se puede afirmar que las tecnologías, como la IA y *machine learning*, y los datos abiertos, tiene un gran potencial para impactar positivamente en los ocho factores y mejorar en los resultados finales.

De manera simple, es claro advertir que la IA podrá ayudar a que se incremente la eficiencia y apego a dichos principios, y por tanto se consiga incrementar la cultura de legalidad, el Estado de Derecho y la justicia.

El deterioro de Estado de Derecho en el mundo es un tema que se le debe prestar atención el aumento en el "autoritarismo" es un llamado a observar si los poderes judiciales son independientes, si existe acceso a la información (y se garantizan los derechos a la libertad de expresión y de prensa libre), transparencia y compromiso con

31.

351 WORLD JUSTICE PROJECT. Sitio web: http://worldjusticeproject.org/ what-rule-law [fecha de consulta: 17 de junio de 2019).

352 TREBILCOCK, M. y DANIELS, R., *Rule of Law reform and development,* UK, Edward Elgar, 2008, p. 56.

353 WORLD JUSTICE PROJECT MÉXICO. Sitio web: https://worldjusticeproject.mx/estado-de-derecho/ [fecha de consulta: 17 de junio de 2019].

la generación de datos abiertos para generar una transformación al sistema de justicia en general.

Nuevamente, insistimos en el valor transformador de la IA y las tecnologías para impactar desde una visión estratégica y operativa en los procesos, la gestión y gobernanza de la información, en el uso de las tecnologías y en las personas. De lo anterior, nos podemos cuestionar sobre: ¿Las tecnológicos emergentes, la IA y el aprendizaje de máquinas, ayudan a construir sociedades más apegadas a la ley?, ¿La IA puede ayudar a combatir la corrupción y mejorar la eficiencia de las autoridades?, ¿Las tecnologías emergentes, como IA, ¿cómo mejoran el cumplimiento regulatorio, el acceso a la información y al gobierno abierto? y ¿cómo la IA hace posible que la justicia sea más accesible para todas las personas? Las anteriores sería parte de las preguntas de investigación.

Como ya señalamos, este texto surge en un momento inicial de una investigación que será más profunda y esperamos lograr tener una muestra representativa de su impacto en los diversos factores. Por ahora, usaremos ejemplos de otras latitudes para acercar aquellas soluciones al escenario de nuestro problemas e hipótesis.

Un ejemplo claro de cómo la IA puede relacionarse con el ámbito del derecho es el caso de la Universidad Estatal de Michigan que, en 2015, creó un programa computarizado (algoritmo) para medir la probabilidad de que la Corte Suprema de Justicia de los Estados Unidos se pronunciara a favor o en contra de un caso específico; la precisión del algoritmo mostró 70% de aciertos en las decisiones tomadas por los jueces.[354]

Otro ejemplo de cómo la IA puede ayudar a fortalecer estos índices es gracias al gobierno digital que aplica IA donde gracias a datos abiertos, los ciudadanos pueden exigir cuentas a sus gobernantes y con ello desarrollar herramientas que contribuyen a hacer efectivos los derechos e incluso a generar valor económico de la información pública de las autoridades.

Con el uso de IA, y datos abiertos, se facilitará la medición y evaluación del desempeño y eficacia de las autoridades y así del propio sistema jurídico. Permitirá medir el desempeño de las propias tareas del Estado, que en materia de justicia articula a los tres poderes: Poder Legislativo (puede medir la eficacia del proceso de creación de una ley y su grado de adopción y cumplimiento); Poder Ejecutivo (a partir de la evaluación de la labor de autoridades en cumplimiento de leyes y garantizando derechos, en justicia administrativa, entre otras); y el Poder judicial, donde es posible mejorar el quehacer de servidores judiciales mediante la generación de datos sobre el proceso de emisión de sentencias o resoluciones, la aplicación de sistemas de

354 HUTSON, Matthew, *Artificial Intelligence prevails at predicting Supreme Court decisions*, 2017. Sitio web: https://www.sciencemag.org/news/2017/05/artificial-intelligence-prevails-predicti - g-supreme-court-decisions [fecha de consulta: 17 de junio de 2019].

asistencia, análisis y predicción por sistemas expertos que faciliten y transparenten la labor del juzgador, disminuyan la subjetividad, reduzcan el rezago de expedientes por resolver y se vigile la aplicación de principios, tratados en materia de DDHH y argumentos que vayan consiguiendo más solidez conforme pase el tiempo.

INTELIGENCIA ARTIFICIAL (IA) Y GOBERNANZA

Una de las inquietudes más recurrentes sobre el empleo de la IA es la automatización o el uso de *machine learning*, y la consecuencia de sustitución de la persona respecto su labor de trabajo. Al respecto, según la Organización para la Cooperación y el Desarrollo Económico (OCDE), los empleos podrían desaparecer en los próximos 15 a 20 años como resultado de la automatización, porcentaje que en México podría ser más alto por tener un alto número de actividades del sector manufactura y actividades altamente automatizables como trabajo en el campo o en la construcción; además de que existe la probabilidad que otro 32% cambie radicalmente en lo que las tareas individuales se automatizan.[355] En mi opinión, cada ola tecnológica ha traído la preocupación respecto del empleo, y es cierto que se perdieron muchos empleos, por ejemplo gracias a la electricidad o la informática; sin embargo, también se espera que se crearán muchos nuevos empleos ofreciendo nuevas oportunidades, además del impacto positivo que se espera conseguir en materias tan diversas, lo cual representa una llamada para orientar la educación, y para asumir nuevos retos como gobiernos y sociedad sobre el futuro positivo posible, no así el momento para luchar contra la innovación. Será mejor estar involucrados en el desarrollo que mirar el mundo cambiar con el temor de lo catastrófico. A lo anterior, los gobiernos (y su capacidad de construir alianzas con el sector privado) será fundamental pues un gran porcentaje de la población no dimensiona la trascendencia de las nuevas habilidades y los trabajos que se crearán que aún no existen.

A lo largo de los años, la IA ha recibido distintos conceptos, estas dependen perfil de quien lo haga la exponga, el campo o disciplina de estudio de interés, entre otras variables. Y debe señalarse que no es un término nuevo y, si bien es popular ahora, no se tiene una definición plenamente aceptada y dista mucho de ser universal. En el Reporte del Panel de Estudio 2015, 100 años de estudio sobre IA, señala que ésta es: "una ciencia y un conjunto de tecnologías computacionales que son inspiradas por las formas en que la gente usa su cuerpo y sistema nervioso para sentir, aprender, razonar y ejecutar acciones"[356]. Otros estudiosos la definen como la rama de las ciencias

355 OCDE, OECD Employment Outlook 2019. The Future of Work, OCDE, Berlín, 2019, p. 3.

356 *One Hundred Year Study on Artificial Intelligence (AI100)*, Stanford University, 2016. Sitio web: https://ai100.stanford.edu/ [fecha de consulta: 17 de junio de 2019]

computacionales que "se encarga del diseño y construcción de sistemas capaces de realizar tareas asociadas con la inteligencia humana"[357]. Sus aplicaciones van desde el reconocimiento en imágenes o video de objetos y personas, hasta el habla y la traducción automática de textos. En pocas palabras, la IA es el nombre que se le da a la actividad, proceso o metodología y conjugación de técnicas y tecnologías y conocimiento, orientados a imitar funciones cognitivas del ser humano. Entre los términos que se identifican en las investigaciones de IA se pueden encontrarse: "*Artificial Intelligence*" a veces indistintamente o sutilmente diferenciado de "*machine learning*" y otras categorías de la IA, tales como Procesamiento de Lenguaje Natural (PLN), Reconocimiento de imagen, visión de computadora, reconocimiento del discurso, aprendizaje profundo de máquina (*Deep machine learning*), análisis semántico, web semántica, asistente inteligente o virtual, análisis predictivo, o sistema inteligente[358].

IA y Derecho

En el ámbito del campo del derecho, la IA ha tenido múltiples interacciones, pero aún hay un mundo por descubrir en esta intersección. Un ejemplo muy conocido son los sistemas expertos jurídicos (SEJ), estos se basan en el conocimiento desarrollado en la actualidad para resolver problemas muy específicos. Según Martínez, un SEJ "es un sistema computacional que puede plantear posibles soluciones a determinados asuntos jurídicos aplicando el conocimiento experto en la materia, así como explicar sus razonamientos. En general, se ha pretendido establecer estas aplicaciones como herramientas de apoyo para los operadores jurídicos en contextos tales como la asesoría o asistencia legal o la función jurisdiccional".[359]

Las personas que ejercen la carrera de derecho, operadores del Derecho, desde cualquier ámbito tienen responsabilidad en materia de innovación jurídica; por un lado, interactuar con las nuevas tecnologías, aprovecharlas para un ejercicio más eficiente y eficaz del Derecho; por otro, velar que estas nuevas tecnologías siempre sean usadas para garantizar y proteger los derechos de las personas.

Como ejemplos de la interacción de actores público y privados, componentes de la gobernanza de la IA, podemos ver cómo en el caso de Estados Unidos (USA) las empresas tecnológicas (Google, Amazon, Facebook, Apple y Microsoft) han estimulado la innovación en IA, y gracias a ellos existe un mercado con suficiente capital de riesgo

357 "Inteligencia artifi ial", Oficina de información científica y tecnológica para el para el Congreso de la Unión. Sitio Web: https://www.foroconsultivo.org.mx/INCyTU/documentos/Completa/INCYTU_18- 012.pdf [fecha de consulta: 17 de junio de 2019].

358 *China AI Development Report 2018,* Institute for Science and Technology Policy at Tsinghua University. Sitio web: http://www.sppm.tsinghua.edu.cn/eWebEditor/UploadFile/China_AI_development_report_2018.pdf [fecha de consulta: 17 de junio de 2019].

359 MARTÍNEZ BAHENA, G., "Inteligencia artificial y su aplicación al derecho" *Alegatos. Revista jurídica,* Universidad Autónoma Metropolitana, Méxic0, 2012, p.833

que estimula la creatividad[360], se incita a empresas o innovadores a seguir generando herramientas que ayuden a los distintos ámbitos de la sociedad, incluido el derecho.

China, por su lado, al contrario que Estados Unidos, ha impulsado un ambiente donde el gobierno, empresas de capital de riesgo y empresas tecnológicas destinan recursos para la investigación, registro tecnológico y comercialización de tecnologías *Deep learning,* lo que ha permitido incrementar el número de *StartUps* de IA. Como resultado de esta unión de distintos actores, China es líder del sector de la IA en materia de patentes, generación de datos sin procesar, artículos de investigación y financiamiento. [361]

La unión entre gobierno, iniciativa privada y academia es importante para empezar a ver la IA como una herramienta de eficiencia en las tareas que se realizan. Ejemplo de lo anterior puede observarse en la estrategia adoptada por China en materia de inteligencia artificia , en la cual se observa una inversión de recursos públicos importante[362], y una estrecha vinculación con el sector académico y los investigadores, advirtiéndose que la estrategia de IA es nacional y está articulada con otras estrategias como la de ciencia y tecnología[363].

Del mismo modo, el gobierno inglés, mediante IA, intentó pronosticar decisiones en la Corte Europea de Derechos Humanos, en materia de tortura, trato degradante y debido proceso, mediante el procesamiento de 584 casos similares[364]. Gobiernos, juristas y empresas tecnológicas colaboran para rediseñar la manera en que las cosas se hacían en el derecho. En Latinoamérica, Colombia es un ejemplo de cómo el gobierno ha implementado IA en instituciones como el Ministerio de Educación y la Contraloría General de la República. En este último, el gobierno y la iniciativa privada se coordinan para vigilar a los contratistas y generar alarmas cuando se presente fraudes, corrupción o no cumplan con los requisitos; la inversión por parte del gobierno ha generado resultados positivos para este ente.[365] En México se desarrolló un documento de Estrategia de IA[366] pero no se ha dado continuidad, y en la cual se destacan algunas recomendaciones en materia de gobernanza: crear un grupo de expertos de distintos sectores y disciplinas, crear una red de participantes de diversas disciplinas y sectores,

360 TREJO CAMPOS, Francisco, "Los desafíos de la inteligencia artificial en el sistema internacional", *Foreign Affairs Latinoamérica,* 2019.

361 *Ibid*.

362 En 2017, el mercado de IA de China alcanzó los 23.700 millones de RMB, un 67% más que el año anterior, y los tres segmentos principales fueron visión artificial (34.9%), voz (24.8%) y procesamiento de lenguaje natural (21%), hardware y algoritmo. Se espera que el mercado crezca un 75% en 2018. *China AI Development Report 2018, op. Cit*.

363 DING, Jeffre , *Deciphering China´s AI Dream. The Context, Components, Capabilities and Consequences of China´s Strategy to Lead the World in AI,* University of Oxford, 2018.

364 LIMÓN, Jaime, "Inteligencia artificial en proce os judiciales", *El Economista,* 2019.

365 Sitio web: https://www.larepublica.co/alta-gerencia/el-gobierno-de-colombia-le--puesta-al-desarrollo-de-la-inteligencia-artificial-2841835 [fecha de consulta: 17 de junio de 2019]

366 Sitio web: https://www.oxfordinsights.com/mexico/ [fecha de consulta: 17 de junio de 2019].

tanto de gobierno federal y locales; crear grupo de trabajo en el Congreso y; establecer a un líder de la estrategia.

Como podemos observar, en el diseño de políticas públicas es cada vez más común que se hable de gobernanza, y de la conformación de actores de diferentes sectores y disciplinas, aunado a la inversión de recursos públicos y mecanismos de colaboración con el sector privado y el sector académico. En tal sentido, una estrategia para la revisión y rediseño del sistema jurídico, empleando tecnologías emergentes -principalmente- habrá de contener un modelo de gobernanza donde el poder judicial tome el liderazgo junto a las autoridades de los otros poderes en gobiernos centrales o federales y locales, y se defina un mapa de ruta que lleve a la transformación del sistema jurídico que involucre a diferentes actores; sector privado, academia y sociedad en general.

INTELIGENCIA ARTIFICIAL, DERECHO Y PRINCIPIOS ÉTICOS

Dentro de cualquier estrategia de aplicación de IA debe estar presente el componente ético, mismo caso deberá atenderse en los procesos de innovación del sistema jurídico y sector legal. Las distintas disciplinas de estudio no pueden, ni deben, permanecer indiferentes ante los cambios que la tecnología ha traído a las sociedades, más aún cuando no se logra dimensionar el impacto y sus consecuencias en la vida de las personas y sus derechos.

El derecho aprovecha las bondades de la IA para la solución de un conjunto de problemas que existen en la disciplina: organización de grandes bases de datos, el orden y clasificación de textos jurídicos (cambiantes con el tiempo, como leyes, sentencias, reglamentos), el modelado de la argumentación razonable con base en normas y precedentes, o incluso para elevar el grado de objetividad en el razonamiento de quienes imparten justicia y con ello acotar acciones como la corrupción o malas prácticas de servidores públicos, etc.

Así que, los profesionales del derecho no sólo tienen que sumarse a la ola de la cuarta revolución por sus bondades para el trabajo interno y especialmente para el derecho de las personas, sino por los nuevos desafíos que trae para su profesión. Un ejemplo, que tal vez se pueda resolver con la teoría de la responsabilidad desarrollada hasta ahora, implica conocer sobre programación y sistemas informáticos, sería el caso de un accidente donde está implicado un auto autónomo ¿quién se hace responsable de las consecuencias del accidente (ya sea destrucción de muebles, muerte o lesiones)? ¿Cuál es la responsabilidad de creadores del auto, las personas que iban en él, del diseñador por encargo del algoritmo? La responsabilidad jurídica en casos como este

amerita innovar en la interpretación y exige a juzgadores y a quien ejerce la abogacía a estudiar nuevas áreas del conocimiento.

La llegada de la cuarta revolución trae consigo desafíos para los operadores jurídicos, en razón de que la automatización modificará su forma de trabajo y en muchos casos, inevitablemente, será causante del despido de un número alto de abogados y abogadas.

La ética juega un papel fundamental, y no es la excepción para el jurista. Deberá enfatizarse el rol de los derechos humanos y poner al centro del desarrollo tecnológico a la persona, sus derechos y a la sociedad, sin caer en el juego perverso de que no es compatible la innovación con el pleno respeto a los derechos humanos.

La facilidad de contar con sistemas capaces de analizar a gran velocidad volúmenes de documentación, extraer de ellos pautas o mejores alternativas de actuación ante casos específicos, hace el trabajo de los profesionistas más eficaz, efectivo y eficiente. En la actualidad, los desarrollos de la IA en el ámbito de derecho se han orientado a estas áreas[367]:

- Modelos para la argumentación y la toma de decisiones;
- Clasificación y xtracción de entidades de textos legales;
- Extracción de información de textos legales;
- Creación y planificación de un sistema legislativo
- Automatización de cláusulas para *Smartcontracts*;
- Servicios LegalTech con IA, con gran variedad de áreas: tributario, penal, contratos, laboral, Propiedad intelectual y administrativo.

A continuación, veremos aspectos donde se encuentra presente la refl xión ética y de derechos humanos en la IA:

a) IA y creación de leyes: directrices éticas en Europa. La persona como centro de acción

Hace un par de años, Elon Musk solicitó a los gobernadores estadounidenses reglamentar la inteligencia artificial "antes de que sea demasiado tarde", pues la consideraba una amenaza contra la humanidad. Aunque hay otros líderes de la innovación y las tecnologías que piensan lo contrario, lo cierto es que vivimos en una etapa llena de incógnitas y los estudiosos del derecho deben adecuarse al cambio, y siempre será mejor acercarse con apertura y al principio, que cuando todo esté realizado, sin la perspectiva de derechos humanos y de aspectos tan relevantes

367 FERNÁNDEZ HERNÁNDEZ, Carlos y BOULAT, Pierre, "Inteligencia artificial y derecho. Problemas y perspectivas", 2015. Sitio web: http://noticias.juridicas.com/conocimiento/articulos--doctrinales/10061-inteligencia-artificial- -derecho-problemas-y-perspectivas/ [fecha de consulta: 17 de junio de 2019].

como la privacidad y protección de datos. El interés del jurista, especialmente de quienes asesoran a congresistas y a líderes de gobierno, será fundamental para evitar la sobrerregulación y conducir una estrategia adecuada en el tema. Espero que las estrategias de IA consideren como área prioritaria la de mejorar el sistema jurídico.

Aspectos éticos.

En 1942, Isaac Asimov propuso tres leyes para robos inteligentes: 1) un robot no hará daño a un ser humano ni permitirá que, por inacción, éste sufra daño, 2) un robot obedecerá las órdenes que reciba de un ser humano, a no ser que las órdenes entren en conflicto con la primera ley y 3) un robot protegerá su propia existencia en la medida en que dicha protección no entre en conflicto con las leyes primera y segunda[368]; claro, estas reglas fueron productos de literatura de ciencia ficción. Sin embargo, hoy, existen leyes para regular las acciones o uso de la IA en ciertas regiones en el mundo:

- Estados Unidos el *Administration's Report on the Future of Artificial Intelligence* creado por el Consejo Nacional de Ciencia y Tecnología en 2016[369];
- Resolución del Parlamento Europeo con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica en 2017[370];
- Europa creó el Grupo de Expertos de Alto Nivel en Inteligencia Artificial conformado por 52 especialistas del ámbito académico, empresarial y de la sociedad civil; este grupo empezó a reunirse para debatir un primer borrador de directrices éticas para el desarrollo y uso de la Inteligencia Artificial, este busca garantizar los derechos y valores de europeos. Este grupo, en abril 2019, presentó siete requisitos esenciales para lograr una inteligencia artificial fiable, la cual debe respetar todas las leyes y reglamentos aplicables, así como una serie de requisitos: intervención y supervisión humanas, robustez y seguridad, privacidad y gestión de datos, transparencia, diversidad, no discriminación y equidad, bienestar social y medioambiental y rendición de cuentas[371];
- Recomendaciones del Consejo de Inteligencia Artificial, de la OCD [372];
- Principios de Asilomar para la IA[373];

368 ASIMOV, Isaac, *Runaround*, Street and Smith, New York, 1942.

369 Sitio web: https://obamawhitehouse.archives.gov/blog/2016/10/12/administrations-report-future-artificial-intelligenc [fecha de consulta: 17 de junio de 2019].

370 Sitio web: http://www.europarl.europa.eu/doceo/document/A-8-2017-0005_ES.html [fecha de consulta: 17 de junio de 2019].

371 COMISIÓN EUROPEA, *Inteligencia artificial: La Comisión continúa su trabajo sobre directrices éticas*, Bruselas, 2019. Sitio web: http://europa.eu/rapid/press-release_IP-19-1893_es.pdf, [fecha de consulta: 17 de junio de 2019].

372 OCDE, *Principios de la OCDE sobre la Inteligencia Artificial*, 2019, Sitio web: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 [fecha de consulta: 17 de junio de 2019].

373 Son 23 principios en torno a la Inteligencia artificial, en materia de áreas como: Investigación, Aspectos éticos y valores, entre estos últimos se encuentran tenas como seguridad, transparencia en los fallos, transparencia judicial, valores humanos, responsabilidad, entre otros. Sitio web: https://futureoflife.org/ai-principles/?cn-reloaded= [fecha de consulta: 17 de junio de 2019].

- Estándares éticos aplicables a la IA[374].

b) IA e impartición de justicia

En 2016, un algoritmo desarrollado por las universidades de Sheffiel y Pensilvania predijo con un 79% de acierto el acierto al fallo que los magistrados del Tribunal Europeo de Derechos Humanos emitirían sobre una sentencia[375], esto fue un claro recordatorio o llamado de atención de la estrechez que la IA tiene con la justicia. ¿Se puede utilizar la IA en la impartición de la justicia? No debemos dudarlo, más bien impulsar que esto suceda en nuestros ámbitos y nuestros países. A pesar de los problemas de presupuesto, es sumamente importante impulsar una Estrategia de IA con visión de Estado y un apartado (o por separado si no existe la primera) una hoja de ruta para implementar IA en el sistema jurídico para que facilite y mejore la búsqueda de información, que asista en la labor de impartición de justicia proponiendo estructuras de resoluciones, mediante modelos predictivos en casos concretos y enfatizando el control y supervisión de las personas expertas. Sin embargo, para interpretar la ley es necesario entender la coyuntura, la realidad social, económica, el tiempo en que se aplican, su espíritu y finalidad, esto corresponde a los juristas, juzgadores, decidir sobre la aplicación de las leyes. "No puede reducirse a la impartición fría y mecánica de preceptos sin tener en cuenta el contexto y circunstancias del caso"[376] pero sí, a través de aplicación de IA podremos reducir los grados de subjetividad de los jueces y exigir mayor transparencia en el uso de argumentos y métodos de razonamiento para alcanzar conclusiones basadas en elementos objetivos, ayudando al juez a aplicar su criterio con base en datos aportados por la IA, considerando precedentes en materia de derechos humanos de tribunales y cortes del resto del mundo. Además, la IA ayudará a evidenciar posibles omisiones en la impartición de justicia, es decir, IA permitirá blindar la impartición de justicia de posibles actos de corrupción, complicidad, subjetividades del leal saber y entender o decisiones personales, vicios como la falta de metodología argumentativa y de interpretación o errores involuntarios, entre otros.

Guibourg, Alende y Campanella, afirman que la informática decisoria suele presentarse como una colección de métodos, medios y propuestas para auxiliar al profesionista en su tarea, antes que para reemplazarlo[377].

---

374 *China AI Development Report 2018, op. cit.*

375 UNIVERSITY COLLEGE LONDON, *AI Predicts Outcomes of Human Rights Trials,* 2016. Sitio web: https://www.ucl.ac.uk/news/2016/oct/ai-predicts-outcomes-human-rights-trials [fecha de consulta: 17 de junio de 2019].

376 LÓPEZ, Javier, "Inteligencia Artificial y Justicia", *Byte,* 2017. Sitio Web: https://www.revistabyte.es/actualidad-byte/inteligencia-artificial-justicia/ [fecha de consulta: 17 de junio de 2019]

377 GUIBOURG, Ricardo, ALENDE, Jorge y CAMPANELLA, Elena, *Manual de informática jurídica,* Astrea, Argentina, p. 11.

Como se mencionó anteriormente, China emplea, de forma experimental, IA en procedimientos de impartición de justicia. El proyecto 206 se implementa en Shanghái, el jefe de la Oficina de Reforma Judicial de la Corte Suprema de Justicia china afirmó que la IA cambiará los procedimientos de litigio y la manera en que los jueces deciden. Uno de los tantos usos del proyecto 206 es que si un fiscal desea iniciar un proceso, el sistema le advierte que el 80% de casos similares no han llevado al levantamiento de cargos.[378]

c) LegalTech, la innovación con IA para la abogacía

LegalTech es el uso de tecnología en el ejercicio del derecho, principalmente del ámbito privado. Esto puede identificarse como servicios jurídicos que aprovechan las innovaciones tecnológicas para automatizar su trabajo[379].

El informe *The Future of Legal: El abogado digital* detalla las tendencias tecnológicas en el sector legal: digitalización de la práctica legal (comprende los servicios de negociación y contratación *online*), el abogado empoderado (oferta de herramientas que ofrecen plantillas para crear y modificar documentos legales y *softwares* que revisan los contratos y posibilitan su firma electrónica), cultura del dato (herramientas que optimizan la gestión de datos operativos y control del tiempo), Inteligencia Colectiva (abogados puedan administrar sus proyectos, recursos, clientes y sus relaciones de forma sencilla desde un único lugar que administra todo el flujo de trabajo), *Legal Gig Economy* (se potencia el talento digital de la economía colaborativa del sector jurídico con plataformas digitales de acceso directo entre particulares y expertos legales), *Digital Selling* (buscadores que utilizan algoritmos para ofrecer información sobre temas legales concretos y aplicaciones que utilizan la IA para calificar las consultas de los consumidores y dirigirlas al proveedor apropiado), servicios jurídicos bajo demanda (prestación de servicios legales online dirigida a pymes e individuos con un servicio personalizado)[380].

En el caso mexicano, según Iracelay, si bien existen algunas opciones disponibles en el mercado considerados como "*LegalTech*", no hay información disponible, pública y auditable sobre el grado de conformación y penetración de este sector. El sector

378 PONTAZA, Dulce, *China imparte justicia con ayuda de inteligencia artificial,* 2017. Sitio web: https://tecreview.tec.mx/china-imparte-justicia-ayuda-inteligencia-artificial/ [fecha de consulta: 17 de junio de 2019].

379 VEGA IRACELAY, Jorge e IBARRA, Ernesto, "El ecosistema LegalTech en América Latina. Especial referencia a México", *LegalTech. La transformación digital de la abogacía,* coord. Moisés Barrio Andrés, La Ley, Madrid, 2019, p. 315.

380 GIL PECHARROMÁN, "Xavier, Las tendencias del LegalTech que revolucionarán el sector", *El Economista,* España, 2019. Sitio web: https://www.eleconomista.es/legislacion/noticias/9952560/06/19/Las-tendencias-del-legaltech-que-revolucionaran-el-sector.html [fecha de consulta: 17 de junio de 2019],

mexicano de servicios jurídicos *"LegalTech"* está en etapa inicial y hay aún mucho por hacer.[381] En este sentido, consideramos fundamental la conformación de *hubs*, programas piloto, alianzas; un ecosistema articulado que sirva para impulsar el surgimiento de nuevas *StartUps*, con apoyo del sector público, privado y academia[382].

Ante el constante desarrollo tecnológico que se vive, el derecho siempre debe velar por las garantías de los ciudadanos, colaborar en los procesos de diseño de estrategias innovadoras para aportar en materia de derechos humanos, y poner a la persona, su dignidad y derechos como centro de todo actuar (político, económico, social), pues además de beneficios, la IA trae consigo desafíos e interrogantes en temas como protección en el trabajo, derecho a trabajar, protección de datos, propiedad intelectual, entre otros. Esta evolución tecnológica no sólo requiere un papel activo de gobierno y juristas, sino de un alto criterio moral de las personas que diseñan estas nuevas formas de tecnología. Con profesionistas que velen por la ética y los derechos de las personas, la IA será la herramienta clave para el jurista del futuro.

Como se ha visto, la importancia de una gobernanza multidisciplinaria, donde distintos sectores se coordinen para el uso de IA en sistemas jurídicos, y velar por la ética y los derechos de la persona como base de toda acción, puede permitir a los profesionistas resultados efectivos y eficientes a favor de los ciudadanos.

DESARROLLO DE HABILIDADES Y FORMACIÓN EN LOS OPERADORES JURÍDICOS

En este punto, es importante abordar brevemente el ámbito del capital humano. Cuál es el valor del desarrollo de nuevas habilidades y cómo un Estado se prepara para afrontar los retos y desafíos que trae consigo la IA y cómo esto se aplicará al mundo del Derecho.

Cada año más estudiantes de la carrera de derecho entran al mundo laboral con nuevas realidades, en donde la tecnología está marcando el camino y dónde probablemente las leyes u ordenamientos que estudiaron están en desuso o no aplican a la práctica, y lamentablemente muchos no encontrarán empleo porque la distribución de oferta y demanda no es favorable. Así, es necesario que estas nuevas generaciones de estudiantes y futuros operadores jurídicos dimensionen el impacto de la cuarta revolución industrial, de la era digital y sus impactos en la sociedad y por ende en el Derecho.

Un primer paso será actualizarse al respecto se actualicen y puedan sumarse al cambio y aprovechar las bondades que trae consigo la cuarta revolución industrial.

381 VEGA IRACELAY, Jorge e IBARRA, Ernesto, *op cit.*, p. 325.

382 Véase el caso de Singapur, en relación con el ecosistema para impulsar el crecimiento del sector LegalTech. Sitio web:https://lawtech.asia/legal-technology-in-singapore/

Hoy más que nunca tenemos acceso a un sinnúmero de fuentes de información gracias a Internet, la cultura de aprendizaje autodidacta crece cada día por circunstancias de tiempo, espacio, laborales, o porque estudiar puede no ser asequible para todos.

El esfuerzo es, y debe ser, compartido entre estudiantes, profesores, investigadores y facultades de Derecho. Ese pequeño ecosistema debe integrarse y abrir nuevas oportunidades acordes a la realidad de la era digital que ya desde hace algunos años están viviendo los profesionales al concluir su carrera. Este texto, busca motivar a los diferentes actores del sector legal en el ámbito académico, y en general a los llamados operadores jurídicos, a impulsar la innovación jurídica, desde todas las trincheras, desde los primeros semestres de la carrera, hasta la implementación de IA en las Cortes supremas.

RECOMENDACIONES

Recomendaciones para estudiantes de derecho

Les invito a cambiar el chip, les propongo pensar en que hoy pueden iniciar la transformación del sistema jurídico aún sin concluir su carrera. Vale la pena preguntar a los profesionales egresados de Derecho, en qué porcentaje resulta valioso memorizar textos legales, por tanto; no permitir que ese sea el método de sus profesores. También, les motivo a ser más autodidactas, a viajar cuanto puedan, estudiar inglés, observar las necesidades de la sociedad y sus vicios, e iniciar con prácticas profesionales -aún sin paga- desde que inician su carrera; la vida de jurista no inicia cuando se obtiene el título. Les recomiendo: Aprendan sobre habilidades digitales, solicitar a sus facultades la materia de "Derecho informático o Derecho de las TIC", tomen cursos o clases relacionadas al pensamiento computacional, no despreciar las matemáticas, leer mucho -incluir temas de la evolución e impacto de las TICs en la sociedad, estar atentos a cómo avanza el mundo y la profesión legal en otros países; desarrollar espíritu emprendedor en el mundo del derecho y trazar su propio camino en su carrera.

Ustedes, los estudiantes de Derecho de hoy y del futuro, habrán nacido inmersos en la era digital, deben aprovecharla, porque además; muchos de las labores legales serán automatizadas.[383]

Los estudiantes de derechos deben informarse sobre futuras prácticas de la economía digital y las tecnologías emergentes como: realidad virtual, robótica e inteligencia artificial, *blockchain, fintech, LegalTech*, drones, telecomunicaciones y 5G,

383 Si bien los algoritmos son efectivos para procesar datos, son más débiles en áreas que requieren inteligencia emocional y juicio humano, como lo es negociar acuerdos, mediar disputas o hacer juicios éticos. W., Daniel y JR., Linna, "Training Lawyers to Assess Artificial Intelligence and Computational Technologies", *LegalTech Lever,* 2018. Sitio web: https://www.legaltechlever.com/2018/09/training-lawyers-assess-artificial-intelligence-computational-technologies/ [fecha de consulta: 17 de junio de 2019].

etc.

Recomendaciones para profesores de derecho y Facultades de Derecho

Los profesores tienen una gran responsabilidad hoy más que nunca, deben enseñar derecho dejando claro a los alumnos que enseñar derecho no es "memorizar o conocer el texto legal", desarrollar en ellos la capacidad de pensamiento crítico, enseñar con casos reales (sentencias y resoluciones), impulsarles al trabajo colaborativo y multidisciplinario, despertar en ellos el espíritu emprendedor, ejemplificar el uso de argumentos y presencia de los principios de Derecho y Derechos Humanos. Dar el ejemplo de innovación, no necesariamente tecnológica. Se debe alimentar la curiosidad de los estudiantes de derecho con herramientas tecnológicas, gestión de proyectos, mejora de procesos, uso del análisis de datos de la investigación empírica.

Las Facultades de Derecho son fundamentales para la innovación del Estado de Derecho de un país, para la transformación del perfil del jurista, y no están exentas del impacto de las TICs en la enseñanza aprendizaje, donde cada vez más personas prefieren aprender a través de Internet. Así, las facultades deben emprender procesos de innovación interna, para que le muestren a los alumnos la cultura de innovación, mejorar los servicios y hacerles vivir experiencia más eficiente. Las facultades deberán motivar a profesores e investigadores a impulsar el espíritu emprendedor en la comunidad estudiantil, impulsar el uso de herramientas tecnológicas colaborativas, y motivar a profesores y alumnos a que sean disruptivos en enseñanza aprendizaje. También deberán rediseñar lo necesario -metodología, infraestructura y currículo- para que todas las materias de la carrera consideren los aspectos relativo a la cuarta revolución industrial, a lo que ayudará en gran medida, contar con programas de Derecho y TIC, y diferentes opciones y niveles de programas relativos al impacto de las tecnologías emergentes. Lo anterior no significa demeritar el estudio de otras vertientes, sino agregar un componente digital a esas materias, a partir del hecho de que las TIC son transversales y están ya transformando las actividades sobre las cuales las diversas ramas del derecho trabajan, así complementarán el conocimiento del impacto de estas tecnologías en la práctica del derecho; además de las cuestiones éticas relacionadas.[384] [385]

Las facultades en todo el mundo deben subirse a la ola tecnológica y ofrecer a futuros y actuales estudiantes la opción de entender los desafíos en materia de

384 Entre varios ejemplos, la Universidad de Ottawa ya cuenta con un Centro de derecho, tecnología y sociedad, donde ofrecen a estudiantes de pregrado o posgrado información acerca de cómo la IA está impactando las sociedades y cómo los profesionistas del derecho pueden hacer frente a estos cambios Sitio web: https://techlaw.uottawa.ca/ [fecha de consulta: 17 de junio de 2019],

385 Otros ejemplos son la Universidad de Toronto, la Universidad Hebrea de Jerusalén, La Universidad de Monash: https://www.law.utoronto.ca/events/technology-and-future-law-lawyering-and-legal-education-conference , https://en.law.huji.ac.il/event/ai-law-and-policy y http://www.monash.edu/pubs/2019handbooks/units/LAW5649.html [fecha de consulta: 17 de junio de 2019],

tecnologías emergentes, y aspectos como: propiedad intelectual, ética, transparencia, privacidad y datos personales. Además, las facultades deben refutar los miedos y afirmaciones acerca de las consecuencias catastróficas que trae la IA en el derecho (el reemplazo de abogados por robots, por ejemplo). Las facultades de Derecho tienen en sus manos la oportunidad de enseñar que la tecnología es aliada del derecho y que el Derecho no siempre va de tras de la tecnología, pues el Derecho bien aplicado (no a partir del texto legal) puede resistir cambios tecnológicos e impactos en la sociedad.

Recomendaciones para profesionales del derecho y autoridades

Profesionales del Derecho u operadores jurídicos, como fedatarios, servidores públicos de los diferentes poderes, que trabajan con el derecho, y especialmente juzgadores deben iniciar proyectos de modernización considerando tecnologías emergentes, sobretodo IA, ma*chine learning* y *blockchain* en su ejercicio diario. Esto traerá como consecuencia: más productividad, eficacia, ahorros de tiempo y dinero y mayor personalización al cliente. A quien ha tenido el valor de emprender en sector *LegalTech* le invito a que transmita ese valor y su experiencia con los estudiantes, de tal forma cambiará la cultura y impulsará a más abogados a ser emprendedores. A las autoridades y gremios de fedatarios, abogados y otros operadores, les animo a impulsar y fomentar proyectos de impacto nacional en materia de innovación del sistema jurídico, donde los poderes, principalmente las Cortes Supremas y órganos de justicia federal lideren proyectos para hacer un Derecho más eficiente, donde se involucren sector privado, congresistas, empresas de tecnologías, investigadores y facultades. Solo así, lograremos elaborar una estrategia de innovación con IA que mejore considerablemente el Derecho (la forma de hacer leyes, la eficacia en los diferentes procedimientos, mejorar cultura de respeto a la ley, más eficiente sistema de impartición de justicia, poner énfasis en cómo mediante IA se puede resolver el rezago de expedientes por resolver y que ello impacte en derechos humanos, especialmente en los casos de mujeres privadas de su libertad.

BIBLIOGRAFÍA

ASIMOV, Isaac, *Runaround*, Street and Smith, New York, 1942.

BUGHIN, Jaques, SEONG, Jeongmin, MANYKA, James, CHUI, Michael, JOSHI, Raoul, *Notes from the AI Frontier. Modeling the Impact of AI on the World Economy,* McKinsey Global Institute, 2018.

China AI Development Report 2018, Institute for Science and Technology Policy at Tsinghua University. Sitio web: http://www.sppm.tsinghua.edu.cn/eWebEditor/

UploadFile/China_AI_development_report_2018.pdf

COMISIÓN EUROPEA, *Inteligencia artificial: La Comisión continúa su trabajo sobre directrices éticas,* Bruselas, 2019. Sitio web: http://europa.eu/rapid/press-release_IP-19-1893_es.pdf, [fecha de consulta: 17 de junio de 2019].

Congreso de la Unión. "Inteligencia artificial" Oficina de información científica y tecnológica para el para el Sitio Web: https://www.foroconsultivo.org.mx/INCyTU/documentos/Completa/INCYTU_18- 012.pdf [fecha de consulta: 17 de junio de 2019].

DE CENDRA, Javier, "El potencial de LegalTech en México: por qué es importante mejorar la penetración de la tecnología en el sistema legal", *El Economista,* México, 2018. Sitio web: https://www.eleconomista.com.mx/opinion/El-potencial-de-LegalTech-en-Mexico-porque-es-importante-acelerar-la-penetracion-de-la-tecnologia-en-el-sistema-legal-20180716-0085.html, [fecha de consulta: 17 de junio de 2019].

DÍAZ, Elías. *Estado de Derecho y sociedad democrática,* Madrid, Taurus ediciones, 1981, o. 31.

FERNÁNDEZ HERNÁNDEZ, Carlos y BOULAT, Pierre, "Inteligencia artificial y derecho. Problemas y perspectivas", 2015. Sitio web: http://noticias.juridicas.com/conocimiento/articulos-doctrinales/10061-inteligencia-artificial-y-derecho-problemas-y-perspectivas/

GIL PECHARROMÁN, "Xavier, Las tendencias del LegalTech que revolucionarán el sector", *El Economista,* España, 2019. Sitio web: https://www.eleconomista.es/legislacion/noticias/9952560/06/19/Las-tendencias-del-legaltech-que-revolucionaran-el-sector.html [fecha de consulta: 17 de junio de 2019],

GUIBOURG, Ricardo, ALENDE, Jorge y CAMPANELLA, Elena, *Manual de informática jurídica,* Astrea, Argentina, p. 11.

HALL, Rachel, "Ready for Robot Lawyers? How Students Can Prepare for the Future of Law", *The Guardian,* London, 2017. Sitio web: https://www.theguardian.com/law/2017/jul/31/ready-for-robot-lawyers-how-students-can-prepare-for-the-future-of-law [fecha de consulta: 17 de junio de 2019],

HUTSON, Matthew, *Artificial Intelligence prevails at predicting Supreme Court decisions,* 2017. Sitio web: https://www.sciencemag.org/news/2017/05/artificial-intelligence prevails-predicting-supreme-court-decisions [fecha de consulta: 17 de junio de 2019).

LIMÓN, Jaime, "Inteligencia artificial en procesos judiciales", *El Economista,* 2019.

LÓPEZ, Javier, "Inteligencia Artificial y Justicia", *Byte,* 2017. Sitio Web: https://www.revistabyte.es/actualidad-byte/inteligencia-artificial-justicia [fecha de consulta: 17 de junio de 2019].

MARTÍNEZ BAHENA, G., "Inteligencia artificial y su aplicación al derecho" *Alegatos. Revista jurídica,* Universidad Autónoma Metropolitana, México, 2012, p.833

MOREL RAMOS, Jorge, *LegalTech en España, muy primeros pasos*. Sitio web: https://terminosycondiciones.es/2016/07/20/legaltech-espana-mucho/ [fecha de consulta: 17 de junio de 2019].

OCDE, OECD Employment Outlook 2019. The Future of Work, OCDE, Berlín, 2019, p. 3.

One Hundred Year Study on Artificial Intelligence (AI100), Stanford University, 2016. Sitio web: https://ai100.stanford.edu/ [fecha de consulta: 17 de junio de 2019)

ONU, *La Inteligencia Artificial como herramienta para acelerar el progreso de los ODS,* ONU Noticias, 2017.

PONTAZA, Dulce, *China imparte justicia con ayuda de inteligencia artificial,* 2017. Sitio web: https://tecreview.tec.mx/china-imparte-justicia-ayuda-inteligencia-artificial/ [fecha de consulta: 17 de junio de 2019].

SCHWAB, Klaus, *La cuarta revolución industrial*, World Economic Forum y DEBATE, 2016, p.11.

Sitio web: https://techlaw.uottawa.ca/ [fecha de consulta: 17 de junio de 2019],

Sitios web: https://www.law.utoronto.ca/events/technology-and-future-law-lawyering-and-legal-education-conference , https://en.law.huji.ac.il/event/ai-law-and-policy y http://www.monash.edu/pubs/2019handbooks/units/LAW5649.html [fecha de consulta: 17 de junio de 2019],

Sitio web: https://link.springer.com/journal/10506 [fecha de consulta: 17 de junio de 2019].

Sitio web: https://www.larepublica.co/alta-gerencia/el-gobierno-de-colombia-le-puesta-al-desarrollo-de-la-inteligencia-artificial-2841835 [fecha de consulta: 17 de

junio de 2019).

Sitio web: https://obamawhitehouse.archives.gov/blog/2016/10/12/administrations-report-future-artificial-intelligenc [fecha de consulta: 17 de junio de 2019].

Sitio web: http://www.europarl.europa.eu/doceo/document/A-8-2017-0005_ES.html [fecha de consulta: 17 de junio de 2019].

TREJO CAMPOS, Francisco, "Los desafíos de la inteligencia artificial en el sistema internacional", *Foreign Affairs Latinoamérica,* 2019.

TREBILCOCK, M. y DANIELS, R., *Rule of Law reform and development,* UK, Edward Elgar, 2008, p. 56.

UNIVERSITY COLLEGE LONDON, *AI Predicts Outcomes of Human Rights Trials,* 2016. Sitio web: https://www.ucl.ac.uk/news/2016/oct/ai-predicts-outcomes-human-rights-trials [fecha de consulta: 17 de junio de 2019].

VEGA IRACELAY, Jorge e IBARRA, Ernesto, "El ecosistema LegalTech en AMérica Latina. Especial referencia a México", *LegalTech. La transformación digital de la abogacía,* coord. Moisés Barrio Andrés, La Ley, Madrid, 2019, p. 315.

VILLAR BORDA, Luis, "Estado de derecho y Estado social de derecho", *Revista Derecho del Estado,* n.20, 2007, p. 74.

W., Daniel y JR., Linna, "Training Lawyers to Assess Artificial Intelligence and Computational Technologies", *LegalTech Lever,* 2018. Sitio web: https://www.legaltechlever.com/2018/09/training-lawyers-assess-artificial-intelligence-computational-technologies/ [fecha de consulta: 17 de junio de 2019],

WORLD JUSTICE PROJECT. Sitio web: http://worldjusticeproject.org/ what-rule-law [fecha de consulta: 17 de junio de 2019).

WORLD JUSTICE PROJECT MÉXICO. Sitio web: https://worldjusticeproject.mx/estado-de-derecho/ [fecha de consulta: 17 de junio de 2019).

WORLD JUSTICE PROJECT. Sitio web: https://worldjusticeproject.org/sites/default/files/documents/M_xico%20%28Spanish%29_0.pdf [fecha de consulta: 17 de junio de 2019).

WORLD JUSTICE PROJECT, *Rule of Law Index 2019,* Washington DC, 2019. Sitio web:

https://worldjusticeproject.org/sites/default/files/documents/WJP-ROLI-2019-Single%20Page%20View-Reduced_0.pdf [fecha de consulta: 17 de junio de 2019).

TIEMPO DE ALGORITMOS: ALGOCRACIA Y DERECHOS CIVILES Y POLÍTICOS

Eje temático: Inteligencia artificial: riesgos y desafíos jurídico

Autora:
Laura Nahabetián Brunet
Doctora en Derecho y Ciencias Sociales
Universidad Mayor de la República Oriental del Uruguay

ABSTRACT
Hoy la vida se desarrolla en el marco de la "*era de las decisiones algorítmicas*".
La utilización de algoritmos plantea desafíos enormes no solo para el área de política específica en la que se operan, sino también para la sociedad en general. La pregunta inmediata es ¿cómo salvaguardar los derechos humanos y la dignidad humana frente a las tecnologías que cambian rápidamente?
El derecho a la vida, el derecho a un juicio justo y la presunción de inocencia, el derecho a la privacidad y la libertad de expresión, los derechos de los trabajadores, el derecho a elecciones libres, incluso el propio Estado de Derecho se ven afectados. Responder a los desafíos asociados con los "algoritmos" utilizados por el sector público y privado, en particular por las plataformas de Internet, es actualmente una de las preguntas más debatidas, en tanto tiene implicancias en las bases mismas de los derechos que constituyen las bases de nuestra identidad nacional: la personalidad humana y la forma republicana de gobierno.
En este sentido, se analiza el fenómeno denominado "Algocracia" así como la incidencia que los algoritmos tienen en los derechos civiles y políticos que se verifican afectados directamente por éstos y que por tanto, de alguna manera, comprometen la democracia.

TIEMPO DE ALGORITMOS:

ALGOCRACIA Y DERECHOS CIVILES Y POLÍTICOS

Laura Nahabetián Brunet[386]

386 Doctora en Derecho y Ciencias Sociales egresada de la Facultad de Derecho de la Universidad Mayor de la República Oriental del Uruguay.

Profesora adjunta de Derecho Informático y Coordinadora del Centro de Derecho Informático de la misma Facultad.

Profesora adjunta de Derecho Constitucional en la Facultad de Derecho de la Universidad Católica del Uruguay y Profesora adjunta de Ética Profesional en la Facultad de Ingeniería de la Universidad de la Empresa.

Doctora © en Ciencias Jurídicas por la Universidad Católica Argentina.

Asesora en el Parlamento Nacional de la República

I. INTRODUCCIÓN

Hoy la vida se desarrolla en el marco de la "*era de las decisiones algorítmicas*".

Los hay para todo, algoritmos que colaboran en el desenvolvimiento de descubrimientos de carácter científico, que colaboran en conocer quién es más factible que evada impuestos, algoritmos que colaboran en la formación de parejas, y un largo etcétera, hasta hace relativamente poco impensados.

A partir de la gigantesca evolución y revolución en el tratamiento de datos, sumado al internet de las cosas, indudablemente la tendencia a la colaboración de los algoritmos y aún más, a la toma de decisiones por su parte, solo pareciera que tenderá a crecer en el futuro cercano.

¿Qué información se pone a disposición de las personas en las noticias que se presentan en las redes sociales? ¿En base a qué se determina el perfil de riesgo crediticio de una persona o qué perfiles ofrecen las mejores oportunidades para obtener un seguro de salud o un empleo, o incluso para que una persona sea considerada un posible delincuente o hasta un terrorista?

Las técnicas automatizadas de procesamiento de datos, como son los algoritmos, no solamente permiten a los usuarios de Internet buscar y acceder a la información, sino que cada vez más se utilizan en los diferentes procesos de toma de decisiones, que antes estaban enteramente en manos de seres humanos.

Los algoritmos pueden ser utilizados para preparar decisiones de carácter netamente humanas o para tomarlas inmediatamente a través de medios automatizados. De hecho, los límites entre la toma de decisiones humana y la automática se difuminan, lo que da como resultado la noción de "toma de decisiones cuasi o semiautomática".

Por lo tanto, la utilización de algoritmos plantea desafíos enormes no solo para el área de política específica en la que se operan, sino también para la sociedad en general. La pregunta inmediata es ¿cómo salvaguardar los derechos humanos y la dignidad humana frente a las tecnologías que cambian rápidamente?

El derecho a la vida, el derecho a un juicio justo y la presunción de inocencia, el derecho a la privacidad y la libertad de expresión, los derechos de los trabajadores, el derecho a elecciones libres, incluso el propio Estado de Derecho se ven afectados. Responder a los desafíos asociados con los "algoritmos" utilizados por el sector público y privado, en particular por las plataformas de Internet, es actualmente una de las preguntas más debatidas, en tanto tiene implicancias en las bases mismas de los derechos que constituyen las bases de nuestra identidad nacional: la personalidad humana y la forma republicana de gobierno.

Dirección electrónica: lnahabetian@gmail.com

Existe una percepción cada vez mayor de que "el software se está comiendo el mundo"[387], ya que los seres humanos sienten que no tienen control sobre los sistemas técnicos que los rodean y no los comprenden. Y esto es ciertamente desconcertante, aunque no necesariamente es negativo, siempre que las personas sean capaces de aquilatar adecuadamente sus implicancias.

Se trata, en definitiva, de un subproducto de esta era de la vida moderna en la que los desarrollos económicos y tecnológicos globalizados producen una gran cantidad de artefactos técnicos impulsados por software y "objetos codificados [388] que incorporan capacidades clave de toma de decisiones relevantes para los derechos humanos.

En función de lo anterior, es fundamental realizar algunos análisis vinculados con la utilización de los algoritmos con base en la toma de decisiones en la órbita pública y política, en tanto, a priori, y como conclusión anticipada, ésta se presenta como problemática.

De hecho, el elemento sustantivo que está presente en esta consideración tiene relación con la legitimidad en la toma de las decisiones; ¿es aceptable desde el punto de vista de la legitimidad que la toma de decisiones esté basada en algoritmos?

Stefano Rodotá afirmaba que la "utilización de la tecnología puede contribuir a establecer una política que rechaza los problemas difíciles, se aísla de la sociedad y cambia la naturaleza de la relación entre el ciudadano y el Estado. Y una política prisionera de la tecnología puede dar la impresión de mayor eficiencia, pero hace más débil la democracia"[389].

Esta afirmación remite al actual y creciente fenómeno de la denominada algocracia.

II. ALGOCRACIA

Se trata de un concepto con un importante potencial de engaño por lo que es necesario especificarlo concretamente.

Algocracia implica un particular sistema de gobernanza, organizado y estructurado en base a algoritmos programados por una computadora. Es decir que se trata de un sistema, en el que se utilizan algoritmos para recopilar, clasificar y organizar datos a partir de los que normalmente se toman las decisiones y, de esta forma, ayudar en su procesamiento y comunicación a través de sistemas de gobierno determinados.

Así, los algoritmos estructuran y limitan las formas en que las personas dentro de esos sistemas interactúan entre sí, con los datos pertinentes y la comunidad afectada

387 Andreessen, M., "*Why Software Is Eating The World*", en Wall Street Journal, edición del 11 de agosto de 2011. Disponible en: http://www.wsj.com/articles/SB10001424053111903480904576512250915629460 (fecha de consulta: 28/07/2019)

388 Kitchin, R. y Dodge, M., *Code/Space Software and Everyday Life*, MIT Press, 2011.

389 Rodotá, S., "Democracia y Protección de Datos", en Pensieri. Disponible en: http://pensieriworld.blogspot.com/2010/12/stefano-rodota_4105.html (fecha de consulta: 30/10/2018)

por ellos. Esto puede hacerse mediante algoritmos de organización de la información de manera tal que incluso pueden forzar cambios en la estructura del entorno físico en el que las personas operan.

Estos sistemas pueden ser automatizados o semi-automatizados, pueden verificar o no, supervisión y aporte de personas.

Por tanto, puede afirmarse que la algocracia es un sistema en el que los algoritmos pueden estructurar y restringir las formas en que las personas actúan. Los límites entre estos sistemas no son precisos y a menudo, se integran y superponen, lo que es sustantivo si se considera contextualmente, que los sistemas algocráticos de toma de decisiones pueden integrarse con los sistemas de toma de decisiones jurídico-burocráticos preexistentes.

En definiti a, es el fenómeno por el cual los algoritmos se apoderan de los sistemas públicos de toma de decisiones. Más precisamente, el término "algocracia" puede usarse para describir sistemas de toma de decisiones en los que algoritmos codificados por computadora estructuran y restringen la forma en que los seres humanos interactúan con estos procesos de toma de decisiones.

III. EL PROBLEMA DEL ALAMBRE DE PÙAS INVISIBLE

La tecnología actual hace posible que casi todos los movimientos de las personas, particularmente aquellos que se desenvuelven "en línea", sean monitoreados, rastreados y procesados.

De hecho es posible que las personas, auto utilicen esta información, como un mecanismo autoexperimental generando diversas métricas y utilizando esa información para mejorar sus dietas, aumentar su productividad y un largo etcétera. Y para muchas personas este es un esfuerzo muy valioso.

Pero, al mismo tiempo que la información es factible de ser utilizada por las personas, también lo es por parte de los gobiernos y las empresas que pueden aprovechar estas tecnologías de seguimiento y procesamiento de datos y utilizarlas para lograr sus fines particulares.

De hecho, los gobiernos pueden hacerlo para controlar la actividad terrorista, rastrear fraudes, evitar la evasión fiscal, entre otras finalidades. Las empresas pueden hacerlo para rastrear las preferencias de los consumidores, crear publicidad dirigida y manipular las decisiones de compra de los consumidores, entre un sinfín de posibilidades.

Incluso las personas podrían pensar que esto es positivo.

¿Quién no quiere detener el terrorismo, acabar con la evasión tributaria y tener experiencias de compra satisfactorias?

Sin embargo, esto tiene un lado no tan positivo.

Es imprescindible analizar el papel de la minería de datos en la creación de un sistema de regulación algorítmica, en el que las decisiones personales son "empujadas" en direcciones particulares por potentes algoritmos de procesamiento de datos. Esto es preocupante porque la base racional de estos algoritmos no es transparente.

Gracias a los teléfonos inteligentes es posible conocer cada vez que se pretende realizar alguna acción incorrecta por lo que no sería necesario efectuar el cálculo moral por cuenta propia sino que los algoritmos del sistema podrían realizar el cálculo moral por sí mismos. Las personas asumen el papel de máquinas de información que alimentan el complejo tecnoburocrático con sus propios datos. ¿Y por qué no, si se promete aire más limpio o vidas más largas y más seguras a cambio de un poco de información?

Es decir que los algoritmos relevan los desordenados procesos de toma de decisiones humana. Los ciudadanos se sienten comprometidos con los algoritmos que les aseguran eficiencia, efectividad, ahorro de tiempo, y a pesar de no estar seguros de cómo funcionan, como de alguna manera sienten temor de descuidar su guía, los mantienen y alimentan. Esto crea una especie de prisión de "*alambre de púas invisible*" que limita el alcance de desarrollo intelectual y moral, así como las propias vidas en general.

Establecido lo anterior, en términos de pluralismo democrático, es fundamental identificar una serie de preocupaciones de derechos humanos provocadas por el creciente papel de los algoritmos en la toma de decisiones. Dependiendo de los tipos de funciones realizadas por los algoritmos y el nivel de abstracción y complejidad del procesamiento automatizado que se utiliza, su impacto en el ejercicio de los derechos humanos variará.

¿Quién es responsable cuando se infringen los derechos humanos sobre la base de decisiones preparadas algorítmicamente? ¿La persona que programó el algoritmo, el operador del algoritmo o la persona que implementó la decisión? ¿Hay una diferencia entre tal decisión y una decisión tomada por las personas? ¿Qué efectos tiene sobre la forma en que se ejercen y garantizan los derechos humanos, incluidos los principios vinculados con el Estado de Derecho y los procesos jurisdiccionales?

Los desafíos relacionados con el impacto de los algoritmos en los derechos humanos y las técnicas automatizadas de procesamiento de datos crecerán; y las dificultades crecen a medida que los sistemas relacionados se vuelven cada vez más complejos e interactúan con los resultados de otros en formas que se vuelven progresivamente impenetrables para la mente humana.

IV. CONSTRUCCIONES SOCIALES A PARTIR DE ALGORITMOS

Si bien la toma de decisiones algorítmica es cada vez más adepta a reemplazar la toma de decisiones humana, los elementos importantes (como la discreción) de los procesos de toma de decisiones no se pueden automatizar y, a menudo, se pierden cuando los procesos de toma de decisiones se automatizan[390]. Sin juzgar su respectiva "calidad", los procesos de toma de decisiones de los seres humanos y los algoritmos son fundamental y categóricamente diferentes, cometen diferentes errores y pueden tener diferentes resultados y, por lo tanto, consecuencias.

Si bien la sociedad y los gobiernos tienen una experiencia considerable en la comprensión de la toma de decisiones humana y sus fracasos, solo están empezando a comprender las fallas, limitaciones y límites de la toma de decisiones algorítmica.

Un desafío clave es la percepción frecuente de que los algoritmos son capaces de crear predicciones neutrales, no discriminatorias e independientes sobre eventos futuros.

Este desafío, sin embargo, se relaciona menos con los algoritmos como herramienta y más con su diseño, así como con la percepción e interpretación humana de su implementación y resultados.

Por lo tanto, la clave para promover el cumplimiento de los derechos humanos en el uso de algoritmos puede ser entender qué algoritmos pueden y no pueden lograrse y no dejar que su uso sea dictado simplemente por consideraciones de eficiencia o eficacia. Nuevamente el imperativo tecnológico interpela profundamente y es imprescindible que un humanismo consciente siente las nuevas bases de los desarrollos éticos y jurídicos del mundo tecnológico.

Tradicionalmente, los desarrolladores han programado algoritmos a mano "para procesar y transformar los datos de entrada en una salida deseada, en base a cálculos específicos [391]. Sin embargo, con la evolución tecnológica, los sistemas sociotécnicos como los algoritmos son cada vez más opacos. Esto no es técnicamente necesario, sino más bien una elección de diseño frecuente que conduce a sistemas algorítmicos cuyo funcionamiento interno no se puede hacer transparente o responsable ante el mundo exterior. Incluso cuando una persona toma una decisión formal, por ejemplo, la decisión de eliminar cierto contenido de una plataforma de medios sociales ésta a menudo puede ser conducida a una decisión preparada algorítmicamente, no teniendo efectivamente el tiempo, contexto o habilidades para tomar una decisión adecuada en el caso individual.

Por lo tanto, si bien puede parecer lógico hacer una distinción entre la toma de decisiones totalmente automatizada y la toma de decisiones semiautomatizada, en la práctica los límites entre ambos son borrosos.

390 Spiekermann, S., *Ethical IT Innovation: A Value-Based System Design Approach*, CRC Press, 2015.

391 Gillespie, T., "*The Relevance of Algorithms*" en Media technologies: Essays on communication, materiality, and society, Cambridge Mass, MIT Press, 2014, págs. 167 - 194.

En ninguno de los dos casos, una persona podrá proporcionar un argumento razonado por el cual una determinada decisión debe tomarse en el caso específico, lo que necesariamente repercute en el derecho del interesado de obtener un recurso efectivo contra una violación de sus derechos humanos.

Cabe señalar que los algoritmos descritos aquí no existen de manera significativa sin la interacción con las personas.

En efecto, las construcciones matemáticas o computacionales no tienen por sí mismas un impacto adverso sobre los derechos humanos, pero sí su implementación y aplicación a la interacción humana. Las tecnologías, en su aplicación a la interacción humana, son construcciones profundamente sociales con implicaciones políticas considerables. Si bien un software de toma de decisiones, por ejemplo, puede ser "sesgado pero ambivalente"[392], no tiene sentido sin un sistema social a su alrededor que proporcione significado e impacto.

Por lo tanto, es demasiado simple culpar al algoritmo o sugerir que ya no se debe recurrir a las computadoras ni a la informática. Más bien, es la construcción social y las normas y valores específicos incorporados en los algoritmos que deben cuestionarse y criticarse.

De hecho, no son los algoritmos en sí, sino los procesos de toma de decisiones en torno a los algoritmos los que deben examinarse en términos de cómo afectan a los derechos humanos.

V. IMPACTOS DE LOS ALGORITMOS EN LOS DERECHOS HUMANOS

Las reservas contra los algoritmos y las técnicas automatizadas de procesamiento de datos generalmente apuntan a su opacidad e imprevisibilidad.

Sin embargo, más allá de estas preocupaciones generales, existe una creciente conciencia de que los derechos humanos se ven particularmente afectados.

En efecto, ya hay evidencia de que el uso de algoritmos puede dar lugar a violaciones de derechos o puede minar el disfrute efectivo de algunos derechos humanos.

1. LIBERTAD DE EXPRESIÓN

La operación de algoritmos y técnicas de procesamiento de datos tiene efectos muy importantes en el derecho a la libertad de expresión, que incluye el derecho a recibir e impartir información.

392 McCarthy, D., "*Open Networks and the Open Door: American Foreign Policy and the Narration of the Internet*", en Foreign Policy Analysis 7, 2011, págs. 89 - 111.

Si bien los efectos positivos de los algoritmos de búsqueda y los motores de búsqueda para el derecho humano a la libertad de expresión se han mencionado repetidamente, su potencial para dañar la libertad de información y la libertad de expresión de personas, grupos y segmentos enteros de sociedades se analiza cada vez más[393]. Las preocupaciones surgen no solo con respecto al derecho individual a la libertad de expresión sino también con respecto al objetivo sustancial de creación de un entorno propicio para un debate público pluralista que sea igualmente accesible e inclusivo para todos.

Los motores de búsqueda actúan como guardianes cruciales para las personas que desean buscar, recibir o impartir información. Es menos probable que el contenido que no está indexado o clasificado por un motor de búsqueda en Internet llegue a una gran audiencia o sea visto en absoluto. Como resultado, el uso de algoritmos puede conducir a la fragmentación de la esfera pública y a la creación de "cámaras de eco" que favorecen solo a ciertos tipos de medios de comunicación, lo que aumenta los niveles de polarización en la sociedad que pueden poner en grave peligro la cohesión social.

El algoritmo de búsqueda también podría estar sesgado hacia ciertos tipos de contenido o proveedores de contenido, por lo que se corre el riesgo de afectar valores relacionados, como el pluralismo y la diversidad de los medios de comunicación. Este es particularmente el caso en el contexto de los motores de búsqueda en línea dominantes[394].

Las predicciones algorítmicas de las preferencias de los usuarios implementadas por las plataformas de las redes sociales guían no solo lo que los anuncios pueden ver, sino que también personalizan los resultados de búsqueda y dictan la forma en que se organizan las fuentes de las redes sociales, incluidas las fuentes de noticias.

Dado el tamaño de plataformas como Google o Facebook, su centralidad para muchas experiencias de Internet como una esfera casi pública y su capacidad para amplificar masivamente ciertas voces, hace que esto no sea de manera alguna un asunto trivial.

Por el contrario, la personalización de la información que reciben los usuarios en función de sus preferencias e intereses predichos puede crear "burbujas de filtro" y puede comprometer sustancialmente la libertad de expresión, que incluye el derecho a la información. Si bien las burbujas de filtro y las cámaras de eco son un concepto

393 Informe 2016 del Relator Especial de las Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y expresión, David Kaye, en el trigésimo segundo período de sesiones del Consejo de Derechos Humanos (A/HRC/32/38), donde señala que los algoritmos del motor de búsqueda determinan lo que los usuarios ven y en qué lugar de prioridad, pudiendo en consecuencia manipularse a efectos de restringir o priorizar su contenido.

394 Pasquale, F., *"Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power"*, en Social Science Research Network, 2016. Disponible en: https://papers.ssrn.com/abstract=2779270 (Fecha de consulta: 28/07/2019).

plausible y, por lo tanto, ampliamente discutido, debe notarse que la evidencia empírica de su existencia en Europa es mixta. Las personas generalmente se informan utilizando un repertorio de fuentes, no solo a través de las redes sociales o búsquedas en Internet.

Es imprescindible considerar, asimismo, que cualquier medida que bloquee el acceso al contenido mediante el filtrado o su eliminación debería estar prescrita por la ley, debiendo ser necesaria en una sociedad democrática. De hecho, de acuerdo por ejemplo, con la jurisprudencia del Tribunal Europeo de Derechos Humanos, cualquier restricción de la libertad de expresión debe corresponder a una "necesidad social acuciante" y ser proporcional a los fines legítimos perseguidos.

Sin embargo, la eliminación de contenido en las plataformas de medios sociales a menudo se realiza a través de procesos semiautomáticos o automatizados. Los algoritmos se utilizan ampliamente para el filtrado de contenido y los procesos de eliminación de contenido, incluso en las plataformas de redes sociales, que afectan directamente la libertad de expresión y plantean cuestiones relacionadas con el Estado de Derecho (cuestiones de legalidad, legitimidad y proporcionalidad). Si bien las grandes plataformas de redes sociales como Google o Facebook han afirmado con frecuencia que las personas eliminan todo el contenido, gran parte del proceso está automatizado y se basa en procesos semiautomáticos.

Ahora bien, existen varias técnicas automatizadas para identificar contenido que se considera que colisiona con los términos de servicio del proveedor, ya sea por contenido extremista, explotación infantil o actos ilegales como la incitación a violencia. Estas técnicas también se pueden usar para deshabilitar o suspender automáticamente las cuentas de usuario. Un desafío particular en este contexto es que se alienta a los intermediarios a eliminar este contenido voluntariamente, sin una base legal clara. Esta falta de una base legal para la eliminación "voluntaria" de contenido automatizado hace que sea aún más difícil garantizar que se respeten las garantías legales básicas, como la responsabilidad, la transparencia o el debido proceso[395].

Se han desarrollado iniciativas, donde los proveedores de servicios intermediarios, dada la presión pública y política, se han comprometido a contrarrestar activamente el discurso de odio en línea a través de técnicas automatizadas que detectan y eliminan todo el contenido ilegal. Si bien no cuestionan la necesidad de enfrentar efectivamente el discurso del odio, tales acuerdos han sido criticados por delegar responsabilidades de aplicación de la ley del estado a empresas privadas, por crear el riesgo de una

395 En su momento el gobierno del Presidente Obama abogó por la detección y eliminación automatizadas de videos e imágenes extremistas. Incluso han habido propuestas para modificar los algoritmos de búsqueda para "ocultar" sitios web que inciten y apoyen el extremismo. El mecanismo de filtrado automatizado para videos extremistas ha sido adoptado por Facebook y YouTube para videos. Sin embargo, no se ha publicado información sobre el proceso ni sobre los criterios adoptados para establecer qué videos son "extremistas" o mostrar "contenido claramente ilegal".

interferencia excesiva con el derecho a la libertad de expresión y por su falta de cumplimiento con principios tales como legalidad, proporcionalidad y debido proceso. Requerir que los intermediarios restrinjan el acceso al contenido basado en nociones vagas como el "extremismo" obliga a monitorear todos los flujos de comunicación y datos en línea para poder detectar lo que puede ser contenido ilegal. Por lo tanto, va en contra del principio establecido de que no debe existir una obligación de supervisión para los intermediarios.

Por otra parte, al ordenar al intermediario que decida qué eliminar como "extremista" y qué no, la autoridad pública transfiere la elección de herramientas y medidas a una parte privada, que luego puede implementar soluciones (como la eliminación o restricción de contenido) que las propias autoridades públicas no podrían prescribir legalmente.

Si bien el imperativo de actuar de manera decisiva contra la propagación de mensajes de odio y la incitación a los delitos por motivos raciales es indiscutible, estas prácticas plantean preocupaciones considerables relacionadas con la previsibilidad y la legalidad de las interferencias con la libertad de expresión.

Además, debe considerarse que en muchas situaciones, el contenido o material extremista que incita a la violencia es difícil de identifica , incluso para una persona capacitada en el tema, debido a la complejidad de los factores que intervienen además del contexto cultural, social, la idiosincrasia y hasta el humor.

Los algoritmos hoy en día no son capaces de detectar ironía o análisis crítico. El filtrado del habla para eliminar el contenido dañino a través de algoritmos, por lo tanto, enfrenta un alto riesgo de bloqueo excesivo y eliminación del lenguaje que no solo es inofensiva sino que también puede contribuir de manera positiva al debate público.

Por tanto, es imprescindible ser cuidadoso, ya que el bloqueo, filtrado o eliminación algorítmica del contenido puede tener un impacto adverso significativo en el contenido legítimo. El dilema ya altamente prevalente de la eliminación de grandes cantidades de contenido legítimo debido a los términos de servicio de las plataformas de Internet se ve exacerbado aún más por la presión ejercida sobre ellos para filtrar activamente de acuerdo con nociones vagas como "extremista", "discurso de odio" o "contenido claramente ilegal"[396].

Además, la preocupación pública en Europa y Estados Unidos ha crecido después de las elecciones estadounidenses en 2016 con respecto a la difusión de información errónea a través de noticias inventadas, intencionalmente falsas y engañosas -llamadas

396 La Corte Europea de Derechos Humanos, cualquier obligación de filtrar o eliminar ciertos tipos de comentarios de usuarios de plataformas en línea supone una carga "excesiva e impracticable" para los operadores y corre el riesgo de obligarlos a instalar un sistema de monitoreo "capaz de socavar el derecho a difundir información en Internet". Caso *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungría*, 2 de febrero de 2016, Asunto N° 22947/13.

"noticias falsas", incluso a través de técnicas automatizadas y en plataformas de medios sociales, ya que éstas, posiblemente tengan una influencia significativa en los procesos de toma de decisiones democráticas.

Como resultado, se han renovado los pedidos para que los estándares de responsabilidad de los medios tradicionales se apliquen a las plataformas de los medios sociales. De hecho algunos académicos han pretendido requerir a Facebook que actúe como un "editor de noticias con responsabilidad editorial de sus temas de actualidad"[397]. La pregunta que sigue es si las plataformas de medios sociales, a través de sus algoritmos que clasifican y consideran las presentaciones de terceros, ejercen una forma de control editorial tradicionalmente realizada por profesionales de los medios y, por lo tanto, se comprometen con responsabilidades específicas de los medios[398].

2. LIBERTAD DE REUNIÓN Y ASOCIACIÓN

Internet y, en particular, los servicios de redes sociales son herramientas vitales para el ejercicio y disfrute del derecho a la libertad de reunión y asociación, y ofrecen importantes posibilidades para aumentar el potencial de participación de las personas en la vida política, social y cultural[399].

La libertad de las personas para utilizar plataformas de Internet, como las redes sociales, establecer asociaciones y organizarse con fines de reunión pacífica, incluida la protesta, es una manifestación de los tradicionales derechos de primera generación reconocidos en todas las declaraciones internacionales de derechos y constituciones democráticas del mundo.

Se ha destacado igualmente en todo el mundo, que las redes sociales y sus algoritmos han facilitado avances en la concreción de estos derechos e incluso se ha sugerido que la difusión y el potencial de las redes, desempeñan un papel destacado en la organización y motivación de activistas y manifestantes.

De hecho, toda restricción al derecho a la libertad de reunión pacífica y a la libertad de asociación debe estar prescrita por la ley, perseguir un objetivo legítimo y

397 Helberger, N. y Trilling, D., "*Facebook Is a News Editor: The Real Issues to Be Concerned about*", en Media Policy Project. Disponible en:

http://blogs.lse.ac.uk/mediapolicyproject/2016/05/26/facebook-is-a-news-editor-the-real-issues-to-be-concerned-about/ (Fecha de consulta: 28/07/2019).

398 Reuters institute, "*Editors vs algorithms: who do you want choosing your news?*" Disponible en: http://reutersinstitute.politics.ox.ac.uk/news/editors-vs-algorithms-who-do-you-want-choosing--your-news (Fecha de consulta: 28/07/2019)

399 Comité de Ministros del Consejo de Europa, Recomendación CM/ Rec(2012)4 sobre la protección de los derechos humanos en redes sociales.

ser necesaria en una sociedad democrática; estos son los elementos centrales que se encuentran a su vez presentes en la regulación internacional de estos derechos.

Ahora bien, la operación de algoritmos en plataformas de redes sociales y la gran cantidad de información personal identificable sobre las personas que está disponible también se puede utilizar para rastrearlas e identificarlas y puede llevar a la clasificación automática de ciertas personas o grupos, incluso ciertos tipos de convocatorias, lo que podría tener un impacto negativo significativo en la libertad de reunión.

Los perfiles y el control de multitudes de los manifestantes no solo tienen lugar en Internet, sino que también se extienden a los métodos de control basados en datos fuera de línea. Teóricamente, los algoritmos utilizados para predecir posibles conflictos y situaciones de protesta también podrían usarse como herramienta preventiva para prevenir manifestaciones o protestas al – por ejemplo – arrestar a ciertas personas antes de que incluso se reúnan.

3. DERECHO A ELECCIONES LIBRES

La operación de algoritmos y sistemas de recomendación automáticos pueden crear las denominadas 'burbujas de filtro' (cámaras de eco totalmente automatizadas en las que los individuos solo ven información que confirma sus propias opiniones o se ajustan a su perfil [400].

Esto tiene efectos trascendentales para los procesos democráticos en la sociedad. Si bien es difícil determinar con precisión el impacto real de las "burbujas de filtro" y la desinformación dirigida en la formación de la opinión política, las cámaras de eco totalmente automatizadas representan el peligro de crear "burbujas ideológicas", a las que puede ser relativamente fácil de ingresar pero difícil de salir, lo que puede tener efectos cruciales en particular en el contexto de las elecciones.

Si bien se ha argumentado desde el advenimiento de Internet que las campañas en línea y las redes de medios sociales probablemente cambiarían la forma en que se ha desenvuelto la política y particularmente las elecciones, es solo más recientemente que la investigación académica ha revelado hasta qué punto la manipulación del contenido en línea en las plataformas de medios sociales puede "inclinar" los resultados de las elecciones.

Durante las elecciones en Estados Unidos, se informó que los investigadores manipularon la plataforma de Facebook para influir en el comportamiento electoral de los usuarios al decirles cómo sus amigos habían dicho que habían votado, sin el

400 Bozdag, E., "*Bias in Algorithmic Filtering and Personalization*", en Ethics and Information Technology 15, 2013, págs. 209 - 227.

conocimiento de los usuarios, y pudieron convencer a un segmento estadísticamente significativo de la población para que votara de determinada form [401].

Hay importantes indicios de que, desde entonces, Facebook ha estado vendiendo servicios de publicidad política relacionados a partidos políticos de todo el mundo, con un comportamiento similar observado durante diferentes procesos eleccionarios en distintas partes del mundo.

Si Facebook y otras plataformas en línea dominantes – de forma deliberada o no – pueden usar su poder para influir en el voto de las personas, esto no es menos importante que el hecho de que, en principio, tienen la capacidad de influir en las elecciones. Investigaciones recientes sugieren que las elecciones pueden ser ganadas no por los candidatos con el mejor argumento político, sino por aquellos que usan la tecnología más eficiente para manipular a los votantes, a veces emocional e irracional[402]. Si bien esto puede no ser un fenómeno completamente nuevo, ciertamente aumentó en escala y efecto, lo que llevó a un cambio de paradigma que podría poner en peligro la democracia misma. Los datos que se acumulan, recolectan y almacenan discretamente a través de tecnologías algorítmicas se han comparado con la nueva "moneda de poder", ya que puede emplearse directamente para la micro-focalización de los votantes, posiblemente con efectos decisivos en las elecciones.

De hecho, los candidatos menos conocidos pueden no tener los medios para costearse las tecnologías de manipulación más efectivas que ayudan a predecir las preferencias de los votantes. Si bien la publicidad política en la televisión está hoy en día regulada y existen requisitos de imparcialidad impuestos a las emisoras públicas, no existen tales equivalentes para el uso de predicciones algorítmicas de preferencias y comportamiento de los votantes que pueden tener un impacto igual o más poderoso en los votantes.

En este contexto, el papel particular desempeñado por los robots sociales en la configuración del debate político y público que conduce las elecciones se ha discutido

401 En el marco de una demostración, investigadores de Facebook mostraron a algunos usuarios un gráfico vinculado con sus noticias, indicando cuántos de sus amigos habían votado ese día y proporcionando un botón para hacer clic si también deseaban hacerlo. Los usuarios que recibieron información sobre la votación de sus amigos resultaron ser un 0.39% más propensos a votar que los demás, y su decisión tuvo un efecto adicional en el comportamiento de voto de sus amigos. Los investigadores concluyeron que un único mensaje en Facebook, entregado estratégicamente, incrementó la participación directamente en 60.000 votantes, y en mérito al efecto dominó, en última instancia provocó que se emitieran 340.000 votos adicionales ese día.

402 The Guardian, "*The great British Brexit robberty: how our democracy was hijacked*", edición del 7 de mayo de 2017. Disponible en: https://www.theguardian.com/technology/2017/may/07/the--great-british-brexit-robbery-hijacked-democracy (Fecha de consulta: 28/7/2019). En el artículo se argumenta que el referéndum Brexit se decidió por unos 600.000 votos; un poco más del 1% del total de votantes registrados, que había sido atacado por una firma que introdujo la recolección masiva de datos en sus técnicas de guerra psicológica, de hecho indicó que en conjunto psicología, propaganda y tecnología son la nueva y poderosa manera de ganar elecciones.

en particular en el contexto de las elecciones estadounidenses de 2016 y el referéndum Brexit.

Los bots sociales son cuentas controladas algorítmicamente que emulan la actividad de los usuarios humanos pero operan a un ritmo mucho mayor (por ejemplo, producen contenido automáticamente o se involucran en interacciones sociales), al tiempo que mantienen su identidad artificial sin revelarla. La investigación sobre el grado en que la presencia de robots de medios sociales afectó la discusión política en torno a las elecciones presidenciales de los Estados Unidos en 2016 sugiere que puede afectar negativamente la discusión política democrática en lugar de mejorarla, lo que a su vez puede alterar la opinión pública y poner en peligro la integridad del proceso eleccionario.

El derecho a las elecciones libres, es un principio sustantivo de la republica en la que se sustenta nuestro sistema jurídico político, lo que de manera alguna debe olvidarse en este contexto tecnológico de alguna manera olvidado de la importancia de la revalorización de los principios y valores esenciales que han conformado nuestra institucionalidad democrática.

Es importante destacar que, el problema no está en la utilización de las redes sociales y de internet, así como el incremento de intermediarios como mecanismos de incidencia política, sino que los desafíos regulatorios relacionados con las elecciones se deben a la falta de una regulación adecuada. La implicancia más trascendente, perniciosa y, a la vez, difícil de detectar del cambio a las redes sociales no es el poder creciente de los intermediarios, sino la incapacidad de la regulación para nivelar el las posibilidades para la competencia política y limitar el papel del dinero en las elecciones.

VI. CONCLUSIONES

Los derechos humanos y las libertades fundamentales son universales, indivisibles, interdependientes e interrelacionados. Como resultado, todos los derechos humanos y la libertad fundamentalmente se ven potencialmente afectados por el uso de tecnologías algorítmicas.

Hay una multiplicidad más de posibles impactos que deberán ser considerados y analizados tales como el derecho a la vida en el contexto de las armas inteligentes y los drones operados algorítmicamente, o en el contexto de la salud y la investigación relacionada. Además, es necesario también avanzar sobre los posibles efectos que la sistematización de puntos de vista y opiniones a través de algoritmos puede tener incidencias complejas sobre el derecho a la libertad de pensamiento, conciencia y religión.

De hecho, el uso cada vez mayor de la automatización y la toma de decisiones algorítmica en todos los ámbitos de la vida pública y privada amenaza con perturbar el concepto mismo de los derechos humanos como escudos protectores contra la interferencia del estado. La asimetría tradicional del poder y la información entre las estructuras estatales y las personas se está desplazando hacia una asimetría del poder y la información entre los operadores de algoritmos – que pueden ser públicos o privados – y quienes actúan y se rigen en razón éstos.

Es común que la información personal sea comparada con una moneda de cambio para obtener acceso a servicios en línea. Los datos pueden ser un producto negociado directamente o pueden tener una función auxiliar como entrada para la creación de perfiles de usuario individuales.

Las plataformas digitales multidimensionales, que son mediadores típicos para la experiencia en línea de la mayoría de las personas, tratan a éstas y a las organizaciones como proveedores de ideas y productos que se asimilan con otros.

El éxito de estas plataformas basadas en datos, ha crecido a través de la oferta de contenido "gratuito" y servicios para reunir masas de información personal, revelando el pasado, el presente e incluso hábitos y preferencias futuros. Las plataformas atraen clientes que pagan en un lado a través de la recolección y análisis de información personal recopilada de los clientes en el otro lado. Esto difumina la distinción tradicional entre consumidor y productor[403].

Ahora bien, la información personal no puede concebirse como un mero activo económico[404], ya que según lo han establecido los tribunales de justicia en diferentes instancias y lugares del planeta. El tratamiento de los datos personales es imprescindible e implica la protección del derecho al respeto de la vida privada y de la libertad de expresión y asociación.

Por otra parte, la algocracia es de hecho parte de un nuevo sistema discursivo en formación bajo el cual los fenómenos son comprendidos y analizados en términos de código. No se trata meramente de la consideración de un tema problema vinculado con la codificación, sino de la propia xistencia personal.

Por tanto, el discurso generalizado a favor del código, el lenguaje y la información deberá nuevamente mutar a un espacio discursivo diferente en el que se puedan inscribir la vida, las personas y sus derechos.

De esta forma, la codificación emerge como un método a priori para ordenar la confusión y caos, político, institucional y social existentes, sus superficies y límites,

403 Brown I., Marsden C., *Regulating Code: Towards Prosumer Law?* February 25, 2013 Disponible en: http://dx.doi.org/10.2139/ssrn.2224263 (Fecha de consulta: 30/10/2018).

404 Consumer Privacy in Network Industries, A CERRE Policy Report, 26 January 2016, págs. 35 - 36.

llevando parámetros ocultos que determinan la forma en que la vida y el mundo se enfrentan.

Como se señaló, la algocracia, añade una tercera dimensión a los sistemas burocráticos y panópticos ya existentes a nivel de gobierno y las amenazas están demasiado cerca.

La gobernabilidad democrática legítima requiere procedimientos de toma de decisiones que protejan la libertad y la autonomía, y que permitan la participación individual y la comprensión de esos procedimientos de toma de decisiones.

La dependencia de los algoritmos de minería de datos socava la libertad y la autonomía y evita la participación activa y la comprensión de los procedimientos de toma de decisiones.

Por lo tanto, la dependencia de los algoritmos de minería de datos es una amenaza para la gobernabilidad democrática, tal como se estableciera.

Así es que debe sostenerse la concluyente afirmación de Rouvroy la que se comparte y se entiende de alguna manera manifiesta una síntesis sustantiva de lo planteado "la relación entre personas y máquinas tiene que liberarse de esta abstracción reductora y seguir manteniendo en el centro de la refl xión y de la proyección institucional los derechos fundamentales, que es además el único camino para salir de las contraposiciones, también abstractas, entre utopía y distopía, entre exaltación y rechazo de la dimensión tecnológica. Las implicaciones normativas de las innovaciones tecnológicas obviamente no pueden relegarse pero deben ser valoradas según los principios que fundamentan el respecto a las personas y a los protocolos de un sistema democrático, que no pueden confiarse a un "creciente gobierno estadístico de lo real"[405].

BIBLIOGRAFÍA

Andreessen, M., "*Why Software Is Eating The World*", en Wall Street Journal, edición del 11 de agosto de 2011. Disponible en:

http://www.wsj.com/articles/SB10001424053111903480904576512250915629460 (fecha de consulta: 28/07/2019)

Bozdag, E., "*Bias in Algorithmic Filtering and Personalization*", en Ethics and Information Technology 15, 2013, págs. 209 - 227.

Brown I., Marsden C., *Regulating Code: Towards Prosumer Law?* February 25, 2013

405 Rouvroy, A., "Privacy, Data protection and the unprecedented Challenges of the Ambient Intelligence", en *Studies in Ethics, Law and Technology*. Berkeley Electronic Press, 2008. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1013984 (Fecha de consulta: 30/10/2018).

Disponible en: http://dx.doi.org/10.2139/ssrn.2224263 (Fecha de consulta: 30/10/2018).

Comité de Ministros del Consejo de Europa, Recomendación CM/ Rec(2012)4 sobre la protección de los derechos humanos en redes sociales.

Consumer Privacy in Network Industries, A CERRE Policy Report, 26 January 2016, págs. 35 - 36.

Gillespie, T., *"The Relevance of Algorithms"* en Media technologies: Essays on communication, materiality, and society, Cambridge Mass, MIT Press, 2014, págs. 167 - 194.

Helberger, N. y Trilling, D., *"Facebook Is a News Editor: The Real Issues to Be Concerned about"*, en Media Policy Project. Disponible en:

http://blogs.lse.ac.uk/mediapolicyproject/2016/05/26/facebook-is-a-news-editor-the-real-issues-to-be-concerned-about/ (Fecha de consulta: 28/07/2019).

Kitchin, R. y Dodge, M., *Code/Space Software and Everyday Life*, MIT Press, 2011.

McCarthy, D., *"Open Networks and the Open Door: American Foreign Policy and the Narration of the Internet"*, en Foreign Policy Analysis 7, 2011, págs. 89 - 111.

Pasquale, F., *"Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power"*, en Social Science Research Network, 2016. Disponible en: https://papers.ssrn.com/abstract=2779270 (Fecha de consulta: 28/07/2019).

Reuters institute, *"Editors vs algorithms: who do you want choosing your news?"* Disponible en: http://reutersinstitute.politics.ox.ac.uk/news/editors-vs-algorithms-who-do-you-want-choosing-your-news (Fecha de consulta: 28/07/2019).

Rodotá, S., "Democracia y Protección de Datos", en Pensieri. Disponible en: http://pensieriworld.blogspot.com/2010/12/stefano-rodota_4105.html (fecha de consulta: 30/10/2018).

Rouvroy, A., "Privacy, Data protection and the unprecedented Challenges of the Ambient Intelligence", en *Studies in Ethics, Law and Technology*. Berkeley Electronic Press, 2008. Disponible en:

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1013984 (Fecha de consulta:

30/10/2018).

Spiekermann, S., *Ethical IT Innovation: A Value-Based System Design Approach*, CRC Press, 2015.

The Guardian, "*The great British Brexit robberty: how our democracy was hijacked*", edición del 7 de mayo de 2017. Disponible en: https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy (Fecha de consulta: 28/7/2019).

INDUSTRIA 4.0, CIDADES INTELIGENTES E IOT

LAS TECNOLOGÍAS DISRUPTIVAS:

LOS RETOS A LA PROTECCIÓN DE DATOS

Eje temático: IoT. Ciudades inteligentes. Medicina y TIC

Autor:
Nayibe Chacón Gómez
Doctora en Ciencias, mención Derecho
Profesora Titular de la Universidad Central de Venezuela

ABSTRACT
Desde finales de la década de los 90 la UNESCO describió tres hechos que demostraban que la humanidad se encontraba inmersa en un nuevo tipo de sociedad, el primer hecho atiende a las organizaciones y empresas, las cuales cada vez dependen en mayor medida del uso inteligente de la información y de sus tecnologías para ser competitivas; el segundo hecho se refiere a que los ciudadanos también utilizamos estas tecnologías en la mayoría de nuestras tareas diarias, generando y consumiendo grandes cantidades de información en el trabajo y en el ocio; y finalmente, el tercer hecho, es el que apunta a las empresas de servicios tecnológicos y que se han convertido en los grandes hipersectores de la economía (UNESCO, 1997). Estos hechos en la práctica se traducen en el desencadenamiento de un tipo de tecnología llamada disruptivas, las cuales permiten darle nuevos propósitos a las cosas de todos los días, con el empleo de la tecnología, "el fenómeno por el cual una innovación transforma un mercado o sector existente introduciendo simplicidad, comodidad, accesibilidad y asequibilidad, donde la complicación y el alto costo son el *status quo*." (LOZA, 2015) En este escenario, este artículo es una introducción al concepto de las tecnologías disruptivas, así como sus principales exponentes: el IoT (*Internet of Things)* y las Ciudades Inteligentes (*Smartcities)*, como insumos del llamado *big data*, para luego atender a los retos que estas tecnologías proponen a la regulación de la protección de datos personales. Lo que se persigue con esta investigación es alertar sobre los cada vez mayores desafíos que presentan los inagotables desarrollos tecnológicos para el derecho, ya que el uso de estas tecnologías en la creación de contenidos deben permitir el respeto a las libertades fundamentales de todos los individuos, lo que incluye la privacidad personal y el derecho a la libertad de opción, conciencia y religión de conformidad con los instrumentos internacionales relevantes.
Palabras clave: Tecnologías Disruptivas, *Smartcities*, IoT, *Internet of Things, big data.*

1) INTRODUCCIÓN A LAS TECNOLOGÍAS DISRUPTIVAS

La aparición y despliegue de las llamadas *tecnologías disruptivas*, término usado en la literatura de tecnología y negocios para describir innovaciones y desarrollos que mejoran un producto en sentidos que el mercado no los espera, típicamente por un bajo precio o diseños para un grupo diferente de consumidores.

> La teoría de la tecnología disruptiva fue acuñada por primera vez por el profesor de Harvard, Clayton M. Christensen en su investigación sobre la industria de discos duros y más tarde popularizado por su libro "*The Innovator's Dilemma*" (LOZA, 2015)

En este sentido, se ha definido a las tecnologías disruptivas como innovaciones que ayudan a "crear una nueva red de valor y que eventualmente interrumpe el mercado actual (en unos pocos años o décadas), desplazando una tecnología anterior". (LOZA, 2015)

Dentro de estas tecnologías encontramos el llamado *Internet de las cosas,* (*Internet of Things* - IoT) que fue inventado como una frase para una conferencia en la compañía *Procter & Gamble* por Kevin Ashton en 1999, y se refiere al mundo en el que cada objeto tiene una identidad virtual propia y capacidad potencial para integrarse e interactuar de manera independiente en la Red con cualquier otro individuo, ya sea una máquina (M2M) o un humano. Se pueden citar como ejemplos del IoT:

1.- **Los zapatos (zapatillas) inteligentes**: el primero de ejemplos de Internet de las cosas está dentro de la categoría de los *wearables*. En un artículo publicado en el portal Computerhoy.com a finales del año 2014, conocí de qué se trataban los *wearables*, les comparto la sencilla información:

> "son equipos compactos, especialmente pensados para que los puedas llevar puestos como si fueran ropa y, en general, son mucho más pequeños que los teléfonos móviles. En un futuro, podrían incluso implantarse en el cuerpo. En cualquier caso, se basan en una tecnología compleja y se trata de un nueva corriente tecnológica que está implantando y en la actualidad." (Computerhoy, 2014)

Los zapatos *SpeedForm Gemini 2* cuentan con hardware capaz de registrar datos como el tiempo y la distancia recorrida, parámetros que después se combinan en una aplicación móvil para extraer valor de ellos. Estos zapatos también tienen la posibilidad de enviar datos GPS para determinar las rutas seguidas por el usuario.

2.- Sensores para el jardín: una de las compañías que ofrecen este producto es *Parrot*. Más conocida por la fabricación de *drones*, la empresa francesa también tiene un catálogo nutrido de sensores. Uno de ellos, el *Flower Power*, está destinado a jardines. El dispositivo registra datos sobre la luz solar, la temperatura, el nivel de fertilizante en el suelo y el de humedad. Con esta información, el sensor analiza el estado del jardín y lo que necesitan las plantas. El dispositivo envía alertas a través de *bluetooth* al *smartphone* del usuario cuando este tiene que regar o practicar otros cuidados.

3.- Garajes inteligentes: más bien puertas de garajes con un controlador. Este dispositivo, llamado *Garageio*, puede controlar el acceso mediante una aplicación. Desde el teléfono (inteligente) se puede abrir y/o cerrar, así como recibir alertas

cuando la puerta se abra. También es posible permitir el acceso a terceras personas desde cualquier parte.

4.- *Wearables* para perros: las mascotas también estarán conectadas. Al menos es la tendencia que se está observando en los últimos años. Un ejemplo de Internet de las cosas en este ámbito es *Fitbark*, un dispositivo que se coloca en el collar de tu perro para monitorizar su actividad. Como si fuera una especie de pulsera inteligente –de hecho el nombre hace referencia a la conocida marca *Fitbit*–, el dispositivo mide la actividad del perro, la calidad de su sueño y ofrece detalles sobre su comportamiento.

5.- Botones inteligentes: Amazon ha llegado a un acuerdo con una serie de marcas de productos domésticos para crear botones inteligentes que funcionan de la siguiente manera: cuando estás en casa y vas a poner la lavadora descubres que apenas queda detergente, hasta ahora lo que hacías era anotarlo en la lista de compra, o mentalmente pensar "vaya, hay que comprar detergente" y olvidarlo al cabo de un instante. La asociación de Amazon con un fabricante de detergente te permite tener un botón inteligente acoplado a la lavadora, para que cuando observes la falta del producto puedas encargarlo solo con pulsar el botón. Amazon recibe la orden de compra –un determinado bote de detergente de una determinada marca– y la procesa para enviarlo directamente a tu casa. (BEJARANO, s/f)

También entre las tecnologías disruptivas encontramos las *Smartcities*, o Ciudades Inteligentes, que se presentan como un modelo pensado por Jeremy Rifkin, economista, escritor y asesor de distintos gobiernos europeos y de la misma Comisión Europea, quien trabaja para dar forma al concepto y visión de la "Tercera Revolución Industrial", la fusión de las tecnologías de Internet con las energías renovables.

> En el futuro, las viviendas, oficinas y fábricas, producirán su propia energía verde y compartirán unas con otras una "Internet energética", del mismo modo en que ahora creamos y compartimos información en línea. Para Rifkin, la Tercera Revolución Industrial es la oportunidad de cambio de modelo antes que se agoten los recursos naturales. (CERCLE TECNOLOGIC DE CATALUNYA, 2014)

> En la actualidad la definició de ciudad inteligente, atiende más a considerarla
> un "sistema de sistemas que funcionan en forma conjunta."
> Entre las tecnologías que configuran una ciudad inteligente pueden mencionarse las redes ópticas de alta velocidad, las redes de sensores, las redes de cable y las redes inalámbricas, imprescindibles para posibilitar los beneficios que aportan sistemas de transporte inteligentes, redes eléctricas inteligentes y redes domésticas. Lo que más distingue una ciudad inteligente de una ciudad tradicional es el vínculo que establece con sus ciudadanos. Los servicios de las ciudades tradicionales posibilitados por las TIC no pueden responder a las transformaciones económicas, culturales y sociales en la misma forma que logran hacerlo los servicios de una ciudad inteligente. Por este motivo, una ciudad inteligente es, ante todo, una ciudad con una dimensión más humana, que obedece a una infraestructura TIC y al desarrollo

> urbano permanente, teniendo siempre en cuenta la sostenibilidad ambiental y económica. (UIT, 2013: 39)

A los fines de dar un contexto característico de las *Smartcities* se puede anotar que según la Unión Internacional de Telecomunicaciones (UIT, 2013) éstas presentan tres (3) rasgos esenciales, a saber: 1º la seguridad de la infraestructura de las tecnologías de la información y comunicación de la próxima generación es fundamental para el éxito de los nuevos servicios de ciudad inteligente y para anticipar la futura demanda de servicios. 2º la ciudad debe contar con un marco de gestión convenientemente definido e integrado. Los numerosos sistemas de una ciudad inteligente funcionarán en armonía únicamente si respetan el cumplimiento estricto de normas comunes. Y 3º una ciudad inteligente necesita usuarios inteligentes, por tanto se precisa de que los ciudadanos conozcan de tecnología y cómo ésta interactúa en su quehacer diario, haciéndose parte inseparable de la vida en sociedad. "Una ciudad inteligente se funda en una red integradora de usuarios de dispositivos inteligentes, y sus habitantes exigen o crean los servicios que más valoran." (UIT, 2013: 40)

En definitiva, en el núcleo de las *Smartcities* lo extraordinario de la tecnología se convierte en lo ordinario de la vida.

2) LAS TECNOLOGÍAS DISRUPTIVAS Y LOS RETOS A LA PROTECCIÓN DE DATOS

El IoT y las *Smartcities*, sumados a otros emprendimientos tecnológicos y los que aparecen cada día, son generadores y consumidores de información personal, ya que la información es su alimento, convirtiendo los datos personales de sus usuarios en el activo más preciado.

> La información ya era valiosa en el pasado, significaba encontrarse en una situación ventajosa respecto a quienes no la tenían. Pero en el presente su valor se acrecienta, ya que antes no existía la posibilidad de convertir informaciones parciales y dispersas en informaciones en masa y organizadas, de interrelacionar esa información y de procesarla con rapidez, como ocurre hoy, en la sociedad de la información. (Herrera, 2004)

Toda esta información forma o compone lo que se ha llamado *big data*, término que comúnmente es utilizado para identificar una formula o conjunto de estas que surge dada la imposibilidad de analizar inconmensurables cantidades de información a través de las formas tradicionales de tratamiento de datos.

Pero son Viktor Mayer-Schönberger y Kenneth Cukier, quienes en el libro: *Big data: La revolución de los datos masivos*, expusieron lo trascendental de esta fórmula tecnológica:

> No existe ninguna definición rigurosa de los datos masivos. En un principio, la idea era que el volumen de información había aumentado tanto que la que se examinaba ya no cabía en la memoria que los ordenadores emplean para procesarla, por lo que los ingenieros necesitaban modernizar las herramientas para poder analizarla. Ese es el origen de las nuevas tecnologías de procesamiento, como *Map-Reduce*, de *Google*, y su equivalente de código abierto, *Hadoop*, que surgió de Yahoo. Con ellos se pueden manejar cantidades de datos mucho mayores que antes, y esos datos –esto es lo importante- no precisan ser dispuestos en filas ordenadas ni en las clásicas tabulaciones de datos… los *big data*, los datos masivos, se refieren a las cosas que se pueden hacer a gran escala, pero no a una escala inferior, para extraer nuevas percepciones o crear nueva formas de valor, de tal forma que transforman los mercados, las organizaciones, las relaciones entre los ciudadanos y los gobiernos, etc. (MAYER-SCHÖNBERGER, 2013)

Así, el *big data* puede referirse al tratamiento y análisis de enormes repositorios de datos, tan desproporcionadamente grandes que es imposible tratarlos con las herramientas de bases de datos y analíticas convencionales. Para ahondar acerca de las tecnologías que convergen en el *big data*, invitamos a la lectura del trabajo de los autores Camargo Vega, Juan José, Jonathan Felipe Camargo Ortega y Luis Joyanes Aguilar, titulado: **Conociendo Big Data**.

No obstante, a los fines de conocer de manera introductoria esta figura, anotares los presupuestos necesarios para hablar de *big data*, es la existencia las bases de datos, que contengan los siguientes elementos o atributos, llamados la triple "V": volumen, variedad y velocidad, los cuales deben estar siempre presentes.

- **Volumen de los datos**: la cantidad de datos a tratar es tan grande que es imposible la utilización de los medios tradicionales hasta ahora conocidos, tales como las hojas de cálculos del *MS Excel* o el lenguaje declarativo de acceso a la bases de datos *SQL*.
- **Variedad de los datos:** los datos recogidos provienen tanto de fuentes estructuradas como no estructuradas: transacciones bancarias, imágenes de satélite, redes sociales, contenidos de páginas web, dispositivos móviles de geolocalización y miles de aplicaciones, las conexiones del internet de las cosas, los servicios web 2.0, e incluso el cuerpo humano (por ejemplo, cuando se utilizan sistemas de identificación biométricos). Este aspecto será tratado más adelante, en la relación existente entre las Redes Sociales y el *big data*. La doctrina sobre la materia del big data reconoce que el elemento de la variedad de los datos, es el de mayor relevancia, ya que extraer información de datos tan diversos supone un gran reto; así,

> "las tecnologías que se han desarrollado para el *big data* permiten, entre otras soluciones, combinar datos a pesar de que no se encuentren almacenados en fiche os con la misma estructura. Así por ejemplo, una cadena de tiendas puede analizar de forma conjunta los datos de ventas con los datos de temperaturas para realizar un modelo predictivo en tiempo real para cada uno de sus locales comerciales." (GIL, 2016: 22-23)

• **Velocidad en la transferencia de los datos**: El *big data* permite transferir datos de forma barata y eficie te, y así se pueden analizar tanto los datos dinámicos que se van creando, como los datos estáticos o históricos que ya han sido almacenados de forma previa, ya que la velocidad a la que se crean y procesan los datos está en continuo aumento, y con frecuencia para las organizaciones es importante poder analizarlos de forma muy rápida, incluso en tiempo real, algo que en ocasiones es imposible con los sistemas tradicionales. "Por ejemplo, el análisis de datos en tiempo real puede ayudar a seguir la trayectoria de huracanes y su intensidad. Esto podría llegar a permitir realizar predicciones sobre dónde pueden producir daños con horas o incluso días de antelación." (GIL, 2016: 22)

La citada autora GIL incorpora tres aspectos más que permiten perfilar el *big data*, los cuales también comienzan por la letra "V": veracidad, visualización y valor de los datos.

• **Veracidad de los datos**: se refiere a la calidad del mismo
Conseguir datos de alta calidad se ha convertido en todo un reto, principalmente importante cuando se trata de datos no estructurados. Sin embargo, tal y como IBM asegura, algunos datos son inciertos por naturaleza, como los sentimientos, el futuro, los sensores GPS que rebotan entre los rascacielos de una ciudad, o los datos creados en entornos humanos como las redes sociales; y ninguna limpieza de datos puede corregirlos. Así, manejar la incertidumbre es una cuestión esencial al tratar con tecnologías *big data*. (GIL, 2016: 23)

• **Visualización**: *Data Visualization*, en inglés, es el ámbito del *big data* que consiste en representar de manera comprensible y medible los datos obtenidos para encontrar patrones y claves ocultas en el tema a investigar. Es entendida como el conjunto de herramientas que posibilitarán comprender los datos gráficamente y en perspectiva contextual.

Uno de los servicios punteros en *Data Visualization* es el que ofrece *CartoDB*, una *startup* española que no ha parado de crecer desde su fundación. Específicamente se centra en mostrar información sobre mapas geográficos, por lo que los contenidos siempre han de ser comparables por zonas. El gran atractivo de *CartoDB*, desde mi punto de vista, es que, además de ser abierto, aprovecha su servicio para mostrar

contenidos que hoy son muy relevantes, como los *tuits*, de manera fácilmente entendible pero a la vez muy potente. Con algunas funciones similares a *CartoDB* encontramos a *Google Fusion Tables*, otra herramienta sencilla con API avanzada que no requiere conocimientos avanzados y que genera gráficas y mapas con información presentada de manera más arcaica y simple que *CartoDB*, pero también comprensible, incluyendo la gestión de capas en datos geográficos. Por último, otra herramienta que se beneficia del enorme avance del *Big Data* es *Tableau Public*, ideal para mostrar información detallada de análisis en mapas interactivos o en gráficos de barras que también permite importar de Excel, por lo que la mitad del trabajo está hecho. Es muy sencilla y rápida, y permite a cualquier persona generar en poco tiempo un gráfico estético y publicable en una web. (HIPERTEXTUAL, s/f)

- **Valor del dato**: la finalidad última de los procesos de *big data* es crear valor, ya sea entendido como oportunidades económicas o como innovación; es éste valor del dato, el que ha hecho posible el emprendimiento del *big data*.

El *big data* llego para quedarse, ya que sus beneficios parecen superar los riesgos que conlleva a los datos de las personas. Ese beneficio es el poder ofrecer una visión cada vez más precisa de las fluctuaciones y rendimientos de todo tipo de recursos, permitir realizar adaptaciones experimentales a cualquier escala de un proceso y conocer su impacto en tiempo casi real, ayudar a conocer mejor la demanda y así realizar una segmentación mucho más ajustada de la oferta para cada bien o servicio, o acelerar la innovación y la prestación de servicios cada vez más innovadores y más eficientes. Los datos para obtener estos conocimientos provendrán tanto de las personas como de los objetos, y con mayor énfasis a medida que el denominado internet de las cosas se generalice. Sin embargo, las previsiones estiman que tan solo el 0,5% de la información será efectivamente procesada. (GIL, 2016: 28-29)

Los riesgos del *big data* que anuncia la doctrina son:

(i) el riesgo de caer en conclusiones erróneas que nadie revisa, ya que el *big data* permite extraer patrones que posteriormente serán predicciones;

(ii) el riesgo que para las personas pueda tener tomar decisiones automatizadas sin un sesgo humano, y que dichas decisiones no den lugar a justificación; y

(iii) el riesgo para la privacidad de las personas y para el tratamiento de sus datos, lo cual se podría resolver a través de la transformación del dato, pasando de ser información que permite identificar a una persona en particular entre un universo, a una información anónima.

Este último aspecto que es analizado con profundidad por la autora Elena Gil, en su estudio, ya que el *big data* desafía o altera de alguna manera las normas de protección de datos hasta ahora conocidas, ya que facilita la llamada reidentificación

de los sujetos a partir incluso de datos anónimos, lo que se traduce en que las técnicas de anonimización ya no parecen ser suficiente para la ofrecer protección, que en definitiva propone un nuevo capítulo en el debate de base de qué datos son personales y cuáles no personales.

> Tradicionalmente, la anonimización consistía en un proceso de dos fases principales. En primer lugar, despojar a los conjuntos de datos de todos los rasgos identificadores personales (PII por sus siglas en inglés *personal identificable information*), como pueden ser nombre, dirección, fecha de nacimiento o número de seguridad social. En segundo lugar, se modificaban o eliminaban otras categorías de datos que podían actuar como identific - dores en dicho contexto concreto (por ejemplo, un banco eliminaría los números de tarjeta de crédito, y una universidad eliminaría los números de identificación de sus estudiantes). De este modo, el resultado aunaba lo mejor de ambos lados: los datos continuaban siendo útiles, y podían ser analizados, compartidos o puestos a disposición del público al tiempo que los individuos no podían ser identificados, y por lo tanto se protegía su privacidad. La anonimización aseguraba la privacidad. Sin embargo, con los nuevos avances, esta situación cambia. El *big data*, al incrementar la cantidad y diversidad de la información, facilita la reidentificac ón de individuos, incluso después de haber sido anonimizados. GIL, 2016: 83.

Este tema ha sido analizado de manera independiente por distintos autores desde la relación existe entre la protección de datos y las Redes Sociales, ya que ha llamado la atención de éstos la posible vulneración de los datos personales con el uso de éstas. Ahora bien, este punto se escapa del alcance de nuestra presentación. No obstante, a los fines de proveer soluciones al estado de la protección de datos, en la actualidad existen leyes que regulan la materia, y han incorporado ciertos compromisos que los responsables de los datos recogidos y almacenados deben cumplir, tales como el principio de responsabilidad (*accountability*) o el principio de privacidad por defecto.

El principio de responsabilidad (*accountability*) conlleva la obligación por parte del responsable de la recogida y almacenamiento de los datos de aplicar los principios de la protección de datos. En este sentido, el Grupo de Trabajo de Protección de Datos creado en virtud de la Directiva 95/46/CE como un organismo europeo, con carácter consultivo e independiente, para la protección de datos y el derecho a la intimidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE, entre la que destaca desempeñar las labores de secretaría la Dirección de Derechos Fundamentales y Ciudadanía de la Unión Europea, estableciendo la necesidad de la inclusión del principio de responsabilidad en las legislaciones nacionales sobre protección de datos centrándose en dos (2) elementos principales: 1) la necesidad de que el responsable del tratamiento adopte medidas adecuadas y eficaces para aplicar los principios de protección de datos; y 2) la necesidad de demostrar, si así se requiere por parte de la autoridad de control independiente o por el propio titular de los datos, que se han adoptado medidas adecuadas y eficaces;

así pues, el responsable del tratamiento de datos deberá aportar pruebas. (Grupo de Trabajo de Protección de Datos, 2010)

Por su parte, el principio de privacidad por diseño (*Privacy by Design*), parte del concepto fue acuñado en la década de los noventa por Ann Cavoukian, Comisionada de Información y Privacidad de Ontario, Canadá; y refiere tanto a una filosofía como a un enfoque por el cual la privacidad se encuentra integrada en el diseño tecnológico mismo, consistente con la arquitectura del sistema de información y con el modelo de negocios. Se presenta como una forma de asegurar que la privacidad va a estar garantizada ante los cambios tecnológicos. (BRIAN, 2012)

Y finalmente citaremos el principio de privacidad por defecto (*Privacy by Default*), que para algunos autores forma parte de la privacidad por diseño, no obstante, en nuestra consideración se trata de un principio autónomo que conduce a que la necesidad de que la persona otorgue su consentimiento para compartir sus datos. Así, la privacidad por defecto se refiere a que cualquier sistema ha de estar configurado de forma que, por defecto otorgue una mayor protección a la privacidad de las personas, de modo que, no se comparta la información del usuario salvo que éste realice una acción o cambie su configuración. La privacidad por defecto otorga un mayor control sobre la propia información ya que, el usuario está protegido, aunque no haga ninguna acción y decide libremente cuándo, cómo y con quién, comparte sus datos. (VIVET, 2014)

A esta lista de principios también se le suman otras prácticas deseables que deben adoptar para la protección de los datos personales, tales como la incorporación de códigos de conductas para los usuarios, la identificación clara y precisa sobre las políticas de almacenamiento y de las llamadas *Cookies* o pequeña información enviada por un sitio web y almacenada en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del usuario, de allí los problemas en materia de protección de datos de carácter personal, entre otras; el tratamiento exhaustivo de todas estas harían nuestro trabajo infinito o de imposible publicación, ya que mientras yo escribo y usted lee se están desarrollando más tecnologías disruptivas y nuevas aplicaciones con nuevos retos para la ciencia jurídica en cuanto a los derechos de protección de los datos de carácter personal.

CONCLUSIÓN

Sobre las ideas expuestas se puede concluir que cada vez más las tecnologías están en nuestras vidas, y cada día dependemos de éstas para casi todos los aspectos de nuestra dinámica habitual, tanto en la casa como en el trabajo; cosas cotidianas son impensables sin la tecnología, por ejemplo, pagar en un establecimiento o ir al cine.

Esta dependencia tecnológica nos hace cada vez más vulnerables, al dejar al descubierto grandes cantidades de información de nosotros mismos, que de otra forma o en otros tiempos nadie conocería, o solo aquellas personas muy cercanas a nosotros. Esta situación hace necesario que pensemos en la formula de minimizar esa vulnerabilidad, de allí que nuestra relación con la tecnología debe repensarse, a los fines de proteger lo que no queremos que nadie conozca.

BIBLIOGRAFIA

BEJARANO, Pablo (s/f): **5 útiles ejemplos de Internet de las cosas que pronto podrás probar**. [Disponible en línea] http://blogthinkbig.com/5-utiles-ejemplos-de-internet-de-las-cosas-que-pronto-podras-probar/ (Última consulta: 12/10/2016)

BRIAN NOUGRÈRES, A. (2012): "La protección inteligente de los datos personales: Privacy by design (PbD)", **Red Académica Internacional de Protección de Datos Personales.** Universidad de los Andes. Facultad de Derecho, Bogotá, núm. 1, julio - diciembre. [Disponible en línea] https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/ok6_-Ana-Brian-Nougreres_FINAL.pdf (Última consulta: 12/06/2019)

CAMARGO VEGA, J.J, J.F. Camargo Ortega y L. Joyanes Aguilar (2015): "Conociendo Big Data", **Revista Facultad de Ingeniería**. Facultad de Ingeniería Universidad Pedagógica y Tecnológica de Colombia, vol. 24, núm. 38, enero-abril. [Disponible en línea] http://www.scielo.org.co/pdf/rfing/v24n38/v24n38a06.pdf (Última consulta: 01/11/2016)

CERCLE TECNOLOGIC DE CATALUNYA (2014): **Hoja de Ruta para la *Smart City***. [Disponible en línea] http://paisdigital.org/PD/wp-content/uploads/2014/06/HojaderutahacialasSmartCities.pdf (Última consulta: 12/10/2016)

GIL, E. (2016): **Big data, privacidad y protección de datos. Agencia Española de Protección de Datos**. Agencia Estatal Boletín Oficial del Estado. Madrid. [Disponible en línea] https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/premios_2015/Big_Data_Privacidad_y_proteccion_de_datos.pdf (Última consulta: 20/09/2016)

Grupo de Trabajo de Protección de Datos del Artículo 29. **Dictamen 3/2010 sobre el principio de responsabilidad. Adoptado el 13 de julio de 2010**. [Disponible en línea] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_

es.pdf (Última consulta: 01/11/2016)

HERRERA BRAVO, R. (2004): **El Derecho en la Sociedad de la Información: Nociones generales sobre el Derecho de las Tecnologías de la Información y las Comunicaciones.** [Disponible en línea] http://www.derechotecnologico.com/estrado/estrado002.html (Última consulta: 01/11/2018)

LOZA MATOVELLE, D. y Dabirian, R. (2015): "Introducción a la Tecnología Disruptiva y su Implementación en Equipos Científicos", **Revista Politécnica Ecuador**, vol. 36, núm. 3. [Disponible en línea] http://www.revistapolitecnica.epn.edu.ec/images/revista/volumen36/tomo3/IntroduccionalaTecnologiaDisruptivaysuImplementacionenEquiposCientificos.pdf (Última consulta: 01/11/2018)

MAYER-SCHÖNBERGER V. y Kenneth Cukier (2013): **Big data: La revolución de los datos masivos**. Edición en castellano: Turner Publicaciones S.L., Extracto [Disponible en línea] http://www.elboomeran.com/upload/ficheros/obras/ xtracto_bigdata_turner.pdf (Última consulta: 25/12/2015)

Unión Internacional de Telecomunicaciones – UIT (2013): Ciudades inteligentes, en: **Actualidades de la UIT**, núm. 5, ejemplar dedicado a: Foro Mundial de Política de las Telecomunicaciones/TIC. [Disponible en línea] https://www.itu.int/bibar/ITUJournal/DocLibrary/ITU011-2013-05-es.pdf (Última consulta: 10/11/2018).

VIVET TAÑA, L.: Big Data y Privacy by Design (PbD). **Observatorio Iberoamericano de Protección de Datos.** [Disponible en línea] http://oiprodat.com/2014/07/23/big-data-y-privacy-by-design-pbd/ (Última consulta: 01/11/2016).

UNESCO (1998): **Reporte mundial**. [Disponible en línea] https://unesdoc.unesco.org/ark:/48223/pf0000110221 (Última consulta: 10/11/2018).

Wearables [Disponible en línea] http://computerhoy.com/tags/wearable (Última consulta: 10/11/2016).

Las mejores herramientas para visualizar grandes cantidades de datos. [Disponible en línea] https://hipertextual.com/presentado-por/bbva/visualizacion-de-datos (Última consulta: 10/11/2016).

EL TRABAJO EN LA INDUSTRIA 4.0., RETOS JURÍDICO-LABORALES

Eje temático: Trabajo en el Siglo XXI. Teletrabajo. Industria 4.0

Autor:
Felipe Miguel Carrasco Fernández
Doctor en Estudios Legales
Investigador de la
Universidad Popular Autónoma del Estado de Puebla (UPAEP) México
felipemiguel.carrasco@upaep.mx

ABSTRACT
Las revoluciones industriales aunadas a sus respectivas innovaciones tecnológicas constituyen factores importantes para el trabajo y el capital al posibilitar la generación de ventajas competitivas para las empresas y contribuir a transformar la organización del trabajo; por tal motivo existe un impacto de las revoluciones tecnológicas sobre los sistemas de relaciones laborales, empleo, estructura social y organización empresarial en la globalización.
Los cambios tecnológicos son procesos inevitables que trasforman los actuales puestos de trabajo y crean otros nuevos; ambos aspectos tienen diversas repercusiones para los trabajadores y empleadores y sus respectivas familias, así como para la evolución tecnológica mediante la incorporación de nuevos procesos en la industria que han propiciado una elevación de la productividad en el trabajo, reducción de los costos de producción, mejoramiento de la calidad de productos y servicios al presentar un impacto cualitativo y cuantitativo en el empleo industrial.
La cuarta revolución industrial caracterizada por la implementación de diversas innovaciones tecnológicas como lo es el internet de las cosas, la robótica y la inteligencia artificial, entro otros aspectos, generan nuevos desafíos legales en la sociedad digital en el ámbito laboral.
El trabajo en la industria 4.0 implica un nuevo análisis de retos jurídicos para los actores involucrados en las relaciones laborales ya que los avances tecnológicos contribuyen al incremento de la polarización en el mercado del trabajo y aumentan la dispersión salarial, en ocasiones en detrimento de los empleados y en otras como oportunidades de nuevos yacimientos de empleo.
Es necesario el análisis de los nuevos paradigmas jurídicos que implica la industria 4.0 en las relaciones laborales, toda vez que ésta genera una transformación, haciéndose necesario adecuar el Derecho del Trabajo a las innovaciones tecnológicas actuales.

1.- INNOVACIÓN TECNOLÓGICA Y TRABAJO

La creciente globalización de la economía experimenta rápidos y profundos cambios derivados de las evoluciones tecnológicas, las cuales persiguen siempre una mayor competitividad, para (Ryder, 2015, p. 14) éstas generan cambios importantes en la manera de organizar el trabajo y la producción.

Las empresas tienen que aumentar la productividad y reducir sus costos, por lo que buscan nuevas tecnologías que aumenten la competitividad mediante la automatización y fragmentación de los sistemas de producción.

La evolución tecnológica no solo afecta la cantidad de los puestos de trabajo, sino también la naturaleza y la calidad de los mismos; al respecto Schumpeter, señala con acierto que la innovación y la tecnología juegan un papel primordial como motores del crecimiento económico.

Para (Sagardoy y Mercader, 2017, p. 2) la innovación se asocia a la tecnología y aunque la primera desde una perspectiva económica va mucho más allá, ésta puede proyectarse sobre los productos o sobre los procesos operativos o comerciales, incluso, podemos hablar de innovaciones organizativas.

Respecto a la discusión de generación o pérdida de empleos derivados de las innovaciones tecnológicas hay tres líneas de pensamiento. La primera en la que se encuentran los denominados tecnooptimistas, quienes consideran que la robotización de las relaciones laborales producto de dichas innovaciones genera nuevos empleos, como en las revoluciones industriales pasadas, al crecer la productividad y en consecuencia el empleo.

El segundo grupo lo constituyen los denominados tecnopesimistas, quienes consideran que la incorporación de las máquinas y de las innovaciones tecnológicas en cada una de las revoluciones industriales han generado cambios en el empleo y propiciado su destrucción de manera masiva en los puestos de trabajo.

Un tercer grupo ecléctico considera que, si bien es cierto, las relaciones laborales sufren cambios derivados de las innovaciones tecnológicas producto de la automatización, robotización el empleo y la utilización de cada vez más algoritmos, éstos destruyen los puestos tradicionales de trabajo y se crean nuevas formas de empleo con cualidades cada vez más calificada que deberán tener las personas que lo ocupen. Este grupo habla de una mutación del empleo acorde a las innovaciones tecnológicas en cada revolución industrial.

Respecto de la automatización de la industria en los siglos XVIII y XIX (Industria 1.0), considera (Molina, 2017, p. 2) que la división del trabajo y la producción en cadena (organización científica del trabajo) del siglo XX (Industria 2.0), y la revolución tecnológica de finales del siglo XX (Industria 3.0), ahora se hablaría de la era de la digitalización de la economía; esto provocaría una mutación en las empresas y sus modelos de negocios, así como en el trabajo y en la economía compartida y no competitiva (Industria 4.0).

Las revoluciones industriales han provocado en palabras de (Mercader, 2019, p. 31) que las innovaciones tecnológicas resulten hoy un factor productivo más importante que el trabajo o el capital, tanto por su escasez como por su carácter estratégico, al posibilitar la generación de ventajas competitivas para las empresas, al tiempo que contribuyen de forma decisiva a transformar la organización del trabajo.

No podemos dudar que las revoluciones tecnológicas impactan en el sistema de las relaciones laborales, en el empleo y en la estructura social; situación que se ha

vivido históricamente en la transición del sistema fordista al posfordismo y se vive actualmente con las innovaciones tecnológicas, la globalización, la descentralización productiva, la tercerización del empleo, la automatización del proceso productivo y la utilización de los robots, incluyendo los algoritmos en la producción. La interrogante será siempre si el Derecho del Trabajo tiene nuevos desafíos jurídicos derivados de los cambios antes citados.

El nuevo modelo productivo según señala (Raso, 2018, p. 13), se desarrolla a partir de las facilidades tecnológicas que posibilitan la circulación de las mercancías, de los capitales y de las transformaciones tradicionales de las organizaciones empresariales y los modos de producción, con lo cual las innovaciones tecnológicas aplicadas a las empresas generan nuevos trabajos permitiendo éstas una mayor vigilancia y control de la jornada laboral, lo que implica la posibilidad de violación de los derechos de privacidad, intimidad e imagen del empleado.

Derivado de lo anterior las innovaciones tecnológicas aplicadas a las empresas generan nuevos trabajos, permitiendo las tecnologías una mayor vigilancia y control de la jornada laboral lo que implica la posibilidad de violación de los derechos de privacidad, intimidad e imagen del empleado; en algunos casos se habla de la tecnosubordinación o del e-monitoreo donde las empresas modifican su organización y procesos productivos, por lo tanto, el modelo taylorista es desplazado frente a los nuevos paradigmas del trabajo ya que los empleados reclaman más autonomía y libertad debido a que se encuentran ante una menor estabilidad y, en ocasiones están en presencia de una brecha tecnológica.

Los sindicatos deben transformarse para así poder dar solución a las nuevas reclamaciones de los trabajadores en la sociedad digital de la actual revolución industrial, donde la sociedad se caracteriza por el desarrollo de la tecnología digital de comunicaciones, los sistemas ciberfisicos combinados con software y sensores.

En la trasformación del trabajo encontramos el impacto de las tecnologías digitales y, para poder comprenderlas debemos entender la interacción de éstas dentro del sistema económico y social, ya que existe una relación estrecha entre tecnología y trabajo que ha contribuido a la economía industrial en una sociedad global.

En consecuencia, como lo expresa (Rifkin, 1997, p. 25) se han incrementado los puestos de trabajo para los profesionales de la información y el conocimiento en desmedro de los trabajadores no calificados, que pasan a engrosar las filas, de lo que Keynes denomina, el desempleo tecnológico.

En virtud del impacto que están produciendo las innovaciones tecnológicas se hace necesario asumir el cambio en las relaciones laborales ya que las constantes transformaciones de la realidad social siempre están cuestionando el ordenamiento jurídico existente al plantear problemas que constituyen nuevos retos para el Derecho del Trabajo como instrumento regulador de las relaciones humanas en la sociedad.

Como lo expone (Ossio, 2003, p. 6) el acelerado desarrollo de la ciencia y la tecnología y su aplicación en los diversos ámbitos de la vida humana plantea retos que debe enfrentar el Derecho como instrumento regulador ante la emergencia de nuevos conflictos que afectan los intereses primigenios de cada persona. Como consecuencia de lo anterior las innovaciones tecnológicas deberán atraer la atención del Derecho del Trabajo para estar acorde a los tiempos actuales.

En relación a la utilización de las nuevas tecnologías de la información y comunicación por parte de los trabajadores en el centro de trabajo (Kahale, 2006, p. 295) expresa que se plantean un conjunto de problemas jurídicos hasta ahora inexistentes, por lo que el Derecho del Trabajo en su carácter dinámico debe evolucionar a medida que surgen nuevas realidades y situaciones laborales.

Hasta ahora no existen normas laborales que regulen específicamente la nueva realidad socioeconómica que actualmente se vive, como lo asevera (Kahale, 2006, p. 296) son muy escasos los convenios colectivos que cobijan el tema de las tecnologías de la información y comunicación en las relaciones laborales. Se puede aseverar que las relaciones laborales que actualmente se denominan postmodernas prueban la prioridad del capital sobre el trabajo y la sustitución de la mano de obra por las innovaciones tecnológicas.

2.- INDUSTRIA 4.0

En cada revolución industrial existe relación entre las innovaciones tecnológicas y las características de las relaciones laborales que se generan en cada una de ellas, esto debido a la utilización de determinadas energías. Es por lo que la legislación laboral debe estar acorde a los cambios propiciados en las revoluciones industriales como consecuencia de las innovaciones tecnológicas y su repercusión en el trabajo; ante dicha situación los reclamos de los trabajadores en la sociedad están en consonancia con éstas.

Así cuando hablamos de la industria 4.0 nos referimos al conjunto de tecnologías que nos ayudan a vincular el mundo físico con el virtual, que en total son once y que son: la robótica, inteligencia artificial, impresión 3D, simulaciones, seguridad informática, desarrollo de software, materiales avanzados, *bigdata*, internet de las cosas, realidad aumentada y computo en la nube.

En la actualidad las innovaciones tecnológicas permiten la visión de la fabricación de mañana (industria 4.0), para Joyanes Aguilar, ésta combina fábricas y maquinas inteligentes, materias primas y productos que se comunican dentro de un internet de las cosas y que impulsan cooperativamente la producción.

El termino Industria 4.0 viene asociado con el nacimiento de la cuarta revolución industrial la cual corresponde a una nueva manera de organizar los medios de producción utilizando las tecnologías digitales y la formación inteligente de datos a partir de *bigdata* a través del internet de las cosas.

El contexto tecnológico, como lo expone (Sánchez, 2018, p. 3) en el que nos encontramos, es de tal magnitud que, aunque se intente caracterizar esa realidad como de nueva revolución tecnológica y se califique como de cuarta revolución industrial, ésta es mucho más que una simple descripción del cambio impulsado por la tecnología, es una realidad compleja, heterogénea con múltiples aristas y que merece ser analizado su impacto jurídico y social el cual se empieza a producir y que en un futuro cercano detonará.

El término Industria 4.0 se acuñó en Alemania en el año 2011 en la Feria tecnológica de Hannover-Messe; fue en 2013, cuando se presentó la iniciativa oficial del gobierno de Alemania y se creó para referenciar a la transformación digital de la industria, también conocida como Fabrica Inteligente o Internet industria.

La convergencia de las tecnologías de la información (TIC) con la sensórica y la robótica han transformado la internet tradicional en internet de las cosas (IoT), el resultado en la industria para (Del Val, 2016, p. 1), ha sido un nuevo modelo organizativo y un cambio disruptivo en la industria que algunos denominan la cuarta revolución industrial.

La Industria 4.0 busca como objetivo principal la creación de fábricas inteligentes mediante la integración de sistemas de fabricación ciberfísicos (virtuales y físicos), por lo tanto, la cuarta revolución industrial en sus orígenes consiste en la creación de máquinas inteligentes y sistemas inteligentes conectados entre sí.

La automatización, para (Joyanes, 2017, p. 1) se basa en los sistemas ciberfísicos facilitados por la nube (*cloud computing*) y el internet de las cosas, con la ayuda indispensable de la fabricación mediante las impresoras 3D y el soporte fundamental de la inteligencia artificial y de *bigdata*, como tecnologías clave para la conversión de grandes volúmenes.

La Industria 4.0 es el producto más tangible de la cuarta revolución industrial y está favoreciendo la fabricación inteligente, para (Joyanes, 2017, p. 2) en un marco revolucionario para diseñar, implantar y gestionar ecosistemas complejos que proporcionan información en tiempo real y posibilitan las interacciones autónomas entre máquinas, sistemas, objetos y cosas.

La Industria 4.0 trae grandes beneficios para las empresas, especialmente a las multinacionales y a los trabajadores; en opinión de (Kahale, 2017, p. 1) se les cambiaran los derechos y deberes de trabajo dentro de la empresa, como son las tareas y los

horarios; donde el sindicato tendrá que prever lo conducente para que la implantación de las nuevas tecnologías no sea el vehículo para destruir y precarizar el empleo.

Debido a la disrupción tecnológica que implica la industria 4.0 los robots colaborativos como lo expone (Del Val; 2016, p. 3) serán capaces de trabajar con seguridad junto a los seres humanos, aprendiendo de ellos y ofreciendo autonomía, fl xibilidad y cooperación.

La digitalización de la mayoría de sectores productivos y la Industria 4.0 abarcan más que solo la tecnología, para (Sierra, 2018, p. 238) las empresas deben estar preparadas para experimentar cambios radicales debido a diversos factores, entre los que se encuentra la necesidad de contar con competencias actualizadas junto con nuevas formas de trabajar.

El ser humano no será reemplazado por una máquina, pues existe una dependencia mutua de interacción con el objetivo de agilizar procesos y métodos para ofrecer productos, servicios y atención de calidad, lo que obligará a tener personal cada vez más calificado y enfocado en la automatización y el desarrollo tecnológico.

Según Forbes, tan sólo en México son más de cuatro millones de pequeñas y medianas empresas (Pymes) que generan 72% del empleo y aportan 52% del Producto Interno Bruto (PIB); estos negocios son los que hacen competitivo a un país, los que atraen inversiones y fortalecen las industrias. Nuestro país enfrenta un escenario con retos que buscan formas innovadoras de seguir creciendo.

3.- RETOS JURÍDICO-LABORALES DE LA INDUSTRIA 4.0

Las sociedades tratan de regir la manera en que se lleva a cabo el trabajo mediante una combinación de instrumentos, legislación, acuerdos voluntarios, instituciones del mercado de trabajo, la interacción de los gobiernos y las organizaciones de empleadores y de trabajadores. Para (Rayder, 2015, p. 21) estas organizaciones se han desarrollado generalmente con base a normas sociales implícitas no escritas de un sólido ideario colectivo que determinan lo que es justo y aceptable y lo que no lo es. En el plano internacional, estas normas se inscriben en el objetivo de la OIT relativo a la justicia social, pero ese mandato universal también da cabida a una rica variedad de especificidades nacionales de legislación sin que ello lo debilite.

En el trabajo 4.0 se cristalizan tres objetivos centrales: los empleados deben estar protegidos contra la sobrecarga y la eliminación de las fronteras del trabajo, para evitar que la configurac ón de los horarios ponga en riesgo su seguridad y salud. Las mayores opciones de seleccionar los horarios deben permitir aumentar la autonomía respecto al tiempo y al lugar. Los nuevos estímulos (Grynspan, 2017, p. 13) para alcanzar una fl xibilidad negociada entre los interlocutores sociales, deben impulsar

nuevos acuerdos dirigidos a una organización innovadora del trabajo y deben crear más espacio para la estructuración de las empresas.

Una moderna protección laboral 4.0 deberá contener los siguientes elementos: adaptación de los conceptos de protección a las nuevas tecnologías (por ejemplo, colaboración hombre-robot); asesoramiento y apoyo a directivos y empleados frente a trabajos fl xibles en cuanto al lugar; estructuración laboral preventiva en estrecha cooperación con los departamentos de desarrollo y por último formación y capacitación de los empleados. Así las relaciones laborales combinarán nuevas y viejas formas de organización del trabajo.

En la era de la automatización, no desaparecerán en América Latina las modalidades tradicionales del trabajo, como son los trabajadores por cuenta propia, las pequeñas cooperativas, la subcontratación oculta o informal ni el trabajo pobre en las cadenas mundiales de suministro, etc. Por lo que el desafío en la época actual es cómo gobernar las transformaciones productivas y sociales productos de las nuevas tecnologías.

La nueva realidad impone condiciones que tienen como consecuencia la destrucción de las formas tradicionales del empleo y del industrialismo clásico, en torno a las cuales se habían construido redes de tutelas y amortiguadores sociales. Taylor, cuando asentó la teoría que permitiría el desarrollo del industrialismo clásico, no imaginó el fuerte componente sindical que acompañaría su modelo.

El sindicato tradicional y el derecho laboral típico nacen como reacción a los excesos del modelo industrial. Taylorismo/fordismo y sindicalismo fueron como hermanos que se odian al ser la presencia de uno condición del otro.

Como expresa Romagnoli, el industrialismo clásico, además de un modelo de producción económica, significó una forma de pensa .

Actualmente las nuevas tecnologías rompen ese patrón igualitario y la industria 4.0 genera un nuevo modelo de trabajo, que aún no genera reactivos ni normas a los modos de producción y utilización del trabajo.

Las organizaciones sindicales desconfían justamente de las nuevas tecnologías, pero en vez de estudiarlas y proponer reglas y límites prefieren anclarse en una visión industrialista con las tutelas tradicionales que reúnen a menos trabajadores. Al respecto expresa (Raso, 2018, p. 25) tenemos un Derecho del Trabajo cada vez con más normas y menos clientes; el problema actual es que mientras reaccionamos con lentitud ante el trabajo automatizado, las nuevas formas de trabajo destruyen los empleos tradicionales en vastas áreas de la producción de bienes y servicios.

Se asume que la digitalización del trabajo, (Jalil, 2018, p. 166) como resultado de la convergencia entre el internet de las cosas, la inteligencia artificial, la robótica y la impresión 3D ha derivado en un nuevo paradigma de producción llamado Industria 4.0.

En una economía basada en la reducción de costes, en fl xibilidad productiva y en maximización del beneficio, (Guerrero, 2018, p. 203) las obligaciones que impone el ordenamiento laboral hacen que el trabajo subordinado sea escasamente atractivo como fórmula de vinculación jurídica. La razón de ello es clara, asistimos a nuevas formas de trabajar que establecen la obsolescencia del Derecho del Trabajo y la importancia del Derecho de las Nuevas Tecnologías y la importancia de adecuar el marco regulatorio laboral a las innovaciones tecnológicas que implica la industria 4.0.

CONCLUSIÓN

1.- Las innovaciones tecnológicas de las revoluciones industriales repercuten en las relaciones laborales.

2.- La industria 4.0 representa nuevos paradigmas para el Derecho del Trabajo y el Derecho Informático, requiriéndose un marco jurídico-laboral que regule el trabajo que se desarrolla en la industria 4.0.

3.- La legislación laboral deberá regular las relaciones de interacción entre la robótica, la inteligencia artificial y los trabajadores.

REFERENCIAS BIBLIOGRÁFICAS

DEL VAL ROMÁN, JOSÉ LUIS., (2016), "Industria 4.0: la transformación digital de la industria". *Conferencia de Directores y Decanos de Ingeniería Informática.* Facultad de Ingeniería de la Universidad de Deusto. En línea: http://coddii.org/wp-content/uploads/2016/10/Informe-CODDII-Industria-4.0.pdf [fecha de consulta: 18 de enero 2019]

GRYNSPAN, MARIANO., (2017), "Digitalización y el Futuro del Trabajo", Sinopsis del estudio 'Trabajar 4.0' elaborado por el Ministerio Federal de Trabajo y Asuntos Sociales de Alemania", *Revista Análisis,* No. 20, Julio 2017, Fundación Friedrich Ebert .En línea: https://library.fes.de/pdf-files/buer_s/argentinien/13617.pdf [fecha de consulta: 11 de febrero 2019]

GUERRERO VIZUETE, ESTHER., (2018), "La economía digital y los nuevos trabajadores: Un marco contractual necesitado de delimitación", *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo,* Volumen 6, núm. 1, enero-marzo de 2018, Escuela Internacional de Alta Formación en Relaciones Laborales y de Trabajo de ADAPT, En línea: http://ejcls.adapt.it/index.php/rlde_adapt/article/view/556/756 [fecha de consulta: 11 de febrero 2019]

JALIL NAJI, MAIEDAH., (2018), "Industria 4.0, competencia digital y el nuevo Sistema de Formación Profesional para el empleo", *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo*, Escuela Internacional de Alta Formación en Relaciones Laborales y de Trabajo de ADAPT, Volumen 6, núm. 1, enero - marzo de 2018, En línea: http://ejcls.adapt.it/index.php/rlde_adapt/article/view/555/755 [fecha de consulta: 18 de enero 2019]

JOYANES AGUILAR, LUIS., (2017), *Industria 4.0 La cuarta revolución industrial,* AlfayOmega / Marcombo; Edición 1ª, España, 2017

KAHALE CARRILLO, DJAMIL TONY., (2017), "El sindicato de la Industria 4.0", *Revista Adapt internacional*, No. 26, enero 2017, Universidad a Distancia de Madrid (UDIMA), En línea: http://www.bollettinoadapt.it/wp-content/uploads/2017/01/El-sindicato-de-la-Industria-4.0..pdf [fecha de consulta: 29 de enero 2019]

KAHALE CARRILLO, DJAMIL TONY., (2006), "Las nuevas tecnologías en las relaciones laborales: ¿Avance o Retroceso?". *Revista de Derecho,* núm. 25, julio, 2006, Universidad del Norte Barranquilla, Colombia, En línea: http://www.redalyc.org/articulo.oa?id=85102508 [fecha de consulta: 10 de febrero 2019]

MERCADER UGUINA, JESÚS R., (2019), "El impacto de la robótica y el futuro del trabajo", *Revista de la Facultad de Derecho de la Universidad Nacional Autónoma de México,* Tomo LXIX, Núm. 273, enero - abril 2019, En línea: http://www.revistas.unam.mx/index.php/rfdm/article/download/62438/54922[fecha de consulta: 28 de enero 2019]

MOLINA NAVARRETE, CRISTÓBAL., (2017), "Derecho y trabajo en la era digital: ¿Revolución industrial 4.0 o economía sumergida 3.0?", *En El futuro del trabajo que queremos, Conferencia Nacional Tripartita*, 28 de marzo de 2017, Palacio de Zurbano, Madrid: Iniciativa del Centenario de la OIT (1919-2019), Vol. 2, 2017 (Volumen II), En línea: https://www.ilo.org/wcmsp5/groups/public/---europe/---ro-geneva/---ilo-madrid/documents/publication/wcms_615487.pdf [fecha de consulta: 29 de enero 2019]

OSSIO ONOFRE, FREDDY., (2003), "La Sociedad de la Información y los nuevos retos para el Derecho". Sociedad, Informática y Derecho. En Línea: http://escueladejuristas.com/sociedad.pdf [fecha de consulta: 25 de febrero 2019]

RASO DELGUE, JUAN., (2018), "América Latina: El impacto de las tecnologías en el empleo y las reformas laborales", *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo,* Volumen 6, núm. 1, enero-marzo de 2018, Escuela Internacional

de Alta Formación en Relaciones Laborales y de Trabajo de ADAPT. En línea: http://ejcls.adapt.it/index.php/rlde_adapt/article/view/549/750 [fecha de consulta: 11 de febrero 2019]

RIFKIN, J., (1997), *El fin del trabajo. Nuevas tecnologías contra puestos de trabajo: El nacimiento de una nueva era,* Editorial Paidos, España, 1997

RYDER, GUY., (2015), *La iniciativa del centenario relativa al futuro del trabajo,* Oficina Internacional del Trabajo, Memoria del Director General, Conferencia Internacional del Trabajo, 104.ª reunión, 2015, En Línea: https://www.ilo.org/ilc/ILCSessions/104/reports/reports-to-the-conference/WCMS_370408/lang--es/index.htm [fecha de consulta: 29 de enero 2019]

SAGARDOY, IÑIGO Y MERCADER, JESÚS R., (2017), "Desarrollo la robotización y justo reparto de la riqueza (Conversación: Trabajo y sociedad)". En línea: https://www.ilo.org/wcmsp5/groups/public/---europe/---ro-geneva/---ilo-madrid/documents/article/wcms_548575.pdf [fecha de consulta: 18 de enero 2019]

SÁNCHEZ-URÁN AZAÑA, Mª YOLANDA Y GRAU RUIZ, Mª AMPARO., (2018), "El impacto de la robótica, en especial la robótica inclusiva, en el trabajo: aspectos jurídico-laborales y fiscales", *Ponencia presentada al Congreso Internacional sobre Innovación Tecnológica y Futuro del Trabajo*, Santiago de Compostela, 5 y 6 de abril 2018, Facultad de Derecho; a Iniciativa de la OIT sobre Futuro del Trabajo, En línea: http://inbots.eu/wp-content/uploads/2018/08/publications/robotica-derecho-del-trabajo-derecho-fiscal-final-mayo2018.p [fecha de consulta: 03 de febrero 2019]

SIERRA BENÍTEZ, ESPERANZA MACARENA., (2018), "El delegado de protección de datos en la industria 4.0: funciones, competencias y las garantías esenciales de su estatuto jurídico", *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo*, Volumen 6, núm. 1, enero-marzo 2018. Escuela Internacional de Alta Formación en Relaciones Laborales y de Trabajo de ADAPT, En línea: http://ejcls.adapt.it/index.php/rlde_adapt/article/view/558/758 [fecha de consulta: 04 de febrero 2019]

INTERNET DAS COISAS E A OBSERVÂNCIA AO DIREITO À PRIVACIDADE DO CIDADÃO

Eixo temático: IoT, cidades inteligentes, medicina e TIC

Autores:
Têmis Limberger
Doutora em Direito Público pela Universidade Pompeu Fabra - UPF de Barcelona (2004), pós-doutora em Direito pela Universidade de Sevilha (2013). Mestre (1997). Graduada (1986) em Direito pela Universidade Federal do Rio Grande do Sul - UFRGS. Professora da Universidade do Vale do Rio dos Sinos - UNISINOS nas seguintes atividades acadêmicas: (a) Graduação em Direito: Direito Administrativo I e II; (b) Programa de Pós-Graduação em Direito: Estado e Administração (Mestrado) e Administração Digital (Doutorado). Avaliadora ad hoc da Revista de Direito do Consumidor, da Revista Brasileira de Direitos Fundamentais e Justiça, da Revista Quaestio Iuris, da Revista Direito Público e da Revista Interesse Público. Procuradora de Justiça do Ministério Público do Estado do Rio Grande do Sul. Membro do Instituto Brasileiro de Direito Eletrônico - IBDE, da Federación Iberoamericana de Asociaciones de Derecho e Informática - FIADI e da Rede Brasileira de Pesquisadores em Direito Internacional. Temas preferenciais: Estado e Administração, Transparência Digital, Transparência da Administração Pública, Novas Tecnologias, Controle Social e Jurisdicional dos Atos Administrativos, Princípio da Publicidade, Direito à Intimidade, Direitos Sociais e Fundamentais. Orientadora de Mestrado e Doutorado.

Gustavo da Silva Santanna
Doutorando e Mestre em Direito pela UNISINOS. Especialista em Direito Ambiental Nacional e Internacional e Direito Público. Procurador do Município de Alvorada/RS. Professor do Centro Universitário FADERGS e da Faculdade Meridional (IMED). Professor convidado dos cursos de pós-graduação em Direito do Estado da UFRGS.

RESUMO
O presente artigo aborda a relação de novas tecnologias, em sua face atual como: internet das coisas (IoT) e *big data,* com o direito à privacidade. O desenvolvimento e a velocidade das tecnologias de informação e comunicação modificaram sobremaneira o comportamento da sociedade. O *locus* de relacionamento jurídico e social, acesso à informação, participação, entre outros direitos, dá-se através da internet. Essa modificaçã social, levou ao que se denomina de Quarta Revolução Industrial, ou seja, uma ressignificação na organização da indústria, que passou, então, a denominar-se de Indústria 4.0. Inicialmente, perceber-se-á que diversas são as formas de se coletar dados dos indivíduos, sendo as "coisas" uma delas. A partir daí, conceitua-se o que é internet das coisas, ou seja, a capacidade de "coisas" coletarem, armazenarem e enviarem dados a uma central. Essa central de armazenamento de dados, deve comportar uma grande quantidade de informações, dando origem ao *big data*. Porém, *big data* não se resume a "acumulação" ou "volume" de dados, preocupando-se, também, com a sua veracidade, velocidade, variedade e valor dos dados coletados. Tendo essas premissas estabelecidas, traça-se, posteriormente, da relação jurídica que existe entre essas duas tecnologias. Posteriormente, verifica-se que o alcance atual da privacidade deve abranger, também, os dados visto que, uma vez processados (ou minerados) esses dados carregam consigo informações que, por sua vez, possuem grande valor econômico. Sustenta-se, ao fim, que para que as coisas possam ter acesso aos dados dos indivíduos, estes devem expressamente dar seu consentimento, devendo, também, estar conscientes da finalidade conferida aos dos dados captados, respeitando-se, assim, o direito à privacidade do indivíduo. A privacidade, por meio de exposição dos indivíduos e seus dados, ressaltar-se-á, ainda que

possua grande valor econômico no âmbito da iniciativa privada, integra o conceito da personalidade do cidadão. Pautado em pesquisa bibliográfica, o presente estudo utilizou-se do método dialético para sua estruturação, na qual o contexto social é ponto de partida para a (re)significação de alguns conceitos

ABSTRACT

This article discusses the relation of new technologies, in its current face as: internet of things (IoT) and big data, with the right to privacy. The development and speed of information and communication technologies have greatly modified the behavior of society. The locus of legal and social relationship, access to information, participation, among other rights, occurs through the internet. This social change led to what is known as the Fourth Industrial Revolution, that is, a re-signification in the organization of industry, which then became known as Industry 4.0. Initially, it will be noticed that there are several ways of collecting data from individuals, with "things" being one of them. From there, it is conceptualized what is the internet of things, that is, the ability of "things" to collect, store and send data to a central. This central data storage, should contain a lot of information, giving rise to the big data. However, big data does not boil down to the "accumulation" or "volume" of data, also worrying about its veracity, speed, variety and value of the data collected. Having these premises established, it is later traced of the legal relationship that exists between these two technologies. Afterwards, it is verified that the current scope of privacy should also cover data since, once processed (or mined), these data carry information that, in turn, has great economic value. In the end, it is maintained that in order for things to have access to the data of the individuals, they must expressly consent, and must also be aware of the purpose given to the data collected, thus respecting the right to privacy of the individual. The privacy, through exposure of individuals and their data, will be highlighted, although it has great economic value within the scope of private initiative, integrates the concept of the personality of the citizen. Based on a bibliographical research, the present study used the dialectical method for its structuring, in which the social context is the starting point for the (re) signification of some concepts.

1 INTRODUÇÃO

As tecnologias de informação e comunicação alteraram a formatação social e cada vez mais as pessoas estão conectadas em mundo digital. Essas mudanças veem modificando, não somente o comportamento social, mas também da indústria, comércio, serviços, entre outras atividades. Uma dessas modificações foi o início da Indústria 4.0, decorrente da quarta Revolução Industrial. Vale lembrar que a primeira Revolução Industrial foi a mecânica substituindo a força humana pela máquina; a segunda foi elétrica, que permitiu a produção de bens em massa, em linha de montagem; a terceira a da automação, com a introdução de computadores e da robótica; e, agora, a quarta, na qual já estamos inseridos, é a que advém da aplicação da inteligência artificial, *big data*, internet das coisas (IoT), realidade aumentada, que "vai além das tecnologias e olha para a cadeia de ponta a ponta, incluindo, por exemplo, armazenagem, logística, reciclagem, energia, trabalhadores, segurança e transporte" (SACOMANCO; SÁTYRO; 2018, p. 28).

A Indústria 4.0 tem por desafio otimizar o uso das tecnologias para melhorar a produtividade, qualidade e sustentabilidade dos produtos, e para tanto, diminuiu o distanciamento entre o "chão da fábrica" (local onde é feita a produção) e os níveis gerenciais (STEVAN JUNIOR; LEME; SANTOS; 2018, p. 36-37). Para tanto, essa nova modalidade industrial necessitou estabelecer uma comunicação entre equipamentos

e operadores e entre os "operários" e os "gerentes", trabalhando com uma ideia de "automação totalmente integrada (TIA)" (STEVAN JUNIOR; LEME; SANTOS; 2018, p. 63), e nessa questão o estudo acerca da internet das coisas e o *big data* torna-se altamente relevante.

Klaus Schwab (2018, p. 148) é categórico ao afirmar que com a quarta Revolução Industrial, será possível até 2025 conectar tudo, literalmente, à internet como: condicionadores de ar, televisão, radio, cafeteira, cortina, tudo funcionando remotamente e, assim, quanto maior a extensão das redes de comunicação, maior a possibilidade de exposição do cidadão. Com isso, todas as coisas serão inteligentes (e com preço acessível), sendo cada produto físico capaz de ser ligado a à rede mundial de computadores: é a internet das coisas. Mas qual é o destino dos dados coletados? O indivíduo/cidadão/consumidor está ciente das informações que estão sendo extraídas? Diante dessas indagações, o direito à privacidade surge como um limitador às intromissões ilegítimas que possam surgir no tratamento dos dados dos indivíduos.

2 INTERNET DAS COISAS (IoT) E *BIG DATA*: UMA INTRODUÇÃO AO TEMA

A internet das coisas – IoT (*internet of thinks*) – compreende-se como um conjunto de bens, coisas (objetos físicos) conectados à internet, por meio de sensores, e que podem ser controlados através dessa rede. Klaus Schwab (2018, p. 148) a considera o elemento central da infraestrutura da quarta revolução industrial, uma vez que "trata de uma gama de sensores inteligentes conectados que coletam, processam e transformam os dados de acordo com a necessidade; os dados são então enviados para outros dispositivos ou indivíduos para atender aos objetivos de um sistema ou usuário." A primeira experiência com a IoT deu-se na década de 90 quando uma torradeira foi ligada e desligada por meio da internet. De lá para cá, os estudos acerca do que pode ser conectado à internet vem aumentando exponencialmente, de carros a eletrodomésticos, praticamente tudo pode ser ligado à rede. Soma-se a isso, o baixo custo de implantação e a alta velocidade com que os dados são compartilhados, o processamento mais barato, o armazenamento em nuvem dos dados (*cloud computing*), tudo contribui para o desenvolvimento dessa tecnologia (DIAS, 2016, posição 308). Percebe-se, portanto, que não são somente as pessoas que podem gerar dados: as coisas também podem. Assim, "quanto maior o número de dispositivos conectados, mais dados são produzidos" (MAGRANI, 2018, p. 21).

> Estes objetos são capazes de coletar grandes quantidades de dados sobre as pessoas e o ambiente e, assim, poderem responder de maneira autônoma a determinadas situações ou disponibilizar informações que aumentam a percepção das pessoas sobre o contexto ao seu redor. Diante disso, podemos

> deduzir que o insumo principal na IoT é a informação, que é gerada e consumida tanto pelas pessoas quanto pelos objetos "inteligentes" (ROZSA; PINTO; MURIEL-TORRADO, 2017, p. 256).

Conforme a quantidades de coisas conectadas aumentam, ampliam também a quantidade dados gerados, unindo-se neste ponto o estudo da IoT ao *Big Data*. Pode-se compreender *Big Data* como uma grande capacidade de armazenamento de dados e com velocidade de processamento reduzida e, ainda que sucinto, este conceito já exige alguns cuidados. Normativamente o Decreto Federal nº 8.777 (BRASIL, 2016) conceituou "dado" como a "sequência de símbolos ou valores, representados em qualquer meio, produzidos como resultado de um processo natural ou artificial". A Lei Federal nº 13.709 de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018), em seu artigo 5º, também estabeleceu conceituações e distinções acerca de dados:

> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófic ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> III - dado anonimizado: dado relativo a titular que não possa ser identific - do, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

Não obstante as diversas conceituações pode-se compreender, basicamente que "dados" são "fatos coletados e normalmente armazenados" (AMARAL, 2016, posição 312), que permitem identificar uma pessoa (LIMBERGER, 2007, p. 61)

Felipe Nery Rodrigues Machado (2018, posição 366-369) coloca o *Big Data* sobre cinco pilares. O primeiro deles é a grande "velocidade" na qual os dados são produzidos. O segundo é o "volume" que diz respeito à quantidade de dados. O terceiro é a "variedade", ou seja, a diversidade de dados produzidos por dia por um indivíduo. A "veracidade" é o que garante que os dados coletados são autênticos e, portanto, passíveis de serem analisados. Por fim, mas não menos importante é o "valor" que os dados possuem, ou seja, a informação que eles carregam. Aqui, inclusive, mais fácil de identific r a distinção entre "dado" e "informação", pois é a partir dos "dados" coletados e estruturados (que podem ser em formato eletrônico ou impresso) que se pode aferir "valor" a eles, em razão da "informação" que carregam. Assim, é que informação é o "dado analisado e com algum significado" (AMARAL, 2016, posição 312). Esse "valor" coletado dos "dados", ou seja, a "informação" extraída dos dados (logo, o dado não é a informação, mas carrega ela) na iniciativa privada, para uma

empresa ou indústria, por exemplo, possuem alto valor financeiro, em razão de proporcionar organização, elaboração de projetos, revisão de metas, projetos de bens, estabelecimento de público alvo, etc., momento em que o estudo acerca da privacidade torna-se relevante.

O *Big Data*, portanto, trata dos dados eletrônicos em formato digital, que possuem um ciclo de vida onde são produzidos, armazenados, transformados, analisados e descartados (CARDOSO JUNIOR; LIMA, 2018, p. 124).

> Big Data não se trata apenas de processos que geram grandes volumes de dados, que precisam de servidores em cluters para serem analisados. Big Data é muito mais que isso: é uma mudança social, cultural é uma nova fase da revolução industrial. Consequentemente, Big Data não trata apenas de problemas de dados solucionados através de MapReduce, ou uma de suas implementações. Big Data é um fenômeno e não uma tecnologia. Big Data também não significa o fim do modelo relacional ou do data warehouse tradicional, que são ótimas em fazer o que se propõe e não são adequadas a resolver problemas de dados para os quais, quando foram desenhadas, não existiam (AMARAL, 2016, posição 405).

Os indivíduos produzem "dados" constantemente, até mesmo através das coisas (da IoT), o que leva a uma segunda fase que é a "mineração dos dados". A mineração de dados (*data mining*) é a "técnica de tratamento e exploração de dados", ou seja, "pré-processamento, extração e exploração de grande quantidade de dados visando estabelecer padrões consistentes" (BOFF; FORTES; FREITAS, 2018, p. 190-191).

Logo, somente, a partir da "mineração dos dados" é que as empresas terão o valor extraído dos dados, ou seja, as informações, agregando-se aí alto valor financeiro. É a partir do tratamento dos dados, que a privacidade aparece mais fragilizada. Não que ela não esteja exposta desde a coleta. O fato é que com o tratamento dos dados, que se inicia com a mineração e a extração da informação que carregam, é que eles passam a ter valor para a indústria e o comércio, e daí sua maior exposição.

Ademais, o *Big Data* é uma tecnologia que permite a análise de qualquer registro, naturais ou não, inclusive em redes sociais, conhecido como *datafication*, em que até mesmo o movimento de um celular, o acionamento de um freio, a gravação de uma câmera, são registros capazes de serem armazenados, transformados, analisados e descartados (AMARAL, 2016, posição 411). Com as informações coletas ou fornecidas, inclusive pela IoT, é possível, portanto, manipular o comportamento, interesses e vontades dos indivíduos (LINDOSO, 2018, p. 250). Percebe-se, pois, que os dados coletados, sejam eles sensíveis ou não, possuem verdadeiro "poder" em razão da informação que carregam, gerando, da análise das informações o ambiente propício para tomadas de decisão.

O sistema de internet das coisas (IoT), deve ser compreendido pelos seguintes fatores: a) quais objetos serão conectados (afinal praticamente tudo pode ser conectado

à internet), b) qual sistema será responsável pela comunicação dos objetos, c) a existência de interoperabilidade entre diversos sistemas utilizados, d) como será feita a análise dos dado, e) a segurança na captura e tratamento dos dados e, f) o feedback dos dados captados e a implantação de alguma melhoria no serviços prestados/analisados (DIAS, 2016, posição 364). Logo, a compreensão acerca do *Big Data* está bem presente na IoT, pois do grande volume de dados gerados e, seus refl xos no processo decisório, é que permite extrair a potencialidade discriminatória e a possibilidade de violação do direito à privacidade. Nessa linha, proteger juridicamente o cidadão de quem detém os dados que dizem respeito a sua pessoa, quer se trate de organismo público ou privado, é medida impositiva, que se vislumbra na observância da privacidade.

3 A OBSERVÂNCIA AO DIREITO DE PRIVACIDADE DO CIDADÃO PELA INTERNET DAS COISAS

O tema direito à privacidade apresenta-se sob vários aspectos e, como visto, a internet das coisas, também possibilita: a coleta, utilização, acesso, transmissão, processamento, armazenamento, enfim, realizada ou viabiliza o tratamento de dados pessoais. Os dados, é bom destacar, podem traduzir aspectos de personalidade, comportamento e preferencias (LIMGERBER, 2007, p. 58), que são úteis e de grande valor econômico na iniciativa privada. O fato é que diante de todas as possibilidades de coleta de dados pelas coisas, a proteção à privacidade tornou-se uma preocupação secundária. Ademais, com o aumento da troca de dados entre pessoas e coisas e entre coisas e coisas, as informações extraíveis também tomaram grandes proporções. Assim, pode-se compreender, também que dados pessoais são todas as informações "nominativas" de qualquer gênero "que permitem identificar uma pessoa de maneira direta" (LIMBERGER, 2007, p. 61).

O artigo 12 da Declaração Universal dos Direitos Humanos assegura que ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, portanto, garante a privacidade do cidadão. Na mesma linha, é a redação do artigo 5º da Constituição da República de 1988 (BRASIL, 1988), ao estabelecer a inviolabilidade da "vida privada, a honra e a imagem" (inciso X), da "casa" (inciso XI) e da "correspondência" (inciso XII). O Marco Civil da Internet (BRASIL, 2014) em seu artigo 3º, II e III, respectivamente, estabelece como princípios a proteção da privacidade e dos dados pessoais, bem como ao direito de inviolabilidade da intimidade e da vida privada (artigo 7º, I). Há, inclusive, em tramitação no Senado Federal uma Proposta de Emenda Constitucional nº 17 (BRASIL, 2019) que incluiria a proteção de dados pessoais entre os direitos e garantias fundamentais do cidadão. Não resta dúvida que a privacidade é direito humano e fundamental, de eficácia

horizontal (LIMBERGER, 2007, p. 38), explicitamente reconhecida, razão pela qual, seu afastamento ou abrandamento, necessita da devida justificativa, também, constitucional, na medida em que cada direito fundamental traz em si uma declaração e um limite (LIMBERGER, 2007, p. 35). Não há que se limitar tais proteções apenas à esfera física/analógica, estendendo-se, também, obrigatoriamente ao âmbito digital/eletrônico. Por óbvio, todos os mecanismos, ou "coisas" aptas a viabilizarem o tratamento dos dados de qualquer cidadão, estão sim, expondo a privacidade. Poderiam "coisas" serem responsabilizadas pela coleta, armazenamento e envio de dados? Certamente não. Contudo, uma vez que esses dados passam a integrar a esfera de outra entidade, como uma empresa, por exemplo, passa ela a ser responsável por estes dados, cabendo-a zelar pela sua gestão/tratamento.

Com bem alerta Stefano Rodotà (2008, p. 23) as "novas dimensões da coleta e do tratamento de informações" forçaram uma nova (re)configuração de determinados conceitos dentre eles o do direito à privacidade. Veja-se que não se está falando aqui de preenchimento de algum cadastro ou ingresso em alguma rede social, e sim de "coisas", como um aspirador de pó "robô", um celular ligado ou um veículo em movimento, que, simplesmente, por estarem nessas condições, são aptos a captar dados e enviá-los a uma central. É claro, que para tanto, deve haver um aceitação explícita do cidadão para o envio desses dados e, como bem destaca o Autor italiano, a defesa da privacidade ou a coleta de dados pode adotar sentidos distintos "dependendo de qual seja o objetivo perseguido através da coleta das informações" (RODOTÀ, 2008, p. 29). Não é à toa que a maior resistência de acesso aos dados dizem respeito às informações econômicas/financeiras (RODOTÀ, 2008, p. 30). Uma vez coletados e processados, os dados passam a ter valor, pois deles são extraídos informações, que expõem nossas preferencias, desejos, necessidades, etc.

Assim, para que os dados sejam coletados, a partir de coisas (IoT) ou não, devem deixar claro ao indivíduo/consumidor os objetivos de sua utilização, uma vez que diante dessa informação, caberá a ele (cidadão) escolher se abre ou não mão de sua privacidade. Qualquer dado/informação, ainda que anônimo, utilizado fora desse objetivo, deve ser imediatamente eliminado (apagado) e os responsáveis pela sua manipulação responsabilizados. Na Alemanha essa aceitação, que envolve diretamente elementos da personalidade, denomina-se: direito à "autodetereminação informativa" ou "autopresentação" que consiste no direito de o próprio indivíduo decidir acerca da divulgação e utilização de seus dados pessoais possibilitando, inclusive, que o indivíduo "se insurja contra as falsas, não autorizadas, degradantes ou deturpadas representações de sua pessoa, bem como o protege das observações secretas e indesejadas de sua personalidade (MENKE, 2015, p. 210). Diferencia-se da autodeterminação que trata do direito de o individuo determinar/definir sua identidade, desde a origem biológica até a orientação sexual. Também se distingui da "autopresentação" que consiste na

garantia de o indivíduo recolher-se para si, de ficar só, abrangendo o sigilo a diários pessoais, boletins médicos e materiais biológicos (MENKE, 2015, p. 210).

Stefano Rodotà (2008, p. 35), inclusive chega a sugerir que se fosse possível redefinir uma classificação acerca da privacidade, o grau máximo de opacidade seria dada àquelas que pudessem gerar práticas discriminatórias, sendo de grau "máximo de transparência àquelas que, referindo-se à esfera econômica dos sujeitos, concorrem para embasar decisões de relevância coletiva". Logo, a privacidade não possui caráter absoluto e sua limitação deve estar condicionada a determinadas circunstâncias, como a exigência legal de seu abrandamento, para evitar eventuais "intromissões ilegítimas" (LIMBERGER, 2007, p. 127-130). Da mesma maneira os dados coletados deveriam ser mínimos, "*no sólo para preservar el derecho a la protección de datos, sino también para darles mayor efectividad*" (BATALLA, 2010, p. 735). Essa preocupação se deve, principalmente, em razão da utilização que pode ser dada aos dados dos indivíduos, uma vez que estes podem ser manipulados por instituições (públicas ou privadas) sem que o indivíduo saiba disso (MENKE, 2015, p. 211). É exatamente no combate à manipulação dos dados e à discriminação que pode ser gerada em razão das informações, que o respeito à privacidade se impõem.

Há de se ter presente, também, que o consentimento na utilização de dados por uma entidade (pública ou privada), ainda que fornecido pela internet das coisas, deve deixar claro, inclusive, a possibilidade compartilhamento (ou não). A utilização desses dados, ainda que com o consentimento do indivíduo, com finalidade diversa daquela inicialmente fornecida, deve gerar, além da indenização, a exclusão/apagamento dos mesmos. Portanto, parte-se, da premissa, que a finalidade na coleta de dados pelas coisas, são legítimas, específicas e conhecidas pelo titular. (BOFF; FORTES; FREITAS, 2018, p. 107)

A proteção dos dados, como bem afirma Rodotà (2008, p. 19), está vinculado à proteção da personalidade e não da propriedade, razão pela qual, ainda que possam adquirir valor, algumas categorias, como natureza médica ou genética, não poderiam ser utilizados de maneira negocial. É por essa razão, que o autor, inclusive, vai exigir especial atenção à "minimização da coleta de dados", na qual nenhum dado pessoal deve ser coletado se a finalidade puder ser alcançada de outra forma (quer dizer, sem o tratamento de dados pessoais). (RODOTÀ, 2008, p. 20)

São por todas essas razões, que o direito à privacidade incialmente atrelado à noção inicial de garantia de ser deixado só, evoluiu até alcançar a gestão das informações criadas a partir da coleta de dados. É, portanto, como escreve Stefano Rodotà (2018, p. 92), a definição de privacidade uma aproximação com o "direito de manter o controle sobre as próprias informações", sejam elas fornecidas pelos indivíduos ou oriunda da internet das coisas. Sendo, portanto, dado toda "informação que permite identificar uma pessoa de maneira direta" (LIMBERGER, 2007, p. 61), irrelevante que tenha sido

adquirido por uma coisa (IoT), necessitando, sempre, do consentimento do indivíduo para sua utilização, incluindo-se, na coleta dos dados, a finalidade dos mesmos.

4 CONCLUSÃO

O conceito de privacidade necessitou se reconfigurar ao mesmo tempo em que as tecnologias evoluíram, porque as intromissões, inicialmente, físicas, passaram a ser, também, por meio digital. Não é por outra razão, que surgiram diversas legislações nacionais e internacionais objetivando proteger juridicamente a privacidade do cidadão. No caso do Brasil, pode-se citar, exemplificativa ente, o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018).

A internet das coisas (IoT), juntamente com o *big data,* são capazes de coletar e armazenar milhões de informações, que uma vez estruturadas, passam a ter substancial valor econômico, em razão de seu alto poder de comercialização, sendo aptas, inclusive, de controlar o comportamento humano. Diante do tratamento que pode ser efetuado a essas informações, o direito à privacidade do cidadão *ex surge* como função limitadora, apta a coibir excessos e intromissões indevidas. São, por tais motivos, que o consentimento expresso do indivíduo é pré-requisito condicionante para que as "coisas" possam colher seus dados. Ademais, o cidadão, para permitir conscientemente sobre a coleta dos dados, deve saber antecipadamente a finalidade que será dada à informação, sob pena de a mesma ser considerar ilícita.

Vislumbrou-se, ainda, que mesmo que possuam alto valor, os dados enquadram-se na categoria de direitos de personalidade, e não de propriedade. Isso de deve ao fato de que uma vez estruturados, os dados podem permitir a identificação do cidadão e, por isso, não são de livre disposição.

Como as "coisas" possuem frágil sistema de segurança, compete ao proprietário do sistema (e não ao cidadão) o dever de zelar para que as informações coletadas tenham a finalidade previamente comunicada. Este é outro motivo que demonstra a importância do consentimento expresso e o objetivo previamente noticiado para as que as "coisas" tenham acesso às informações dos indivíduos.

5 REFERÊNCIAS BIBLIOGRÁFICAS

AMARAL, Fernando, **Introdução a ciência de dados: mineração de dados e Big Data**, Rio de Janeiro, Alta Books, 2016, Documento disponível para Kindle.

BATALLA, Antoni Roig. Intimidad y administración electrónica. **Administración electrónica: la ley 11/2007, de 22 de junio , de acceso electrónico de los ciudadanos**

a los Servicios Públicos y los retos jurídicos del e-gobierno en España, coords. HUESO, Lorenzo Coutinho; TORRIJOS, Julián Valero, Valencia, Tirant, 2010, p. 729-748.

BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade: do direito às novas tecnologias na sociedade da informação**, Rio de Janeiro, Lumen Juris, 2018.

BRASIL. Constituição da República Federativa do Brasil de 1988. **Presidência da República,** Brasília, DF, 1988. Site: http://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm [Data da consulta: 02 de junho de 2019].

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Presidência da República**, Brasília, DF, 2014. Site: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm [Data da consulta: 03 de junho de 2019].

BRASIL. Decreto nº 8.777, de 11 de maio de 2016. Institui a Política de Dados Abertos do Poder Executivo federal. **Presidência da República,** Brasília, DF, 2016. Site: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8777.htm [Data da consulta: 02 de junho de 2019].

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). **Presidência da República**, Brasília, DF, 2016. Site: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm [Data da consulta: 02 de junho de 2019].

BRASIL. **Proposta de Emenda à Constituição**, nº 17, de 2019. Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Site: https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1559567994616&disposition=inline [Data da consulta: 02 de junho de 2019].

DIAS, Renata Rampim de Freitas, **Internet das coisas sem mistérios: uma nova inteligência para os negócios**, São Paulo, Netpress Books, 2016, Documento disponível para Kindle.

CARDOSO JUNIOR, Ataíde Pereira; LIMA, Alessandro Wendel Borges de, A segurança

da informação na indústria 4.0. **Industria 4.0: conceito e fundamentos**, coords. SACOMANO, José Benedito; GONÇALVES, Rodrigo Franco; SILVA, Márcia Terra da; [et.al.], São Paulo, Bluncher, 2018.

LIMBERGER, Têmis, **O direito à intimidade na era da informática: a necessidade de proteção dos dados pessoais**, Porto Alegre, Livraria do Advogado, 2007.

LINDOSO, Maria Cristiane Branco, Conflitos no uso da tecnologia do Big Data: violação de privacidade e discriminação pelo processamento de dados. **Tecnologia jurídica e direito digital: I Congresso Internacional de direito e tecnologia**, coords. FERNANDES, Ricardo Vieira de Carvalho; COSTA, Henrique Araújo; CARVALHO, Angelo Gamba Prata de, Belo Horizonte, Fórum, 2018, p. 241-262.

MACHADO, Felipe Nery Rodrigues, **Big data: o futuro dos dados e aplicações**, São Paulo, Érica, 2018, Documento disponível para Kindle.

MAGRANI, Eduardo, **A internet das coisas**, Rio de Janeiro, FGV Editora, 2018.

MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. **Direito, inovação e tecnologia**, coords. MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P., São Paulo, Saraiva, 2015, p.205-230.

RODOTÀ, Stefano, **A vida na sociedade da vigilância: a privacidade hoje**, Trad. de Danilo Doneda e Luciana Cabral Doneda, Rio de Janeiro, Renovar, 2008.

ROZSA, Vitor; Dutra, Moisés Lima; PINTO, Adilson Luiz; MURIEL-TORRADO, Enrique, O paradigma tecnológico da internet das coisas e sua relação com a ciência da informação, **Inf. & Soc.:Est**., João Pessoa, v. 27, n. 3, p. 255-266, set./dez. 2017.

SACOMANCO, José Benedito; SÁTYRO, Walter Cardoso, Indústria 4.0: conceitos e elementos formadores. **Indústria 4.0: conceito e fundamentos**, coords., SACOMANO, José Benedito; GONÇALVES, Rodrigo Franco; SILVA, Márcia Terra da; [et.al.], São Paulo, Bluncher, 2018.

SCHWAB, Klaus, **Aplicando a quarta revolução industrial**, Trad. Daniel Moreira Miranda, São Paulo, Edipro, 2018.

STEVAN JUNIOR, Sergio Luiz; LEME, Murilo Oliveira; SANTOS, Max Mauro Dias, **Industria 4.0: fundamentos, perspectivas e aplicações**, São Paulo, Érica, 2018.

TELETRABALHO

LOS ELEMENTOS ESENCIALES DEL CONTRATO DE TRABAJO EN LAS NUEVAS FORMAS LABORALES EN UN MUNDO GLOBALIZADO - CALL CENTERS, AIRBNB Y UBER

Eje temático: Trabajo en el siglo XXI - Teletrabajo

Autora:
Danny Alejandra Cuevas López
Alumna de grado, Universidad Santo Tomás

ABSTRACT
Una de las tareas que el derecho laboral debe abordar son las lagunas jurídicas que hay ante la evolución de las formas tradicionales de trabajo, de modo que el presente artículo de investigación busca plantear la existencia del contrato de trabajo que tienen las plataformas digitales con los teletrabajadores, al cumplirse los elementos esenciales del contrato de trabajo que requiere la relación laboral para nacer a la vida jurídica, partiendo de los conceptos básicos que permiten materializar el trabajo digno. Siendo relevante para la doctrina jurídica, dado que la incorporación en la vida cotidiana de las nuevas formas de trabajo, requiere que todos los países se prepararen para afrontar y dar solución a todos los futuros pleitos legales, como las demandas laborales que ya se han venido presentando en Estados Unidos, frente a la existencia de la relación laboral entre las plataformas digitales y sus respectivos trabajadores. En este orden de ideas, tiene como finalidad consolidar nuevos conocimientos de la prestación personal de servicios, la subordinación, la remuneración y las formas como las plataformas digitales tergiversan el contrato de trabajo para evitar obligaciones laborales frente a sus trabajadores. Por lo tanto, primero se estudiará el concepto de trabajo digno, los elementos esenciales del contrato de trabajo según la legislación colombiana y finalmente, se analizará cada uno de los elementos esenciales del contrato de trabajo para Colombia frente a los Call Centers, Airbnb y Uber. En consecuencia, la importancia de desarrollar los conceptos básicos de trabajo y trabajador, permite tener una perspectiva que este a la vanguardia con las nuevas formas laborales que brindan las plataformas digitales del mundo globalizado y, amplificar los elementos esenciales para la existencia del contrato de trabajo, mediante derecho comparado y pronunciamientos de la Organización Internacional del Trabajo (OIT).

INTRODUCCIÓN

Han transcurrido 18 años desde que inició el siglo XXI trayendo consigo la era de la tecnología y a su vez eventos importantes han acaecido en la vida del hombre desde entonces, ejemplos de esto ha sido la interconexión en tiempo real con personas mediante dispositivos electrónicos, sistemas GPS que permiten la búsqueda satelital, hacer trámites bancarios desde el celular, realizar compras online en tiendas ubicadas

a la vuelta de la esquina o en otro continente y que los productos lleguen a la puerta de la casa del comprador, pagar facturas desde dispositivos móviles y trabajar sin que la persona salga de la casa usando tecnologías de la información o como se conoce teletrabajo. En concordancia, la inmersión en esta nueva era permitió que surgiera a su paso, nuevas formas de trabajo poniendo en reto el derecho laboral, ya que debe encargarse de evolucionar el concepto de que es trabajo, que es trabajador y la protección de los todos los derechos de los trabajadores frente a las nuevas modalidades del trabajo.

Por consiguiente, se estudiará ¿si existe una relación laboral en las nuevas formas de trabajo en un mundo globalizado?

A lo largo de la historia han surgido varias definiciones acerca de lo que es el trabajo, según el contexto histórico, el contexto social, el país, la disciplina que lo estudie o como se haya descrito normativamente en cada jurisdicción, por lo cual se iniciará con un concepto general que brinda el Director Regional Adjunto de la Oficina Regional de la Organización Internacional del Trabajo para América Latina y el Caribe, Levaggi (2004) define al trabajo como "el conjunto de actividades humanas, remuneradas o no, que producen bienes o servicios en una economía, o que satisfacen las necesidades de una comunidad o proveen los medios de sustento necesarios para los individuos" (párr.3)[406].

1. EL TRABAJO DIGNO EN LA NORMATIVIDAD COLOMBIANA

Concepto que ha evolucionado dejando en firme que no se puede hablar de una noción aislada de trabajo, esta requiere de una dignificación del trabajo, es decir, el trabajo debe concebirse bajo el entendido de unas garantías universales y las condiciones en que el trabajador presta el servicio, sean las que un individuo merezca teniendo en cuenta su dignidad humana y su condición de ser humano.

El trabajo digno se materializa en un horario digno de trabajo, un salario mínimo digno y un sistema completo de seguridad social hacia los trabajadores.

El horario digno de trabajo se refiere a un horario máximo de horas laborales que no exceda el establecido por cada ley y en caso de excederse un pago extra por cada hora laborada adicional al horario de trabajo. Un salario mínimo digno que sea capaz no solo de cubrir las necesidades del trabajador y su núcleo familiar en alimentación, vestuario, educación y recreación, sino que también el trabajador tenga la seguridad que menos de ese salario no va a recibir. Y un sistema de seguridad social que dé al trabajador todas las prestaciones laborales de salud, pensión y riesgos laborales.

406 Sitio Web: https://www.ilo.org/americas/sala-de-prensa/WCMS_LIM_653_SP/lang--es/index.htm [Fecha de última consulta: 20 de agosto de 19]

Ese grupo de obligaciones para el empleador y derechos para el trabajador son los que de cierto modo califican al trabajo como digno, junto con las disposiciones consagradas en los Derechos Económicos Sociales y Culturales y en la Constitución Política de Colombia en el artículo 25[407], donde se incluye la igualdad de oportunidades para los trabajadores, mínimo vital, estabilidad en el empleo, irrenunciabilidad a los beneficios mínimos, facultad de transigir y conciliar, situación más favorable al trabajador, primacía de la realidad sobre las formalidades, garantía a la seguridad social y la protección especial a la mujer y a la maternidad.

Los cuales son derechos que siempre van a prevalecer sobre cualquier mandato, convenio o contrato celebrado entre el empleador y trabajador, en el que el trabajador va a ser el más protegido por el derecho laboral.

2. ELEMENTOS ESENCIALES DEL CONTRATO DE TRABAJO EN EL CÓDIGO SUSTANTIVO DE TRABAJO COLOMBIANO

Esos derechos laborales al ponerlos en acción entre las partes, van a consagrarse en una fuente que es el contrato de trabajo, por medio del cual se van a establecer las condiciones de esos derechos laborales, la forma como se van a materializar, bajo que términos legales y establecer los tres elementos esenciales estipulados en el artículo 25 del Código Sustantivo de Trabajo[408], que son la prestación personal del servicio, la subordinación y el salario.

2.1 Prestación personal del servicio

Respecto a la actividad personal del trabajador, no es otra cosa que la prestación del servicio o ejecución del trabajo personalmente por el trabajador contratado. Si el contrato de trabajo se firmó con determinada persona, será esa persona y no otra quien tiene que desarrollar las actividades contempladas en el contrato. (Madero, 2012, p. 22)[409].

La prestación personal del servicio que se refiere el código es intuito personae, es decir que quien firma el contrato de trabajo o pacta la relación laboral verbalmente será la misma persona quien realizará el trabajo, esta prestación personal no se refiere a que el trabajo sea prestado físicamente, pues como se explicará más adelante las

407 Constitución Política de Colombia, publicada en la Gaceta Constitucional No. 116 de 20 de julio de 1991

408 Código sustantivo del trabajo. Diario oficial de la República de Colombia No 27.622, del 7 de junio de 1951

409 Madero, Y. (2012). *Guía laboral 2012*. Bogotá. ECOE. ISBN: 9586487687

nuevas concepciones laborales permite trabajar mediante plataformas digitales, sin la presencia física de la persona.

2.2 Subordinación

El segundo elemento, y el más importante de todos, hace referencia a la obligación del trabajador de acatar las órdenes que le imparta su patrón. La continuada subordinación a que se riere la ley, no es otra cosa que la facultad que tiene el empleador de disponer de la capacidad de trabajo de su empleado, según su conveniencia y dentro de los parámetros pactados en el contrato de trabajo. La subordinación es la obligación que tiene el trabajador de acatar las órdenes que le imparta su empleador. (Madero, 2012, p. 22)[410].

Existen medios de subordinación expresos que tradicionalmente se encuentran pactados en el contrato de trabajo, pero existen otros medios de subordinación que los trabajadores se adhieren con el simple hecho de vincularse a una plataforma digital, que no son convencionales como los que comúnmente se conoce, pero si estipulan reglas que debe seguir el trabajador, las cuales al no cumplirse le traerá repercusiones a este último, es decir, que las plataformas digitales tienen mecanismos para controlar el mal comportamiento de sus trabajadores.

2.3 Salario

El tercer elemento corresponde a la contraprestación económica que recibe el trabajador por su trabajo, contraprestación comúnmente conocida como salario. (Madero, 2012, p. 22)[411]

Es claro que el trabajador recibirá una remuneración por el trabajo prestado, por tanto, la autora permite dejar a libre apreciación respecto de quien es la persona que pagará por su trabajo, si es la plataforma digital o son los usuarios que usan el servicio que los trabajadores prestan.

3. ELEMENTOS ESENCIALES DEL CONTRATO DE TRABAJO EN COLOMBIA FRENTE A LAS PLATAFORMAS DIGITALES

3.1 Los Call Centers

410 ídem
411 ídem

Los Call centers son un ejemplo de una forma de trabajo muy común en el siglo XXI, debido a que el usuario telefónico tiene "(una cadena de opciones rutinarias (una compra de una pizza, de un boleto, la solicitud de una información, etcétera) o bien la complejidad de una atención a un cliente que requiere asistencia técnica o que va a plantear una queja)". (Micheli, 2006, p. 2)[412]

Es decir, al existir la necesidad de prestar un soporte técnico a los consumidores frente a los problemas o fallas que pudieran presentar los dispositivos electrónicos, las empresas se encargaron de capacitar personas, en adelante teleoperadores que presten servicios técnicos desde cualquier parte del mundo mediante vía telefónica, sin necesidad de que un especialista tenga que desplazarse al lugar donde se encuentre el dispositivo o que por el contrario este deba enviarse hasta donde se encuentre el especialista para que lo revise.

Lo primero que se puede evidenciar es que el teleoperador no hace una prestación de servicio personal al cliente y pueda que tampoco a su empleador, ya que no es necesario que todos los teleoperadores se encuentren en una determinada oficina para realizar su trabajo, sino que desde su casa puede recibir la llamada y realizar el trabajo o la atención al cliente frente a la necesidad que presente. De hecho, lo que busca principalmente los Call center es prestar un servicio en cualquier momento, por eso es muy habitual que haya cubrimiento del servicio en cada continente y que el usuario tenga una atención de tiempo completo.

Aunque no pareciera que se configure el primer elemento del contrato de trabajo, si se presenta, debido a que el trabajador realiza una actividad humana y presta un servicio en beneficio de otro. El punto clave a estudiar sería si el concepto de la "prestación personal del servicio" permite que ese servicio sea prestado mediante una llamada telefónica. Pero como se mencionó al inicio, las nuevas formas de trabajo necesitan que los conceptos se amplíen o sean concebidos de otra manera, como lo expresa Beltrán y Sánchez (2002)[413].

La idea que se tiene de relación laboral está fundada en los criterios de unidad de tiempo, lugar y acción. Con el devenir de nuevas tecnologías, como la informática, se aprecia que estos parámetros se deshacen; y nacen en consecuencia, figuras como el teletrabajo, donde el lugar a prestar el servicio no será necesariamente las instalaciones de la empresa, y los horarios para cumplir las labores establecidas por el empleador no podrán ser controladas directamente por él en muchos casos (p. 52).

412 Micheli, J. (3/5 enero-mayo 2007). *Los call centers y los nuevos trabajos del siglo XXI. CONfines.*

413 Beltran, A. y Sanchez, L. (2002). *Las relaciones laborales virtuales: el teletrabajo* (Trabajo de grado). Pontificia Universidad Javeriana, Bogotá

La subordinación y la remuneración también son un problema complejo de determinar en el teletrabajo, ya que un estudio realizado en Chile por Flores, C (2014)[414] determinó que el teleoperador:

Desempeñaba labores bajo un esquema de contratación llamado outsourcing o triangulación laboral (relación laboral que en la totalidad de los casos se produjo de forma individualizada). En este esquema se establece una relación de subcontratación, donde lo que la empresa mandante contrata con la empresa de CC es el contacto con los clientes, la administración de dicha relación efectuada por un tercero (p. 196).

Conviene precisar que el outsourcing es una subcontratación, donde una empresa le da facultades a otra para que se encargue de una determinada labor, por ejemplo, recursos humanos, contratación o contabilidad, es decir, que existe un intermediario entre el trabajador y la empresa principal quien requiere un servicio.

El recurso de las empresas de telecomunicaciones a la externalización, la deslocalización y la subcontratación indica que mantienen relaciones contractuales comerciales con proveedores externos (que se rigen por criterios de precio y calidad, entre otros) en vez de relaciones de trabajo directas con su personal (Organización Internacional del Trabajo, 2015 p. 21)[415].

Dependiendo las facultades entregadas por la empresa principal al intermediario este puede desde establecer las condiciones de subordinación y la remuneración o simplemente concretar con la empresa principal quien se encarga de subordinar y quien se encarga de pagar el salario a los trabajadores.

Este método de contratación dificulta la existencia de una relación laboral entre el trabajador y la empresa principal, pero para evaluar quien tiene la relación laboral con el trabajador se debe estudiar cada caso en particular, dependiendo lo pactado en el contrato y la normatividad laboral en cada país.

3.2 Airbnb

Una plataforma digital muy usada por los viajeros es Airbnb que es un nuevo modelo de empresa en el mundo y su vez una evolución del concepto de hotelería.

Mediante esta aplicación una persona, en adelante "anfitrión" puede ofrecer en renta su casa por un determinado tiempo, estipular qué normas debe cumplir la persona quien desee rentar el lugar, en adelante "viajero" durante la estadía, puede establecer el precio que desee cobrar por día, los días mínimos de estadía que se

414 Flores, C. (2014). *Condiciones de trabajo en la industria de call center en Chile: La situación laboral de los teleoperadores de empresas tercerizadas ubicadas en santiago* (tesis de pregrado). Universidad Academia De Humanismo Cristiano, Santiago.

415 Organización Internacional del Trabajo. (2015). *Las relaciones de trabajo en los servicios de telecomunicaciones y en el sector de los centros de llamadas.* Ginebra. ISBN: 978-92-2-330048-7.

le permite rentar al viajero, recibir el pago anticipado por la renta del lugar y tener referencias personales de quien es la persona que se hospedará.

A cambio, el viajero va a tener una variedad de opciones en la renta de lugares durante sus viajes, va a encontrar precios cómodos a comparación si él se hospedará en un hotel, puede decidir si desea compartir la estadía con más personas o por el contrario desea un lugar completamente privado, etc.

En comparación al trabajo del Call center, el trabajo como anfitrión de un Airbnb si se evidencia la prestación personal del servicio ya que requiere la interacción entre el anfitrión y el viajero previo, durante y posterior al hospedaje, se pacta una remuneración a cambio de la estadía, pero es difícil evidenciar el elemento de subordinación para la existencia de un contrato de trabajo.

Pues bien, al momento de que una persona desea suscribirse a la aplicación de Airbnb como anfitrión ella debe cumplir con ciertos requisitos como lo son, brindar una estancia cómoda al huésped, contar con implementos de limpieza que cualquier hotel tendría, dar una respuesta rápida a las solicitudes de alojamiento, entre otras. Cabe señalar que al no cumplir alguna de las reglas Airbnb tiene la facultad de expedir una evaluación inmediata, bloquear la posibilidad de reservación o suspender la cuenta del anfitrión.

Surgiendo consigo las siguientes preguntas ¿puede una plataforma digital como Airbnb ser empleador de una persona? ¿existe una relación de subordinación entre el anfitrión y la aplicación Airbnb?

El empleador "puede ser persona natural o jurídica y es quien ordena y recibe el servicio" (Chavarro y Cortes, 2017, p. 11)[416], en otras palabras, una plataforma digital constituida como persona jurídica puede ser empleador de una persona natural y al momento que decide aceptar cada una de las directrices que le impone para ser trabajador, se logra demostrar el elemento de subordinación en el contrato de trabajo.

En ese mismo orden de ideas, destacamos los razonamientos de quienes propenden por una nueva concepción de la subordinación, que gire no solamente en torno al dominio de la relación laboral, sino en torno al control productivo, que permita dar respuesta a las nuevas formas productivas y de ejercicio del poder empresarial y que tenga en cuenta nuevos indicios vinculados a las ideas de coordinación y de producción, relacionados con la inserción del trabajador en un ámbito organizativo que no le es propio (Gnecco, 2011, p.145)[417].

416 Chavarro, J. y Cortes, G. (2017). *Cartilla laboral y seguridad social 2017*. Bogotá. Grupo Editorial Nueva Legislación. ISBN: 978-958-56087-1-9.

417 Gnecco Mendoza, G. (2011). La relación de trabajo. En: J. Herrera Vergara, G. Valdés Sánchez y S. Corradetti, ed., *Globalización. El cambio del derecho del trabajo*. Bogotá: Universidad de Rosario.

3.3 Uber

Finalmente, se analizará los elementos del contrato de trabajo en la plataforma digital Uber, esta aplicación da la oportunidad de que los conductores de automóviles presten un servicio de transporte a los usuarios, los cuales van a establecer donde una ruta de viaje y la aplicación va a calcular el costo aproximado.

Al igual que en la plataforma digital Airbnb, consta de una prestación personal del servicio por parte del conductor de Uber, una determinación de las condiciones de trabajo que debe cumplir el conductor para poder trabajar en esta empresa y unas sanciones tanto económicas como restrictivas laboralmente en caso de incumplimiento, denotando el elemento de subordinación.

Como se indicó al inicio, en Airbnb quien establece el precio del servicio es el anfitrión, en oposición en Uber quien establece el precio que el usuario debe pagar al conductor por la prestación del servicio es la aplicación, teniendo en cuenta la distancia del viaje, el clima, la hora y el lugar de solicitud, entre otros.

Un punto en convergencia que tiene Airbnb y Uber es la remuneración, ya que ninguna de estas empresas les paga a sus trabajadores por la prestación del servicio, por el contrario, toman una comisión por cada servicio realizado por su trabajador, poniendo en duda si existe un contrato de trabajo en cuanto al elemento del salario.

Un informe traducido por la Biblioteca del Congreso Nacional de Chile (2018)[418] afirma:

> "la Unemployment Insurance Appeal Board del Estado de Nueva York en julio de 2018, determinó que existe una relación laboral entre Uber y los conductores y que ella permite sostener que estos últimos son trabajadores. Esta calificación se dio en el marco de una apelación por la no concesión de beneficios como desempleados de tres ex conductores vinculados a Uber (p. 6).

Es claro que el sistema normativo de Estados Unidos es diferente al de Colombia, por ende, sus fallos serán igual, pero para el caso en estudio el pronunciamiento de la Corte es garantista al dar respuesta a los derechos que tienen los trabajadores de las plataformas digitales.

La necesidad de abordar jurídicamente estas nuevas formas de trabajo "Se trata simplemente de dinamizar, protegiendo a quienes tienen un estatus jurídico, que tal vez hoy no está tan determinado por cuenta de las nuevas formas de trabajo y protegiendo a los empresarios que son los que generan el empleo" (Ospina, 2018, párr. 12) [419].

418 Biblioteca del Congreso Nacional de Chile. (2018). *Uber y conductores. Legislación comparada sobre relación laboral.*

419 Ospina, N. (2018). Ámbito Jurídico. Columnista online. *Trabajadores de plataformas digitales: ¿nuevo estatus jurídico?*

Dentro de este contexto, la problemática planteada debe conllevar a los juristas laborales a la creación de un derecho laboral garantista para el trabajador de las plataformas digitales que integran la evolución en esta era. El cual debe estar en armonía, primero con la Constitución Política, con los derechos sociales, económicos y culturales y los tratados internacionales.

Y, por el contrario, no dejándose dilucidar ante las formas de contratación no convencionales, que no especifican las obligaciones taxativamente, pero que, si existe diferentes mecanismos de control incluso más agresivos que los tradicionales para los trabajadores, reluciendo el elemento principal para la existencia del contrato de trabajo que es la subordinación.

CONCLUSIONES

Finalmente se puede concluir, que se ha presentado una notable evolución en las formas tradicionales de trabajo, por lo tanto, en Colombia el derecho laboral debe estar a la vanguardia para solucionar los pleitos legales que se pudieran presentar en un futuro, sin desconocer el derecho interno y las normas internacionales.

Segundo, es necesario ver desde una perspectiva amplificada los elementos del contrato de trabajo para afirmar la existencia de la relación laboral entre las plataformas digitales y sus trabajadores.

Tercero, para determinar la existencia del vínculo laboral ante las nuevas formas de trabajo se debe realizar un estudio respecto a cada plataforma digital y cuáles son las condiciones que debe aceptar el trabajador para suscribirse a ella, donde el elemento más importante para dar respuesta si existe no el contrato de trabajo será la subordinación.

Por último, las nuevas formas de contrato de trabajo como el outsourcing han venido camuflando las obligaciones que tiene los empleadores con el propósito de evadirlas. Por eso es importante la intervención oportuna del derecho laboral frente a estos contratos laborales.

REFERENCIAS

Beltran, A. y Sanchez, L. (2002). *Las relaciones laborales virtuales: el teletrabajo* (Trabajo de grado). Pontificia Universidad Javeriana, Bogotá. Recuperado de https://www.javeriana.edu.co/biblos/tesis/derecho/dere4/Tesis-31.pdf

Biblioteca del Congreso Nacional de Chile. (2018). *Uber y conductores. Legislación comparada sobre relación laboral*. Recuperado de https://www.bcn.cl/

obtienearchivo?id=repositorio/10221/25909/1/BCN_Uber_laboral_actualizado_PA_CW_GW__2_.pdf

Chavarro, J. y Cortes, G. (2017). *Cartilla laboral y seguridad social 2017*. Bogotá. Grupo Editorial Nueva Legislación. ISBN: 978-958-56087-1-9. Recuperado de http://app.vlex.com.crai-ustadigital.usantotomas.edu.co/#CO/search/jurisdiction:CO+content_type:4/empleador/p2/CO/vid/679242881

Código sustantivo del trabajo. Diario oficial de la República de Colombia No 27.622, del 7 de junio de 1951

Constitución Política de Colombia, publicada en la Gaceta Constitucional No. 116 de 20 de julio de 1991

Flores, C. (2014). *Condiciones de trabajo en la industria de call center en Chile: La situación laboral de los teleoperadores de empresas tercerizadas ubicadas en santiago* (tesis de pregrado). Universidad Academia De Humanismo Cristiano, Santiago. Recuperado de http://bibliotecadigital.academia.cl/bitstream/handle/123456789/2428/TSOC%20188.pdf?sequence=1&isAllowed=y

Gnecco Mendoza, G. (2011). La relación de trabajo. En: J. Herrera Vergara, G. Valdés Sánchez y S. Corradetti, ed., *Globalización. El cambio del derecho del trabajo*. Bogotá: Universidad de Rosario. Recuperado de https://app-vlex-com.crai-ustadigital.usantotomas.edu.co/?r=true#CO/vid/430192618

Levaggi, V. (9 de agosto 2004). Organización Internacional del Trabajo. ¿Qué es el trabajo *decente?*. Recuperado de https://www.ilo.org/americas/sala-de-prensa/WCMS_LIM_653_SP/lang--es/index.htm

Madero, Y. (2012). *Guía laboral 2012*. Bogotá. ECOE. ISBN: 9586487687. Recuperado de https://app-vlex-com.crai-ustadigital.usantotomas.edu.co/#CO/sources/6845

Micheli, J. (3/5 enero-mayo 2007). *Los call centers y los nuevos trabajos del siglo XXI. CONfines*. Recuperado de https://confines.mt .itesm.mx/articulos5/michelij.pdf

Organización Internacional del Trabajo. (2015). *Las relaciones de trabajo en los servicios de telecomunicaciones y en el sector de los centros de llamadas*. Ginebra. ISBN: 978-92-2-330048-7. Recuperado de https://www.ilo.org/wcmsp5/groups/public/---ed_dialogue/---sector/documents/publication/wcms_409417.pdf

Ospina, N. (2018). Ámbito Jurídico. Columnista online. *Trabajadores de plataformas*

digitales: ¿nuevo estatus jurídico? Recuperado de https://www.ambitojuridico.com/noticias/columnista-online/laboral-y-seguridad-social/trabajadores-de-plataformas-digitales-nuevo

DESARROLLADORES DE APLICACIONES, LA "FUERZA LABORAL" DE GOOGLE

Eje temático: Trabajo en el Siglo XXI. Teletrabajo. Industria 4.0

Autor:
Oscar Rodrigo Paredes Fernández
Lic. En Ciencias Jurídicas y Políticas[420]
Docente de planta
Universidad Privada Boliviana
Facultad de Ciencias Empresariales y Derecho
Carrera de Derecho

ABSTRACT
Desde el advenimiento del teletrabajo hasta el desarrollo de las plataformas colaborativas actuales, se ha podido evidenciar una marcada influencia en la población laboralmente activa, derivada de las ventajas y oportunidades que hoy brindan los entornos virtuales de trabajo. Pasando por las experiencias de computación en la nube, hasta el desarrollo de ·ecosistemas" (como el caso de Google) vemos que la realidad del trabajo en la era de internet ha cambiado y continúa en constante evolución y transformación, eso conlleva, por un lado, un análisis de las ventajas, así como las desventajas que se generan, pero resulta innegable que dichos efectos se insertan más en un plano positivo, siempre y cuando los Estados (y sus gobiernos) procuren la viabilización de políticas adecuadas, mismas que sirvan tanto de fomento como de control de las relaciones laborales desarrolladas en un entorno digital. Entre todas las posibilidades de trabajo enmarcadas en el entorno informático y digital actual, podemos fácilmente ubicar a empresas que lideran el camino y que se sirven de modelo a seguir. Tal es el caso de Google, con un ejército de más de 60.000 trabajadores distribuidos en diversas ciudades y países, además de un soporte mucho mayor de desarrolladores en todo el planeta quienes se encuentran generando, gestionando y produciendo los adelantos o las mejoras y actualizaciones de las principales aplicaciones y servicios del gigante de internet, procurando mostrarse para que puedan apreciar su talento y habilidad, en procura de alcanzar una relación mas fuerte o un vínculo laboral estable. En ese camino, Google, amplia las opciones y oportunidades para programadores, diseñadores y desarrolladores, con plataformas como Google Developers (Antes Google Code-in) así como Google Careers, que se ponen al alcance de todos (bajo el mismo lema de los fundadores de la empresa) y nos permite hablar de una fuerza laboral global que se convierte en una parte integrante del motor de Google y de sus desarrollos actuales.

ANTECEDENTES

Ya son varios años los que nos separan del advenimiento de Internet y sus efectos de transformación de la sociedad. Para quienes integramos el inmenso grupo

420 Con Maestría en Administración de empresas mención recursos humanos, programa concluido, en elaboración de la tesis para defensa. Con Maestría en Seguridad, Defensa y Desarrollo, elaborando el trabajo final de grado. Diplomado en Altos Estudios Nacionales, Diplomado en Docencia Universitaria. Educador Google Nivel 1 Certificado y próximo a certificar nivel 2

de los "migrantes digitales", nos resulta fácil el poder evidenciar las transformaciones operadas dentro de nuestras sociedades. Antiguamente, la labor investigativa por ejemplo, se limitaba a nuestras fuentes de información, por lo menos las que fueran asequibles, como ser bibliotecas, hemerotecas o si teníamos suerte el acceso a expertos de un área o tópico que nos regalaban parte de su valioso tiempo, circunstancias que con el advenimiento de Internet y el surgimiento de la Word Wide Web (en su fase 1.0) significó una gran transformación en lo que se refiere al acceso, gestión y procesamiento de la información, mucho más con la evolución de la web a los entornos 2.0, 3.0, 4.0 y actual debate de los ecosistemas 5.0 y 6.0, que nos cambian la faceta del uso de Internet como herramienta a diversos fines, con una fl xibilidad impresionante, innovadora y transformadora. Este hecho, evidenciable en diversos campos del conocimiento humano no puede estar al margen de un área tan tradicional como es la del ámbito laboral. Luego de grandes transformaciones operadas por el advenimiento de la revolución industrial que nos permitió la transición de la producción, el trabajo artesanal y manufacturado a la producción y trabajo industrial, a escala, luego automatizado con el advenimiento de las máquinas y equipos para alivianar el trabajo de obreros y empleados, mismo que ahora nuevamente sufre una transformación, pero esta vez operada por la denominada sociedad del conocimiento, o la revolución del conocimiento, donde Internet se muestra como la plataforma y herramienta que permita dar un salto cualitativo y cuantitativo, algo que se evidencia en la preocupación de la Organización Internacional del Trabajo, que el 2018 conformó La Comisión Mundial sobre el futuro del trabajo, donde se plantearon diversas situaciones que bien pueden ser resumidas en la siguiente aseveración:

> *"Se prevé que el incremento de la digitalización y la automatización tenga una incidencia significativa tanto en la calidad como en la cantidad de los empleos. Las nuevas modalidades de trabajo y de empleo están transformando la naturaleza y las condiciones de la actividad laboral, al modificar las exigencias en materia de competencias profesionales y reemplazar las formas tradicionales de trabajo y de fuentes de ingresos."* (Organización Internacional del Trabajo, 2018)

Tal como acontecía luego de la revolución industrial, como fenómeno transformador de la sociedad, la llamada revolución del conocimiento (resultado de la gestión de datos para la sistematización de la información y la generación del conocimiento) potenciada por el desarrollo informático y tecnológico, trae consigo una serie de cambios tanto positivos como negativos, ya que si bien puede derivar en la creación de empleos y favorecer a la ampliación de ofertas dentro del mercado laboral, también acarrea consecuencias negativas en lo que se viene a denominar como "destrucción de empleo" como bien señala Irmgard Nübler (economista principal de la OIT):

> *"La reciente ola de innovación y cambio tecnológico ha dado origen a un animado debate sobre el futuro del trabajo. Algunos consideran que la innovación tecnológica destruirá puestos de trabajo a gran escala, pronosticando un futuro sin empleos. Otros, confían en que serán movilizadas fuerzas que crearán nuevos empleos y hasta una época dorada de creación de empleos de calidad. Este optimismo es sustentado por la experiencia histórica que muestra que a las fases iniciales de la destrucción de empleos a la larga siguió una fuerte creación de empleos. Una de las preguntas fundamentales entonces es si la actual ola de cambio tecnológico generará, una vez más, un proceso sostenido de creación de empleos. Otra de las preguntas es de qué manera las políticas pueden apoyar este proceso para satisfacer las aspiraciones de las sociedades."* (Nübler, 2017)

La misma autora nos presenta el panorama y derrotero que debiera seguirse con el propósito de favorecer la ampliación de las ofertas dentro del mercado laboral, por intermedio de la postura que tendrían que asumir las administraciones públicas y sobre todo los tomadores de decisiones a momento de plantear políticas laborales y económicas que permitan potenciar los adelantos tecnológicos e informáticos que nos lleven a un escenario de desarrollo propicio de las relaciones laborales. Dicha labor descansa en la comprensión de los efectos del desarrollo tecnológico así como los servicios, soportes y plataformas derivadas de este, para poder mediar en una transición de las relaciones laborales tradicionales, caracterizadas por la presencia física de los trabajadores, los horarios rígidos, la verticalidad de las decisiones y otros factores, para luego dar paso a la evolución de dichas relaciones, gracias a las ventajas que pueden proveer el actual y futuro desarrollo tecnológico.

> *"…el cambio tecnológico es un proceso complejo, incierto y no linear que llega en oleadas, produciendo por lo tanto fases de destrucción de empleos y de creación de empleos. Este proceso no ocurre de manera automática, sino que es impulsado por diversas fuerzas a nivel económico, político y de la sociedad."* (Nübler, 2017)

Pondero bastante la posición de Nübler al aseverar que los efectos positivos (creación) y negativos (destrucción) pueden ser impulsados por el accionar de la administración pública tanto como por la gestión privada. Si partimos de la última, es innegable que las administraciones privadas, a través de diferentes emprendimientos empresariales, han podido evidenciar hace años el carácter estratégico de las plataformas digitales y los soportes que estas pueden brindar al desarrollo de procesos productivos y a la provisión de servicios. Teniendo como antecedente más cercano los servicios de teletrabajo, pasando por las fuerzas laborales remotas a un mercado global de servicios y productos, que emplean a internet como herramienta principal para generar un "ecosistema" favorable, que como señala Nübler, permita *"la transición hacia "épocas doradas" de creación de empleo* [las que] *fueron siempre impulsadas por nuevas opciones sociales y políticas."* (Nübler, 2017)

Entre las empresas que lograron comprender que Internet puede traer consigo una serie de condiciones favorables para la generación de servicios y plataformas de

desarrollo de sus emprendimientos, podemos citar a dos grandes dentro del sector como son Alphabet Inc., empresa más conocida por su marca (y empresa subsidiaria) Google y por otra parte Amazon Inc., organizaciones que identificaron la ventaja que puede proveer una plataforma de trabajo virtual, potenciada por el advenimiento y crecimiento de Internet.

ALPHABET INC. LA "NUEVA" EMPRESA DE LARRY PAGE Y SERGEI BRIN

Se trata de la empresa matriz o consorcio de empresas cuyos titulares, Larry Page (Director Ejecutivo), Sergei Brin (Presidente de Alphabet) y Sundar Pichai (Director ejecutivo de Google) fundaron el 10 de agosto de 2015, con el objeto de albergar una serie de empresas donde la principal subsidiaria resulta ser Google, la que sumada a Calico (Empresa dedicada a la investigación en biotecnología), Capital (Empresa de inversión), Fiber (Proveedora de conexión a internet), Lie Science (Relacionada a la investigación e innovación en el área médica), Nest (Empresa especializada en el área de domótica), Ventures (Empresa de inversión) y X Lab (empresa de investigación e innovación), las que juntas forman el consorcio, que en opinión del propio Larry Page les permitirán hacer *"cosas mucho más ambiciosas y a largo plazo"* (Page, 2015). Con esto se pretende dar un giro hacia un negocio corporativo con empresas subsidiarias que se manejen de manera independiente en parte, pero bajo el abanico de la empresa matriz. Lo que se mantiene de todas formas es la lógica con la que nació Google, que en las propias palabras de sus fundadores: *"Google is not a conventional company. We do not intend to become one". (Google no es una compañía convencional. No tenemos la intención de convertirnos en una - Larry Page and Sergei Brin)* algo que con el transcurso de los años se puso de manifiesto en el desarrollo de proyectos disruptivos y "alocados" (como señalan sus fundadores) que han posicionado a Google dentro un marco referencial de emprendimientos en el sector de las telecomunicaciones, la tecnología y el desarrollo de la Internet, que pudiera permitirles un manejo sostenible y sin sobre saltos, algo muy lejano a la mística de los fundadores, como expresan en el comunicado oficial del lanzamiento de Alphabet: *"We've long believed that over time companies tend to get comfortable doing the same thing, just making incremental changes. But in the technology industry, where revolutionary ideas drive the next big growth areas, you need to be a bit uncomfortable to stay relevant."[…] "This new structure will allow us to keep tremendous focus on the extraordinary opportunities we have inside of Google."* (Page, 2015) y así ha sido desde que Sundar Pichai[421] se puso al frente del gigante de Internet en agosto de 2015. La serie de

421 El actual Director Ejecutivo de Google, se incorporó a la empresa en el 2004 ingresando al departamento de innovación de productos, destacándose con el desarrollo de Google Drive y el paquete de ofi ática de la empresa, pasando también por proyectos como Gmail, Maps, la creación de un nuevo formato de video WebM y dese agosto de 2015 terminó al frente de la empresa al recibir la confianza de Larry Page, para conducir el destino del gigante, tarea en la que ha demostrado ser la mejor

innovaciones y la búsqueda incesante de nuevos emprendimientos o como mejorar los servicios estrella de la empresa, ha sido y será siempre su nota determinante, para lograr aquello requiere de un "ejercito" de desarrolladores, que potencian día a día los servicios que brinda la empresa, brindando soporte a las aplicaciones de Google, así como las tecnologías abiertas de Internet.

Desde marzo de 2005, Google vio por conveniente el poder potenciar el desarrollo de aplicaciones tanto móviles como web, razón por la que decide crear una comunidad de desarrolladores a través del sitio denominado Google Code (Actualmente Google Developers) con el objeto de promover la difusión y crecimiento de software libre y código abierto relacionados con los servicios y productos de la empresa. Los proyectos open source se fundamentan en el fomento de la colaboración y el desarrollo tecnológico, que favorezcan la resolución de problemas diarios, con la participación de emprendedores desde diferentes locaciones por intermedio de Internet. A partir del 2007 se llevaron a cabo competencias dirigidas a estudiantes de secundaria en los proyectos de código abierto, desarrollándose año tras año hasta cambiar por Google Code-In. Con participantes desde los 13 años y premios desde 100 hasta 500 dólares fue popularizándose año tras año con la inclusión de nuevos "desarrolladores" que mostraban sus creaciones y las comparten con el mundo. De la misma manera, Google, con el paso de los años fue ampliando la base original de Google Code, con la adquisición de otras empresas o el desarrollo de nuevos productos. Actualmente, los desarrolladores pueden participar para acrecentar y fortalecer los proyectos ligados a: Android, Cloud Platform, Firebase, Maps Platform, TensorFlow, Web, You Tube, de la misma manera pueden favorecer a su crecimiento por intermedio de servicios y plataformas Firebase, Google Ads, Google Analytics, Google Play, Search, Web Plug and Notification APIs o proyectos que les permitan acceder a ganancias dentro del ecosistema de googlea través de AdMob, Google Ads API, Google Play, Google Play Billing, Interactive Media Ads (ver https://developers.google.com/) proyectos, servicios y productos que se ponen a disposición de todo aquel que desee incursionar en el soporte, crecimiento y mejora de la plataforma de Google y otras empresas.

Las ventajas que provee el surgimiento de una comunidad global de desarrolladores vinculados a Google, se puede evidenciar en el crecimiento soporte y desarrollo de Android, según datos publicados en el Blog de Desarrolladores de aplicaciones y código para el sistema operativo se menciona que cada mes, se tiene un promedio de 750.000 APKs y grupos de aplicaciones en la consola de Google Play, mucho de esta participación se debe también a los diferentes canales puestos a disposición por parte de Google, además del sitio de desarrolladores, desde el 2008, Google, ahondando en el propósito de poder crear una comunidad de desarrolladores que permita un crecimiento estable y significativo en el desarrollo de sus aplicaciones, productos y servicios así como su

opción para liderar las operaciones, con un trabajo duro y la innovación constante.

propia plataforma, se lanzó el proyecto de congresos de desarrolladores, denominados Google I/O con el objetivo de que programadores de diferentes orígenes puedan presenciar: el lanzamiento de nuevos productos, las presentaciones de desarrolladores en jefe de diferentes proyectos de la empresa y procesos de aprendizaje que permitan un benefici conjunto gracias a la entrega del código abierto del software de soporte de las aplicaciones para que todo aquel interesado pueda realizar sus aportes a la mejora de este. A lo largo de los años, el congreso a permitido el crecimiento y posicionamiento de aplicaciones móviles y para los servicios web de la empresa, con innovaciones cada vez más llamativas y que muestran el entusiasmo de los "colaboradores" de Google, lo que repercute en la cantidad de aplicaciones desarrolladas, descargadas e instaladas a través de la plataforma. Año tras año, la empresa va ampliando la gama de servicios, así como el acceso al código a los desarrolladores.

TRABAJAR PARA GOOGLE

Además de poder poner a prueba aplicaciones para ver si estas son aceptadas y comercializadas por Google Play u otros servicios, también se puso a disposición un nuevo servicio denominado Google Careers, donde se alienta a quien desee participar para que pueda diseñar, crear y "construir" códigos para todos (Design, Create, Build Code for everyone). Actualmente la plataforma para búsqueda de trabajo presenta un total de 4154 opciones, desde pasantías o internados, trabajo temporal, tiempo parcial, tiempo completo, dirigido a estudiantes, profesionales (licenciatura y postgrado) y asociados con el objeto de brindarles oportunidades de empleo con el gigante de internet, teniendo la oportunidad de acceder a equipos de trabajo en el desarrollo de Ingeniería y Tecnología, Ventas servicio y soporte, Marketing y Comunicaciones, Diseño, Estrategias de negocios, finanzas, área legal, soporte a recursos humanos, etc, con una lista que cada vez va incrementando a favor de la empresa y todo aquel con la pretensión de acceder a un puesto de trabajo en Google, donde se pretende equilibrar las oportunidades como indican en su sitio:

> *"At Google, we don't just accept difference—we celebrate it, we support it, and we thrive on it for the benefit of our employees, our products and our community. Google is proud to be an equal opportunity workplace and is an affirmative action employer. We are committed to equal employment opportunity regardless of race, color, ancestry, religion, sex, national origin, sexual orientation, age, citizenship, marital status, disability, gender identity or Veteran status. We also consider qualified applicants regardless of criminal histories, consistent with legal requirements."* (Google Careers, 2019)

En líneas generales, la empresa se muestra como un entorno abierto donde cada persona tiene las mismas posibilidades de acceso a sus ofertas de trabajo, ya sea de

forma presencial o de forma virtual (a distancia) cooperando en el desarrollo de sus servicios, productos y su propia plataforma. Si bien esto puede entenderse como una circunstancia favorable, tampoco debemos dejar de lado la incidencia negativa que puede generarse en caso de establecer barreras de acceso demasiado rigurosas, esto en términos del beneficio que genera para las empresas la llegada de mano de obra calificada o de alto nivel, la que puede ser remunerada de forma apropiada o muy por debajo de la media en los países sede de las empresas, que en este caso concreto sería Estados Unidos. Tal como señala Nübler *"La importante enseñanza que aporta la historia es que los procesos de creación de empleo se activan por las consecuencias tanto intencionales como involuntarias de las innovaciones dirigidas a economizar mano de obra."* (Nübler, 2017). Si tomamos como referencia el sueldo promedio de los desarrolladores de acuerdo a la región de origen de estos, podemos comprender bastante lo señalado por Nübler, aspecto que profundizaremos más adelante.

PARTICULARIDADES DE LA RELACIÓN CONTRACTUAL ESTABLECIDA CON GOOGLE

Toda relación laboral se encuentra ligada a acuerdos o contratos laborales, donde se determinan las condiciones para la prestación del trabajo, como ser el horario, los materiales o insumos a ser empleados y demás circunstancias que deben ser acatadas por el personal contratado, denotando una relación de subordinación que debe ser cumplida a cabalidad, caso contrario afecta la relación con el empleador, sobre todo en lo concerniente con el pago. Sin embargo, cuando nos referimos a los desarrolladores de aplicaciones que ofertan sus "productos" a Google, no podemos ubicarlos como trabajadores de la empresa, pues no se traza ninguna relación laboral, al no existir subordinación o dependencia, más por el contrario, los derechos y obligaciones que se determinan para las partes están condicionadas por el acuerdo de distribución que Google exige a los desarrolladores para regular la promoción y distribución de sus "productos" en la plataforma de Google, más específicamente Google Play Console. Todo desarrollador que acepte el acuerdo forma un contrato vinculante en relación con el uso de la plataforma Google Play, para el caso de las aplicaciones para los dispositivos Android. Entre las condiciones establecidas en el acuerdo se determina la distribución de las aplicaciones que sean entregadas por los desarrolladores que "gocen de una buena reputación", conforme las reglas descritas en el mismo acuerdo. En el apartado 3 del acuerdo suscrito se determina que la relación entre Google y los desarrolladores será de tipo comercial, concretamente de distribución, asumiendo el rol de "agente o proveedor de servicios de mercado", cobrando una tarifa para poder acceder a los mismos. Para la contraprestación, Google exige la habilitación de una

cuenta de pago válida por intermedio de un servicio de pago (de orden bancario o financiero) que será empleada para la monetización de los productos presentados en la plataforma. La comercialización de los productos se rige tanto por las disposiciones legales de la región en la que los "productos" (aplicaciones) sean distribuidos además de regirse a las reglas que correspondan a la Unión Europea o a Estados Unidos, en lo concerniente a la condición de Google como comerciante registrado. En el tema impositivo, será Google el que determine la obligación de pago de estos, pudiendo determinar la recaudación por intermedio del procesador de pagos o proveedor autorizado a través de la retención del importe para luego remitirlo a la autoridad fiscal que corresponda según la venta de los productos. También se determina que en los países donde Google no asuma dicho rol, le corresponderá al desarrollador determinar si el producto está sujeto a obligaciones impositivas y por ende proceder con el pago de las tasas exigidas.

En ocasiones, de acuerdo con lo que determine el desarrollador, los productos podrán ser distribuidos de forma gratuita, por lo que se exime del pago de la tarifa de transacción además de mantenerse de forma gratuita a menos que se determinen cargos adicionales los que se correlacionarán con versiones alternativas o suplementarias al producto.

Como podemos apreciar, todo lo anterior se sujeta a las condiciones normales referidas a un contrato de distribución, sin embargo, si nos referimos a los derechos de propiedad intelectual y la protección de datos, se evidencian una serie de particularidades que es preciso identifi ar, como ser que Google en ningún momento asumirá la condición de titular o "propietario" de los productos (aplicaciones, apk, api u otro) que el desarrollador suba a la plataforma; de la misma manera respecto al desarrollador, ya que este en ningún momento puede asumir la titularidad de los sdk o api´s de Google, debiendo asumir además cualquier responsabilidad sobre el manejo de los datos de los usuarios que usen dichas aplicaciones, procurando la confidencialidad de los datos capturados, además de sujetarse a las reglas previstas en el acuerdo con Google, las que incluyen la obligación de dar aviso a los usuarios de que la información colectada solo puede ser empleada para los fines de la aplicación, salvo que se adopten acuerdos particulares, los que regirán más allá de lo descrito y establecido en el acuerdo con Google. Dichos acuerdos, comúnmente denominados EULA por sus siglas en inglés (End User License Agreement) o acuerdos de usuario final, donde se establecen los derechos y obligaciones asumidas por el desarrollador (individual o empresarial) y el usuario de la aplicación, dejando a Google como responsable del canal de distribución del software, pero sin asumir mayores responsabilidades.

Otro aspecto relevante radica en el hecho de que el desarrollador al subir su producto a la plataforma (Play Console) otorga a Google y sus afiliados una licencia limitada, no exclusiva y libre de regalías durante el plazo de vigencia del acuerdo

suscrito, con el objeto de poder mostrar las características de la Marca del Desarrollador (las que deben ser enviadas por este a Google) para su uso únicamente en línea o en dispositivos móviles y, en cualquier caso, únicamente en relación con la distribución y venta del producto, permitiendo la inclusión de elementos visuales de la aplicación (capturas de pantalla, videos demostrativos, etc. a través de Google Play o cualquier otro soporte a decisión de la empresa y en contra partida Google le otorga al desarrollador la licencia de uso de la marca Android para fines de marketing, siempre y cuando se sujete al manual y guía de marca debidamente aprobado.

Otro aspecto que consideramos pertinente poner de manifiesto, es el referido a la privacidad e información, ya que Google determina en el acuerdo con los desarrolladores que estos se encuentran bajo la previsión de la política de privacidad de la empresa, circunstancia que va acorde con la tendencia desatada luego del caso Cambridge Analytica y la captura de datos por intermedio de la plataforma de Facebook, algo que marcó al mercado de la información y de las plataformas.

Ya en la parte final del acuerdo se incluyen los descargos de responsabilidad aplicables a la relación entre Desarrolladores, Usuarios y el propio Google, mismos que transcribimos a continuación en su idioma original:

> 12. DISCLAIMER OF WARRANTIES
> 12.1 YOU UNDERSTAND AND EXPRESSLY AGREE THAT YOUR USE OF THE PLAY CONSOLE AND GOOGLE PLAY IS AT YOUR SOLE RISK AND THAT THE PLAY CONSOLE AND GOOGLE PLAY ARE PROVIDED "AS IS" AND "AS AVAILABLE" WITHOUT WARRANTY OF ANY KIND.
>
> 12.2 YOUR USE OF THE PLAY CONSOLE AND GOOGLE PLAY AND ANY MATERIAL DOWNLOADED OR OTHERWISE OBTAINED THROUGH THE USE OF THE PLAY CONSOLE AND GOOGLE PLAY IS AT YOUR OWN DISCRETION AND RISK AND YOU ARE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR COMPUTER SYSTEM OR OTHER DEVICE OR LOSS OF DATA THAT RESULTS FROM SUCH USE.
>
> 12.3 GOOGLE FURTHER EXPRESSLY DISCLAIMS ALL WARRANTIES AND CONDITIONS OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.
>
> "13. LIMITATION OF LIABILITY
> 13.1 TO THE MAXIMUM EXTENT PERMITTED BY LAW, YOU UNDERSTAND AND EXPRESSLY AGREE THAT GOOGLE, ITS SUBSIDIARIES AND

AFFILIATES, AND ITS LICENSORS WILL NOT BE LIABLE TO YOU UNDER ANY THEORY OF LIABILITY FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES THAT MAY BE INCURRED BY YOU, INCLUDING ANY LOSS OF DATA, WHETHER OR NOT GOOGLE OR ITS REPRESENTATIVES HAVE BEEN ADVISED OF OR SHOULD HAVE BEEN AWARE OF THE POSSIBILITY OF ANY SUCH LOSSES ARISING.

14. Indemnificatio
14.1 To the maximum extent permitted by law, You agree to defend, indemnify, and hold harmless Google, its affiliates and their respective directors, officers employees and agents, and Authorized Providers from and against any and all third party claims, actions, suits, or proceedings, as well as any and all losses, liabilities, damages, costs, and expenses (including reasonable attorneys' fees) arising out of or accruing from (a) Your use of the Play Console and Google Play in violation of this Agreement; (b) infringement or violation by Your Product(s) of any Intellectual Property Right or any other right of any person; or (c) You or Your Product(s)' violation of any law.

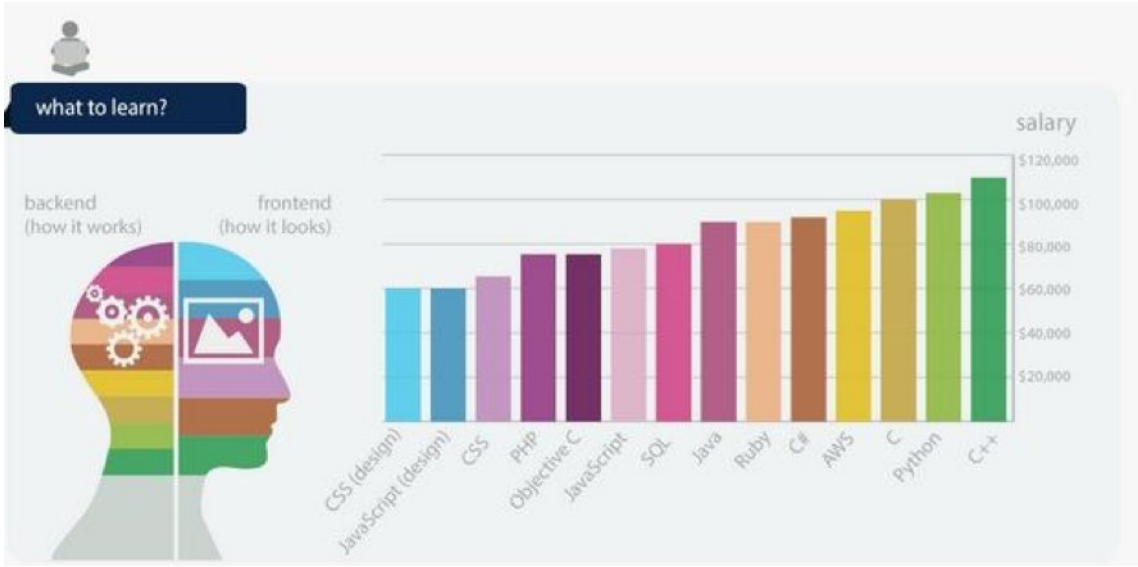
14.2 To the maximum extent permitted by law, You agree to defend, indemnify, and hold harmless the applicable Payment Processors (which may include Google and/or third parties) and the Payment Processors' affiliates directors, officers employees, and agents from and against any and all third party claims, actions, suits, or proceedings, as well as any and all losses, liabilities, damages, costs, and expenses (including reasonable attorneys' fees) arising out of or accruing from Your distribution of Products via Google Play." (Google, 2019)

Si bien este acuerdo es el que rige para las relaciones entre los desarrolladores y la empresa, no resulta ser el único, pues si consideramos a Google como el ecosistema que es, podemos apreciar un sinfín de servicios, soportes y plataformas, cada una de ellas con sus particularidades, así como sus reglas, contenidas la mayor parte de ellas en acuerdos tipo contratos de adhesión, fuera de las políticas de privacidad y seguridad de alcance general además de las políticas de orden comercial y de pago, pero que por el volumen que operaciones y de mercado que permite alcanzar, se presenta como una palestra de suma importancia para cualquier desarrollador, con el propósito de abrirse camino en un entorno digital cada vez más competitivo, algo que las cifras de Android pueden demostrar con vehemencia, gracias a los más de 2.000 millones de usuarios en la plataforma, que no conoce de fronteras ni de límites.

¿"FUERZA LABORAL" GLOBAL?

Gracias al desarrollo actual de la tecnología y la avidez de la población por acceder a mejor y mayor cantidad de datos para generar conocimiento, permite posicionar a empresas dedicadas a la automatización de la información, como es el caso de Google. Pero ¿Cómo incide esto en la generación de empleo y en las relaciones laborales? Si recurrimos a lo señalado por Kucera, *"los trabajos suelen componerse de tareas fácilmente automatizables y de otras que no lo son. Se plantea entonces la cuestión de si la automatización de los procesos de trabajo dará como resultado una reducción de la fuerza laboral, o si las tareas restantes podrían compartirse entre la fuerza de trabajo existente. La respuesta a esta cuestión depende de cómo se organiza la actividad laboral en un lugar de trabajo determinado y de la medida en que las tareas que no son fácilmente automatizables se pueden agrupar para crear nuevos puestos de trabajo"* (Kucera, 2017) Bajo ese entendido, lo que lleva a cabo Google a través de su ecosistema global, es permitir el vínculo entre diferentes participantes a lo largo y ancho del planeta, con grupos de desarrolladores, asociados (partners) y emprendedores que nutren cada vez más sus servicios, aplicaciones y productos, con una carga innovativa de importancia que a su vez se robustece con las dinámicas sociales y culturales de cada región de la que provienen sus "colaboradores" y trabajadores. Sin duda un ejemplo de crecimiento a escala, lo que le ha permitido alcanzar el sitial que hoy ostenta. Pero la interrogante es si con esta práctica, ¿terminan realmente favorecidos quienes "colaboran" con Google? ¿no se está más bien fomentando la conformación de estructuras oligopólicas para dominación del mercado? Como se menciona en la nota informativa número 6 de la OIT, sobre la influencia de la tecnología en la calidad y cantidad de empleo, la implantación de nuevas plataformas de macrodatos, que permiten acumular un volumen de información impresionante sobre el comportamiento y las preferencias de los consumidores, incide de forma positiva en la eficiencia de la economía, pero a su vez se genera una serie de dudas en cuanto a si se genera o no beneficio para las sociedades en su conjunto o si las ventajas generadas terminan siendo captadas por un pequeño número de empresas dominantes, como es el caso de Google (Organización Internacional del Trabajo, 2018), fuera de la existencia de trabajos de bajo costo o no remunerados en el actual mercado digital.

EL SUELDO DE LOS PROGRAMADORES



Fuente: Grafico xtraído de: https://computerhoy.com/noticias/software/sueldo-programadores-descubierto-31147

Como se puede evidenciar los programadores mejor pagados son aquellos que desarrollan sus códigos en lenguaje C++ con un ingreso promedio anual cercano a los 110.000 $us. mientras que aquellos ligados al diseño de programas frontend (vinculados a lo que los usuarios ven en las páginas, sitios y servicios puestos a disposición) resultan ser los peor pagados con una media de 60.000$us año. Claro que estas cifras reflejan la situación de programadores y desarrolladores en un contexto determinado, que no solo se circunscribe a Estado Unidos de Norteamérica, tal como revela el estudio de Funders & Founders sobre el salario de los programadores elaborado en el 2014. También es importante trazar la diferencia entre programadores de "oficina" vs. Independientes (freelancers) ya que también, dependiendo de la locación desde la que realicen su trabajo se presentan diferencias interesantes (Pascual, 2015).

SUELDOS PROMEDIO DISTRIBUIDOS POR ZONA

Fuente: Infografía extraída de: https://computerhoy.com/noticias/software/sueldo-programadores-descubierto-31147

Mientras los programadores que prestan sus servicios en empresas como trabajadores de planta o en oficina llegan a cobrar más, los independientes o freelancer suelen cobrar menos (en algunos casos cobran más) como podemos apreciar en el caso del Brasil, que de acuerdo con el estudio de Funders & Founders, un programador de oficina factura al año aproximadamente unos 32.000.-$us. mientras que un independiente llega a obtener en un año un promedio de 36.000.-$us. claro que dichas cifras están sujetas a la propia voluntad de los programadores, sobre todo los freelancer, ya que el monto puede disminuir dependiendo múltiples factores, que van más allá de la calidad del código o programa, así como los lenguajes de programación.

La presencia masiva de apasionados por la tecnología y el desarrollo de aplicaciones, sea como desarrolladores, diseñadores, administradores y otros, los que desde su enfoque y perspectiva terminan nutriendo a los productos y servicios de Google, se ha convertido en una constante, alimentada por las propias políticas de la empresa, ya que las opciones se plantean no solo a aquellos que tienen la formación o la destreza para programar, sino para un horizonte más amplio de participantes, a los que la propia Google forma y fomenta a través de proyectos como Google Developers Academy, actualmente denominada Google Developers Training, donde se enfatiza que: “Whether you’re an experienced developer or just getting started, we can point

you to training that will help you develop high-quality apps that are both useful and marketable." (ver https://developers.google.com/training/) donde se ofertan una serie de cursos y tópicos, según las necesidades de desarrollo de programadores que quieren ampliar su base de conocimiento, así como entusiastas que desean sumar habilidades y destrezas que los preparen para un mercado laboral global en franca expansión.

HORIZONTES DE TRABAJO POR INTERNET. A MODO CONCLUSIÓN

Google, entre muchos otros más, genera una serie de entornos y ecosistemas para que profesionales en diferentes áreas del conocimiento, vinculadas directa e indirectamente con el desarrollo tecnológico e informático puedan emprender en el desarrollo de aplicaciones, productos, servicios, bases de datos y productos, que resulten de utilidad y puedan a la vez significar ingresos, los que se comparten con una empresa que hace años comprendió que, más allá de las bondades que puede generar un proceso de outsorsing, el desarrollo de plataformas de trabajo "colaborativo" puede traer consigo ventajas sostenibles y sustentables, donde la innovación y creatividad sea la nota predominante.

El crecimiento de Internet, así como las posibilidades que brinda a empresas como Google, ha permitido generar un "ejercito virtual" de desarrolladores, quienes desde la influencia que ejercen los ejecutivos y programadores en jefe de diversos proyectos de la empresa (startups y empresas subsidiarias) y la posibilidad de acceder y mejorar los códigos abiertos, para permitirles mostrarse a un mercado altamente competitivo y demandante, donde las oportunidades no le resultan del todo lejanas, pero todavía se desarrollan bajo patrones desiguales en cuanto a la distribución de los dividendos y donde la "titularidad" o los "beneficios" se concentran todavía en grandes conglomerados como beneficiarios directos del crecimiento que se evidencia en el rubro.

Es ponderable, que Google, como lo manifies an sus fundadores, no es una empresa convencional, sino una que plantea un nuevo ecosistema, basado en su pilar fundamental: el constante emprendimiento, lo que nos lleva a vislumbrar el derrotero que tuvo en los recientes años y los que tendrá en la aventura que implica el trabajo en uno de los gigantes de internet.

Además, no debemos dejar de lado las consideraciones a momento de generar políticas y normas que por un lado protejan a los trabajadores del nuevo entorno de desarrollo, sin que ello signifique el advenimiento de barreras burocráticas insalvables y tampoco la desprotección de los intereses de los trabajadores.

Bibliografía

Google. (15 de Abril de 2019). Google Play Developer Distribution Agreement.

Google Careers. (7 de mayo de 2019). Obtenido de https://careers.google.com/teams/

Kucera, D. (2017). *New automation technologies and job creation and destruction dynamics, Employment Policy Brief (Ginebra, OIT)*. Ginebra: OIT.

Nübler, I. (3 de mayo de 2017). *Organizacion Internacional del Trabajo*. Obtenido de Organización Internacional del Trabajo - Noticias: https://www.ilo.org/global/about-the-ilo/newsroom/news/WCMS_552360/lang--es/index.htm

Organización Internacional del Trabajo. (2018). *Nota Informativa #5 La calidad del trabajo en la economía de las plataformas. Comisión Mundial sobr eel futuro del trabajo.*

Organización Internacional del Trabajo. (2018). *Nota Informativa #6 La influencia de la tecnología en la calidad y la cantidad del empleo *Comisión Mundial sobre el Futuro del Trabajo)*.

Page, L. (10 de Agosto de 2015). Comunicado de prensa, creación de Alphabet. Estados Unidos.

Pascual, J. A. (9 de Julio de 2015). El sueldo de los programadores, al descubierto. España.

ANÁLISIS DEL TELETRABAJO COMO FORMA DE PRESTACIÓN DE SERVICIO

Eje temático: Teletrabajo

Autora:
Sulmer Paola Ramírez
Doctora en Ciencias Mención: Derecho (UCV). Especialista en Derecho del Trabajo y Seguridad Social (UCAT) Especialista en Derecho Administrativo (UCAT) Especialista en Negocios con América Latina (UPF). Certificación Internacional en Coaching y PNL (ICC). rofesora de Derecho de las TIC Universidad Católica del Táchira (UCAT), profesora de Pregrado y Postgrado. Asesora de empresas del sector público y privado. E-mail: sulmerp@yahoo.com.
Venezuela

RESUMEN
Se trata del análisis del Teletrabajo como forma de prestación de servicio, pasando por su definición, elementos, tipos, ventajas e inconvenientes de su implementación, su reconocimiento jurídico. Así como el análisis de la supervisión propia del teletrabajador mediante el uso de equipos de video-vigilancia y sistemas de geolocalización, que enfrentan el ejercicio del derecho a la libertad de empresa y poder de control del empleador, frente al ejercicio de derechos del teletrabajador como la intimidad y protección de sus datos personales, debiendose aplicar las normas de ponderación del derecho, que pasan por los criterios de idoneidad, necesidad y proporcionalidad. Finalizando con la favorabilidad que representa el uso de técnicas propias de la programación neurolingüística en la comunicación entre el empleador y el teletrabajador tanto para el cumplimiento de las obligaciones inherentes a la relación de trabajo, como para el ejercicio de la supervisión propia de la relación laboral.

1. DEFINICIÓN DE TELETRABAJO

El Teletrabajo, conocido igualmente como teledesplazamiento (telecommuting), trabajo en red (networking), trabajo a distancia (remote working) o trabajo en casa (teleworking), ha sido explicado por varios autores, sin encontrarse una definición unánimemente aceptada. Etimológicamente el término Teletrabajo procede de la unión de la palabra griega "tele", usada como prefijo, que significa lejos, y de la palabra trabajo (en latín tripaliare, de tripalium, instrumento de tortura), que es la acción de trabajar.

Sin embargo, bajo una óptica jurídica-conceptual, no puede equipararse Teletrabajo con trabajo a lo lejos o a la distancia. Se trata de supuestos, que aunque no son totalmente diferentes entre sí, se produce entre ellos una suerte de relación género-especie, pudiéndose decir que todo Teletrabajo es trabajo a distancia, pero no todo trabajo a distancia es Teletrabajo.

Jack Nilles citado por Thibaulth[422] (2000) fue el primer autor en utilizar el término Teletrabajo, lo definió como: "cualquier forma de sustitución de desplazamientos relacionados con la actividad laboral por tecnologías de la información" o de forma más gráfica "la posibilidad de enviar el trabajo al trabajador, en lugar de enviar el trabajador al trabajo". (p.24)

Por su parte, la Organización Internacional del Trabajo (OIT) citada por Gaeta (1995)[423] lo definió como: "…forma de trabajo efectuada en un lugar alejado de la oficina central o del centro de producción y que implica una nueva tecnología que permite la separación y facilita la comunicación". (p. 10)

En el Acuerdo Marco Europeo sobre el Teletrabajo suscrito en el año 2002[424] se define el Teletrabajo como "…una forma de organización o de realización del trabajo, utilizando las tecnologías de la información en el marco de un contrato o de una relación de trabajo, en la cual un trabajo que podría ser realizado igualmente en los locales de la empresa se efectúa fuera de estos locales de forma regular."

Realizadas las referencias internacionales que anteceden de la definición de Teletrabajo, lo defino como:

> "aquella prestación personal de servicio, ejecutada por cuenta ajena fuera de la sede física de la empresa, que se caracteriza por la utilización de medios telemáticos o informáticos como indispensables herramientas de trabajo".

Dependiendo de la inclinación académica de los distintos estudiosos que han definid el Teletrabajo, destacando físicos, abogados, ingenieros, sociólogos, psicólogos, entre otros, varía la orientación y definición de este. Lo que si es innegable es que esta forma de prestación de servicio ha captado la atención de los legisladores en varios países, muestra de ello es la Ley número 191 del 16 de julio de 1998 sobre la implantación del Teletrabajo en la Administración Pública italiana, el Acuerdo Marco Europeo sobre el Teletrabajo suscrito en el año 2002. Por su parte el Parlamento Andino mediante la Recomendación N° 204 de Octubre de 2010, planteó la implementación en los países andinos de lineamientos, políticas públicas e instrumentos para el fortalecimiento y establecimiento subregional del Teletrabajo como instrumento de fl xibilización laboral, desarrollo social, económico, de integración y cohesión subregional.

Solo por citar algunos ejemplos de regulación del Teletrabajo, señalo que Costa Rica promulgó el Decreto 34704-MP-MTSS de Teletrabajo de 2008 y Colombia cuenta

422 Thibaulth, J. *El Teletrabajo,* Consejo Económico y Social, Barcelona, 2000.

423 Gaeta, L. *Il telelaboro: legge e contratazione,* Giornali di Diritto del Lavoro e di relazioni industriali", Roma, 1995.

424 Acuerdo marco europeo sobre teletrabajo suscrito el 16-07-2002 en Bruselas Disponible: https://www.uned.ac.cr/viplan/images/acuerdo-marco-europeo-sobre-teletrabajo.pdf. Consultada: 01/04/2019

con la ley 1221 del 16 de julio de 2008 que tiene por objeto promover y regular el Teletrabajo como un instrumento de generación de empleo y autoempleo mediante la utilización de las TIC. Ambos países han desarrollado los respectivos instrumentos jurídicos para la implementación del Teletrabajo como forma de ejercicio de la prestación de servicio. Así Colombia promulgó la Guía Jurídica del Teletrabajo[425], cuyo objetivo es dar a conocer los procedimientos jurídicos que una entidad del sector público debe tener en cuenta a la hora de implementar el teletrabajo para sus funcionarios públicos.

Por su parte Costa Rica dictó la Guía para Implementar el Teletrabajo en las Instituciones Públicas y empresas privadas[426] buscando posicionar el Teletrabajo como un medio que impulsa las acciones de modernización en las instituciones del Sector Público, así como la reducción de costos en diferentes rubros, el incremento en la productividad de los funcionarios, la reducción en el consumo de combustibles, promueve la inserción laboral, la protección del medio ambiente y el equilibrio entre la vida personal y laboral de los teletrabajadores[427].

2. ELEMENTOS DEL TELETRABAJO

De la propia definición de Teletrabajo se extraen sus elementos esenciales, a saber:

a. La prestación personal del servicio: ejecutada fuera de la sede física de la empresa: en el Teletrabajo, la prestación del servicio en su mayor parte se ejecuta fuera de la sede física de la empresa y por ende fuera de sus sucursales y dependencias, sin importar la distancia que haya entre el lugar donde el teletrabajador está prestando sus servicios y las instalaciones de la empresa, solo importa que esté ejecutando su labor fuera de la misma, lo que en lo absoluto debe asimilarse a falta de control, debido a que la utilización de medios telemáticos e informáticos, herramientas fundamentales del Teletrabajo, permiten como se verá más adelante, ejercer en la mayoría de los casos, un mayor control sobre la prestación de servicio del teletrabajador.

b. La utilización de medios telemáticos o informáticos como indispensables herramientas de trabajo: el Teletrabajo se caracteriza por la utilización de medios telemáticos o informáticos que permiten ejecutar y externalizar la actividad encomendada, además de favorecer una constante y más rápida comunicación con la empresa. No se trata solo de un trabajo ejecutado fuera del inmueble de la empresa, sino que, además es requisito indispensable que con el uso intensivo del teléfono, fax,

425 https://www.teletrabajo.gov.co/622/w3-article-8423.html. Consultada: 13/08/2019.

426 http://www.mtss.go.cr/elministerio/despacho/teletrabajo/guia_teletrabajo_sector_privado.pdf Consultada: 15/08/2019.

427 Disponible en: http://www.mtss.go.cr/elministerio/despacho/teletrabajo/Guia_implementacion_Teletrabajo .pdf. Consultada: 15/05/2019.

correo electrónico, video terminal, video conferencia, entre otras técnicas informáticas y telemáticas existentes, se haga posible la prestación de dicho servicio.

Ahora bien, no toda prestación de servicios a distancia, realizada con los medios telemáticos, merece la calificación de Teletrabajo, bien porque puede ser que la mayor parte de esa actividad no se preste a distancia, o bien porque el uso del ordenador con el software aplicativo instalado en el mismo por la empresa, se aplica durante menos del cincuenta por ciento del horario de trabajo y durante el resto de la jornada se dedica a otra actividad, criterio éste seguido por la doctrina alemana. Quedan por tanto excluidos los casos en los que el ordenador cumple funciones de máquinas de escribir, o que el fax y correo electrónico se utilizan sólo para enviar la información que ha sido recabada.

El Teletrabajo, consiste fundamentalmente en recibir, tratar y enviar informaciones inmateriales por naturaleza, lo que le distingue del trabajo a domicilio tradicional basado en el intercambio de bienes materiales cuantificables y fungibles.

Aplicado a un caso práctico, se observa que el traductor no teletrabaja cuando desarrolla su actividad de modo tradicional y envía el resultado por el correo de la empresa. En cambio, si ese mismo traductor recibe el texto a traducir en su terminal portátil, realiza la traducción encomendada en su equipo telemático o informático, utiliza el correo electrónico como medio de comunicación con la empresa, recibe las instrucciones a través de un modem y transmite la traducción al empleador por vía telemática, si podría considerarse que está teletrabajando.

3. TIPOLOGÍA DEL TELETRABAJO

Concebido inicialmente como trabajo a domicilio, este fenómeno se ha extendido hasta alcanzar a cualquier sitio desde donde sea posible conectarse a una red. Hay personas que trabajan en casa o en un telecentro, pero también cada vez más en el avión, en el tren, en las habitaciones de un hotel o en la empresa del cliente, mediante una conexión directa o transmitiendo las especificaciones o el resultado del trabajo por correo o mensajería.

La tipología del Teletrabajo, con mayor aceptación en la doctrina, es la que atiende a un criterio locativo, que comprende a los teletrabajadores que prestan sus servicios en el domicilio, en un telecentro o en forma itinerante, distinguiéndose estos tres tipos de teletrabajo:

a-Teletrabajo a domicilio: Conocido también como "Electronic Home Work", se refiere al ejecutado en el propio hogar del teletrabajador. Sustituyéndose la sede de la empresa, su oficina, en la que prestan sus servicios, por su propio domicilio como

el lugar en que se lleva a cabo el trabajo habitual. Trabajo que puede ser realizado en grupo familiar o individualmente y para un empleador o para varios empleadores.

La mayoría de las empresas que utilizan el Teletrabajo a domicilio optan por la solución denominada "Teletrabajo alternado", en el que los empleados sólo teletrabajan en casa una parte del tiempo, transcurriendo el resto de la jornada laboral en la oficina. Esta forma de Teletrabajo ofrece mayores posibilidades de comunicación entre el empleado y la empresa que el trabajo en casa a tiempo completo.

b-Teletrabajo en centros de trabajo o telecentros: En este supuesto, el teletrabajador no se desplaza de su domicilio a la sede de la empresa, sino que lo hace a un centro específicamente diseñado para el desarrollo del trabajo, vale decir a un telecentro, conocido como lugar de trabajo con recursos compartidos y con las instalaciones informáticas y de telecomunicaciones necesarias para llevar a cabo el desarrollo de determinada actividad.

Estos centros están dirigidos a todo tipo de empresa, pero principalmente a las pequeñas y medianas (PYMES), debido a que pone al alcance de estas microempresas, avanzadas tecnologías informáticas y telemáticas, que de no ser así, su uso les estaría prácticamente prohibido por su alto coste.

c-Teletrabajo móvil o itinerante: Cuando el puesto de trabajo no está situado en un lugar determinado, sino que el teletrabajador, con una movilidad permanente, como un verdadero argonauta, dispone de un equipo telemático portátil que le permite desempeñar su actividad en cualquier lugar.

La Academia Internacional de Teletrabajo para América Latina y el Caribe en su primer informe sobre el estado del Teletrabajo en América Latina y el Caribe[428], al referirse a los tipos de Teletrabajo, resalta los siguientes aspectos presentes en el Teletrabajo en atención a su tipo:

> "1.Relación de Dependencia: cuando se trabaja para un patrono.
> 2. Independiente: cuando se trabaja de forma autónoma.
> 3.Teletrabajo fijo: cuando el teletrabajo se realiza en un lugar determinado
> 4.Teletrabajo móvil: cuando el teletrabajo se ejecuta en diferentes locaciones."

Es importante destacar, que al ser el Teletrabajo un hecho social de estudio jurídico es de vital importancia el análisis de las características de dicha prestación de servicio, para así determinar su maraco jurídico regulador.

Si el Teletrabajo es ejecutado personalmente por el teletrabajador, bajo subordinación, dependencia cuenta y riesgo del empleador, y mediante una contraprestación, gana fuerza su amparo bajo la legislación propia de derecho laboral, a diferencia de la prestación de servicio ejecutada bajo la forma de teletrabajo, que se

428 Disponible: https://cidtt.org/wp-content/uploads/2018/03/Estado-del-Teletrabajo--en-Am%C3%A9rica-Latina.pdf. Consultada: 10/08/2019.

realiza por cuenta y riesgo propio del teletrabajador, sin subordinación ni dependencia, asunto en el que se pudiese estar en presencia de una labor sujeta al amparo del derecho civil. En todo caso, se sugiere el estudio detallado de las características propias de dicha prestación de servicio, para así determinar su marco jurídico regulador.

4. VENTAJAS E INCONVENIENTES DEL TELETRABAJO

El Teletrabajo tiene aspectos valiosísimos para su implementación tanto en el sector público como en el sector privado, destacando entre otros: reducción de los traslados *in itinere*, lo que se traduce en reducción de las emisiones contaminantes de los vehículos de transporte, mayor fl xibilidad en la organización del trabajo, tanto para el teletrabajador como para el empleador, reducción de costos en alquiler o mantenimiento de sedes físicas de la empresa, permite atraer y retener el talento humano, optimización de las tecnologías disponibles que se traduce generalmente en aumento de la productividad, estimula la ocupación de colectivos que tienen dificultades para la inserción laboral y social, muchas veces por razones de accesibilidad. Dentro de estos colectivos se encuentran: personas con discapacidad o con capacidades especiales, personas de la tercera edad, habitantes de zonas rurales, entre otros.

Aspectos favorables del Teletrabajo que fueron resaltados en el foro de diálogo mundial organizado por la OIT que reunió a representantes de gobiernos, de empleadores y de trabajadores de todo el mundo con la finalidad de intercambiar las políticas y las prácticas para maximizar los beneficios del teletrabajo. [429]

Por otra parte, se encuentran algunos inconvenientes derivados de la implantación del teletrabajo como forma de prestación de servicio, entre ellos está: la escasa regulación específica del Teletrabajo lo que favorece cierto grado de inseguridad jurídica para el teletrabajador y su empleador, el Teletrabajo en el domicilio, sino no se cuenta con una debida organización del tiempo, puede producir la disolución del concepto "tiempo de trabajo", vale decir, la confusión entre el trabajo y el ocio o vida personal y familiar del teletrabajador, la privacidad e intimidad del teletrabajador puede verse en riesgo por el uso de programas y dispositivos que bajo el argumento del ejercicio del poder de control del empleador, violen estos derechos, además de poder atentar contra el derecho a la protección de datos personales del teletrabajador.

Lo anteriormente expuesto, deja en evidencia la necesidad que existe del pleno conocimiento por parte del teletrabajador de las condiciones que rigen su prestación de servicio bajo la forma de Teletrabajo, así como los riesgos que puedan existir contra el ejercicio de sus derechos y libertades y los mecanismos que tiene en su defensa. Por ello, es fundamental la práctica de una excelente comunicación en la relación de

429 Disponible: https://www.ilo.org/global/about-the-ilo/newsroom/news/WCMS_534817/lang--es/index.htm Consultada: 14/08/2019.

teletrabajo, atendiendo entre otros aspectos a las técnicas propias de la programación neurolingüística, especialmente, los canales de representación de la información, y las técnicas de elaboración y transmisión del mensaje, que analizo al final del siguiente punto.

5. LA SUPERVISIÓN DEL TELETRABAJADOR MEDIANTE EL USO DE LAS TIC

5.1 Monitorización Laboral

El derecho a la libertad de empresa, denominado igualmente derecho al libre comercio, es la facultad que tiene toda persona de dedicarse libremente a la actividad económica de su preferencia sin más limitaciones que las establecidas en el ordenamiento jurídico que le sea aplicable. Este derecho en el ámbito laboral se traduce en el poder de control y supervisión que tiene el empleador sobre su teletrabajador, que entre otros aspectos abarca la monitorización de la actividad desempeñada por éste.

El punto argüido del derecho de control que tiene el empleador sobre la prestación del servicio de su teletrabajador está en los límites de este, en virtud a que dicho control debe realizarse respetando entre otros, el derecho a la privacidad, intimidad, honor y reputación del teletrabajador, quien puede sentirse afectado por el control que sobre su activad realice el empleador.

El desarrollo de las tecnologías de la información y las comunicaciones TIC ha incidido directamente en los medios y formas de realizar tanto la prestación de servicio del trabajador, como la supervisión y control de la misma por parte del empleador, existiendo la posibilidad material de utilizar mecanismos que por su naturaleza pueden estar todo el tiempo "alertas", vale decir, siempre registrando la actividad laboral del teletrabajador, tal es el caso de las cámaras de video o el uso de software que registre las actividades realizadas por el teletrabajador a través de medios telemáticos e informáticos.

Es importante destacar que en todo momento de la relación de trabajo, vale decir, desde el i nicio de la misma hasta su extinción y luego de ella, deben ser respetados los derechos al secreto de las comunicaciones, honor, reputación, vida privada e intimidad del teletrabajador, protección de datos personales, entre otros, e igualmente debe respetarse el legítimo derecho del empleador de ejercer el control y supervisión de los teletrabajadores que emplee en su actividad comercial.

Al existir derechos contrapuestos en una misma situación como sería el derecho a la intimidad del teletrabajador y a su privacidad en la empresa, frente al ejercicio del derecho a la libertad de empresa y poder de control del empleador, se deben aplicar

las normas de ponderación del derecho, que pasan por los criterios de Idoneidad, Necesidad y proporcionalidad, que explico en el siguiente apartado sobre video-vigilancia laboral, y que tienen como fundamento entre otros instrumentos, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos[430] en su punto 7 ponderación del derecho a la protección de datos personales.

5.2 Video-Vigilancia y Sistemas de Geolocalización en el Ámbito Laboral como Mecanismo de Supervisión de los Teletrabajadores

La video-vigilancia es una tecnología de captación de imágenes y en algunos casos sonidos e imágenes, que instalada en lugares específicos, permiten grabar, almacenar y reproducir lo allí sucedido. Por su parte los sistemas de geolocalización permiten obtener la ubicación geográfica real de un objeto y en este caso del equipo de tecnología empleado por el teletrabajador para la prestación de sus servicios, lo que trae como consecuencia posibles riesgos para la protección de los datos personales, la intimidad y vida privada de quienes estén en el espectro de captación de la imagen o sonido, ya que puede quedar grabada en el respectivo equipo la imagen de una persona y los sonidos que ésta emita, además de su actuar y su ubicación geográfica, pudiendo ser posteriormente un sujeto identific do o identificable por quienes tengan acceso a las grabaciones captadas por el equipo de video-vigilancia.

Dadas las características de la tecnología de video-vigilancia y de los sistemas de geolocalización, los empleadores los han utilizado como medios de supervisión del trabajador en sus diferentes formas de prestación de servicio, entre ellas el Teletrabajo, enfrentándose así el derecho que tiene el empleador de control sobre la prestación de servicio del teletrabajador y el derecho del teletrabajador a su intimidad, vida privada y la protección de sus datos personales, lo que ha conllevado a que la reglamentación de su uso se haga cada vez con mayor detalle. Como referencia de dicha reglamentación, señalo lo establecido en los artículos 89 y 90 de la Ley 3/2018, del 5 de diciembre de 2018, de Protección de Datos Personales y garantía de los derechos digitales de España LOPD[431], que establecen:

> "Artículo 89. Derecho a la intimidad frente al uso de dispositivos de video-vigilancia y de grabación de sonidos en el lugar de trabajo.
> 1. Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en

430 Disponible: Estándares de Protección de Datos Personales para los Estados Iberoamericanos aprobados por la Red Iberoamericana de Protección de Datos el 20-06-2017. Disponible: http://www.redipd.org/noticias_todas/2017/novedades/common/Estandares_Esp_Con_logo RIPD.pd f#Testo %20en%20espa%C3%B1ol. Consultada: 05/07/2019.

431 Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673. Consultada: 28/06/2019

el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida…."

"Artículo 90. Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.
1. Los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo.
2. Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión."

De los citados artículos se desprenden entre otros aspectos, los siguientes:

a-El reconocimiento expreso de los sistemas de cámaras, videos cámaras y sistemas de geolocalización como medios de supervisión y control del empleador sobre el cumplimiento de las obligaciones laborales del trabajador en su prestación de servicio, lo que incluye a juicio de quien escribe a los trabajadores que prestan su labor mediante el Teletrabajo.

b-El deber del empleador de instalar los equipos de video-vigilancia y sistemas de geolocalización dentro del marco legal y con los límites inherentes al mismo, vale decir, respetando las normas que regulan la protección al derecho y libertades del teletrabajador, para ello es importante verificar si la instalación de dichos equipos como medio de supervisión del teletrabajador supera el juicio de proporcionalidad debiéndose constatar si cumple las condiciones señaladas en el punto 7 ponderación del derecho a la protección de datos personales, contenido dentro del Capítulo I de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos, a saber:

-Idoneidad, que hace referencia de la posibilidad de conseguir el objetivo del empleador en la supervisión con la instalación de equipos de video-vigilancia.

-Necesidad, en el sentido que no exista otra medida distinta a la instalación de dispositivos de video-vigilancia para la supervisión del cumplimiento de las obligaciones del trabajador derivadas de su relación laboral.

-Ponderación y equilibrio, conocida igualmente como proporcionalidad en sentido estricto, en virtud que de la instalación de equipos de video vigilancia para la

supervisión del trabajador, resulten más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto.

c-El deber de los empleadores de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la instalación de equipos de video vigilancia y sistemas de geolocalización como medios de supervisión de las obligaciones del trabajador derivadas de la relación laboral. Es de gran importancia determinar el alcance de dicho deber de informar, siendo de gran importancia informar al teletrabajador de la instalación de los equipos de video vigilancia y de los sistemas de geolocalización si es el caso, además de la finalidad de su instalación y el uso que puede ser dado a la información que sea captada por dichos equipos, entre otros usos, el que sirvan de fundamento para la aplicación de medidas a favor o en contra del teletrabajador.

En cuanto a la oportunidad de informar al teletrabajador sobre la existencia o instalación de equipos de video-vigilancia en la empresa, es importante destacar que existen dos momentos principalmente para realizar dicha notificación

a.- Al inicio de la relación de teletrabajo, informándole al trabajador que dentro de las condiciones está la supervisión de sus actividades mediante cámaras de video vigilancia, que captarán imágenes y sonidos que son de uso del empleador para verificar el cumplimiento de sus obligaciones laborales y así mismo notificarle al trabajador que dicha información puede servir de fundamento para la aplicación de medidas disciplinarias en su contra inclusive la finalización de la relación de trabajo por despido.

b-Durante la relación de teletrabajo, en aquellos supuestos que la instalación de los equipos de video-vigilancia sea posterior a la fecha de inicio de la relación de trabajo, destacando que dicha notificación debe realizarse previamente a la puesta en funcionamiento por parte de la empresa de los equipos de video-vigilancia.

Como conclusión señalo que la notificación previa al teletrabajador sobre la instalación de equipos de video-vigilancia en el lugar de trabajo y de los sistemas de geolocalización que sean instalados, es fundamental para garantizar el respeto a los derechos y libertades de los teletrabajadores y fortalecer la validez legal del material captado por dichos equipos, destacando que la referida notificación se sugiere realizarla de la forma más explícita posible, indicando no solo la existencia o instalación de los señalados equipos, sino también la finalidad de los mismos y el tratamiento que puede ser dado por la empresa a los datos allí recogidos, pudiendo ser empleados inclusive en procedimientos en contra del teletrabajador o a su favor según sea el caso.

Lo conveniente a efectos de la notificación en referencia, es la redacción de formatos que expliquen al teletrabajador en leguaje sencillo y claro lo aquí señalado y de esta forma esté en conocimiento de los medios de supervisión del empleador y las consecuencias que del uso de dichos medios se pueden derivar. Explicación que

de ser realizada en uso de las técnicas de programación neurolingüística potencia el entendimiento por parte del teletrabajador, como se explica en el siguiente punto.

5.3 Uso de Técnicas de Programación Neurolingüística en la Comunicación y Supervisión de la Relación Laboral

La buena comunicación, entendida como la transmisión efectiva del mensaje, que implica la comprensión de éste por el destinatario, es el eje central, pilar fundamental del éxito de la mayoría de las relaciones interpersonales, entre ellas, las relaciones laborales. La programación neurolingüística, brinda una serie de técnicas que son herramientas aliadas para la comunicación en todas las actividades propias de la relación de trabajo, destacando la supervisión ejecutada por el empleador en ejercicio de su derecho a la libertad de empresa a través del cual está facultado para realizar el control de la actividad desempeñada por el teletrabajador en relación a su prestación de servicio.

El cumplimiento por parte de los teletrabajadores de las labores que le hayan sido encomendadas o que se desprendan de la naturaleza de su servicio es punto de vital importancia en el desarrollo de la relación de trabajo o de la denominada relación de empleo público en el sector público. Para ello es fundamental la comprensión por parte del teletrabajador de las obligaciones inherentes a su relación de trabajo, lo que pasa por analizar con mayor detenimiento el proceso para el logro de este objetivo, en otras palabras, cuáles son los pasos que se sugieren para alcanzar la meta de cumplimiento efectivo de labores por parte del talento humano de la empresa y de una supervisión efectiva de dicha labor, lo que haré siguiendo técnicas de Programación Neurolingüística aplicadas a la comunicación entre las partes. Dicho esto, distingo tres pasos principales, expuestos bajo la óptica del empleador como emisor del mensaje que transmite al teletrabajador:

a.- Elaboración del mensaje, el empleador como emisor del mensaje, tiene el deber de estructurar el mismo, en el sentido que contenga lo que efectivamente quiere transmitir, para ello se sugiere que dicho mensaje se formule en positivo, sea determinado, cierto, alcanzable y que su ejecución dependa del destinatario. Esto responde a la pregunta ¿Qué actividad quiere que ejecute el teletrabajador? y ¿Cómo quiere que se ejecute dicha actividad?

b.-Prueba de congruencia, que responde a la pregunta ¿Para qué quiere que el teletrabajador ejecute la actividad que le asignó? Si la respuesta está en sintonía con el mensaje elaborado, se procede al siguiente paso, de lo contrario se debe reformular el mensaje.

c.-Transmisión del mensaje, es en este punto, donde las TIC juegan su rol protagónico, siendo por excelencia el actual medio de transmisión del mensaje y de ejercicio del poder de control que tiene el empleador sobre la actividad laboral del teletrabajador, ya sea que lo transmitido se comunique a través de correo electrónico, mensaje de texto, redes sociales de internet, video-conferencia, audio, mensajería, teléfono, entre otros medios. Independientemente de la Tecnología de Información y Comunicación que se emplee para la transmisión del mensaje, se debe tener en cuenta que el receptor del mismo maneja diferentes canales de representación de la información, lo que comúnmente es conocido a grandes rasgos como: canal auditivo, visual y kinestésico.

Así, el canal auditivo identifica a aquellas personas que captan de una mejor manera el mensaje que es percibido a través del sentido del oído, ya sea en audio o en conversación telefónica. Por su parte el canal visual, caracteriza a aquellas personas con mejor entendimiento de la información que perciben a través del sentido de la vista, en este caso se sugiere presentar el mensaje en forma escrita, por correo electrónico, mensaje de texto entre otras formas y el canal kinestésico hace referencia a aquellas personas que perciben de una mejor y más efectiva manera, la información que reciben a través de los sentidos del gusto, tacto y olfato, lo que es un reto para el desarrollo de la tecnología actualmente. Como caso de ejemplo de este último canal, podría implementarse el acompañar la llamada telefónica, video conferencia o área de trabajo con un olor característico adaptado al logro del objetivo planteado en determinado mensaje o con el uso de elementos que activen el sentido del tacto y el gusto.

Por regla general es uno el canal de representación de la información que predomina en el destinatario del mensaje, aumentándose exponencialmente las posibilidades de comprensión de lo transmitido, si la información va dirigida a su canal de predominio.

En todo momento se sugiere estar alerta a las respuestas recibidas de parte del teletrabajador, teniendo el empleador la apertura necesaria para modificar la forma de transmitir el mensaje, hasta conseguir el objetivo, siendo ésta una habilidad propia de la buena comunicación tal y como lo señalan Joseph O´Connor y John Seymour en su libro PNL para Formadores (2003)[432].

Dicho lo anterior, es conveniente calibrar al teletrabajador como destinatario del mensaje, lo que significa determinar el canal de comunicación que en él predomina, siendo esto posible entre otras formas, con la aplicación de test ya existentes a realizarse en cualquier momento de la relación laboral, considerando que el momento ideal es antes del inicio de esta, incluso desde la entrevista pre empleo.

Ante la dificultad de calibrar a cada teletrabajador, se sugiere presentar la información abarcando en la medida de las posibilidades los tres canales de

432 O´Connor J, *PNL Para Formadores,* Ediciones Urano S.A. España, 2003.

representación de la información, lo que podría traducirse en la información presentada en un video, en el cual además el teletrabajador percibe la información a través del sentido del oído y de la vista llegando a los receptores en los que predomina el canal auditivo y visual, lo que se podría complementar según el caso con recursos dirigidos a los sentidos del gusto, tacto y olfato para llegar con igual efectividad a los destinatarios kinestésicos.

La buena comunicación entre las partes de una relación laboral, permite transmitir de una manera mucho más efectiva, clara, sencilla y directa, las funciones inherentes a la relación de trabajo, permitiendo igualmente realizar de mejor manera el feedback propio de la supervisión, ya que facilita el entendimiento por parte del teletrabajador del campo de oportunidad que se le presenta en su prestación de servicio, en otras palabras, que está haciendo de forma inadecuada, para entender con que otras formas de ejecución correcta de la labor cuenta.

Además que la transmisión efectiva del mensaje facilita el entendimiento por parte del teletrabajador de los mecanismos de supervisión que son utilizados por el empleador (dispositivos de video-vigilancia, geolocalización, sistemas biométricos, etc.), hecho tan importante, que afectan de forma definitiva las decisiones de los operadores jurídicos ante una información transmitida o no en la forma debida al teletrabajador.

REFERENCIAS BIBLIOGRÁFICAS

Gaeta, L. (1995) "Il Telelaboro: Legge e Contratazione". Roma: Giornali di Diritto del Lavoro e di Relazioni Industriali.

O´Conner, J (2003) "PNL para Formadores". España: Ediciones Urano S.A.

Thibaulth, J. (2000). "El Teletrabajo". Madrid: Consejo Económico y Social.

Acuerdo marco europeo sobre teletrabajo suscrito el 16-07-2002 en Bruselas. Disponible: http://www.ugt.es/teletrabajo/teletrabajo.htm. Consulta: 01/04/2019.

Estándares de Protección de Datos Personales para los Estados Iberoamericanos aprobados por la Red Iberoamericana de Protección de Datos el 20-06-2017. Disponible: http://www.redipd.org/noticias_todas/2017/novedades/common/Estandares_Esp_Con_logo RIPD.pdf#Testo%20en%20espa%C3%B1ol. Consultada: 05/07/2019.

Guía Jurídica para el Teletrabajo en el Sector Púlbico y Privado en Colombia: Disponible: https://www.teletrabajo.gov.co/622/w3-article-8423.html. Consultada: 13/08/2019

Guía Técnica para la Implementación del Teletrabajo. Costa Rica: Disponible: http: // www.mtss.go.cr/elministerio/despacho/teletrabajo/guia_teletrabajo_sector_privado.pdf. Consultada:15/08/2019.

Informe sobre el Estado del Teletrabajo en América Latina y el Caribe. Academia Internacional de Teletrabajo para América Latina y el Caribe https://cidtt.org/wp-content/uploads/2018/03/Estado-del-Teletrabajo-en-Am%C3%A9rica-Latina.pdf. Consultada: 10/08/2019.

Ley 3/2018, del 5 de diciembre de 2018, de Protección de Datos Personales y garantía de los derechos digitales de España. Disponible: https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673. Consultada: 28/06/2019.

E-COMMERCE

ESTADOS UNIDOS VERSUS CHINA FRENTE A LOS DESAFÍOS FISCALES DE LA OCDE Y EL G-20 EN EL *E-COMMERCE*

Eje temático: E-Commerce, *Smart Contracts* y pagos electrónicos

Autores:
Antonio Faúndez-Ugalde
Profesión y categoría académica: Abogado, doctor en derecho y profesor investigador asociado.
Universidad: Pontificia Universidad Católica de alparaíso (Chile)

María Teresa Blanco Lobos
Profesión y categoría académica: Contador auditor, magíster en tributación y profesora investigadora adjunto.
Universidad: Pontificia Universidad Católica de alparaíso (Chile)

Mario Pino Moya
Profesión y categoría académica: Contador auditor, profesor investigador agregado.
Universidad: Pontificia Universidad Católica de alparaíso (Chile)

RESUMEN
El presente artículo analiza los enfoques opuestos que se han evidenciado entre Estados Unidos y China en el comercio digital o *e-commerce,* intensificados con los últimos eventos que hacen referencia a una guerra comercial entre ambas naciones, para posteriormente explicitar cómo dicha disputa ha trascendido e impactado en los lineamientos normativos fiscales propuestos por la OCDE y el G-20, organismos que han orientado sus esfuerzos en lograr encontrar un consenso internacional respecto a las normas de tributación en la economía digital. Estados Unidos se ha posicionado en el comercio digital de servicios, donde seis de las diez empresas de internet más importantes del mundo son compañías estadounidenses; en cambio, China ha puesto énfasis en el comercio tradicional de bienes físicos a través de transacciones materializadas por internet. Así, para el estudio será esencial comenzar con un detallado análisis sobre el enfoque tanto de Estados Unidos como de China y las medidas jurídicas que cada uno de ellos ha adoptado frente al *e-commerce*, para luego contrastar estas posiciones con los informes emitidos por la OCDE y el G-20. Considerando lo anteriormente expuesto, la presente investigación plantea como hipótesis que el conflicto comercial entre Estados Unidos y China ha impactado directamente en la normativa internacional que se busca instaurar al alero de la OCDE y del G-20, con relación al *e-commerce*. Los resultados confirm n que la posición de Estados Unidos frente a la OCDE y el G-20, ha sido apoyar la deslocalización de beneficios, orientada a buscar una solución con relación a aquellas jurisdicciones que tienen una baja o nula tributación, permitiendo establecer reglas de interbloqueo para reforzar la capacidad impositiva de aquellos que realizan operaciones a nivel de *e-commerce*. Sin embargo, Estados Unidos se ha adelantado, aplicando de manera unilateral estas medidas jurídicas, generando barreras arancelarias que mayormente han ido en contra de China y que ha impactado en el *e-commerce*, como es el caso del desarrollo de la red 5G, en donde el país estadounidense decretó un bloqueo comercial a la empresa china Huawei.

PALABRAS CLAVES: *e-commerce*, economía digital, impuestos, OCDE, plataformas de internet.

1. INTRODUCCIÓN

Hoy, en los países con alto desarrollo tecnológico, tales como Japón, Estados Unidos y los de la Euro Zona, la economía digital es del orden de 7% al 8% del PIB, y hacia fine de esta década se prevé un 12% (Lever, Yukich y Cruz, 2016, p. 6). Esta expansión del comercio internacional ha sido impulsada en gran parte por la irrupción de plataformas digitales, herramientas que han permitido que los consumidores puedan acceder a bienes y servicios, tangibles e intangibles, de la más variada índole, siendo vendidos o prestados a través del comercio electrónico o digital. El comercio electrónico ha sido definido como "la entrega de productos y servicios a través de internet por parte de empresas de cualquier sector de la industria, y de productos asociados, como teléfonos inteligentes y sensores conectados a internet" (Fefer et al., 2017, p. 1). Dichas transacciones en el comercio digital pueden ser entre empresas (*business to business* o *B2B*); entre empresa y consumidor (*business to consumers* o *B2C*); entre empresa y la administración (*business to administrations* o *B2A*); entre empresa y los empleados (*business to employee* o *B2E*), o entre consumidores (*consumer to consumer* o *C2C*). Así, el desarrollo tecnológico se ha constituido en la cuarta revolución industrial, fenómeno que habría comenzado al inicio de este siglo y se caracterizaría por un internet más ubicuo y móvil, por sensores más pequeños y potentes que son cada vez más baratos, y por la inteligencia artificial y el aprendizaje de la máquina (Schwab, 2016, p. 5).

Si bien los mercados mundiales se han visto beneficiados por la nuevas tecnologías, especialmente, en la reducción de costos de recopilación de información (Bardopoulos, 2015, p. 29; Nattrass et al., 2003, p. 309), en el ámbito del derecho tributario, los efectos han impactado negativamente en la recaudación fiscal (Agrawal, 2017; Bacache-Beauvallet y Bloch, 2018; Bacache-Beauvallet, 2018; Belleflamme y Toulemonde, 2018; Bourreau et al., 2018; Bloch y Demange, 2018) y el costo de implementación de sistemas fiscales electrónicos (Yilmaz y Coolidge, 2013; Banco Mundial, 2016, p. 17), dando paso a una evasión tributaria que los países han intentado regular de manera unilateral, generando casos de doble tributación internacional que afecta principios constitucionales de cada Estado.

La Organización para la Cooperación y el Desarrollo Económicos (OCDE) y el Grupo de los 20 (G-20[433]), se han constituido en las entidades más importantes a nivel mundial en generar grupos de trabajos destinados a lograr un consenso internacional común frente a las normas de fiscalidad en la economía digital. Históricamente, las instrucciones de la OCDE se han constituido en verdaderas guías de interpretación

433 El grupo de los 20 (G-20) está compuesto por las principales economías del mundo, esto es, la Unión Europea, Alemania, Arabia Saudita, Argentina, Australia, Brasil, Canadá, China, Corea del Sur, Estados Unidos, Francia, India, Indonesia, Italia, Japón, México, Reino Unido, Rusia, Sudáfrica y Turquía.

jurídica como una forma de solucionar los conflictos normativos frente a la doble tributación que pueda experimentar un contribuyente. Faúndez-Ugalde (2018, p. 164) indica que los comentarios o informes elaborados en el seno de la OCDE, si bien no son jurídicamente vinculantes para un país, en su redacción han participado representantes de los Estados miembros de dicha entidad, constituyendo, en consecuencia, fuente de interpretación jurídica de un convenio de acuerdo con lo señalado en el artículo 31 de la Convención de Viena sobre derecho de los tratados. Según esta última disposición, los tratados deben interpretarse de buena fe conforme al sentido corriente que haya de atribuirse a los términos en el contexto del mismo y teniendo en cuenta su objeto y fin, esto es, se debe considerar toda práctica ulteriormente seguida en la aplicación de un tratado. Ejemplo de lo anterior se puede mencionar el caso de países como Canadá e Inglaterra, en donde la jurisprudencia ha aceptado los comentarios de la OCDE como guía para la interpretación de los convenios, como ocurrió en el caso *Cudd Pressure Control Inc con The Queen*, en el que la Corte canadiense sostuvo que "los comentarios de la OCDE, por lo tanto, pueden proveer alguna asistencia para discernir el contexto legal que anteceden a las convenciones de doble tributación en el derecho internacional" (Rohatgi, 2008, p. 104). El mismo criterio declaró la Corte inglesa en el caso *Sun Life Assurance of Canada con Pearson*: "Es común [...]que se haga referencia a los comentarios como guía para la interpretación del tratado" (Rohatgi, 2008, p. 105). La International Fiscal Association (IFA) indicó que, aun no siendo legalmente vinculables para los Estados contratantes, pues no forman parte de los convenios de doble imposición firmados por los Estados, los comentarios adquieren una fuerza considerable cuando las cláusulas de los convenios se conforman de acuerdo con los postulados del modelo de convenio (García, 1996, p. 92).

Considerando lo anterior, los trabajos desarrollados por la OCDE con relación a la economía digital, son de suma importancia en el establecimiento de una regulación común internacional, cuyos alcances interpretativos pueden tener un impacto negativo como consecuencia de la política y las relaciones internacionales entre los países, como se pretende comprobar en este trabajo con relación al conflicto entre Estados Unidos y China.

Así, en el año 2013, la OCDE presentó un plan de acción denominado *Erosión de la base imponible y traslado de beneficios* (BEPS, por sus siglas en inglés), que cuenta con quince áreas estratégicas de trabajo, creadas para combatir la disminución o erosión de la base tributable a través de conductas evasivas, y para garantizar que los beneficios se graven allí donde se realizan las actividades económicas que los generan y donde se crea valor (OCDE, 2014a, p. 3). Precisamente, la acción 1 BEPS aborda los desafíos de la economía digital para la tributación de las empresas multinacionales. Sin embargo, los últimos informes presentados en los años 2018 y 2019, dejan en evidencia que los países se han dividido en dos pilares normativos, en donde uno de

ellos ha sido encabezado por Estados Unidos. Aquí radica la problemática a desarrollar, esto es, establecer los alcances del enfoque estadounidense como principal opositor al comercio desarrollado por China y cómo ha incidido en el marco normativo que intenta unificar la OCDE y el -20.

Considerando lo anterior, la hipótesis a validar consiste en que el conflicto comercial entre Estados Unidos y China ha impactado directamente en los pilares normativos desarrollados al alero de la OCDE y del G-20 con relación al *e-commerce*. Así, para el estudio será esencial desarrollar el enfoque tanto de Estados Unidos como de China y las medidas que cada uno de ellos ha adoptado frente al *e-commerce*, para luego contrastar estas posiciones con los informes emitidos por la OCDE y el G-20.

2. ESTADOS UNIDOS VERSUS CHINA

La guerra comercial entre Estados Unidos y China ha sido declarada desde el año 2018. El conflicto se centra en los aranceles que las dos potencias han instaurado, provocado una disminución del comercio y una desconfianza en los mercados financieros, perturbando las cadenas de suministro mundiales y pone en peligro la recuperación prevista del crecimiento mundial al término del 2019 (Cerutti et al., 2019) y, también, para el año 2020 de acuerdo con las últimas declaraciones de la directora gerente del Fondo Monetario Internacional (Pozzi, 2019). Vaswani (2019) señala que tres serían las barreras comerciales que aún no superan estas dos potencias: primero, Estados Unidos sostiene que China concede subsidios a sus empresas estatales posicionándolas en competencia directa con las empresas estadounidenses; segundo, China ya ha incomodado a Estados Unidos en sectores claves como el aeroespacial, el de semiconductores o la red 5G, y, tercero, Estados Unidos acusa a China de robar propiedad intelectual de empresas estadounidenses, forzándolas a transferir tecnología a China. Así, entonces, el aumento de las barreras comerciales podría perturbar las cadenas de suministro mundiales y frenar la expansión de nuevas tecnologías (Cerutti et al., 2019).

Gao (2018, p. 319) indica que las empresas estadounidenses son, en su mayoría, proveedores de servicios relacionados con la búsqueda en línea, redes sociales o contenido; así, entre las diez empresas de internet más importantes del mundo, seis son compañías estadounidenses como Amazon, Alphabet (Google), Facebook, Priceline, Ebay, Netflix, mientras que las cuatro restantes son compañías chinas, incluidas JD.com, Tencent, Alibaba, Baidu. Esto ha llevado a Estados Unidos a mantener más participación en los acuerdos internacionales relacionados con el *e-commerce,* desde el Acuerdo de Comercio de Servicios (TISA, por sus siglas en inglés) (S oba, 2013) hasta su ingreso, en el año 2016, en la agenda de negociación del comercio digital ante la

Organización Mundial de Comercio (OMC). Sin embargo, comparativamente, China ha fortalecido su posición tecnológica en general, teniendo como principal objetivo al 2045 de liderar la innovación global. En esta línea en China, cada año, se gradúan cinco veces más estudiantes en STEM (ciencia, tecnología, ingeniería y matemáticas) que en Estados Unidos; en 2018, China ya superó a Estados Unidos en gasto en innovación y desarrollo (I+D) y en publicaciones científic s (STM Report); desde hace 5 años, China es el país que registra más patentes; cada año, China produce 30 mil doctores en materias científicas y tecnológicas; hace 10 años, China desarrollaba el 1% de las transacciones globales de *e-commerce* y hoy es el 42% y procesa 11 veces más pagos móviles que Estados Unidos (Rosales, 2018).

Estados Unidos ha formulado sus propuestas sobre el comercio digital considerando los siguientes aspectos: recomienda el libre movimiento de información, salvo en lo que se refiere a los servicios finan ieros; plantea libertad de acceder y utilizar los servicios y aplicaciones de su elección, excluyendo las prácticas razonables de administración de red, así como aquellos diseñados para evitar daños en la red; prohibición a los países para requerir que los proveedores de servicios almacenen o procesen datos en el territorio del país anfitrión como condición para suministrar un servicio o invertir, y fomentar la adopción de la autenticación electrónica y las firmas electrónicas.

En cambio, las propuestas de China se ocupan mayormente del comercio de bienes, incluso cuando se mencionan los servicios, se caracterizan como auxiliares que ayudan a facilitar el comercio de bienes. Jack Ma, el fundador de Alibaba, en febrero de 2016, llevó a cabo la propuesta "e-WTP" o *Electronic World Trade Platform*, para enfatizar que su objetivo era construir una plataforma en lugar de una organización. La propuesta estaba orientada a respaldar el concepto de la plataforma electrónica de comercio mundial (eWTP), una iniciativa de todos los interesados dirigida por el sector privado, como un vehículo para el diálogo público privado que puede incubar las reglas para fomentar el comercio electrónico (B-20, 2016).

China hizo su primera presentación sobre comercio electrónico en la OMC en noviembre de 2016, declarando que su finalidad solamente era aclarar y mejorar las reglas comerciales multilaterales existentes a la fecha, a diferencia de Estados Unidos que sus propuestas van más allá de los estrechos límites del marco regulatorio de la OMC, lo que ha generado una influencia en los últimos informes de la OCDE y del G-20, como veremos a continuación.

3. IMPACTO EN LOS PILARES NORMATIVOS DE LA OCDE Y DEL G-20

En el año 1997 fue celebrada en Turku, Finlandia, la conferencia titulada *Eliminación de barreras al comercio electrónico mundial*, en la que los representantes de gobiernos y empresas se reunieron para debatir de manera informal sobre los retos planteados por el comercio electrónico internacional a los sistemas tributarios (OCDE, 2002, p. 3). Luego, a menos de un año, se llevó a cabo la conferencia de Ottawa, publicándose el marco normativo sobre tributación fiscal del comercio electrónico y recibiendo la OCDE los votos de confianza para coordinar y continuar llevando a cabo este trabajo. Así, en esta última conferencia se declaró que los principios que regulaban el comercio convencional también debían ser aplicados al comercio electrónico. Estos principios jurídicos –que configuraron el denominado *Marco tributario*– son los siguientes: neutralidad, eficiencia, certeza y simplicidad, efectividad y justicia, y fl xibilidad (OCDE, 2002, p. 4).

En el año 2013, a instancia de los países miembros del G-20, la OCDE publicó un plan de acción BEPS, estructurado en 15 acciones. La acción 1 consistió en identificar las principales dificultades que planteaba la economía digital, para la aplicación de las normas de fiscalida internacional y desarrollar opciones detalladas para abordar estas dificul ades, con un enfoque holístico y considerando tanto la imposición directa como la indirecta (OCDE, 2014b, p. 33).

En septiembre de 2013 se creó el grupo de expertos sobre fiscalidad de la economía digital (GEFED), como un órgano auxiliar al comité de asuntos fiscales de la OCDE, cuya principal tarea fue elaborar un informe destinado a identificar los problemas planteados por la economía digital y sus posibles soluciones. El GEFED dejó en claro que los principios jurídicos que formaron parte del marco tributario de la conferencia de Ottawa del año 1998, siguen siendo un importante referente hoy día y, reforzados en su caso, pueden constituir la base para valorar las posibles opciones con miras a afrontar los desafíos fiscales de la economía digital (OCDE, 2014a, p. 31).

El informe final del plan de acción BEPS del año 2015, en lo que respecta a la acción 1, no recoge todas las soluciones previamente generadas en el informe GEFED del 2014. Así, el documento únicamente adopta como cambios la modificación de la lista de excepciones a la definición de establecimiento permanente y sostener el criterio antifragmentación de las operaciones entre entidades del mismo grupo. De esta manera, el informe recomendó que las decisiones definitivas debían ser reflejadas en un informe final a entregarse el año 2020, generándose un informe provisional en el año 2018, el que parte de la base de que, a la fecha, aún no existe consenso respecto de la adopción de la serie de medidas tendientes a hacer frente a los desafíos fiscales derivados de la economía digital (OCDE, 2018, p. 174).

El informe del 2018 realiza una clasificación de las distintas posturas asumidas por los países. Un primer grupo, se muestra contrario a la aplicación de acciones que modifiquen el actual marco normativo de fiscali ad en materia digital. A estos países,

les acomoda la actual regulación ya que se han convertido en jurisdicciones de destino de empresas digitales. Un segundo grupo, considera que es menester adoptar medidas no necesariamente modificando las reglas de fis alidad en materia digital, pero con la salvedad de aplicar los principios jurídicos de tributación tomando como consideración fundamental el valor de los datos y la participación del usuario. Un tercer grupo, en el que se encuentra Estados Unidos, sostiene que todo cambio o modificación en las reglas de fiscalidad internacional debe aplicarse con carácter generalizado a toda la actividad económica, pues se estima que la digitalización de la economía es un cambio general que afecta a la economía en su conjunto, y no únicamente a los negocios más digitalizados.

En el marco de la nueva fase de trabajo posterior al informe provisional emitido el año 2018, la OCDE emitió en enero de 2019 una nota guía que ha implicado una verdadera revolución en cuanto al reconocimiento de propuestas concretas en materia de tributación en la economía digital. Así, en febrero de 2019, la OCDE publicó un documento de consulta titulado *Addressing the tax challenges of the digitalization of the economy,* el que fue sometido a consulta pública en marzo del mismo año.

Estas propuestas parecen provenir del grupo de estados cuyas jurisdicciones han resultado más desfavorecidas a causa de la baja tributación por parte de empresas altamente digitalizadas, en desmedro, no solo de los estados afectados, sino también respecto a empresas que desarrollan el comercio convencional o tradicional. El comunicado de la OCDE establece que las propuestas se basan en dos pilares, esto es, la deslocalización de beneficios y el nexo de atribución de la potestad tributaria, con las limitantes que cada Constitución Política reconoce en cada Estado[434].

El primer pilar está orientado a buscar una solución con relación a aquellas jurisdicciones que tienen una baja o nula tributación en el *e-commerce*. En cambio, el segundo pilar considera la capacidad impositiva de cada país en función de dónde se entienda creado el valor, planteando tres posibles nexos: la localización de los usuarios de estos negocios altamente digitalizados; el Estado donde tiene lugar la generación y desarrollo de intangibles de marketing, y, el concepto de presencia digital significativa, vinculado al concepto de establecimiento permanente[435].

434 Generalmente se habla de la potestad tributaria o, más precisamente, la competencia legislativa, como el poder que tienen las entidades de un Estado para instaurar los tributos o establecer prohibiciones de carácter fiscal, o, como señala Fonrouge (1997, p. 325), es la facultad o la posibilidad jurídica del Estado de exigir contribuciones con respecto a personas o bienes que se hallan en su jurisdicción. Como bien indica Massone (1979, p. 28), la potestad tributaria no se debe confundir con los derechos subjetivos, es decir, no es un derecho de crédito que tiene el Estado en contra de una persona. Esta facultad de crear disposiciones jurídicas no se ejerce en forma deliberada, sino que está sujeta a distintos límites que doctrinariamente han sido analizados en base a los denominados principios jurídicos: legalidad, equidad, capacidad contributiva, derecho de propiedad, la no confiscatoriedad, entre otros.

435 Se ha definido establecimiento permanente como una prolongación, en otro país, de la actividad empresarial de su casa central, que puede o no estar relacionada con un lugar fijo de operaciones (Faúndez-Ugalde y Blanco, 2009, p. 34; Faúndez-Ugalde, 2014).

Ha sido el primer pilar sobre la deslocalización de beneficios en donde Estados Unidos ha marcado mayor presencia, explorando dos conjuntos de reglas de interbloqueo diseñadas para dar a las jurisdicciones un remedio en los casos en que los ingresos estén sujetos a una tributación nula o muy baja. Estados Unidos propone el reforzamiento de la capacidad impositiva de los países en aquellos casos en los que la otra jurisdicción aplique tipos impositivos reducidos sobre los beneficios en cuestión (Ortega, 2019). Aquí resalta el cuestionamiento estadounidense de que China concede subsidios injustos a sus empresas estatales para competir internacionalmente, ayudando, incluso, a las empresas privadas chinas, porque las firmas foráneas que tratan de competir con éstas en el país asiático no tienen las conexiones o la escala necesaria en un mercado básicamente **cerrado** en el que se requiere de un socio local para operar (Vaswani, 2019). Así, lo que busca este pilar es crear una norma que faculte al Estado-fuente a gravar beneficios sujetos a baja tributación en el Estado-residencia; y, viceversa, una regla que negase la deducibilidad de gastos generados por pagos a personas o entidades situadas en territorios considerados de baja tributación.

Es claro que el objetivo de Estados Unidos es establecer un marco normativo destinado a proteger su economía local, generando barreras arancelarias que mayormente han ido en contra de China y que ha impactado en el *e-commerce*. Prueba de ello ha sido la incomodidad alegada por Estados Unidos en sectores claves como la red 5G, argumentando que Huawei estaría compitiendo en forma desleal por liderar las nuevas TICs, quien habría utilizado dolosamente a bancos estadounidenses para financi r a Irán para comprar equipos de Huawei (Agosin, 2018). Esto llevó, recientemente, a que el Departamento de Comercio de Estados Unidos ingresara a Huawei a una lista de compañías con las que las empresas estadounidenses no pueden negociar a menos que tengan una licencia especial, afectando la relación de esta empresa china con Google.

Así, estos antecedentes comprueban que las políticas públicas que ha desarrollado Estados Unidos han tenido impacto directo en el ordenamiento jurídico internacional y, por lo tanto, en la interpretación y aplicación del derecho. En tal sentido, las medidas unilaterales establecidas por Estados Unidos pueden incidir en la interpretación jurídica internacional, afectando, incluso, los acuerdos internacionales vigentes entre los Estados, en especial, aquellos que han ratificado la Convención de Viena sobre derecho de los tratados.

4. CONCLUSIONES

La guerra comercial entre Estados Unidos y China ha generado impacto en los últimos informes emitidos por la OCDE y el G-20, destinados a lograr un acuerdo

normativo internacional común con relación a la tributación en el *e-commerce*. Así, la posición de Estados Unidos ha sido clara en apoyar el primer pilar del referido informe, sobre la deslocalización de beneficios, el que está orientado a buscar una solución con relación a aquellas jurisdicciones que tienen una baja o nula tributación en el *e-commerce*, estableciendo reglas de interbloqueo para reforzar la capacidad impositiva. Sin embargo, Estados Unidos ya ha aplicado unilateralmente reglas sustentadas en el cuestionamiento de que China concede subsidios injustos a sus empresas, lo que ha incidido en el marco normativo internacional que intenta instaurar la OCDE y el G-20, como se reflejan en los últimos informes de estos últimos organismos. Lo anterior también se aprecia con el desarrollo de la red 5G, en donde Estados Unidos ha impuesto unilateralmente a sus empresas la limitante de negociar con la empresa Huawei a menos que tenga una licencia especial. Si bien los hechos anteriores forman parte de las políticas públicas que ha desarrollado Estados Unidos en el ámbito de la tributación, los mismos se pueden constituir en fuente de interpretación jurídica de acuerdo con lo señalado en el artículo 31 de la Convención de Viena sobre derecho de los tratados.

Por lo tanto, las medidas unilaterales que ha adoptado Estados Unidos en bloquear a países como China, no es más un reflejo de su clara intención de estatuir a nivel OCDE y del G-20, una norma internacional que faculte al Estado-fuente a gravar beneficios sujetos a baja tributación en el Estado-residencia, o bien, una regla que negase la deducibilidad de gastos generados por pagos a personas o entidades situadas en territorios considerados de baja tributación.

5. REFERENCIAS

AGOSIN, MANUEL. "Guerra comercial". Revista Económica&Administración, Nº 173, 2018. **págs. 6-9.**

AGRAWAL, DAVID. "The Internet as a Tax Haven? The Effect of the Internet on Tax Competition". 2017 Disponible en SSRN: https://dx.doi.org/10.2139/ssrn.2328479

B-20, BUSSINES 20. "Towards an Innovative, Invigorated, Interconnected & Inclusive

World Economy: B20 2016 Policy Recommendations to the G20". 2016. Disponible en: http://en.b20-china.org/documents/doc/1/2.

BACACHE-BEAUVALLET, MAYA. "Tax competition, tax coordination, and e-commerce". Journal of Public Economic Theory, vol. 20, nº 1, pp. 100–117. DOI:10.1111/jpet.12254

BACACHE-BEAUVALLET, MAYA Y FRANCIS BLOCH. “Special issue on taxation in the digital economy”. Journal of Public Economic Theory, vol. 20 nº1, 2018. págs. 5-8. DOI:10.1111/jpet.12285.

BANCO MUNDIAL. “World development report 2016: Digital dividends”. Washington D.C.: World Bank. 2016.

BARDOPOULOS, ANNE. “eCommerce and the effects of technology on taxation”. 2015. Disponible en Springer: DOI: 10.1007/978-3-319-15449-7.

BELLEFLAMME, PAUL Y ERIC TOULEMONDE. “Tax incidence on competing two-sided platforms”. Journal of Public Economic Theory. vol. 20 nº 1, 2018. págs. 9–21. DOI:10.1111/jpet.12275.

BLOCH, FRANCIS Y GABRIELLE DEMANGE. “Taxation and privacy protection on Internet platforms”. Journal of Public Economic Theory, vol. 20 nº 1, 2018. págs. 52–66. DOI:10.1111/jpet.12243.

BOURREAU, MARC, BERNARD CAILLAUD Y ROMAIN DE NIJS. “Taxation of a digital monopoly platform”. Journal of Public Economic Theory, vol. 20, nº 1, 2018. págs. 40–51. DOI:10.1111/jpet.12255.

CERUTTI, EUGENIO, GITA GOPINATH Y ADIL MOHOMMAD. “Los efectos de las tensiones comerciales entre Estados Unidos y China, Fondo Monetario Internacional”. 2019. disponible en https://blog-dialogoafondo.imf.org/?p=11232.

FAÚNDEZ-UGALDE, ANTONIO. “El problema del concepto actual de establecimiento permanente en los convenios de doble tributación internacional frente a los nuevos desafíos fisc les en la economía digital”. Revista Chilena de Derecho y Tecnología, vol. 7 nº 1, 2018, págs. 155-173. DOI: 10.5354/0719-2584.2018.48223.

FAÚNDEZ-UGALDE, ANTONIO Y MARÍA BLANCO. “Establecimientos permanentes: aspectos tributarios”. Santiago: Librotecnia. 2009.

FAÚNDEZ-UGALDE, ANTONIO. “Los establecimientos permanentes y el comercio internacional desarrollado en forma electrónica: ¿Una adecuación conceptual en los convenios de doble tributación internacional?”. Revista Jurídica Unicuritiba, vol. 4 nº 37, págs. 6-33. 2014. Disponible en http://bit.ly/2JH0bvZ.

FEFER, RACHEL, SHAYERAH AKHTAR Y WAYNE MORRISON. “Digital Trade and U.S. Trade Policy”. CRS Report for Congress, R44565. 2017. Disponible en https://

fas.org/sgp/crs/misc/R44565.pdf.

FONROUGE, CARLOS. “Derecho financiero”. Buenos Aires: Depalma. 1997.

GAO, HENRY. “Digital or Trade? The Contrasting Approaches of China and US to Digital Trade”. Journal of International Economic Law, vol. 21 nº 2, 2018. págs. 297-321. DOI: 10.1093/jiel/jgy015.

GARCÍA, FRANCISCO. “El establecimiento permanente, análisis jurídico tributario internacional de la imposición societaria”. Madrid: Tecnos. 1996.

LEVER, GEORGE, YERKA YUKICH Y MARÍA CRUZ. “La economía digital en Chile”. Santiago: Centro de Estudios de la Economía Digital Cámara de Comercio de Santiago. 2016.

MASSONE, PEDRO. “Principios de derecho tributario”. Valparaíso: Edeval. 1979.

NATTRASS, NICOLI, JEREMY WAKEFORD Y SAMSON MURADZIKWA. “Macroeconomics theory and policy in South Africa”. South Africa: David Philip. 2003.

OCDE, ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS. “Taxation and electronic commerce, implementation of the Ottawa taxation framework conditions”. París: OECD Publishing. 2002. DOI: http://www.oecd.org/ctp/administration/2673607.pdf.

OCDE, ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS. “Cómo abordar los desafíos fiscales de la economía digital”. París: OECD Publishing. 2014a.

OCDE, ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS. “Plan de acción contra la erosión de la base imponible y el traslado de beneficio ”. 2014b Disponible en: https://doi.org/10.1787/9789264207813-es.

OCDE, ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS. “Tax Challenges Arising from Digitalisation – Interim Report 2018, Inclusive Framework on BEPS”. OECD Publishing. 2018. DOI: https://doi.org/10.1787/9789264293083-en.

ORTEGA, MARIO. “Economía digital: la OCDE plantea tributar allí donde se crea el valor o aplicar un impuesto mínimo mundial”. 2019. Disponible en: https://amp.expansion.com/blogs/garrigues/2019/02/12/economia-digital-la-ocde-plantea.html.

POZZI, SANDRO. “Lagarde urge a terminar de inmediato la tensión por la guerra arancelaria”. El País (5 de junio de 2019), disponible en: https://elpais.com/economia/2019/06/05/actualidad/1559738146_801527.html.

SCHWAB, KLAUS. “La cuarta Revolución Industrial”. Barcelona: Editorial Debate. 2016

S OBA, LAINE. “Opening negotiations on a plurilateral Trade in Services Agreement (TiSA)”. Library of the European Parliament. 2013. Disponible en: http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2013/130582/LDM_BRI(2013)130582_REV1_EN.pdf.

ROHATGI, ROY. “Basic international taxation”. Londres: Legis. 2008.

ROSALES, OSVALDO. “El conflicto económico Estados Unidos-China”. Revista Económica&Administración, Nº 173, 2018. págs. 10-14. Disponible en: http://www.fen.uchile.cl/uploads/images/files/revista_173(2).pd .

VASWANI, KARISHMA. “Guerra comercial: 3 cosas en las que China y Estados Unidos nunca se podrán de acuerdo”. BBC. 2019. disponible en: https://www.bbc.com/mundo/noticias-46830998.

YILMAZ, FATIH Y JACQUELINE COOLIDGE. “Can e-filing reduce tax compliance costs in developing countries?”. *Policy Research Working Paper,* 6.647: 2013. Págs. 1-57. DOI: 10.1596/1813-9450-6647.

EL IMPACTO DEL DINERO ELECTRÓNICO EN LA INCLUSIÓN FINANCIERA – REALIDAD PERUANA

Eje tematico: E-Commerce, Smart Contracts y Pagos Electrónicos

Autor:
Edda Karen Céspedes Babilón
Abogada Investigadora Especialista en Derecho Informático y TIC
Directora de Comunicaciones e Informática Jurídica del Colegio de Abogados de Lima
Doctoranda en Derecho.
Universidad Nacional Federico Villarreal

RESUMEN
La llegada de Internet fue pieza fundamental para el Desarrollo Global de la Civilización Humana, y trajo consigo grandiosos avances en todos los ámbitos profesionales, aumentando la celeridad en todo tipo de procesos y servicios que nos permiten vivir en una constante y vertiginosa Transformación Digital con innovaciones tendentes a la interacción multidisciplinaria, veloces y eficaces.
La Digitalización ha alcanzado al ámbito empresarial reestructurando políticas y procedimientos debido a su trascendencia. De tal forma, que actualmente, contamos con servicios inteligentes, que nos permite reducir gastos, tiempo y espacio, que benefician no sólo a la población sino principalmente a las empresas y corporaciones que, en un balance general, además de ahorrar costos, generan mayor eficiencia
Esta eficiencia se extiende a la facilidad de contar en la actualidad, con medios de pagos electrónicos, los cuales vienen evolucionado conforme a las necesidades tecnológicas y se espera que, en un futuro cercano, el dinero en físico, sea canalizado por intermedio de softwares, aplicaciones y sistemas que puedan reemplazarlo y representar su valor.
En este sentido, debemos mencionar el sistema de monedas virtuales o Criptomonedas, las cuales se caracterizan por ser seguras en tanto cuentan con un valor financiero neutro. Sin embargo, las Criptomonedas, en su diversidad de uso y forma como el Bitcoin, Ethereum, Ripplex, y otras emergentes; aún no se encuentran reguladas.
Al respecto, existen diversas controversias, afirmando muchos que no es necesaria su regulación, porque perdería su esencia tecnológica y otras opiniones que difieren al respecto, indicando que debería asegurarse su correcto funcionamiento empleando leyes y procedimientos que las regulen en las Transacciones del Sistema Financiero, y asegurando de tal forma, una herramienta tecnológica que viene interactuando y creciendo positivamente en el mercado, dando lugar a un mejor desarrollo económico.
Es así que en el ámbito empresarial ha surgido una nueva industria financiera llamada *Fintech,* porque como su nombre lo indica, se trata de aplicar la tecnología a toda la rama financiera. Esto a su vez, ha suscitado el surgimiento de las *Startups* como un emprendimiento social que fomenta un ambiente de competitividad a nivel internacional y facilita la Inclusión Financiera.
En este sentido, en el Perú se ha dado un gran paso en materia legal al promulgarse la "Ley 29985, Ley que Regula las Características Básicas del Dinero Electrónico como Instrumento de Inclusión Financiera". En tal forma, estas alternativas de pago que vienen surgiendo deberán regularse para mejorar la competitividad en el mercado.
Palabras clave: Internet, Desarrollo Digital, Criptomoneda, Bitcoin, y Medios de Pago.

I. LA ERA DIGITAL

Desde una perspectiva psicológica, la Era Digital ha irrumpido progresivamente en el comportamiento humano desde finales del siglo XX. Esta generación inicia su permanencia en la sociedad con el despertar de la señal de una red inalámbrica, ya sea para obtener un libro de 500 páginas o una película de 160 minutos de duración.

Entonces podremos considerar a la Era Digital como la era del avance hacia el aprendizaje. La sociedad en general ha comenzado a recopilar una gran cantidad de datos y aspectos históricos específicos de la vida e información sociocultural, los cuales ahora los podemos encontrar en las plataformas de búsqueda digital por Internet (*Gloogle, Yahoo, Opera Mini*, etc.) La Era Digital también está inmersa en el ámbito científico, colaborando con la metodología para reclasificar la variable espacio-tiempo. (Don Tapscott, 2009)[436]

No podemos dejar de mencionar los cambios en temas socio-económicos, teniendo en cuenta la interacción mundial en temas empresariales, económicos, de Estado y Sociedad; como consecuencia de ello, esta era tecnológica permite el desarrollo de naciones emergentes que según su desprendimiento logran escalar a nivel de potencias mundiales; un claro ejemplo es Latinoamérica, en la cual están surgiendo empresas y emprendedores que son los nuevos líderes mundiales gracias a la digitalización.

A. Surgimiento Empresarial en la Era Digital

Evans, P. (1999),[437] afirma que el *Big Data*[438] está reconfigurando los negocios, transformando la organización interna y la arquitectura de las empresas. Evans describe los dos motores de las tecnologías de la información (TI) que están remodelando la organización interna, las estrategias de negocios y las estructuras empresariales:

---

436 *Las nuevas generaciones utilizan la tecnología digital de una forma muy diferente de cómo lo hicieron otras, ya que han desarrollado reflejos y comportamientos que usan con sus teléfonos celulares o en internet, y están revolucionando esta* última *convirtiéndola en un lugar para compartir y conectarse en "una clase de centro comunitario cibernético".* Don Tapscott,2009 Libro "La Generación Net" publicado 16 de diciembre del 2009

437 *La nueva economía de la información está haciendo a un lado las bases de la estrategia comercial tradicional. Según Blown to Bits, la definición de su negocio, la definición de la industria y la ventaja competitiva están simultáneamente disponibles. Evans y Wurster argumentan que, con la extensión de la conectividad y los estándares comunes, sus clientes tendrán cada vez más acceso a un universo de alternativas, sus proveedores explotarán el acceso directo a sus clientes y los competidores enfocados seleccionarán las partes más rentables de su valor cadena. Con una claridad intransigente y ejemplos vívidos, Blown to Bits se dirige directamente a los líderes empresariales y corporativos actuales. Este libro innovador muestra cómo construir nuevas estrategias que reflejan la nueva economía de la información y explica cómo aprovechar las fuerzas que configuran la ventaja competitiva de hoy*. EVANS Philip, Boston Consulting Group "Blown to Bits: How the New Economics of Information Transforms Strategy" (1999)

438 *Bigdata*; Capacidad de tratar grandes volúmenes de datos en un tiempo aceptable.

- El primero es la deconstrucción de las cadenas de valor: la descomposición de negocios verticalmente integrados a medida que los estándares y la interoperabilidad sustituyen a las interfaces gestionadas.
- El segundo es la polarización de las economías de masa, lo que se traduce en que, en determinados sectores, las economías de escala y de experiencia están desapareciendo, mientras que en otros se intensifican.

Evans afirma no creer que el *Big data* sea un fenómeno aislado o único, sino un ejemplo de un conjunto de tendencias más amplias y profundas que están reconfigurando el mundo de los negocios

El Surgimiento Empresarial nos sitúa frente a las partes de una transacción ante un público virtual. Los nuevos sistemas de pago como el *E-Money* o Criptomonedas y el emprendimiento digital como las *Startups, Fintech,* etc. en interacción nos demuestran un ecosistema de desarrollo empresarial de garantía y confianza.

B. Medios de Pago en la Era Digital:

- Dinero Electrónico - E-Money

E- money, moneda electrónica o Dinero Digital. Se emite en forma electrónica o a través de la utilización de una red de ordenadores, internet y sistemas de valores digitalmente almacenados como el caso del *Bitcoin*, es un medio de pago digital equivalente a una determinada moneda. Se estima que en un tiempo no muy lejano las personas a nivel mundial utilizaran este medio de pago digital, el cual va simplificar muchas cosas.

- Criptomoneda

Es un sistema monetario que no tiene un valor por el material del que está hecha o por su utilidad física, sino porque así está convenido. La diferencia entre un billete de 100 dólares y un trozo de papel con el texto de 100 dólares escrito con crayones es que las personas a través de instituciones nos ponemos de acuerdo para decir que uno tiene valor y el otro no; la manera en el que cualquier moneda define su valor es por su importancia en el mercado, mientras más personas estén interesadas en comprarlas son más valiosas como sucede en una subasta si mucha gente está interesada en un artículo ofrece más por él y su precio en el mercado será más alto. Existen cientos de Criptomonedas, que son llamadas así gracias a su naturaleza encriptada. Es decir, protegidas a través de una codificación. Esta característica las convierte en un sistema

monetario muy atractivo porque es difícil de alterar o *hackear* y porque no es controlada por un banco o por un gobierno como las monedas tradicionales. Las Criptomonedas optan por usar un sistema de transacciones descentralizado conocido como *Blockchain*, que son cadenas de bloques que funcionan de la siguiente manera:

- Cada transacción que se hace, es llamada bloque y adquiere un código único e irrepetible.
- Ese bloque queda registrado para siempre con información detallada como el emisor y receptor del intercambio cantidad entre otros datos.
- La red de usuarios registra la operación de manera virtual e inmediata.
- Ese bloque se une a una enorme cadena donde se encuentran enumeradas absolutamente todas las operaciones que se han realizado con esa criptomoneda y se muestran de manera cronológica. Debido a que está duplicada en muchas cuentas, es imposible alterar o borrar una operación que ha sido añadida al *blockchain*. La seguridad de la criptomoneda radica en la tecnología en sí misma que al repetir la operación en miles de usuarios y computadoras alrededor del mundo, y al mismo tiempo, el fraude sería prácticamente imposible de cometer porque cada uno de ellos tiene un registro que comprueba lo que realmente sucedió. Es decir, podría ser factible de *hackear* una computadora, pero con miles de personas monitoreando y registrando todos los movimientos de criptomonedas en diferentes computadoras, es prácticamente imposible porque todos los usuarios supervisan esa cadena de bloques, lo que ha convertido al *blockchain* en un sistema muy atractivo para realizar compra-venta, *e-commerce* y diferentes operaciones comerciales. Sin embargo, debemos tener mucho cuidado de invertir en criptomonedas porque su valor puede subir y dispararse, como de un momento a otro decaer estrepitosamente. La criptomoneda avizora volverse más segura, conforme la aceptación de las instituciones, como una transacción válida, sin embargo, es recomendable sólo invertir en criptomonedas arriesgando el dinero que uno esté dispuesto a perder. Rico Carrillo (2018)

- Bitcoin

Se llama *Bitcoin* a un tipo de criptomoneda que fue creada en el 2009. Se trata de dinero electrónico (virtual) y no oficial que puede utilizarse como medio de intercambio en operaciones comerciales. La creación del *Bitcoin* está atribuida a Satoshi Nakamoto, siendo su identidad un misterio.

II. CRIPTOMONEDAS, SISTEMAS DE PAGO Y DINERO ELECTRÓNICO EN

EL PERÚ

Primero debemos diferenciar que el respaldo del dinero electrónico, es el dinero del curso legal, es por ello que se requiere que el valor monetario este almacenado previamente en un soporte electrónico; el respaldo de las monedas virtuales es el respaldo en la tecnología y en los participantes en la red: El consenso de la mayoría es el aval de la transacción. (Rico Carrillo, M. 2018)

En este sentido, se dice que está cerca el fin del dinero en efectivo. Sin embargo, la realidad nos muestra una situación no tan inmediata. Las principales limitaciones son los elevados niveles de informalidad y corrupción, así como una insuficiente inclusión financiera en muchos países a nivel mundial. Después de un pronunciado impulso en el periodo 2010-2015 en la adopción de las tarjetas de crédito y de débito como medio de pago por parte de los consumidores peruanos, el avance se moderó, según un informe de Tecnocom, empresa española de consultoría y tecnología.

Según estos datos, en el último año del periodo analizado, Perú registró un crecimiento a ritmo anualizado de 9.6% de tarjetas de débito —en tercer lugar, en América Latina, después de México (13.5%) y Chile (12.9%— pero con una merma en las tarjetas de crédito, con un retroceso de 0.8%, en comparación con un crecimiento interanual en Chile de 27.6% y en Colombia, con 8.4%.

El POS básico sigue siendo el producto más solicitado, con un 80% de participación, seguido por el MPOS, o Mobile POS, que es un dispositivo más chico y cómodo que el POS tradicional, con un 15%. Expresado por Leandro Martín Ferreira, gerente general de Marco Marketing Perú.

Si hablamos a nivel mundial en Dinamarca el 75% de los habitantes realizan pagos a través de tarjetas de créditos y se piensa eliminar el dinero en efectivo, realidad que más adelante se implementará en la mayoría de países.

Según señaló Stefan Krautwald[439] en el Diario Gestión, el Perú es el tercer país con el mayor número de transacciones de criptoactivos (medio digital de intercambio que utiliza criptografía) en Latinoamérica, solo por detrás de Colombia y Venezuela. Krautwald, dijo también, que es muy importante para el Perú estar a la vanguardia en esta industria. Actualmente se mueven billones de inversión que podrían llegar al país, así como BIT Point hoy apuesta por este mercado. "Los gobiernos deben esforzarse por generar confianza para que los inversionistas vengan a crear valor en el Perú, sin duda esto generará miles de puestos de empleos y buenos ingresos para la Nación, vía impuestos", expresó. Asimismo, destacó que los *exchanges* de criptomonedas más grandes del mundo tienen hoy un volumen de cripto activos de hasta US$ 1 billón diarios. "Estas no son cifras alcanzables y reales para un país como Perú en

439 Miembro del Consejo de Directores de LATAM, tras anunciar que BIT Point, líder mundial japonés, inició sus operaciones en el Perú, desde el 01 de junio del 2019.

una primera etapa de operaciones. Sin embargo, sí vemos que Perú puede tener un potencial interesante en conjunto con el sistema financiero xistente", mencionó.

Tal como lo indica la Dra. Rico Carrillo[440] una de las diferencias fundamentales entre el sistema de pago de monedas virtuales frente al Dinero Electrónico es que las monedas virtuales no tienen como contraparte física el dinero de curso legal, como sucede con el Dinero Electrónico, por lo tanto, los sujetos participantes y el régimen jurídico son notablemente diferentes.

III. LEY DEL DINERO ELECTRÓNICO - MARCO JURÍDICO PERUANO - LEY 29985 LEY QUE REGULA LAS CARACTERÍSTICAS BÁSICAS DEL DINERO ELECTRÓNICO COMO INSTRUMENTO DE INCLUSIÓN FINANCIERA, REGLAMENTADO CON EL DECRETO SUPREMO Nº 090-2013-EF

En enero de 2013 se promulgó la Ley 29985 Ley que Regula las Características Básicas del Dinero Electrónico como Instrumento de Inclusión Financiera, Reglamentado con el Decreto Supremo Nº 090-2013-EF, cuyos objetivos son:

- Regular la emisión de dinero electrónico.
- Determinar las empresas autorizadas a emitirlo.
- Establecer el marco regulatorio y de supervisión de las Empresas Emisoras de Dinero Electrónico (EEDE).

A. Concepto de Dinero Electrónico - Artículo 2 Ley N° 29985

El Dinero Electrónico es un valor monetario representado por un crédito exigible a su emisor, el cual tiene las siguientes características:

- Es almacenado en un soporte electrónico.
- Es aceptado como medio de pago por entidades o personas distintas del emisor y tiene efecto cancelatorio.
- Es emitido por un valor igual a los fondos recibidos.
- Es convertible a dinero en efectivo según el valor monetario del que disponga el titular, al valor nominal.
- No constituye depósito y no genera intereses.

440 *Una de las diferencias fundamentales entre estos dos sistemas de pago es que las MV no tienen como contraparte física el dinero de curso legal, como sucede con el dinero electrónico, por lo tanto, los sujetos participantes y el régimen jurídico es notablemente diferente. Las MV no involucran la participación de los factores financieros tradicionales; el emisor generalmente es una empresa privada no financiera, es por ello que las normas de regulación y supervisión del sector financiero no son aplicables. En los esquemas de MV el control íntegro lo asume el emisor, quien gobierna la red y administra la emisión*

y circulación del dinero. Revista del Foro N°105 Colegio de Abogados de Lima 2018.

B. Emisores de Dinero Electrónico (Art. 5 Ley 29985)

Conforme al Art. 5 de la Ley 29985, los emisores de Dinero Electrónico no pueden establecer un límite a la vigencia de los fondos de dinero electrónico distinto al reglamentado. Cuando transcurran diez (10) años sin que una cuenta de dinero electrónico tenga movimientos y sin que medie reclamación durante ese lapso, dichos fondos son remitidos a la Dirección General de Endeudamiento y Tesoro Público del Ministerio de Economía y Finanzas para ser destinados a programas de inclusión financiera.

La Ley indica que están sujetos a los límites de emisión de dinero electrónico de una Unidad Impositiva Tributaria (UIT) por transacción, de acuerdo a las condiciones que se establezca en su reglamentación. Sujetándose a las disposiciones de encaje y a las que conforme a la Ley 29440, Ley de los Sistemas de Pagos y de Liquidación de Valores, formule el Banco Central de Reserva del Perú.

C. En el Artículo 6. La Ley 29985 resalta la Protección al Usuario

- **Garantía de recursos.** Indica que los emisores de Dinero Electrónico deben constituir fideic misos por el valor del Dinero Electrónico emitido conforme a las disposiciones que dicta la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones, resaltando que dicho Organismo de Control puede regular otras modalidades alternativas de garantía para los fondos de dinero electrónico emitidos.
- **Protección de Datos**. La emisión de dinero electrónico constituye un servicio financiero, y la información del usuario de dinero electrónico y de las operaciones que realice están sujetas a la Ley 29733, Ley de Protección de Datos Personales, y a la protección que establece el artículo 2, inciso 5, de la Constitución Política del Perú.

  La Ley 29733 fue promulgada el 03 de Julio del 2011, teniendo como objetivo garantizar el derecho fundamental a la Protección de Datos Personales a través de su adecuado tratamiento, en un marco de respeto a los demás derechos fundamentales que en ella se reconoce. Es de aplicación a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realiza en el territorio nacional y resalta su objeto de especial protección a los datos sensibles. Su Reglamento es el Decreto Supremo 003-2013-JUS, promulgado el 22 de marzo del 2013.
- **Las Modalidades de Contratación.** Aplicables al dinero electrónico, pueden ser escritas, electrónicas u otras, de acuerdo a la naturaleza de los productos,

sus características y las circunstancias en que estos se ofrecen, deben estar en concordancia con lo dispuesto en la Ley 29571, Código de Protección y Defensa del Consumidor; la Ley 28587, Ley Complementaria a la Ley de Protección al Consumidor en Materia de Servicios Financieros, y las normas reglamentarias emitidas para garantizar su cumplimiento.

• El objetivo de la **Ley 28587 Ley Complementaria a la Ley de Protección al Consumidor en Materia de Servicios Financieros** es complementar las disposiciones de la Ley de Protección al Consumidor con relación a los servicios prestados a los usuarios por las empresas de operaciones múltiples del sistema financiero sujetas a la regulación específica de la Superintendencia de Banca y Seguros y Administradoras Privadas de Fondos de Pensiones.

• El Articulo 2 de la Ley "Transparencia en la información"; indica que las empresas están sujetas a brindar a los usuarios toda la información que éstos demanden de manera previa a la celebración de cualquier contrato propio de los servicios que brindan. Dicha obligación se satisface con la puesta a disposición de los usuarios de los formularios contractuales en sus locales, así como en la página web que tengan habilitada al efecto, debiendo designar personal especializado para brindar asesoría a sus clientes sobre los alcances de los mismos.

° La Ley 29571 Código de Protección y Defensa del Consumidor dicta el Código que establece las normas de protección y defensa de los consumidores, instituyendo como un principio rector de la política social y económica del Estado la protección de los derechos de los consumidores, dentro del marco del artículo 65 de la Constitución Política del Perú y en un régimen de economía social de mercado, establecido en el Capítulo I del Título III, Del Régimen Económico, de la Constitución Política del Perú.

Teniendo como finalidad que los consumidores accedan a productos y servicios idóneos y que gocen de los derechos y los mecanismos efectivos para su protección, reduciendo la asimetría informativa, corrigiendo, previniendo o eliminando las conductas y prácticas que afecten sus legítimos intereses. En el régimen de economía social de mercado establecido por la Constitución, la protección se interpreta en el sentido más favorable al consumidor.

Es importante destacar que la referida Ley **29985, Ley del Dinero Electrónico en el Perú,** ha restringido su provisión exclusivamente a entidades que estén bajo el ámbito de supervisión del sistema financiero y, principalmente, a transacciones a través de la Banca Móvil con fin de garantizar la seguridad y confiabilidad del uso del Dinero Electrónico en un país como Perú, cuya población está dispersa geográficamente y cuyos niveles uso de telefonía móvil son los mayores en la región,

el uso de la tecnología móvil (celulares) como canal de acceso a servicios financieros no sólo reduciría considerablemente los costos de transacción, sino que eliminaría las barreras de acceso al sistema financiero.

IV. ERA DIGITAL E INCLUSION FINANCIERA - REALIDAD PERUANA

El Perú como país emergente se encuentra inmerso en la digitalización nacional. Al final del 2018, el Presidente Martín Vizcarra declaró que en la medida que tengamos una visión descentralizada, el país puede elevar su competitividad, favoreciendo el bienestar de las personas con una perspectiva de crecimiento profesional. Para concretar esta medida se creó el "Comité de Alto Nivel por un Perú Digital, Innovador y Competitivo", órgano de carácter estratégico y dependiente de la Presidencia del Consejo de Ministros (PCM).

Este nuevo ente tendrá como objetivo la coordinación multisectorial, articulación y promoción de las acciones relacionadas al desarrollo del Gobierno Digital. El comité estará integrado por el titular de la PCM, el Secretario de Gobierno Digital, un representante del Despacho Presidencial, y los titulares o representantes de los ministerios de Economía, Educación, Producción y Transportes y Comunicaciones. (R. Embajador 2019)

En 2018, el valor de las transferencias electrónicas creció 42%, siendo el instrumento electrónico más utilizado para realizar pagos digitales minoristas por parte de los clientes de las empresas del sistema financiero. Ello debido al desarrollo de aplicaciones móviles por parte de la banca.

El segundo instrumento en importancia en el monto de operaciones fue la tarjeta de débito, seguida por la tarjeta de crédito, que crecieron 22% y 14%, respectivamente, indicado por el Banco Central de Reserva (BCR).

a) Comercio Exterior

En materia de Comercio Exterior, el mundo ve con buenos ojos a Perú. Según Alfred Nader, (Gestión.pe.2018)[441] actualmente ocupamos el puesto seis en Latinoamérica, pues Contamos con el sistema de Western Unión, Global Pay una plataforma que nos brinda la facilidad de hacer transferencias seguras para realizar pagos con una cartera de 130 monedas que cuenta con certificado digital. El foco de esta iniciativa son las pymes y el apoyo a las nuevas empresas o emprendedores emergentes de esta Era como son los *Startups* y las *Fintech*.

- **Startups en Perú:** (Portal PQS)

- Chazki Empresa de envío de paquetes. Inició sus operaciones 2015, en 2016

441 Alfred Nader, *vicepresidente para América Latina y el Caribe de Western Union "Yo creo mucho en Perú, y confío en que los próximos tres años Perú será uno de los tres mayores mercados para nuestro negocio en América Latina"*, reveló a Gestión.pe. 1 de mayo del 2018 Lima

ingresó a Argentina y en 2017 llegó a México.

- Crehana: Comunidad creativa donde las personas exploran sus habilidades.

- Joinnus: Plataforma digital para eventos y en la que se puede comprar entradas en segundos.

• **Fintech Perú**

Según la consultora Finnovista, existen alrededor de 47 fintechs en Perú, posicionándonos terceros en Latinoamérica, detrás de Colombia y Chile. (Gestión) Las más innovadoras en Perú: (PQS)

- Latin Fintech: Es la primera fintech peruana de préstamos en línea. A través de su producto www.holaandy.com ha desembolsado préstamos desde el inicio de sus operaciones y busca seguir ayudando a quienes deseen un crédito rápido y de forma sencilla.

- Independencia: Especializada en el manejo y evaluación de data tradicional y alternativa que otorga préstamos online a partir de una experiencia 100% digital.

- Tienda Pago: Se define como una plataforma digital que permite a los pequeños comerciantes en los mercados emergentes financiar su mercancía semanal.

b. E-Money

En 2018 el BBVA Continental habilitó su red nacional a 1,800 cajeros para que los afiliado a BIM (Billetera Móvil) puedan retirar dinero en efectivo — sólo en moneda nacional — sin la necesidad de Internet y de una tarjeta.

c. BIM (Billetera Móvil)

Inició sus operaciones en febrero del 2016 desde entonces ha tenido un crecimiento vertiginoso tanto en número de clientes como de transferencias. Es una iniciativa del sistema financiero y el gremio bancario y abrió un terreno innovador en los medios de pago distintos al efectivo que existen en el mercado, permite enviar y recibir dinero, pagar por la compra de productos y servicios, hacer recargas de celulares, así como realizar el pago de tasas tarifarias a través de mensajes de texto de un celular convencional, no inteligente. (APAM 2018)

V. CONCLUSIONES

Nuestro país se encuentra inmerso en la Revolución Tecnológica, impulsada por Internet, la computación en la nube e Internet de las cosas (IoT), entre otros; lo que trae consigo una fluyente repercusión vertiginosa y cambios necesarios en los patrones de consumo, la forma de producir, comercializar bienes y servicios, así como en las cualificaciones y perfiles de trabajo que actualmente exige el mercado.

Con miras a la Inclusión Financiera el Gobierno Peruano muestra su interés con la promulgación de leyes como la LEY Nº 29985 Ley del Dinero Electrónico.

Sin embargo, aún falta mucho por hacer y deben acelerarse cambios urgentes en las políticas públicas, enfocándolas al ciudadano de a pie con el fin de promover mayor Concientización Digital que permita la aplicación de las tecnologías en todo ámbito y para un mejor desarrollo socio-económico de nuestro país.

VI. REFERENCIAS BIBLIOGRAFICAS

EVANS, Philip - Boston Consulting Group "Blown to Bits: How the New Economics of Information Transforms Strategy" (1999)

NADER, Alfred - Diario Gestión "En tres años, Perú estaría en Top 3 de Latinoamérica en transacciones internacionales" 1 de mayo del 2018 – Lima

MORELOS, Eduardo, - Director de Startupbootcamp Fintech México. "UN CAMINO DE DOBLE SENTIDO - La competición de instituciones financieras y FinTechs, una mirada en América Latina" - México 2017

PATIÑO, Manuel, Diario Gestión, "En tres años, Perú estaría en Top 3 de Latinoamérica en transacciones internacionales" 5 de mayo del 2018 – Perú

RICO CARRILLO, Mariliana "El Pago Electrónico en Internet: Estructura Operativa y Régimen Jurídico". Thomson Reuters Legal Limited - 2012, Pamplona - España

RICO CARRILLO, Mariliana, "Naturaleza Jurídica del Bitcoin y las Criptomonedas". Revista del Foro N°105 – Colegio de Abogados de Lima - 2018 Lima, Perú.

SLOTNISKY, Débora J. "Transformación digital" 2016 – Argentina.

TAPSCOTT, Don - Libro "La Generación Net" publicado 16 de diciembre del 2009 – EEUU.

VII. WEBGRAFÍA

https://asbanc.com.pe/Paginas/Noticias/DetalleNoticia.aspx?ItemID=443 (Consulta 25 de Mayo 2019)

http://progresomicrofinanzas.org/diner -electronico/ (Consulta 25 mayo 2019)

https://www.ipe.org.pe/portal/la-era-digital-llego-al-peru/ (Consulta 25 mayo 2019)

https://andina.pe/agencia/noticia-valor-de-operaciones-los-sistemas-pagos-subio-37-eneromayo-2018-715257.aspx (Consulta 29 de Mayo 2019)

https://gestion.pe/economia/peru-tercer-pais-mayores-transacciones-criptomonedas-latinoamerica-268891 (Consulta 02 junio 2019)

https://www.asbanc.com.pe/prensa/Reduccion-del-uso-del-dinero-en-efectivo-en-el-Peru.pdf (Consulta 03 de Junio 2019)

https://www.apam-peru.com/web/dinero-electronico-los-planes-de-la-billetera-movil-en-el-2018/ (Consulta 19 de Junio 2019)

https://gestion.pe/blog/te-lo-cuento-facil/2018/12/la-emergente-industria-fintech en-el-peru.html (Consulta 20 junio 2019)

https://gestion.pe/tu-dinero/pagos-electronicos-subio-40-2018-instrumento-usado-258951 (Consulta 23 junio 2019)

https://gestion.pe/tu-dinero/pagos-electronicos-expanden-peru-ventajas-seguridad-149137 (Consulta 25 junio 2019)

https://www.pqs.pe/emprendimiento/startups-peru-potencial-crecimiento-internacional (Consulta 25 junio 2019)

https://www.pqs.pe/emprendimiento/startups-peru-potencial-crecimiento-internacional (Consulta 25 junio 2019)

https://www.pqs.pe/tecnologia/startups-fintech-innovadoras-per (Consulta 25 junio 2019)

https://revistaembajador.com/la-era-digital-en-peru/ (Consulta 26 junio 2019)

DIREITOS INTELECTUAIS NA ERA DIGITAL, APLICATIVOS E SOFTWARES

RESGUARDO DE LA PROPIEDAD INTELECTUAL Y LA INFORMACIÓN GENERADA POR INSTITUCIONES PÚBLICAS Y LEY DE ACCESO A LA INFORMACIÓN

Eje temático: Derechos Intelectuales en la Era Digital

Autor:
Diego Adrián Moreno Carrasco
Abogado
Magíster en Derecho y Nuevas Tecnologías
Universidad de Chile

RESUMEN
En la sociedad actual, la información y el conocimiento constituyen uno de los principales activos económicos para la creación de nuevos bienes y servicios. De ahí la importancia de la existencia de reglas claras para su protección y gestión. En este trabajo se analizará el caso específico de aquella información generada en instituciones públicas, y que por reglas de transparencia es susceptible de ser requerida y los problemas jurídicos y tecnológicos que esto plantea, respecto del desarrollo de actividades de investigación, y de generación de nuevo conocimiento, entendiendo ese conocimiento también como información, cuando no se contemplan excepciones específicas para la entrega de esta, relacionadas con la propiedad intelectual y/o protección de bases de datos, lo que puede eventualmente afectar el desarrollo de estas actividades.

I. INTRODUCCIÓN

La sociedad actual afronta una confluencia y/o coexistencia de distintos paradigmas que rigen el comportamiento tanto de los individuos, como de las organizaciones que estos conforman. Expresiones como "Sociedad de la Información"; "Sociedad del Conocimiento"; "Sociedad de Red" (Reyes 2011, p. 194); se unen a otros nuevos paradigmas "Sociedad de la Transparencia" (Han, 2016, Pp. 12;77)[442], y que dan cuenta de las profundas transformaciones sociales propiciadas a través de la mejora constante de las tecnologías de la información y comunicaciones, pero que van

442 El autor señala que "(…) la sociedad de la transparencia es la sociedad de la información (…)", (Han, 2016, p. 77), lo que nos reconduce al primer concepto, información; "(…) Quien refiere la transparencia tan solo a la corrupción y a la libertad de información desconoce su envergadura. La transparencia es una coacción sistémica que se apodera de todos los sucesos sociales y los somete a un profundo cambio (…)" (Han, 2016, p. 12).

más allá de eso, generando "(…) una transformación significativa de las estructuras sociales, económicas, culturales, y por supuesto del poder (…)" (Reyes, 2011, p.193).

Un ejemplo de donde se confrontan estos paradigmas, y de las reglas legales creadas como consecuencia de su construcción lógica, es en aquellos casos en que instituciones públicas generan activos protegibles Propiedad Intelectual (PI), o que recopilan y sistematizan información que tiene valor económico, capaz de crear nuevos bienes y servicios digitales, que también requieren protección, pero que a su vez por ser instituciones públicas se encuentran sometidas a constantes requerimientos legales de información derivados de leyes de transparencia, que pueden propiciar apropiaciones no autorizadas de información o extracciones de bases de datos por terceros con distintas finalidades. La inexistencia de mecanismos de resolución adecuados puede generar inseguridad jurídica, respecto de la efectiva protección de los activos generados por estas instituciones, y también desincentivar la actividad creativa y la inversión que requieren para desarrollarse. El avance de los medios tecnológicos genera también nuevos retos a solucionar, respecto de la efectiva protección de estos activos, como revisaremos más adelante.

El presente trabajo tiene por objeto analizar los aspectos jurídicos más importantes relacionados con el resguardo de la PI y de la información generada por instituciones públicas, en caso que sea solicitada dicha información a través de los mecanismos contemplados en la Ley de Transparencia y Acceso a la Información Pública (LTAIP).

La especific dad de este tema a tratar, en mi consideración, viene dada por la naturaleza jurídica pública de estas instituciones, que las hace objeto de estos requerimientos de información pública, y por los alcances de la protección de la PI en el contexto de una sociedad cada vez más digitalizada, que reivindica el valor, principalmente económico del conocimiento, la información y los datos[443], para el desarrollo de actividades que permitan generar nuevos bienes y servicios.

A través de una solicitud de acceso (que en el caso chileno no requiere expresión de causa) se puede obligar a una institución a la entrega de información protegida por PI, vulnerando el objeto de la protección de esa información, igual que para el caso de las bases de datos[444], respecto de la información solicitada, incluyendo aquella

443 En sentido amplio, incluyendo por ejemplo contratos de I+D, licencias, softwares, secretos industriales, acuerdos de confidencialidad, entre otros

444 DIARIO OFICIAL DE LA UNIÓN EUROPEA, https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A31996L0009 [Verificado con fecha 13 de agosto de 2019]. La Directiva N°96/9/CE del Parlamento Europeo y del Consejo, de 11 de marzo de 1996 sobre la protección jurídica de las bases de datos, establece una protección adicional a la reconocida por el derecho de autor a los creadores de bases de datos que presenten atributos de originalidad, para impedir "(…) la extracción y/o reutilización no autorizadas del contenido de una base de datos a falta de un régimen armonizado relativo a la competencia desleal o de la correspondiente jurisprudencia (…)" (Considerando 6°); y también "(…) Considerando que la fabricación de una base de datos requiere una gran inversión en términos de recursos humanos, técnicos y económicos, y que las bases de datos se pueden copiar o se puede acceder a ellas a un coste muy inferior al necesario para crearlos de forma independiente (…) (Considerando 7°)". Vale decir, reconoce por un lado la necesidad general de proteger las bases de da-

almacenada en medios digitales[445], y permiten su obtención (extracción) y posterior reutilización y/o explotación comercial no autorizada a partir de la solicitud efectuada.

Revisaremos también algunos casos ocurridos en la Universidad de Chile (en adelante UCH)[446], principal institución pública del país en materia de generación de conocimiento e información protegible, para determinar el tipo de soluciones otorgadas por los entes administrativos y judiciales en estos casos en que se trata de proteger dicho tipo de información y los retos jurídicos que esto plantea, al no existir una excepción específica para la solución de estos casos.

II. ECONOMÍA DEL CONOCIMIENTO Y LA INFORMACIÓN EN LA ERA DIGITAL. PROPRIEDAD INTELECTUAL Y BASES DE DATOS

En la economía actual, la creación de riqueza que se sustenta en conocimiento e información, ambos recursos inmateriales. Dentro de estos, se consideran como relevantes desde el punto de vista económico los que adquieren originalidad y materialidad. Como ha señalado la Organización Mundial de la Propiedad Intelectual (OMPI), los activos intangibles son aquellos que representan el mayor valor en el mundo empresarial, siendo estos eventualmente protegibles mediante Propiedad Intelectual (PI), en consideración a que, por un lado, "(…) La PI facilita el funcionamiento de los mercados de las tecnología de varias maneras (…)"[447] (Ompi, 2015, p.41).

Por otro lado, la propiedad intelectual se ha definido como aquella que

> […]busca la protección jurídica de la identidad comercial, a través de las marcas comerciales, las denominaciones de origen, las indicaciones geográficas y los nombres de dominio, por un lado, y la protección de la innovación y la creatividad, a través de las patentes de invención, los modelos de utilidad, los diseños y dibujos industriales y los derechos de autor y derechos

tos, sean cual sean sus formas (art. 1), y que las extracciones o reutilizaciones no autorizadas pueden generar consecuencias negativas desde el punto de vista económico y o técnico, considerando la inversión que requiere su generación.

445 DIARIO OFICIAL DE LA UNIÓN EUROPEA, https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019L0790&from=EN [Verificado con fecha 13 de agosto de 2019]. Recientemente, la Directiva 2019/790 del Parlamento Europeo y del Consejo de 17 de abril de 2019 relativa a los derechos de autor y derechos afines en el mercado único digital, estableció nuevas regulaciones para las actividades de minería de textos y datos de contenidos, reconociendo que estas pueden "(…) comportar actos protegidos por derechos de autor, por el derecho sui generis sobre las bases de datos, o por ambos, en particular la reproducción de obras u otras prestaciones, la extracción de contenidos de una base de datos, o ambos, lo que sucede, por ejemplo, cuando se normalizan los datos en el proceso de minería de textos y datos (…)" (Considerando 8°).

446 CONSEJO PARA LA TRANSPARENCIA. Para efectos de análisis del presente artículo, se analizarán los pronunciamientos recaídos sobre las decisiones amparo C42-15; C215-17; y C4730-2018.

447 En este sentido, ha señalado la OMPI que "(…) los títulos de P.I. ofrecen una delimitación de esos activos y una garantía de exclusividad en el mercado. Por tanto, los derechos de P.I. transmiten información importante que puede resultar útil en la elaboración de contratos (…)". (Ompi, 2015, p.41)

conexos, por el otro (INSTITUTO DE ESTUDIOS JUDICIALES, FUNDACIÓN HACER CHILE , 2015, p. 7).

Desde ese punto de vista, una gestión adecuada de la PI potencia e incentiva la inversión en investigación, desarrollo e innovación en los países. Tanto las universidades, como los centros de la investigación y las industrias, son los mayores generadores de nuevos conocimientos e información. Lo anterior involucra la suscripción de distintos tipos de contratos destinados a proteger esa información y/o conocimiento, siendo frecuente la suscripción de acuerdos de confid ncialidad; la estipulación de regalías derivadas de contratos de licencia; contratos para resguardar el manejo de base de datos, entre otros[448] (Ompi, 2017, p.23).

Respecto de las bases de datos, (Schuster, s.f., p. 1) afirma que "(…) la producción de bases de datos y la distribución de estas forman parte de una industria "de contenido", que tiene repercusiones directas en la infraestructura de la información (…)" y que las compilaciones de información han adquirido cada vez más importancia, gracias al avance de la tecnología, excediendo la regulación existente el derecho de autor para compilaciones de obras (también puede ser sólo información, y sin las características de originalidad exigidas por el derecho de autor), lo que implicaría que "(…) los realizadores de bases de datos, que aportan una inversión sustancial, gocen de la protección de los frutos de dicha inversión (…)"(Schuster, s.f., Pp. 1-3). Para el autor lo anterior obliga superar la concepción de originalidad requerida por el derecho de autor respecto de las bases de datos, para efectos de otorgar protección jurídica a esas compilaciones, lo que plantea el desafío jurídico de buscar un mecanismo para otorgar protección jurídica a las bases de datos no originales, una protección jurídica *sui generis*.

III. ANÁLISIS DE CASOS. CAUSALES DE SECRETO O RESERVA. CONFIDENCIALIDAD DE LA INFORMACIÓN. DERECHOS DE CARÁCTER COMERCIAL Y ECONÓMICO

A continuación, revisaremos algunos casos que han ocurrido en la UCH, en los cuales se le ha solicitado información respecto de actividades de investigación e innovación, datos, es decir conocimiento e información, susceptible de tener valor económico.

448 Según la OMPI, la transferencia de conocimientos tecnológicos y comerciales de un lugar a otro pueden ser resguardados de distintas formas. "(…) Tales conocimientos a menudo están sujetos a diversas formas de propiedad intelectual (PI), tanto PI registrada, por ejemplo, patentes y diseños industriales, como PI no registrada, tales como los derechos de autor o los secretos comerciales. En segundo lugar, la tecnología, el diseño y el desarrollo de marcas determinan el éxito en el mercado y, por lo tanto, afectan a la distribución de valor en las cadenas globales de valor (…)".(Ompi, 2017, p.23)

Estas solicitudes han sido realizadas invocando la LTAIP, e involucrando Consejo para la Transparencia (CPLT) en primera instancia, y a los tribunales superiores de justicia en segunda instancia, a través del procedimiento administrativo especial establecido para tal efecto.

Cabe señalar que en la legislación chilena no existe una causal específica de excepción al ejercicio del derecho de acceso relacionada con PI, o para bases de datos, de tal manera que no existe una excepción legal expresa para estos casos, como ocurre el caso de la Ley Modelo Interamericana sobre Acceso a la Información para la PI, que contempla como excepción al derecho de acceso, la información de "(…) 3. patentes, derechos de autor y secretos comerciales (…)" (Organización de los Estados Americanos, 2010, p.13). De esta manera, la excepción más utilizada en la ley chilena es la de protección de los "derechos de carácter comercial o económico".

3.1 Calificación derecho/interés económico. Especificaciones técnicas. Cláusulas de confidencialidad. Acceso a bases de datos

i) Especificaciones Técnicas. El CPLT ha sido reiterativo en señalar que para que aplique la reserva legal, debemos referirnos a la afectación de un *derecho comercial o económico*[449], que según el reglamento de la LTAIP, corresponden a aquellos que el ordenamiento jurídico atribuye a las personas, "a título de derecho y no de simple interés"[450]. Esta regla ha sido manifestada por el CPLT en primera instancia, por ejemplo en un caso para denegar el acceso a cierta parte de la información solicitada, por aparecer explícitamente información de una tecnología protegida, y en otro caso, para permitir el acceso a la información del contrato de licencia, que no explicita la descripción técnica de una tecnología protegida mediante patente[451]. También ha sido reiterada por la Corte Suprema, siendo esta última quien ha señalado que, antes de determinar si existe un derecho económico o comercial, se trata de información pública, por expresa disposición del constituyente, respecto de la cual no se configura ninguna causal de reserva, y respecto de la cual, en palabras de la propia Corte, más

449 CONSEJO PARA LA TRANSPARENCIA, Decisión Amparo N° C42-15, considerando 5°; Decisión Amparo C215-17, considerando 2°

450 Reglamento Ley de Transparencia y Acceso a la Información Pública N° 20.285. Artículo 7 N° 2

451 CONSEJO PARA LA TRANSPARENCIA, en el primer caso decisión Amparo C42-15, considerandos 8°, 9°, 10° y 11°; y para el segundo caso, Decisión Amparo C215-17, considerando 8°. Resulta interesante destacar además la confusión conceptual en la que incurre el Consejo, que parece suponer que por no publicarse las especificaciones técnicas de la patente en el contrato de licencia, no hay una afectación de los potenciales derechos económicos y comerciales que pueda generar la tecnología, primero porque no razona respecto de lo referido al valor comercial de la negociación y los porcentajes de regalías de dichos contratos, y segundo porque el sistema de protección de patentes, lo que genera al solicitarse la protección de una determinada invención es precisamente volver público en contenido y descripción de esa invención ante una oficina de registro, ello a cambio del monopolio estatal de explotación comercial garantizado por el Estado por un determinado lapso de tiempo.

allá de los tecnicismos utilizados en el contrato de licencia, no se evidencia la entrega de información que pueda tener un valor económico o comercial que sea necesario reservar en pos del desarrollo de la actividad económica de la empresa y que constituya un derecho, "(…) pues no se vislumbran en ellas la referencia a cuestiones ligadas a especificaciones técnicas de las patentes cuyo uso se concede (…)", no detentando por ello valor económico estas[452].

ii) Confidencialidad. También han sido rechazadas las estipulaciones contractuales que contienen cláusulas de confidencialidad, ya que estas a juicio del CPLT no convierten a los contratos que las contienen, *per se*, en secretos, en la medida que estos "no se enmarcan en los supuestos de reserva que establece el artículo 8°, inciso 2°, de la Constitución Política, las que además deben establecerse en leyes de quorum calificado [453]. A mayor abundamiento, el propio Tribunal Constitucional ha señalado que "el documento secreto o reservado ingresa a un órgano del Estado, está obligado a respetar el principio de publicidad"[454], de tal manera que un documento que por disposición de las partes era secreto, pasa a ser público.

iii) Acceso a bases de datos. En un caso se solicitó el listado de directorio de todos los dominios comprados a través del portal *nic.cl*[455], que funciona bajo la dependencia de la UCH, y respecto del cual en primera instancia el CPLT accedió a la entrega de la información solicitada, en el entendido que esta era información "(…) registrada e ingresada digitalmente en las bases de datos de la Universidad (…)"[456], que se encuentra en poder de un órgano de la administración del Estado, y que por ende era pública, pero que se trataba de todos los dominios comprados en el portal NIC Chile, para el país, información que permite a su vez asociar esta información con el número IP asignado que el usuario de dominio eligió libremente usar[457]. Esta última circunstancia señalada por la Corte de Apelaciones al conocer el Reclamo de Ilegalidad de esta causa, y denegar la entrega de la información solicitada, destaca la importancia

452 CORTE SUPREMA, Recurso de Queja Rol N° 45.850-2017, considerando 10°.

453 CONSEJO PARA LA TRANSPARENCIA, Decisión Amparo C215-17, considerando 10°

454 TRIBUNAL CONSTITUCIONAL. Requerimento de Inaplicabilidad, Rol 2870-2015, considerando 20°.

455 NIC CHILE, es un centro perteneciente a la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile, encargado de la administración del Registro de Nombres de Dominio .CL, que identifica a Chile en la red Internet. Desde este rol, es responsable frente a la comunidad local y global de su funcionamiento de manera segura y eficie te, para permitir que personas, empresas e instituciones construyan su identidad en Internet, bajo .CL. Información disponible en https://www.nic.cl/acerca/index.html [Verificado con fecha 24 de mayo de 2019]. A su vez, según lo dispuesto en el Decreto Universitario Exento N° 0022140 de 2017 que lo crea, "cumple tareas en materia de investigación, extensión, y prestación de servicios en materias relacionadas con redes computacionales, y especialmente, en el ámbito de nombres de dominio de internet"

456 CONSEJO PARA LA TRANSPARENCIA, Decisión Amparo C4730-18, considerando 11°.

457 CORTE DE APELACIONES DE SANTIAGO, Reclamo de Ilegalidad Rol N° 39-2019. Considerando 12°

del nombre de dominio, "(…) análogo a un signo comercial empresarial o bien por su uso sin esos fines (…) [458], además de que la entrega

> " […] en la forma total e indiscriminada que se solicita, implica afectación a los derechos de los titulares de los nombres de dominio.cl, en su dimensión de derechos de carácter comercial y económico", ya que la información entregada corresponde al metadato, y es a partir de ese "metadato" entregado que los terceros pueden acceder a la información individual de cada usuario, "mediante el simple expediente de aplicar un programa de despliegue de registro de dominio.cl, o lo que se denomina sistema de algoritmos del mega dato al dato individual; lo que importa acceder de ese modo a la información que tiene el carácter de reservada, considerando que incluye a particulares, personas jurídicas, compañías, fundaciones públicas y privadas, sociedades, cooperativas y órganos del Estado, chilenos y extranjeros, que conforme enseñan las reglas de la sana crítica, en cuanto máxima de experiencia y conocimientos científicos asentados, guardan información reservada que fácilmente se puede obtener a partir del registro en Excel de "metadatos", atendido que se trata de un nombre de dominio que es indivisible con su titular, del que necesariamente se desplegará sin dificultad la información confidencial y estratégica de cada usuario con contenido económico, extrayéndolo del total de la base de datos de NIC Chile.cl; amén del uso criminal que podría hacerse de la información en relación a fraudes cibernéticos, aun estando de buena fe el requirente al transferir a cualquier título la información depositada en su favor […]"[459].

IV. OTRAS CONSIDERACIONES RELACIONADAS

i) Normativas: Se advierte que actualmente no existe una refl xión del conjunto del ordenamiento jurídico. Existe una lógica sistémica de la propiedad intelectual basada en el monopolio otorgado por el Estado a los autores o creadores de alguna obra o invención, que queda sin resguardo, en caso que dichas actividades sean realizadas dentro de una institución pública, porque existe la posibilidad permanente que esa información sea requerida mediante solicitud de acceso a la institución pública, sin expresión de causa, posibilitando la extracción de la información con valor comercial. Igual caso ocurre con la no protección jurídica de las bases de datos.

ii). Identificación en entornos digitales. Propiedad Intelectual en entornos digitales. La LTAIP opera a también través de plataformas virtuales[460], estableciéndose en los portales de servicios públicos mecanismos de identificación para la solicitud de información, que incluyen el nombre, apellido y dirección de correo electrónico del solicitante. De esta manera, muchas de estas solicitudes son realizadas por personas que existen en el mundo virtual o ciberespacio, y no necesariamente en el mundo físico, lo que nos lleva a la conclusión que las solicitudes se pueden formular a través de la creación de cuentas en la red (e-mails) e información del solicitante, que no necesariamente se condice

458 Ibid.
459 Ibid. Considerando 19°.
460 Ley N° 20.285. Diario Oficial de la República de Chile, Santiago, 30 de Agosto de 2008. Art. 12

con sus características físicas en el mundo real, y que agregan aún más incertidumbre respecto de la identific ción de quien realiza la solicitud. Al respecto, Johnson and Post (1996), han señalado que, a propósito de las actividades en línea regulables por una una posible ley del ciberespacio, la identificación de las personas es un aspecto que plantea nuevos desafíos "(…) For example, the law of the Net must deal with persons who "exist" in Cyberspace only in the form of an e-mail address and whose purported identity may or may not accurately correspond to physical characteristics in the real world (…)" (p. 1401).

Respecto de la PI, es necesario volver a considerar que una de las justificaciones de la protección es el derecho exclusivo del titular (monopolio) para controlar la reproducción, distribución, y comercialización del trabajo de autores o creadores, como recompensa al esfuerzo creativo, con lógica territorial. Pues bien, esta justificación se hace más difícil de controlar con la información existente en entornos digitales, en la medida que desaparecen las barreras físicas territoriales que justifican la PI, y que desde el punto de vista de los medios técnicos hacen difícil el control de la información, obras, creaciones que pueden distribuirse a mayor velocidad y en cualquier lugar del mundo: "(…) In the absence of global agreement on applicable copyright principles, the jurisdictional problems inherent in any attempt to apply territorially based copyrights regimes to electronic works simultaneously available everywhere around the globe are profound (…)" (Johnson and Post, 1996, p. 1383).

iii) ¿Datos abiertos? Cabe también preguntarse si podemos entender que la información solicitada es dato abierto, ya que se encuentran en poder de organismos públicos, muchos de los cuales promueven la apertura de datos. Al respecto, el Banco Mundial ha definido los datos abiertos como aquellos que "(…) cualquier persona los puede utilizar, re-utilizar, o redistribuir, tomando a lo sumo medidas para preservar el origen y la condición de Datos Abiertos (…)"[461].

Señala también el Banco Mundial que los datos abiertos deben poseer dos dimensiones: 1) ser abiertos en términos jurídicos, vale decir , deben ponerse en un sitio de acceso público u ofrecerse en condiciones liberales de uso y con mínimas restricciones; y 2) ser técnicamente abiertos, lo que significa que "(…) deben publicarse en formatos electrónicos que pueden leerse con máquinas y que preferentemente no sean exclusivos, de modo que cualquier persona puede acceder a ellos y usarlos mediante herramientas de software comunes y gratuitas (…)"[462].

Si bien algunos gobiernos promueven estrategias de política pública de datos abiertos[463], con la finalidad de generar nuevos bienes y servicios, es condición

461 BANCO MUNDIAL. Aspectos fundamentales de los datos abiertos. Recurso en línea disponible en http://opendatatoolkit.worldbank.org/es/essentials.html [Verificado con fecha 13 de agosto de 2019]

462 Ibíd.

463 Ibíd. Por ejemplo Australia; Brasil; Costa Rica; Chile; Ghana; India; Italia; Kenya; Mol-

necesaria que esos datos sean abiertos desde el punto de vista jurídico, vale decir libre de restricciones para su uso, lo que por cierto no ocurre con la información protegida por PI, ni con ciertas categorías jurídicas relacionadas con la protección jurídica *sui generis* (bases de datos).

V. CONCLUSIONES

En la sociedad actual, la información y el conocimiento constituyen uno de los principales activos económicos para la creación de nuevos bienes y servicios. De ahí la importancia de la existencia de reglas claras para su protección y gestión. En este trabajo se analizó el caso específico de aquella información generada en instituciones públicas, y que por reglas de transparencia es susceptible de ser requerida. Lo anterior, genera incertidumbre jurídica respecto del desarrollo de actividades de investigación, desarrollo y generación de nuevo conocimiento, entendiendo ese conocimiento también como información, más aún si consideramos que la normativa chilena no contempla como excepción específica para la entrega de dicha información, la relacionada con la PI, y/o protección de bases de datos. Es previsible que esta situación ocurra también en otras legislaciones que no contemplen excepciones expresas en la materia, dado que la respuesta del sistema jurídico en su conjunto no ha sido uniforme, respecto de la posible solución para este tipo de casos, más bien parece estar recién adaptándose a ellos.

Respecto del último punto, algunos elementos que han quedado en evidencia al analizar los pronunciamientos son la falta de profundización en la argumentación relacionada con la PI respecto de esa información, y la influencia de las nuevas tecnologías en la forma en cómo se interpretan derechos tradicionalmente reconocidos y regulados, o las nuevas tendencias regulatorias, como la protección jurídica de las bases de datos.

Por ahora la solución en el caso chileno se relaciona con la conceptualización de la "afectación de un derecho económico o comercial" exigido por la LTAIP como excepción a otorgar el acceso versus el interés económico y comercial. En principio, pareciera no haber solución, ya que tanto el CPLT como los tribunales superiores han señalado que la afectación debe referirse a un "derecho" y no "simple interés". En las actividades de transferencia tecnológica de los resultados de I+D las expectativas de las partes juegan un rol fundamental, trasformando los contratos de licencias, confidencialidad, de investigación, u otros dichas expectativas (que tienen valor comercial por su carácter de reservado), la creación de bases de datos con ciertos tipos de datos, en derechos, que es algo que no ha sido considerado aún, ello para

dova; Marruecos; Filipinas; Federación de Rusia; Reino Unido; Estados Unidos de América.

evitar también que el ejercicio abusivo del derecho de acceso a la información pública perjudique los derechos de terceros, y que es lo que proponemos como criterio de análisis para la resolución de este tipo de casos[464].

La consideración del valor económico de la información, respecto de la cual recaen derechos de la misma índole, es clave por ahora para la adecuada solución de estas solicitudes, y también para el resguardo del desarrollo de dichas actividades en instituciones públicas, fundamentales para el desarrollo económico de cualquier país. De igual manera, resulta esperable en el futuro la consideración de excepciones derivadas de información protegida por PI o de bases de datos desarrolladas con finalidad económica, de tal manera de evitar extracciones de datos para actividades de extracción de datos, siempre que estos no sean abiertos y accesibles al público, que es otra estrategia de gobierno para fomentar actividades en el contexto de la economía digital y que no se relaciona con lo expuesto en este trabajo. Un ejemplo de esto de excepción específica se encuentra en la Ley Modelo Interamericana sobre Acceso a la Información, que contempla la excepción para el derecho de autor, propiedad industrial y secretos industriales, y que puede ser tenida en consideración como una forma de solución. A ello debería incluirse una excepción también referida a las bases de datos, en aquellos casos en que su obtención, verificación o la presentación de dicho contenido representen una inversión sustancial desde el punto de vista cualitativo o cuantitativo, como lo dispone la Directiva 96/9/CE del Parlamento Europeo y del Consejo, en su artículo 7.

Finalmente, hay que considerar que las solicitudes de información se dan también en un contexto de cambio tecnológico, en donde el ejercicio de los derechos cambia respecto de lo que entendemos como contenido del derecho, y la forma en que se ejercen estos. El progreso digital continuará generando nuevos desafíos respecto de la generación de nuevas regulaciones y/ o adaptaciones, para hacer efectivo el ejercicio de esos derechos.

REFERENCIAS BIBLIOGRÁFICAS

464 CORTE SUPREMA. Voto de minoría, considerando 1° y 2° del Recurso de Queja 45.840-2017, respecto del amparo C215-17. Este señaló que la celebración de un contrato de licencia para la empresa "(…) forma parte de la planificación estratégica de cada unidad empresarial en pos de alcanzar sus propósitos u objetivos; configurándose, de aquel modo, un bien económico sobre el cual recae un derecho de la misma índole(…)", recayendo lo requerido sobre "[…]información utilizada en un actividad industrial que generalmente no es conocida ni fácilmente accesible por quienes desarrollan la misma actividad y cuyo valor comercial es consecuencia precisamente de su carácter reservado, habiéndose adoptado por sus poseedores, medidas conducentes es pos de resguardar tal condición[…]".

HAN, Byung-Chul. *La sociedad de transparencia*. Herder Editorial, Barcelona, 2016. Pp. 12; 77

INSTITUTO DE ESTUDIOS JUDICIALES, FUNDACIÓN HACER CHILE. *Manual de Propiedad Intelectual casos prácticos y análisis Teórico*. Santiago de Chile, Marzo de 2015. p. 7

JOHNSON R., David and POST, David. *Law and Borders- The Rise of Law in Cyberspace*. Standford Law Review, 1996. Pp. 1383; 1401. Artículo en línea disponible en https://www.researchgate.net/publication/220167130_Law_and_Borders_-_The_rise_of_law_in_Cyberspace [Verificado con fecha 13 de agosto de 2019].

ORGANIZACIÓN DE ESTADOS AMERICANOS. Comisión de Asuntos Políticos y Jurídicos. *Ley Modelo Interamericana sobre Acceso a la Información*. Agosto 2010. p. 13 Disponible en https://www.oas.org/dil/esp/CP-CAJP-2840-10_Corr1_esp.pdf [Verificado con fecha 13 de agosto de 2019].

ORGANIZACIÓN MUNDIAL DE LA PROPIEDAD INTELECTUAL. *Informe Mundial sobre la Propiedad Intelectual en 2015: La innovación revolucionaria y el crecimiento económico*. Ginebra, Suiza. Informe año 2015. p.41. Disponible en https://www.wipo.int/edocs/pubdocs/es/wipo_pub_944_2015.pdf [Verificado con fecha 24 de mayo de 2019]

ORGANIZACIÓN MUNDIAL DE LA PROPIEDAD INTELECTUAL. *Capital Intangible en las cadenas globales de valor*. Ginebra, Suiza. Informe año 2017. p.23 Disponible en https://www.wipo.int/edocs/pubdocs/es/wipo_pub_944_2017.pdf [Verificado con fecha 24 de mayo de 2019].

REYES OLMEDO Patricia. "La sociedad Red y el Gobierno de la Información", en *Ciudadanas 2020, el gobierno de la información*. Santiago de Chile, 2011. Pp. 193-194

SCHUSTER, Santiago. *Bases de datos originales y no originales*. Artículo disponible en http://www.scdbeta.scd.cl/curso_prop_int/curso_1/Bases%20de%20datos%20originales%20y%20no%20originales.pdf [Verificado con fecha 24 de mayo de 2019]

SITIOS WEB

www.bcn.cl
www.consejotransparencia.cl
www.eur-lex.europa.eu
www.oas.org
www.scdbeta.scd.cl

www.wipo.int
www.worldbank.org

OS MÉTODOS ONLINE DE RESOLUÇÃO DE DISPUTAS COMO INSTRUMENTOS DE ACESSO À ORDEM JURÍDICA JUSTA: EXPERIÊNCIA E DESAFIOS

Eixo temático: Direitos Intelectuais na Era Digital, Aplicativos e Softwares

Autores:
Julia Rugno
Graduanda em Direito pela Universidade Federal do Rio de Janeiro (UFRJ). Acadêmica de Direito.

Rafael Stefanini Auilo
Doutor e Mestre em Direito Processual pela Universidade de São Paulo (USP). Graduado em Direito pela Pontifícia Universidade Católica de São Paulo (PUC-SP). Autor de livros e artigos. Advogado e árbitro.

RESUMO
Este trabalho pretende analisar os métodos alternativos (e adequados) de solução de controvérsias à luz do acesso à ordem jurídica e suas relações com as novas tecnologias. Será dado especial atenção aos métodos denominados de Online Dispute Resolution (ODRs). Será analisado como esse método tem sido implementado no mundo e seus resultados obtidos, bem como os desafios para expansão do método em uma sociedade que é marcada pela *cultura da sentença*.

ABSTRACT
This article intends to analyze the alternative (and appropriate) dispute resolution methods in the light of access to justice and their relations with new technologies. Special attention will be given to the Online Dispute Resolution (ODRs) methods. It will be analyzed how this method has been implemented in the world and in Brazil and its results, as well as the challenges for its expansion in a society marked by *culture of the award*.

Sumário: I. Introdução. II. Os métodos online de solução de conflito (ODRs). III. As experiências estrangeira e brasileira: o avanço dos ODRs e os desafi s de sua implementação. IV. Conclusão. V. Bibliografia

I. INTRODUÇÃO

A vida em sociedade é marcada por insatisfações e conflitos. Os conflitos entre os sujeitos, de maneira geral e sociologicamente, são ruins para a sociedade como

um todo, especialmente para seu desenvolvimento e para a própria vida em grupo. Durante muito tempo a resolução desses confli os foi vista como um monopólio do Estado e chegou a ser tão supervalorizada que os demais meios de solução de conflitos eram menosprezados.[465]

No entanto, por meio das ondas renovatórias do processo civil, em especial quando o processo civil passou a ser visto como *instrumento* de consecução dos fins da jurisdição, essa visão modificou-se (e continua modificand -se). Além dos juízes, árbitros, mediadores e conciliadores também trabalham para pacificar conflitos. Esse, aliás, é o ponto comum entre a jurisdição estatal e os meios alternativos de solução de conflitos: a busca pela pacificação das disputas, eliminado, assim, os conflitos. Trata-se de um dos principais escopos da jurisdição e a razão principal pela qual muitos doutrinadores acabam por denominar esses métodos de solução de conflitos como métodos também jurisdicionais.[466]

Não se admite mais um sistema de solução de conflitos engessado, focado somente na atividade estatal e, principalmente, voltado para uma *cultura da sentença*. Busca-se pensar hoje em um sistema fl xível e adaptável às "necessidades funcionais decorrentes da variação dos objetivos substanciais a perseguir".[467]

Nesse novo cenário, os estudos dos métodos alternativos de solução conflitos (ADRs) se intensificaram e isso gerou frutos institucionalmente. Em 2010, por exemplo, foi editada pelo Conselho Nacional de Justiça a Resolução n. 125, que instituiu a Política Judiciária Nacional de tratamento adequado de conflitos. Referida resolução foi inspirada por estudo realizado por professores de todo o Brasil e membros do Conselho Consultivo do DPJ-CNJ.[468]

No estudo que embasou a Resolução CNJ n. 125 foi reconhecida que a crise do Poder Judiciário nacional, tem como principais fatores a baixa qualidade dos serviços jurisdicionais estatais e a demora e pouca efetividade da prestação jurisdicional.[469] O estudou comprovou que é possível ver aquilo que aqueles que advogam nos tribunais pátrios veem há tempos: a despeito da Constituição Federal proclamar ser uma garantia o acesso à ordem jurídica, ela não é vista na prática pelo jurisdicionado. Ou seja, embora haja formalmente uma garantia de acesso à justiça, na prática ela não é vista de forma substancial.

O referido estudo tem clara preocupação com o alcance daquilo que se denomina acesso à ordem jurídica *justa*, ao reconhecer que com a implementação de soluções

465 DINAMARCO, Cândido Rangel. *Instituições de direito processual civil*, vol. I, 8ª ed., São Paulo: Malheiros, 2016, p. 210.

466 DINAMARCO, Cândido Rangel; LOPES, Bruno Vasconcelos Carrilho. *Teoria geral do novo processo civil*, São Paulo: Malheiros, 2016, p. 31.

467 DINAMARCO, Cândido Rangel. *A instrumentalidade do processo*, 14ª ed., São Paulo: Malheiros, 2009, p. 37.

468 WATANABE, Kazuo. *Cognição no processo civil*, 4ª ed., São Paulo: Saraiva, 2012, p. 35.

469 WATANABE, Kazuo. *Cognição no processo civil*, 4ª ed., São Paulo: Saraiva, 2012, p. 36.

mais adequadas aos conflitos "o Judiciário Nacional estará adotando um importante filtro da litigiosidade, que, ao contrário de barrar o acesso à justiça, assegurará aos jurisdicionados o acesso à ordem jurídica justa".[470]

Para se obter o acesso à justiça não basta garantir a ampla possibilidade de acessos aos tribunais brasileiros, isto é, garantir a mera possibilidade de ajuizamento de demandas. Para além disso, é necessário que o jurisdicionado receba uma tutela jurisdicional *de qualidade*, *tempestiva* e *efetividade*.[471] E a implementação dos métodos alternativos de solução de controvérsias (também denominados *adequados*, pois cada método pode e deve ser desenhado para determinado tipo de controvérsia) contribui justamente para efetivação desse trinômio. Aliás, a implementação de soluções diversas de conflitos, tidas como mais adequadas para cada caso, tende a favorecer a substituição da *cultura da sentença* pela *cultura da pacificação*, o que também traz resultados positivos para uma melhor prestação da tutela jurisdicional. É uma questão quase que matemática: desafogar o Poder Judiciário e transferir a atividade jurisdicional para um terceiro ou mesmo munir os litigantes de ferramentas que permitam ou facilitem sua autocomposição leva a uma melhor possibilidade de as demandas que realmente desaguarem no Estado-juiz serem julgadas de forma tempestiva, célere e, acima de tudo, com qualidade na aplicação do direito. Trata-se de questão quase que matemática: com menos casos para julgar, mais rápido e com melhor qualidade tramitará o processo judicial por todas as instâncias, ordinárias ou extraordinárias, da justiça brasileira.[472]

Ao se analisar os problemas do Poder Judiciário elencados no mencionado estudo do CNJ, não se pode deixar de lembrar que os Juizados Especiais até tentaram, e inicialmente conseguiram, reduzir os efeitos deletérios da inefetividade da tutela jurisdicional ao promoverem um sistema mais célere e simples de resolução de conflitos. Entretanto, passados os anos, a insistência pela *cultura da sentença* continua a fazer com que o volume de processos apenas aumente[473], principalmente os decorrentes das relações de consumo, fazendo com que caia a qualidade da prestação da tutela jurisdicional. É certo e intuitivo que com maior carga de trabalho, menor a qualidade

---

470 WATANABE, Kazuo. *Cognição no processo civil*, 4ª ed., São Paulo: Saraiva, 2012, p. 37.

471 DINAMARCO, Cândido Rangel. *Instituições de direito processual civil*, vol. I, 8ª ed., São Paulo: Malheiros, 2016, p. 207.

472 WATANABE, Kazuo. *Cognição no processo civil*, 4ª ed., São Paulo: Saraiva, 2012, p. 42.

473 De acordo com o relatório *Justiça em Números de 2018*, aproximadamente 80 milhões de processos tramitam no Poder Judiciário brasileiro, o que significa um aumento de 44 mil novas ações em relação ao relatório passado. A taxa de congestionamento dos Juizados Especiais é de 56,7% e são ajuizadas mais demandas judiciais do que aquelas que são efetivamente julgadas, o que definitivamente não contribui para um acesso a uma ordem jurídica justa. (o relatório está disponível em http://cnj.jus.br/files/conteudo/arquivo/2018/08/44b7368ec6f888_383f6c3de40c32167.pdf – acesso em 11 de agosto de 2019). *Cfr.* também: POMPEU, Ana. *Judiciário brasileiro tem 80,1 milhões de processos em tramitação*. Disponível em: https://www.conjur.com.br/2018-ago-27/judiciario-brasileiro-801-milhoes-processos-tramitacao (acesso em 11 de agosto de 2019).

do serviço que será prestado e isso não é diferente com os magistrados que estão literalmente afogados cada vez mais em processos.

Atualmente, os processos que tramitam pelo procedimento dos Juizados Especiais são custosos tanto para alguns litigantes[474], quanto para o Estado e muitas vezes demoram a ser extintos.[475] Os Juizados Especiais tornaram-se uma panaceia, concentrando milhares demandas que poderiam ser evitadas. A situação atual dos Juizados Especiais vai de encontro ao princípio norteador do acesso à ordem jurídica justa (que, por sua vez, era o principal fundamento para criação desse procedimento). *O feitiço virou contra o feiticeiro*.[476]

Simultaneamente ao crescente aumento dos litígios e o afogamento do Poder Judiciário com as demandas, outro fenômeno vem ocorrendo na sociedade: a expansão do emprego da tecnologia nas mais variadas áreas. Cada vez mais o mundo está conectado e o grande propósito dessa expansão, além de aproximar, foi facilitar a vida delas, principalmente com o uso da internet. Atualmente, grande parte das atividades cotidianas é realizada por meio de apenas um clique. Exemplos não faltam, mas para este artigo destaca-se o do crescente aumento das compras *online*.

De uns tempos para cá o *boom* de plataformas de compras e vendas de produtos pela internet (*e-commerce*) levou a um aumento exponencial dos conflito envolvendo as relações de consumo – conflitos estes que basicamente são resolvidos perante os Juizados Especiais. Aliás, se antes a litigiosidade contida era um fato determinante para a facilitação do acesso à justiça por meio da criação dos Juizados Especiais, hoje a *cultura da sentença* e a ideia de *procurar o seu direito para tudo que ocorra* contribui justamente para o contrário.

Em razão do crescente aumento dos custos do processo (diretos ou marginais) e da falta de celeridade e efetividade da prestação jurisdicional, importantes sociedades empresárias começaram a pensar formas diferentes de solucionar essa grande quantidade de disputas que vinham surgindo. Foi nesse cenário, inclusive pensando em evitar que o alto número de disputas gere claro descrédito de suas próprias atividades perante o consumidor, que surgiram os métodos online de resolução de disputas, os chamados ODRs (Online Dispute Resolution).

---

474 DALMASO MARQUES, Ricardo. "A resolução de disputas online (ODR): do comércio eletrônico (e seus meios de pagamento) ao seu efeito transformador sobre o conceito e a prática do acesso à justiça". In: *Novos Estudos de Direito Bancário*. Curitiba: Editora Íthala.

475 A despeito da ausência de custos em primeiro grau, muitas vezes os litigantes acabam tendo que contratar advogados e não raras as vezes deparam-se com custos marginais ao processo, mas que são necessários para seu desenvolvimento, como o deslocamento em caso de audiência ou mesmo para acompanhamento processual nos casos em que há ainda processos tramitando de maneira física – outra crítica, mas que fica para um outro momento

476 WATANABE, Kazuo. "Relevância político-social dos juizados especiais cíveis (sua finalidade maior)". In: *Acesso à ordem jurídica justa: conceito atualizado de acesso à justiça, processos coletivos e outros estudos*, Belo Horizonte: Del Rey, pp. 33-39, 2019, p. 39.

II. OS MÉTODOS ONLINE DE SOLUÇÃO DE CONFLITO (ODRs)

Como visto, os ODRs nasceram com a proposta de serem uma alternativa eficiente, célere, de menor custo e facilitadora do acesso à justiça. Um casamento da tecnologia com os meios alternativos de resolução de conflitos.[477] Pelos ODRs, oferece-se uma plataforma online, desenhada para solucionar determinados tipos de conflitos, e as partes litigantes ou negociantes, via heterocomposição ou autocomposição, acabam resolvendo seus imbróglios sem ter que necessariamente deslocarem-se para o foro judicial ou precisarem de um juiz togado para resolver seus problemas. Ou seja, sua diferença para as outras formas de solução de conflito está em seu *design* e forma de acesso, não em sua natureza jurídica que é também jurisdicional, partindo-se do pressuposto que visam à pacificação dos conflito.

Basicamente os ODRs desenvolvem-se em negociação automatizada e assistida, mediação e arbitragem online e ombudsman online.[478] Ou seja, os ODRs não tratam apenas de resolução de disputas propriamente ditas, mas também de prevenção. Seu papel não se restringe a solucionar o conflito posto, mas também em os preveni .[479]

Apesar de terem sua origem no setor de *e-commerce*, é importante destacar que que os ODRs podem ser utilizados em diversos outros setores da economia como a saúde ou mesmo em disputas contratuais menos complexas, por exemplo.[480]

Os ODRs, além de serem um método alternativo de solução de controvérsias, também podem ser considerados um método *adequado* a depender do conflito posto. Diz-se adequado, pois, como já afirmado, cada demanda exige um método mais adequado para ser empregado na solução do conflito. No caso, por ora, os ODRs têm se mostrado mais adequados na solução de conflitos de natureza consumerista ou de conflitos de menor compl xidade.

III. AS EXPERIÊNCIAS ESTRANGEIRA E BRASILEIRA: O AVANÇO DOS ODRs E OS DESAFIOS DE SUA IMPLEMENTAÇÃO

477 BECKER, Daniel; LAMEIRÃO, Pedro. *Online Dispute Resolution (ODR) e a ruptura no ecossistema da resolução de disputas*. Disponível em https://www.ab2l.org.br/online-dispute-resolution-o-dr-e-ruptura-no-ecossistema-da-resolucao-de-disputas/ (acesso em 8 de agosto 2019).

478 PORTO, Antônio José Maristrello; NOGUEIRA, Rafaela; QUIRINO, Carina de Castro. "Resolução de conflitos on-line no Brasil: um mecanismo em construção". In: *Revista de Direito do Consumidor*, Vol. 114/2017, DTR\2017\7031, pp. 295-318, nov./dez. 2017.

479 DALMASO MARQUES, Ricardo. "A resolução de disputas online (ODR): do comércio eletrônico (e seus meios de pagamento) ao seu efeito transformador sobre o conceito e a prática do acesso à justiça". In: *Novos Estudos de Direito Bancário*. Curitiba: Editora Íthala.

480 LEORATTI, Alexandre. *TJRJ lança ferramenta de conciliação online para os casos da área da saúde*. Disponível em: https://www.jota.info/coberturas-especiais/inova-e-acao/tjrj-conciliacao-online--saude-12032019 (acesso em 7 de agosto de 2019).

Tratando-se de ODRs é imprescindível destacar a experiência da gigante de comércio eletrônico E-bay, que foi a primeira sociedade empresária que se tem notícia a implementar esse de método de solução de conflitos. A ideia dos criadores do ODR da E-bay foi desenhar uma plataforma em que tanto os consumidores quanto o comerciante tivessem a possibilidade de resolver seus problemas de forma inteiramente online e amigavelmente, dispensando-se dessa maneira o Poder Judiciário.

Atualmente o E-bay utiliza um software de negociação que resolve aproximadamente 60 (sessenta) milhões de disputas por ano.[481] Além disso, na plataforma há a opção de contratar um mediador via mundo virtual no valor de US$ 15,00 (quinze dólares americanos).[482] Sem dúvidas, os resultados alcançados pela plataforma impressionam, bastando verificar quantas demandas deixaram de ser ajuizadas perante o Poder Judiciário.

Seguindo esse modelo, recentemente a União Europeia também implementou uma plataforma de ODR[483], que é totalmente gratuita, disponível em todas as línguas oficiais da União Europeia que visa resolver conflitos oriundos de obrigações contratuais de compra e venda entre um consumidor que resida na União Europeia e um comerciante estabelecido também na União Europeia.[484] A função da plataforma é servir de intermediário entre os possíveis litigantes.

No Brasil, os ODRs já são uma realidade. Exemplo disso, foi o lançamento feito pela Secretaria Nacional do Consumidor do Ministério da Justiça do *consumidor.gov*, que consiste em uma plataforma que o consumidor faz o cadastro e registra determinada reclamação e o fornecedor (já devidamente cadastrado) se manifesta no prazo de 10 (dez) dias. Após essa etapa, o consumidor pode comentar o retorno, expor se o problema foi resolvido ou não.[485]

Recentemente, foram divulgados alguns números por parte do Governo Federal sobre o *consumidor.gov*. Foram registradas 1.720.000 (um milhão e setecentas e vinte mil) reclamações de consumidores na plataforma e um índice médio de solução de conflitos de 81% (oitenta e um por cento).[486] Foi divulgado também que há 494

481 BECKER, Daniel; MAIA, Andreia. *ODR as an effective method to ensure access to justice: the worring, but promissing brazilian case*. Disponível em https://www.mediate.com/articles/becker-odr-effe - tive.cfm (acesso em 8 de agosto de 2019).

482 BECKER, Daniel; MAIA, Andreia. *ODR as an effective method to ensure access to justice: the worring, but promissing brazilian case*. Disponível em https://www.mediate.com/articles/becker-odr-effe - tive.cfm (acesso em 8 de agosto de 2019).

483 *Cfr.* https://ec.europa.eu/consumers/odr/main/?event=main.trader.register (acesso em 8 de agosto de 2019).

484 BARROS, João Pedro Leite. *Online Dispute Resolution – perspectivas de Direito Comparado*. Disponível em https://www.conjur.com.br/2019-fev-26/joao-leite-barros-questoes-online-dispute-resolution (acesso 7 de agosto de 2019).

485 Consumidor.gov. Disponível em: https://www.consumidor.gov.br/pages/conteudo/publico/1 (acesso em 7 de agosto de 2019).

486 Consumidor em Números. Disponível em: https://www.justica.gov.br/news/collective-nitf-content-1552676889.94/arquivos/consumidor-em-numeros-2018_portal.pdf (acesso em 8 de agosto 2019).

(quatrocentas e noventa e quatro) sociedades empresárias cadastradas no sistema. Os resultados de todas as reclamações registradas no portal tornam-se públicas e os consumidores podem ter acesso às informações sobre os índices de resolução de conflito de cada sociedade. [487]

Dentre as pautas prioritárias definidas pelo Governo Federal divulgadas pelo estudo "consumidor em números" estão a *(i)* redução de litigiosidade nos conflitos de consumo, *(ii)* o aumento da transparência sobre coleta, processamento, uso e compartilhamento de dados pessoais e *(iii)* a ampliação do o alcance das ações de educação sobre consumo.[488]

A difusão do *consumidor.gov* pelo Brasil, tem resultado em práticas interessantes no Poder Judiciário. Já existem decisões suspendendo ou extinguindo processos a fim de que a plataforma do *consumidor.gov* seja utilizada em primeiro lugar para a tentativa de resolução do conflito [489] Tais decisões estão reconhecendo que o "Poder Judiciário não pode e não deve ser considerado a primeira e única porta para demanda de consumidores".[490]

Além da iniciativa do Governo Federal, há empresas que já oferecem em suas próprias plataformas serviços de ODR como é o caso do Mercado Livre. Com a implementação do ODR a empresa atingiu o patamar de incríveis 98,9% (noventa e oito ponto nove por cento) de *desjudicialização* dos conflitos que têm origem nas operações comerciais realizadas por meio de sua plataforma de venda. [491] O Mercado Livre possui diversas plataformas para tentar resolver o conflito antes que eventual demanda seja ajuizada perante o Poder Judiciário. As partes podem até mesmo contar com um mediador.

Existem também diversas *lawtechs* e *legaltechs* que oferecem esse tipo de serviço, como é o exemplo do Acordo Fechado, Concilie Online, eConciliar, Justto (Arbitranet), Mol, Sem Processo, D'acordo, dentre outras. [492]

---

487 Consumidor.gov. Disponível em: https://www.consumidor.gov.br/pages/conteudo/publico/1 (acesso em 7 de agosto de 2019).

488 Consumidor em Números. Disponível em: https://www.justica.gov.br/news/collective-nitf-content-1552676889.94/arquivos/consumidor-em-numeros-2018_portal.pdf (acesso em 8 de agosto 2019).

489 GONÇALVEZ, Caroline Visentini Ferreira; DALMASO MARQUES, Ricardo. *Acesso à orem jurídica justa nas relações de consumo e a tecnologia*. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/acesso-a-ordem-juridica-justa-nas-relacoes-de-consumo-e-a-tecnologia-15032019#_ftnref4 (acesso em 6 de agosto de 2019).

490 GONÇALVEZ, Caroline Visentini Ferreira; DALMASO MARQUES, Ricardo. *Acesso à orem jurídica justa nas relações de consumo e a tecnologia*. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/acesso-a-ordem-juridica-justa-nas-relacoes-de-consumo-e-a-tecnologia-15032019#_ftnref4 (acesso em 6 de agosto de 2019).

491 FREITAS, Tainá. *Como o mercado livre atingiu 98,9% de "desjudicialização" na resolução de conflitos*. Disponível em https://www.startse.com/noticia/nova-economia/64894/mercado-livre-odr--resolucao-conflit_ (acesso em 10 de agosto de 2019).

492 Radar de Lawtechs e Legaltechs. Disponível em: https://www.ab2l.org.br/radar-lawtechs/ (acesso em 7 de agosto de 2019).

Isso tudo indica que há um grande potencial de crescimento para ser alcançado e o futuro é promissor. No entanto, a despeito dessas louváveis iniciativas, ainda há amplo campo e ao mesmo tempo um desafio para ser explorado no Brasil. Como afirma Kazuo Watanabe, a estrutura mental conservadora do jurisdicionado brasileiro (e até mesmo dos operadores do Direito), apegada ao passado, é obstáculo para novas alternativas de resolução de disputas.[493] Uma mudança de visão sobre a importância da diversificação dos modos de acesso à justiça e o entendimento que esse acesso não basta ser formal (ou fic ício), ele tem que ser substancial é um passo imprescindível para o sucesso não somente dos ODRs, como também do próprio futuro daquilo que se entende por *tutela jurisdicional justa, tempestiva e efetiva*.

Outro passo imprescindível à expansão dos ODRs é a sua utilização pelos Tribunais de Justiça em casos menos complexos, repetitivos, tais como aqueles envolvendo as relações de consumo relacionadas ao *e-commerce*.[494] No entanto, há muita resistência ainda por parte dos advogados em incentivar essas medidas. Exemplo dessa resistência foi a atitude da Ordem dos Advogados do Brasil – Seccional do Estado do Rio de Janeiro (OAB-RJ) em protestar contra o sistema automatizado de soluções de conflitos que o Tribunal de Justiça do Estado do Rio de Janeiro está desenvolvendo. A justificativa do protesto seria que a "medida exclui a participação de advogados na resolução de conflitos, já que os casos serão analisados via internet por um robô".[495] Trata-se de protesto preconceituoso e que decorre de uma velha visão que todo e qualquer conflito deve desaguar perante um juízo e vara e que o advogado é necessário para todo e qualquer litígio – o advogado é imprescindível para uma correta administração da justiça, mas ele não é necessário para solucionar qualquer pendência que surja entre dois ou mais sujeitos.

Esse receio manifestado pelos operadores do Direito com as novas formas de resolução de disputas se dá muito por conta também da própria formação do profissional do Direito. No Brasil, ela é voltada para a perpetuação da *cultura dos conflitos*, visto que poucas faculdades oferecem como disciplina obrigatória os métodos alternativos (adequados) de solução de conflitos (mediação, conciliação e arbitragem). Para o Ministro Dias Toffoli é importante que se compreenda que outros meios que não os tradicionais podem e são mais adequados e eficientes para alcançar a pacificação

493 WATANABE, Kazuo. *Cognição no processo civil*, 4ª ed., São Paulo: Saraiva, 2012, p. 29.

494 RAINEY, Daniel. *Access to justice and ODR*. Disponível em: http://odr.info/access-to--justice-and-odr-by-daniel-rainey/ (acesso em 10 de agosto de 2019).

495 PÁDUA, Luciano. *OAB-RJ protesta contra sistema automatizado de solução de conflitos*. Disponível em https://www.jota.info/justica/oab-rj-protesta-contra-sistema-automatizado-de-solucao--de-conflitos-1903201 (acesso em 7 de agosto de 2019). Nesse mesmo sentido: WOLKART, Erik Navarro; BECKER, Daniel. *Entre gritos e sussurros*. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/entre-gritos-e-sussurros-28032018#sdfootnote12sym (acesso em 10 de agosto de 2019).

social.[496] Apenas em 2018 o Conselho Nacional de Educação estabeleceu essa disciplina como obrigatória nos cursos de Direito.[497]

Não foi a primeira vez, nem será a última manifestação contra o uso de tecnologia no Direito, em especial nas soluções de conflitos [498] Nesse ponto, Erick Navarro Wolkart e Daniel Becker assinalam que o avanço tecnológico no Direito exigirá atividades mais refl xivas e que necessitam de uma interação humana e consequentemente melhor qualificação profissiona .[499] Aliás, essa afirmação inclusive serve para desmistificar o preconceito observado nas manifestações contrárias ao uso desses métodos online: essas ferramentas não visam desprestigiar a profissão, mas sim favorecer o acesso à ordem jurídica justa; além disso, seu uso não extinguirá a função do advogado, apenas fará com que ele desenvolva novas competências que se farão necessárias futuramente.

É importante que institucionalmente haja maior e cada vez melhor divulgação e apoio a essas plataformas online de solução de conflitos, bem como a sociedade seja educada para sua utilização. Os ODRs não servem para substituir por completo o Poder Judiciário ou mesmo os outros métodos alternativos de solução de conflitos e de modo algum tem-se tal pretensão. Ao reverso, eles servem basicamente para endereçar determinados tipos de conflitos que não demandem sua solução em presença física ou que não dependam do Poder Judiciário. Os ODRs não são uma panaceia para todos os problemas do acesso à ordem jurídica justa, mas podem servir como mais um aliado para sua consecução.

IV. CONCLUSÃO

Diante da sobrecarga do Poder Judiciário, inclusive dos Juizados Especiais, os métodos alternativos (e adequados) de solução de controvérsias surgiram para quebrar paradigmas na comunidade jurídica, para transformar a *cultura da sentença* em uma *cultura da pacificação*.

---

496 CREPALDI, Thiago; VALENTE, Fernanda. *Maior acesso à justiça não é causa da morosidade, afirmam juristas*. Disponível em: https://www.conjur.com.br/2019-mar-01/maior-acesso-justica-nao--causa-morosidade-afirmam-jurista (acesso em 11 de agosto de 2019).

497 Como bem pontuado pelo conselheiro do CNJ, Valdetário Monteiro, a adoção obrigatória de cadeiras de conciliação, mediação e arbitragem pode transformar uma prática de judicialização dos conflitos nos cursos de direito. *Cfr.* HERCULANO, Lenir Camimura. *Conciliação será matéria obrigatória nos cursos de direito*. Disponível em: http://cnj.jus.br/noticias/cnj/88448-conciliacao-sera-materia--obrigatoria-nos-cursos-de-direito (acesso em 11 de agosto de 2019).

498 Nesse sentido: *Diretores da OAB fazem protesto silencioso contra o PJE*. Disponível em: http://www.oabpa.org.br/index.php/noticias/4977-diretores-da-oab-fazem-protesto-silencioso--contra-o-pje. (acesso em 10 agosto de 2019). Ver também: *OAB diz que processo eletrônico caótico exclui cidadão*. Disponível em: https://jornaldebrasilia.com.br/brasil/oab-diz-que-processo-eletronico-caotico-exclui-cidadao/ (acesso em 10 de agosto de 2019).

499 WOLKART, Erik Navarro; BECKER, Daniel. *Entre gritos e sussurros*. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/entre-gritos-e-sussurros-28032018#sdfootnote12sym (acesso em 10 de agosto de 2019).

Com o avanço da tecnologia, os ODRs tornaram-se uma realidade para facilitar para todos o acesso à ordem jurídica justa, inclusive porque muitas vezes os ADRs não se mostram adequados para solucionar determinados tipos de conflitos, visto que podem ser igualmente custosos.[500] Os ODRs desenvolveram-se muito nos últimos anos, com experiência em diversos países estrangeiros seja no campo institucional como a União Europeia, ou seja na iniciativa privada como a plataforma criada pelo E-bay.

No Brasil, o Governo Federal e a inciativa privada têm trabalhado para expandir esses serviços ainda pouco conhecido e utilizados pelos brasileiros. Parece se estar no caminho certo, tendo em vista as experiências positivas vivenciadas pelo Mercado Livre, *consumidor.gov* e demais *lawtechs* e *legaltechs*. Mas ainda há um logo caminho para ser percorrido.

Independente das áreas que os ODRs sejam utilizados (sua aplicação é mais clara no *e-commerce*, mas não é restrita a ele), é inegável que o maior desafio é fazer com que a mentalidade da sociedade seja desjudicializada, pois ainda muito apegada à *cultura da sentença*, bem como que as instituições entendam que sua função não é proteger os interesses próprios, mas principalmente os interesses do jurisdicionados, que querem a pacificaçã de seus conflitos de forma célere, barata e eficaz. A mentalidade voltada para uma *cultura de conflito* (judicialização de tudo) ocorre também pela própria formação educacional do profissi nal do direito, que não recebem nas faculdades de Direito um treinamento para buscar mais a pacificação dos conflitos que sua perpetuação. É um trabalho da sociedade, especialmente da comunidade jurídica, compreender que tais ferramentas expandem e efetivam o acesso à ordem jurídica, e ao mesmo tempo trabalham em favor da pacificação dos conflitos (escopo social e principal da jurisdição). O caminho é longo e árduo, mas o futuro (inclusive próximo) é promissor.

V. BIBLIOGRAFIA

(AUTOR DESCONHECIDO) https://ec.europa.eu/consumers/odr/main/?event=main.trader.register (acesso em 8 de agosto de 2019).

(AUTOR DESCONHECIDO). *Diretores da OAB fazem protesto silencioso contra o PJE*. Disponível em: http://www.oabpa.org.br/index.php/noticias/4977-diretores-da-oab-fazem-protesto-silencioso-contra-o-pje. (acesso em 10 agosto de 2019).

500 A arbitragem e a mediação tradicionais são métodos alternativos de solução de controvérsia e por vezes mostram-se adequados a depender do litígio posto. No entanto, esses métodos podem ser custosos e, por isso, acabam sendo mais adequados em casos de maior complexidade ou mesmo que demandem sigilo (que também é um tema espinhoso e deve ser tratado numa seara própria). O que é importante ter em mente é que cada método de solução de conflito pode ser desenhado para cada tipo de litígio e nunca haverá uma resposta certa ou padrão. Sua análise sempre dependerá muito do caso concreto e o mais importante é que todos os operadores do Direito adquiram consciência disso.

(AUTOR DESCONHECIDO). *OAB diz que processo eletrônico caótico exclui cidadão.* Disponível em: https://jornaldebrasilia.com.br/brasil/oab-diz-que-processo-eletronico-caotico-exclui-cidadao/ (acesso em 10 de agosto de 2019).

BARROS, João Pedro Leite. *Online Dispute Resolution – perspectivas de Direito Comparado.* Disponível em https://www.conjur.com.br/2019-fev-26/joao-leite-barros-questoes-online-dispute-resolution (acesso 7 de agosto de 2019).

BECKER, Daniel; LAMEIRÃO, Pedro. *Online Dispute Resolution (ODR) e a ruptura no ecossistema da resolução de disputas*. Disponível em https://www.ab2l.org.br/online-dispute-resolution-odr-e-ruptura-no-ecossistema-da-resolucao-de-disputas/ (acesso em 8 de agosto 2019).

BECKER, Daniel; MAIA, Andreia. *ODR as an effective method to ensure access to justice: the worring, but promissing brazilian case*. Disponível em https://www.mediate.com/articles/becker-odr-effective.cf (acesso em 8 de agosto de 2019).

Conselho Nacional de Justiça (CNJ). *Justiça em números 2018*. Disponível em: https://www.cnj.jus.br/files/conteudo/arquivo/2018/09/8d9faee7812d35a58cee3d92d2df2f25.pdf (acesso em 11 de agosto de 2019).

Consumidor.gov. Disponível em: https://www.*consumidor.gov*.br/pages/conteudo/publico/1 (acesso em 7 de agosto de 2019).

Consumidor em Números. Disponível em: https://www.justica.gov.br/news/collective-nitf-content-1552676889.94/arquivos/consumidor-em-numeros-2018_portal.pdf (acesso em 8 de agosto 2019).

CREPALDI, Thiago; VALENTE, Fernanda. *Maior acesso à justiça não é causa da morosidade, afirmam juristas*. Disponível em: https://www.conjur.com.br/2019-mar-01/maior-acesso-justica-nao-causa-morosidade-afirmam-jurista (acesso em 11 de agosto de 2019).

DALMASO MARQUES, Ricardo. "A resolução de disputas online (ODR): do comércio eletrônico (e seus meios de pagamento) ao seu efeito transformador sobre o conceito e a prática do acesso à justiça". In: *Novos Estudos de Direito Bancário*. Curitiba: Editora Íthala.

DINAMARCO, Cândido Rangel. *A instrumentalidade do processo*, 14ª ed., São Paulo: Malheiros: 2009.

DINAMARCO, Cândido Rangel. *Instituições de direito processual civil*, vol. I, 8ª ed., São Paulo: Malheiros, 2016.

DINAMARCO, Cândido Rangel; LOPES, Bruno Vasconcelos Carrilho. *Teoria geral do novo processo civil*, São Paulo: Malheiros, 2016.

FREITAS, Tainá. *Como o mercado livre atingiu 98,9% de "desjudicialização" na resolução de conflitos*. Disponível em https://www.startse.com/noticia/nova-economia/64894/mercado-livre-odr-resolucao-conflit (acesso em 10 de agosto de 2019).

GONÇALVEZ, Caroline Visentini Ferreira; DALMASO MARQUES, Ricardo. *Acesso à orem jurídica justa nas relações de consumo e a tecnologia*. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/acesso-a-ordem-juridica-justa-nas-relacoes-de-consumo-e-a-tecnologia-15032019#_ftnref4 (acesso em 6 de agosto de 2019).

HERCULANO, Lenir Camimura. *Conciliação será matéria obrigatória nos cursos de direito*. Disponível em: http://cnj.jus.br/noticias/cnj/88448-conciliacao-sera-materia-obrigatoria-nos-cursos-de-direito (acesso em 11 de agosto de 2019).

LEORATTI, Alexandre. *TJRJ lança ferramenta de conciliação online para os casos da área da saúde*. Disponível em: https://www.jota.info/coberturas-especiais/inova-e-acao/tjrj-conciliacao-online-saude-12032019 (acesso em 7 de agosto de 2019).

PÁDUA, Luciano. *OAB-RJ protesta contra sistema automatizado de solução de conflitos*. Disponível em https://www.jota.info/justica/oab-rj-protesta-contra-sistema-automatizado-de-solucao-de-conflitos-1903201 (acesso em 7 de agosto de 2019).

POMPEU, Ana. *Judiciário brasileiro tem 80,1 milhões de processos em tramitação*. Disponível em: https://www.conjur.com.br/2018-ago-27/judiciario-brasileiro-801-milhoes-processos-tramitacao (acesso em 11 de agosto de 2019).

PORTO, Antônio José Maristrello; NOGUEIRA, Rafaela; QUIRINO, Carina de Castro. "*Resolução de conflitos on-line no Brasil: um mecanismo em construção*". In: *Revista de Direito do Consumidor*, Vol. 114/2017, DTR\2017\7031, pp. 295-318, nov./dez. 2017.

Radar de Lawtechs e Legaltechs. Disponível em: https://www.ab2l.org.br/radar-lawtechs/ (acesso em 7 de agosto de 2019).

RAINEY, Daniel. *Access to justice and ODR*. Disponível em: http://odr.info/access-to-justice-and-odr-by-daniel-rainey/ (acesso em 10 de agosto de 2019).

WATANABE, Kazuo. *Cognição no processo civil*, 4ª ed., São Paulo: Saraiva, 2012.

WATANABE, Kazuo. "Relevância político-social dos juizados especiais cíveis (sua finalidade maior)". *In*: *Acesso à ordem jurídica justa: conceito atualizado de acesso à justiça, processos coletivos e outros estudos*, Belo Horizonte: Del Rey, pp. 33-39, 2019.

WOLKART, Erik Navarro; BECKER, Daniel. *Entre gritos e sussurros*. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/entre-gritos-e-sussurros-28032018#sdfootnote12sym (acesso em 10 de agosto de 2019).

RETRIBUCION DE LOS AUTORES POR LA REPRODUCCION DIGITAL DE SUS OBRAS EN INTERNET

Eje Temático: Derechos Intelectuales en la era digital

Autor:
Horacio Fernandez Delpech
Abogado y Profesor Universitario. Profesor Emérito de la Universidad del Salvador. Buenos Aires. Republica Argentina y Profesor Titular de Derecho Empresario de la Universidad Austral. Buenos Aires. República Argentina
República Argentina

ABSTRACT
La ponencia esta referida a las diferentes formas que existen para retribuir a los autores por la reproducción digital de sus obras. Para ello se parte del concepto de reproducción, en los Convenios Internacionales y normativas de los estados, como el principal derecho que tienen los autores con relación a sus obras de autorizar su reproducción. Estableciendo que la reproducción sin la correspondiente autorización de los autores convierte a esas reproducciones en reproducciones ilícitas, así como que dentro del concepto de reproducción protegido se encuentran las reproducciones digitales y las reproducciones en Internet.
Se analizan luego las licencias individuales estructuradas en diferentes tipos de contratos de edición, como la forma originaria de retribuir a los autores. Luego y ya en el plano de los derechos de reproducción digital se referencia el Copyright y el Copyleft, como los dos sistemas básico que existen y se utilizan , pasando luego a las nuevas formas de reproducción como son las nuevas licencias colectivas digitales tales como las que utiliza Netflix, Amazon y otras empresas, y la gestión colectiva de derechos digitales, para por ultimo terminar referenciando los nuevos sistemas de copia privada sujetas a una justa retribución para los autores, vigente en Europa y en muchas naciones iberoamericanas y la reciente retribución a los editores de prensa por el uso digital de sus obras por parte de los proveedores de servicios, establecida recientemente por la nueva Directiva Europea sobre derechos de autor en el Mercado Digital.

I. INTRODUCCIÓN

Dentro de los derechos que todo autor tiene sobre su obra literaria, artística o científica, el derecho básico y fundamental es el Derecho de Reproducción, que es exclusivo de los autores, sus herederos y los editores a quienes se les haya cedido una obra, y que les permite únicamente a ellos autorizar la reproducción de esa obra. Estos titulares del derecho son los únicos que pueden autorizar la reproducción de sus obras intelectuales.

Consecuentemente toda reproducción que se realice sin esa autorización es una reproducción ilegal generadora de responsabilidad para el infractor.

Casi todas las legislaciones del mundo partiendo de su ley madre, el Convenio de Berna, [501] protegen a las obras intelectuales contra la reproducción sin la autorización del titular de los derechos de propiedad intelectual, y establecen *"los autores de obras literarias y artísticas protegidas por el presente Convenio gozarán del derecho exclusivo de autorizar la reproducción de su obras por cualquier procedimiento y bajo cualquier forma"*.

Este amplio concepto de reproducción utilizado por el Convenio me permite poder afirmar que el mismo es no solo aplicable a la obra escrita, sino también a la obra digital.

Como reafirmación de ello el **Tratado sobre Derechos de autor de la OMPI (TODA o WCT)** [502] ,vigente desde el 6 de Marzo de 2002, reafirma la obligación de cumplimiento del Convenio de Berna, e introduce expresamente el entorno digital en la protección de los derechos de autor, al establecer en la declaración concertada respecto del art. 1.4. el siguiente párrafo:

> *"El derecho de reproducción, tal como se establece en el Artículo 9 del Convenio de Berna, y las excepciones permitidas en virtud del mismo, son totalmente aplicables en el entorno digital, en particular a la utilización de obras en forma digital. Queda entendido que el almacenamiento en forma digital en un soporte electrónico de una obra protegida, constituye una reproducción en el sentido del Artículo 9 del Convenio de Berna"*

Es por ello que este concepto de reproducción utilizado por las diferentes legislaciones y por el Convenio de Berna, es no solo aplicable a la obra intelectual en un formato tangible, sino también a la obra digital de formato intangible, y nos encontramos entonces en esta era de la información y la comunicación en que vivimos, que las nuevas tecnologías que facilitan enormemente la reproducción y divulgación de las obras del intelecto, en soportes no tradicionales, producen y facilitan la permanente reproducción de las obras en formas digitales incluso cuando esas obras que han sido digitalizadas son subidas a Internet.

Muchos consideran que existe el libre derecho de reproducción de la obra digital en Internet, ya que los derechos de propiedad intelectual en particular el derecho exclusivo de los autores a autorizar la reproducción de sus obras, no existen en la red, en donde todo se se podría copiar y reproducir sin necesidad de requerir al titular de los derechos sobre la obra autorización para subir esa obra a Internet.

Como lo he sostenido muchas veces [503], ello no es así, ya que los derechos de propiedad intelectual no son, como dicen algunos, un impuesto que limita el acceso

501 Convenio de Berna para la Protección de las Obras Literarias y Artísticas del 9 de septiembre de 1886, completado, revisado y enmendado en 1896, 1908, 1914, 1928, 1948, 1967, 1971

502 TODA sigla en español y WCT sigla en ingles y que corresponde a Tipo Copyright Treaty http://www.wipo.int/wipolex/es/treaties/text.jsp?file_id=29515

503 FERNANDEZ DELPECH, Horacio – Manual de los Derechos de autor. Editorial He-

a los bienes culturales, por el contrario son el mejor estímulo para la creación y para defender una justa retribución por la tarea realizada.

Para poder subir una obra intelectual, musical o audiovisual digitalizada a Internet es necesario contar con la autorización expresa del autor o del titular del derecho de propiedad intelectual sobre esa obra. De no ser así, esa subida a internet , se convierte en un accionar ilícito.

Aparece así como un mal de esta época la piratería digital en Internet. El usuario acepta la piratería como un modo normal de acceder a una obra, de forma más barata o gratuita, la mayoría de las veces sin tomar ni siquiera conciencia que tal acto es ilícito y puede generarle responsabilidad.

II. LICENCIAS INDIVIDUALES

Tradicionalmente la forma de retribuir a los autores por sus creaciones intelectuales, siempre fueron las licencias individuales. Estas licencias se instrumentaban a través de contratos de edición, en los cuales los autores cedían los derechos sobre una obra para ser publicada o editada, y los editores (editoriales, discográficas, empresas cinematográficas, etc.) se comprometían a que por la publicación o difusión de la obra le abonarían al autor derechos de autor, fijados generalmente en un porcentaje sobre el precio de venta de la obra.

En general las legislaciones han definido al contrato de edición, estableciendo que habrá contrato de edición cuando el titular del derecho de propiedad sobre una obra intelectual, se obliga a entregarla a un editor y éste a reproducirla, difundirla y venderla.

Normalmente el contrato de edición se refiere a la reproducción grafica de la obra, pero este contrato se aplica cualquiera sea la forma o sistema de reproducción o publicación.

De allí entonces que este contrato no solo se refiere a la edición grafica de la obra, sino que también puede darse con relación a la grabación sonora o a la fijación audiovisual, y en los últimos años la irrupción de las nuevas tecnologías de la información y la comunicación, han hecho que podamos encontrar también este contrato de edición vinculado con la reproducción digital, o sea la reproducción en formatos intangibles y con la subida de estos archivos digitales a la red Internet, que configura también una reproducción de la obra.

Podemos entonces hablar al menos de seis tipos de contratos de edición:

- Contrato de edición gráfic

liasta Buenos Aires, 2011

- Contrato de edición de obra musical
- Contrato de edición de obra audiovisual
- Contrato de edición digital
- contrato de edición para reproducir digitalmente una obra en Internet

Se ha discutido si el contrato de edición grafica, comprendía a la edición digital y a la subida de esa obra a Internet.

La jurisprudencia, en un comienzo contradictoria, se ha afirmado hoy en día en el criterio de que el editor que posee un contrato de edición grafica no puede digitalizar la obra y explotarla en formato electrónico o subirla a Internet sin la expresa autorización del autor.

La Corte Suprema de Estados Unidos en Sentencia del 25 de junio de 2001, expreso que, de no haberse cedido el derecho a reproducir la obra digitalmente, el editor no puede emprender por sí mismo ni autorizar a un tercero (licenciar) la explotación de tal obra en otros medios.

Convengamos entonces que tanto para poder digitalizar una obra como para poder subirla a Internet, es necesario poseer un contrato especifico con el titular de los derechos sobre esa obra.

Como antes dijera, la forma típica de esos contratos son las licencias individuales, en las cuales el titular del derecho de propiedad sobre una obra intelectual, se obliga a entregarla a un editor a fin de que este la digitalice y luego la reproduzca, difunda y venda a través de la red Internet.

III. NUEVOS MODELOS DE LICENCIAMIENTO DE DERECHOS COPYRIGHT Y COPYLEFT

Pero hoy en día esas licencias individuales se vuelven insuficientes frente al nuevo panorama en donde se distribuyen masivamente las obras en forma digital a través de Internet sin requerir previamente la correspondiente cesión de derechos por parte de su titular, llegando así estas a miles de usuarios que bajan las canciones, libros, etc. de Internet, sin pagar ningún derecho, y en donde obviamente esta conducta es ilícita y defrauda al autor.

Es por ello que aparecen en los últimos años nuevos modelos de licenciamiento de derechos digitales para internet.

En primer termino debemos precisar que existen entonces dos tipos de licenciamiento de derechos digitales que generalmente aparecen vinculados a los contenidos digitales: **Copyright y Copyleft.**

- **Copyright** significa que todos los derechos están reservados y que la obra

solo se puede utilizar, modifica , reproducir o distribuir, contando con el la autorización expresa del autor o del titular de los derechos de propiedad intelectual sobre esa obra. Se simbolizada este sistema con una C en un círculo y la leyenda: Todos los derechos reservados. Se requiere aquí la autorización expresa del autor y, en muchos casos, el pago por su uso. Cualquier contenido que encontremos en Internet que no especifique algún tipo de licencia, está automáticamente protegido por Copyright.

• **Copyleft,** se identifi a con la letra C invertida en un círculo. y es una alternativa a las restricciones de derechos que imponen las normas planteadas en el copyright.

Este tipo de licencia permite usar, reproducir y distribuir el contenido con la única condición de que se reconozca en el contrato o licencia la autoría del titular del derecho. Es el sistema opuesto al Copyright y no requiere autorización alguna, ni generalmente ningún pago pues deriva de una condición previa que es que el autor o el titular del derecho a sometido a la obra a este sistema. Dentro de este sistema encontramos fundamentalmente las licencias las licencias Creative Commons que han servido de base en los últimos tiempos para la producción de obras literarias, musicales y animadas.

Con relación a Creative Commons, se trata de una organización sin fines de lucro, que promueve la utilización legal de contenidos protegidos por derechos de autor, mediante las licencias Creative Commons. Estas licencias permiten al autor de una obra protegida por derechos de autor elegir de que manera dará a conocer su obra y cuales son las condiciones para su uso y reproducción, mediante modelos de contratos o de licenciamiento o licencias de derechos de autor creative commons, que ofrecen al autor titular de los derechos sobre una obra protegida, en una forma simple y estandarizada, otorgar permiso a los usuarios gratuitamente para usar y compartir la obra bajo los términos y condiciones que se establezcan en la licencia. En algunos casos poemos encontrar hoy en día convenios entre Creative Commons y entidades de gestión colectiva de derechos de autor.

Destaco que estas licencias tienen las siguiente características básicas, conforme se referencia en el propio sitio de esta empresa.

Atribución: En cualquier explotación de la obra autorizada por la licencia será necesario reconocer la autoría (obligatoria en todos los casos).

No Comercial : La explotación de la obra queda limitada a usos no comerciales.

Sin obras derivadas : La autorización para explotar la obra no incluye la posibilidad de crear una obra derivada.

Compartir Igual : La explotación autorizada incluye la creación de obras

derivadas siempre que mantengan la misma licencia al ser divulgadas.

IV. NUEVAS LICENCIAS DIGITALES. GESTIÓN COLECTIVA

Pero además de estos tipos de licenciamiento Copyright y Copyleft, podemos encontrar hoy en día encontrar también:

- nuevas licencias digitales por las cuales se ceden, o venden libros, archivos musicales, cinematográficos o de texto, para que sean colocados en sitios de Internet (Netflix, Spotify, Amazon, etc.), de donde el usuario los puede bajar pagando un importe dinerario;
- la gestión colectiva de derechos digitales.

En el caso de Netflix esta empresa proporciona a sus usuarios mediante una tarifa plana mensual un streaming de contenido multimedia. Para ello se asocia con proveedores de contenido para obtener los derechos de licencia de streaming de una gran variedad de series y películas.

Se las denomina licencias de derechos de transmisión.

El usuario que compra la obra paga, directamente o mediante una suscripción, una cantidad mínima, pero multiplicado por miles de usuarios se convierte en cantidades de dinero interesante con el cual el vendedor puede retribuir a los autores o recuperar lo abonado en caso de que haya adquirido previamente los derechos.

V. LA GESTIÓN COLECTIVA DE LOS DERECHOS DIGITALES

Existen ciertas formas de explotación de las obras intelectuales en las que se hace imposible, o muy difícil, el efectivo control y cobro de los derechos de autor por parte de los titulares de estos derechos.

Me refiero específicame te a la obra música o audiovisual transmitida por radio, televisión, en fiestas y locales, o la representación de obras, o el fotocopiado de libros.

Tradicionalmente surgen así entidades que representan a los autores y editores y perciben colectivamente los derechos de quien utilizan las obras reproduciéndolas.

Es así como las entidades de gestión colectiva, negocian tarifas y las condiciones de utilización con los usuarios, otorgándoles licencias y autorizaciones de uso, al mismo tiempo que perciben de estos regalías que luego distribuyen regalías, entre los titulares de derechos.

La OMPI en su documento Gestión colectiva del Derecho de autor y los derechos conexos ha definido a la gestión colectiva como: el ejercicio del derecho de autor y los

derechos conexos por intermedio de organizaciones que actúan en representación de los titulares de derechos, en defensa de sus intereses.

Esta gestión Colectiva llega hoy también al entorno digital donde la transmisión y reproducción de obras por intermedio de Internet, puede ser controlada ejercida por entidades especificas.

En estos casos es donde la gestión colectiva aparece como un medio efectivo de protección, control y cobro de los derechos de los autores, editores y titulares de derechos conexos.

En los sistemas de gestión colectiva los titulares de derechos de propiedad intelectual transfieren sus derechos a una sociedad de gestión colectiva local, o simplemente conceden a ésta una licencia no exclusiva para que los represente.

Desde ese momento la entidad de gestión colectiva actúa como representante autorizado por el autor, y en cumplimiento de tal función se encarga de autorizar a terceros la utilización de la obra. El tercero desde ese momento puede utilizar la obra abonando a la entidad los derechos correspondientes. El importe de estos derechos responde a una tarifa estándar de referencia publicada por la entidad o a un convenio entre la entidad y el usuario. Los importe recaudados se distribuyen entre los miembros de la entidad. Esta última tarea es posiblemente la mas dificil, pues requiere de un estudio de quienes son los titulares con derechos y en que medida y de que forma deben recibir las utilidades que se reparten. Las entidades de gestión colectiva representan y cobran derechos no solo de titulares de derechos nacionales, sino también con relación a titulares de derechos extranjeros. Por su parte otros países ejercen esa gestión colectiva con relación a titulares de derechos y obras argentinas. Se habla así del repertorio nacional o del repertorio internacional de estas entidades.

Es así como en muchos países existen entidades que tienen a su cargo la gestión colectiva de los derechos de propiedad intelectual sobre las copias digitales de obras literarias y artísticas. Tal el caso del Centro Español de Derechos Reprográficos CEDRO, en España [504] o del Centro de Administración de Derechos Reprográficos de Argentina CADRA y de la Sociedad Argentina de Autores y Compositores SADAIC, en la Argentina.

Como lo analizo en mi Manual de derechos de Autor, las entidades de gestión colectiva de derechos de propiedad intelectual, efectúan está tarea:

- en forma delegada por sus legítimos titulares (gestión colectiva voluntaria),

504 CEDRO se define como la asociación de autores y editores de libros, revistas, periódicos y partituras que en su nombre gestiona de forma colectiva los derechos de propiedad intelectual derivados de la fotocopias y la copia digital de sus obras (del sitio Web de CEDRO https://www.cedro.org/actualidad/cedro-informa)

• por mandato legal (gestión colectiva obligatoria), de acuerdo con la legislación vigente y a sus estatutos.

En el caso de las entidades de gestión colectiva voluntaria, es necesaria la existencia de una afilia ión o contrato con la entidad, por el cual el titular del derecho cede a esta última la administración de los derechos de percepción por la comunicación publica de las obras. Esta cesión no implica transferencia del derecho, sino solo un mandato para el ejercicio de ese derecho en cuanto a la administración y cobro de los derechos.

En el caso de las entidades de gestión colectiva obligatoria, la representatividad de los titulares de derechos no requiere acto alguno por parte de éstos, ya que tal representatividad resulta de una norma legal que establece la gestión colectiva de determinado sector y otorga la representatividad a alguna entidad en particular.

No puedo dejar de señalar que la Directiva del Parlamento Europeo y del Consejo sobre los derechos de autor en el mercado único digital, aprobada recientemente, reconoce a los editores de publicaciones de prensa el cobro de una remuneración justa y equitativa por el uso digital de sus publicaciones de prensa por proveedores de servicios de la sociedad de la información.

VI. LA COPIA PRIVADA Y LA RETRIBUCIÓN DE LOS EDITORES DE PUBLICACIONES DE PRENSA

Pero no puedo concluir este trabajo sin referirme a dos formas particulares de retribuir a los autores por la reproducción de sus obras. Me refiero a la copia privada y a la retribución a los editores de publicaciones de prensa por el uso o reproducción de sus obras por parte de los proveedores de servicio de la sociedad de la información.

El sistema de **copia privada** existe en gran parte de los países Europeos y en algunos otros países. En todos estos sistemas se permite la reproducción de una obra a la cual se ha tenido acceso legitimo, para su uso privado.

No nos olvidemos que cualquier reproducción de una obra , aun de una obra adquirida lícitamente, requiere la autorización de su autor para posteriormente poder reproducirla.

En los países en que rige el sistema de copia privada se admite la reproducción de una obra cumpliendo con las siguientes condiciones:

1. Que se trata de una obra a la que se ha tenido un acceso legitimo;
2. Que la reproducción sea para exclusivo uso del copista;
3. Que la copia no sea objeto de utilización colectiva ni lucrativa;
4. Que exista una compensación equitativa para el autor;

Con relación a la compensación equitativa a que da lugar la copia privada, generalmente la misma esta dada por un canon abonado por los fabricantes, importadores y distribuidores de dispositivo que puedan utilizarse para efectuar reproducción de obras.

En España el régimen de copia privada transito por varias etapas. La Ley de Propiedad Intelectual [505] establece que una persona física puede realizar una copia de una obra ya divulgada cuando sea para su exclusivo uso privado y sin fines comerciales. La contrapartida a este derecho obliga a establecer una vía para que los titulares de los derechos sobre la obra reproducida reciban una compensación equitativa. [506]

A tal fin desde1993 rigió el sistema conocido como «canon digital» que era abonado por las empresas que fabricaban y distribuían equipos, soportes y dispositivos que permitían la realización de copias privadas de obras protegidas.

El 30 de noviembre de 2011 el Gobierno dictó el Real Decreto-ley 20/2011, y suprimió de forma inesperada el sistema de compensación equitativa por copia privada, vigente desde 1993 en España.

Desde entonces La financiación de la compensación equitativa por copia privada estaba a cargo de una partida de los Presupuestos Generales del Estado de cada año. Sin embargo recientes decisiones judiciales han dejado sin efecto este sistema de financiación, y Mediante el **Real Decreto-ley 12/2017 en vigencia desde el 1 de agosto de 2017,**[507] se tiende a sustituir el actual sistema de compensación equitativa financiado con cargo a los Presupuestos Generales del Estado por un modelo basado

505 Real Decreto-ley 12/2017, de 3 de julio, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, en cuanto al sistema de compensación equitativa por copia privada. (BOE núm. 158, de 4 de julio de 2017) http://www.wipo.int/wipolex/es/details.jsp?id=17103

506 Ello deriva de la Directiva 2001/29/CE del Parlamento Europeo y del Consejo, de 22 de mayo de 2001, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información, enla cual el art 5 establece «Los Estados miembros podrán establecer excepciones o limitaciones al derecho de reproducción contemplado en el artículo 2 en los siguientes casos:

b) en relación con reproducciones en cualquier soporte efectuadas por una persona física para uso privado y sin fines directa o indirectamente comerciales, siempre que los titulares de los derechos reciban una compensación equitativa, teniendo en cuenta si se aplican o no a la obra o prestación de que se trate las medidas tecnológicas contempladas en el artículo 6;

507 Real Decreto-ley 12/2017, de 3 de julio, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, en cuanto al sistema de compensación equitativa por copia privada. (BOE núm. 158, de 4 de julio de 2017) http://www.wipo.int/wipolex/es/details.jsp?id=17103

en el pago de un importe a abonar por los fabricantes y distribuidores de equipos, aparatos y soportes de reproducción.

Con relación a **la retribución de los editores de publicaciones de prensa**, en el ámbito Europeo, la reciente Directiva del Parlamento Europeo y del Consejo sobre los derechos de autor en el mercado único digital, aprobada el 28 de Marzo de 2019, establece que los Estados miembros reconocerán a los a los editores de publicaciones de prensa derecho de autor directo sobre el uso en línea de sus publicaciones de prensa por parte de los proveedores de servicios de la sociedad de la información, durante el termino de 20 años. De esta forma se establece que los editores de prensa tendrán derecho a recibir una remuneración "justa y adecuada" por el uso digital de sus obras por parte de los proveedores de servicios, respetándose los derechos en favor de los autores y otros titulares de derechos.

CONCLUSIÓN

Hemos visto como continúan totalmente vigentes los derechos de los autores de obras por la reproducción y por la reproducción digital de sus obras.

A las forma clásicas y tradicionales de retribución por autorizar la reproducción de sus obras, se han ido agregando con el tiempo nuevas formas, como la gestión colectiva de los derechos digitales, la copia privada e incluso no hace mucho se ha legislado a nivel europeo la retribución a los editores de prensa por el uso digital de sus obras por parte de los proveedores de servicios de la sociedad de la información.

BIBLIOGRAFIA

ARRABAL, Pablo - Manual práctico de propiedad intelectual e industrial, Ediciones Gestión, España, 1991.

COLOMBET, Claude - Grandes principios del derecho de autor y los derechos conexos en el mundo: estudio de derecho comparado, Ediciones UNESCO/CINDOC, Madrid, 1997.

CORREA, Carlos M. - Derechos de propiedad intelectual competencia y protección del interés público, Editorial B de F, Buenos Aires, 2009.

DELLA COSTA, Hector - Derecho de Autor y su novedad, Fundación Editorial de Belgrano, Buenos Aires, 2006.

EMERY, Miguel Angel - Propiedad Intelectual, Ley 11723 Comentada, anotada y

concordada con los tratados internacionales, Editorial Astrea, Buenos Aires, 1999.

FERNANDEZ BALLESTEROS, Carlos A. - Marco Jurídico Internacional del Derecho de Autor y de los Derechos Conexos. De Berna (1886) a los Tratados de la OMPI (1996) , Documento Desarrollado en la II Jornada de Derecho de Autor en el Mundo Editorial, Buenos Aires, 28 y 29 de Abril de 2004. (Inédito).

FERNANDEZ DELPECH, Horacio - Protección Jurídica del Software, Editorial Abeledo-Perrot, Buenos Aires, 2000.

FERNANDEZ DELPECH, Horacio - Internet: Su Problemática Jurídica, Editorial Lexis Nexis, Buenos Aires, 2004.

FERNANDEZ DELPECH, Horacio . Manual de los Derechos de autor. Editorial Heliasta Buenos Aires, 2011

FERNANDEZ DELPECH, Horacio - Nueva Directiva de la Unión Europea sobre Conservación de Datos de Tráfico, Revista de Contratación Electrónica, Nº 68, Editora de Publicaciones Científicas y rofesionales, Madrid, Febrero 2006.

FERNANDEZ DELPECH, Horacio – La reproducción de las obras intelectuales por los usuarios de Internet en la doctrina, en la legislación iberoamericana y a la luz de los últimos documentos internacionales, Número Especial de Jurisprudencia Argentina - LexisNexis, Buenos Aires, 25 de febrero de 2004.

FERNANDEZ DELPECH, Horacio - Medidas Tecnológicas de protección de la Propiedad Intelectual, los actos elusivos, la protección jurídica contra la elusión, Revista Electrónica del Centro Colombiano del Derecho de Autor

FERNANDEZ NUÑEZ, Javier - Derechos Intelectuales, Ley 11723 y su Reglamentación Comentada y Anotada, Editorial Lexis Nexis, Buenos Aires, 2004.

GARROTE FERNANDEZ, Ignacio - El derecho de autor en internet: los tratados de la OMPI de 1996 y la incorporación al derecho español de la directiva 2001/29/CE, Editorial Comares, Granada, 2003.

GARROTE FERNANDEZ, Ignacio - La reforma de la copia privada en la Ley de propiedad intelectual, Editorial Comares, Granada, 2005.

IGLESIAS PRADA, José Luis - Los derechos de propiedad intelectual en la Organización Mundial del Comercio (OMC) : el acuerdo sobre los aspectos de los

derechos de propiedad intelectual relacionados con el comercio, Centro de Estudios para el Fomento de la Investigación, España 1997.

ITHURRALDE, María Pía – La expresión del autor como único objeto de protección, LL 27.11.2009.

LIPSZYC, Delia - Derechos de autor y derechos conexos – Ediciones Unesco-Cerlac-Zavalia, Buenos Aires, 2007.

LIPSZYC, Delia – El derecho de autor y los derechos conexos en el acuerdo sobre los ADPIC (o TRIPs), LL, 1996-E-1395.

LIPSZYC, Delia – Nuevos temas de derecho de autor y derechos conexos, Editorial Zavalia, Buenos Aires, 2004.

MOUCHET, Carlos – Los Derechos de los Autores e Intérpretes de Obras Literarias y Artísticas, Monografías Jurídicas, Abeledo Perrot , Buenos Aires, 1966.

NUÑEZ, Javier F. - *DERECHOS INTELECTUALES. LEY 11723 Y SU REGLAMENTACIÓN, Abeledo Perrot, Buenos Aires, 2004.*

PALAZZI, Pablo A. - La exclusión del régimen de Derecho de Autor de las ideas, sistemas, métodos, aplicaciones practicas y planes de comercialización, Documento Nº 6, Centro de Tecnología y Sociedad, Universidad de San Andrés, (Inédito).

NOVA LEI DE PROTEÇÃO DE DADOS PESSOAIS E GDPR

UMA ANÁLISE DO DIREITO AO ESQUECIMENTO NO DIREITO BRASILEIRO

Eixo Tematico: Proteção de Dados Pessoais

Autores:
Antonio Carlos Efin
Doutor em Direito das Relações Sociais pela PUC/SP; Professor titular da Pontifícia Universidade Católica do Paraná - PUCPR, onde leciona na graduação, especializações, mestrado e doutorado; Professor da Escola da Magistratura do Paraná; membro do Instituto dos Advogados do Paraná; Advogado militante em Curitiba/PR. Presidente da Comissão de Direito do Consumidor da OABPR. Membro Consultor da Comissão Especial de Defesa do Consumidor, Conselho Federal da OAB. E-mail: ace@eradv.com.br

Eduarda Alencar Maluf Kiame
Pós-graduanda em Direitos Humanos e Questão Social pela PUCPR. Graduada (PUCPR 2019). Advogada. Eduarda_kiame@hotmail.com

Palavras Chave: Direito ao Esquecimento, Direitos da Personalidade, Tutela dos dados pessoais, Direito à privacidade

RESUMO
O Direito ao Esquecimento tem como finalidade impedir que um fato, mesmo que verídico, ocorrido em momento pretérito, tenha exposição em público por tempo prolongado, causando sofrimento ou transtornos. O direito ao esquecimento fundamenta-se na dignidade da pessoa humana e na cláusula geral de proteção e promoção da personalidade em suas múltiplas dimensões, há a necessidade de ponderar princípios constitucionais, como a liberdade de expressão e o direito à informação. O desenvolvimento tecnológico viabiliza a coleta, o armazenamento e a associação de informações pessoais dos usuários da internet, que são armazenados por tempo indeterminado e seu uso pode ser nocivo, existindo a necessidade de se desenvolver um controle para o armazenamento e utilização das informações pessoais. As fontes da pesquisa foram doutrinas, artigos e jurisprudências brasileiras. A pesquisa jurisprudencial fixou-se nas decisões do Supremo Tribunal de Justiça e do Supremo Tribunal Federal. É fundamental ressaltar que investir em tecnologias da informação e comunicação perpassa pela segurança da informação, inclusive no que tange à proteção de dados e à privacidade. O Estado, como garantidor de direitos dos indivíduos interviu para a garantia e defesa dos direitos fundamentais de seus cidadãos, com a promulgação da Lei nº 13.709/2018 que passou regulamentar o tratamento dos dados pessoais na *Internet*. Haja vista que a lei é bem recente, ainda não há o que se falar em eficácia ou não da proteção dos direitos dos proprietários dos dados que circulam pela rede, o que se espera é a adequação de todos os sistemas até a data prevista na legislação para que haja maior tutela em relação aos dados.

ABSTRACT
The Right To Be Forgotten is intended to prevent a fact, even if true, occurring in the past, from being exposed in public for a long time, causing suffering or inconvenience. The right to oblivion is based on the dignity of the human person and on the general clause of protection and promotion of personality in its multiple dimensions, there is a need to consider constitutional principles, such as freedom of

expression and the right to information. Technological development enables the collection, storage and association of personal information of Internet users, which are stored indefinitely and their use may be harmful, and there is a need to develop a control for the storage and use of personal information. The sources of the research were Brazilian doctrines, articles and jurisprudence. The jurisprudential research was fixed in the decisions of the Supreme Court of Justice and the Federal Supreme Court. It is important to emphasize that investing in information and communication technologies runs through the security of information, including data protection and privacy. The State, as guarantor of individuals' rights, intervened to guarantee and defend the fundamental rights of its citizens, with the enactment of Law 13709/2018, which regulated the treatment of personal data on the Internet. Considering the law is very recent, there is nothing to speak about whether or not to protect the rights of data owners circulating on the network, which is expected to be the adequacy of all systems by the date provided in the legislation so that there is greater protection over the data.

INTRODUÇÃO

O presente artigo tem como objetivo principal a demonstração da aplicação do direito ao esquecimento no Direito Brasileiro. A modernidade líquida, assim chamada por Bauman (2013), tem como um de seus danos colaterais a progressiva eliminação da antes delimitada esfera do espaço público e do espaço privado, ressaltando também que, na atual sociedade de hiperinformação, há inúmeros riscos à privacidade e à autonomia individual.

Diante da imprecisão entre a esfera pública e privada atualmente, o direito ao esquecimento tem como finalidade impedir que um fato, ocorrido em momento passado, mesmo que verídico, tenha exposição em público por tempo prolongado, causando transtornos e sofrimento. Há também a necessidade de ponderar o direito ao esquecimento com princípios constitucionais, como a o direito à informação e a liberdade de expressão.[508]

O desenvolvimento tecnológico viabiliza a coleta, o armazenamento e a associação de informações pessoais dos usuários da internet por meio de cadastros diversos como em redes sociais, sites de busca e compra; facilitando também o acesso a estes bancos, que podem ser armazenados e reinseridos na Internet, com o fundamento da livre manifestação do pensamento e também da liberdade de expressão. Os dados coletados são armazenados por tempo indeterminado e o uso destas informações pode ser nocivo, existindo a necessidade de se desenvolver um controle para o armazenamento e utilização das informações pessoais.[509]

Ressalta-se que os bancos de dados podem gerar prejuízos patrimoniais e morais ao consumidor, tornando-se a evidente redução da esfera protegida da intimidade; pois as informações pessoais dos consumidores têm valor às empresas, deste modo,

508 JORGE, Maykon Cristiano; IOCOHAMA, Celso Hiroshi. A tutela inibitória como meio de efetivação do direito ao esquecimento e proteção da dignidade da pessoa humana. *Revista Brasileira de Direito Processual – RBDPro*, Belo Horizonte, ano 24, n. 95, p.203-226, jul./set.2016.

509 LIMA, Cíntia Rosa Pereira de. Direito ao Esquecimento e internet: o Fundamento Legal no Direito Comunitário Europeu, no Direito Italiano e no Direito Brasileiro. *Doutrinas Essenciais de Direito Constitucional*. Vol. 8/2015, p.511-543.

traduz-se o direito ao esquecimento no direito a ser deixado em paz aplicado às relações de consumo.[510]

A proteção de dados pessoais é realizada na medida em que se tutela a pessoa limitando o tratamento das informações que lhe digam respeito. No contexto atual, uma atuação demorada no controle de determinada informação de certa pessoa que circula na internet pode ser irremediável.[511]

Assim sendo, o direito ao esquecimento é considerado um direito fundamental implícito, deduzido de outras normas, como a dignidade da pessoa humana, a cláusula geral de proteção e promoção da personalidade em suas múltiplas dimensões; e também de direitos fundamentais mais específicos, como é o caso da tutela da privacidade, da honra, do nome e da imagem.[512]

O DIREITO AO ESQUECIMENTO E O DIREITO À INFORMAÇÃO E À LIBERDADE DE EXPRESSÃO

O direito ao esquecimento tem como finalidade principal impedir que um fato, mesmo que verídico, ocorrido em momento pretérito, tenha exposição em público por tempo demasiadamente prolongado, acarretando em sofrimento ou transtornos; objetivando-se defender o ser humano da irresponsabilidade do exercício ao direito de informação. Nesta seara, surge a necessidade de ponderar o direito ao esquecimento com princípios constitucionais, como a liberdade de expressão e o direito à informação.[513]

Os critérios do consentimento, da eticidade e do interesse público orientam a identificação da licitude no tratamento e exposição da imagem alheia, com fulcro na existência de um núcleo indevassável de segredo pessoal que deve ser preservado. Caso esse referido núcleo privado não fosse admitido, a vida em sociedade significaria a renúncia de todo o espectro de humanidade do indivíduo, inclusive dentro da sua esfera mais íntima.[514]

Ainda que o direito à informação seja protegido no art. 5°, XIV, da Constituição: "é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando

510 RAMOS, André de Carvalho. Direito ao Esquecimento e o Controle Indireto dos Bancos de Dados de Consumo. *Revista de Direito do Consumidor*. Vol 104/2016, p. 131-147, Mar- Abr/ 2016.

511 LIMA, Cíntia Rosa Pereira de. Direito ao Esquecimento e internet: o Fundamento Legal no Direito Comunitário Europeu, no Direito Italiano e no Direito Brasileiro. *Doutrinas Essenciais de Direito Constitucional*. Vol. 8/2015, p.511-543.

512 SARLET, Ingo. Tema da Moda, Direito ao Esquecimento é anterior à internet. Disponível em: <http://www.conjur.com.br/2015-mai-22/direitos-fundamentais-tema-moda-direito-esquecimento-anterior-internet >. Acesso em 17 junho. 2019.

513 JORGE, Maykon Cristiano; IOCOHAMA, Celso Hiroshi. A tutela inibitória como meio de efetivação do direito ao esquecimento e proteção da dignidade da pessoa humana. *Revista Brasileira de Direito Processual – RBDPro*, Belo Horizonte, ano 24, n. 95, p.203-226, jul./set.2016

514 MARTINS, Sérgio Ludovico. Critérios para identificação do núcleo indevassável do direito de imagem, partindo da análise de recentes decisões judiciais. *Revista de Direito Privado*, vol. 74/2017, p. 93-115, fev. 2017.

necessário ao exercício profissional". (BRASIL, 1998). É importante ressaltar que há limites para o exercício e conteúdo do direito à informação, não podendo gerar um prejuízo pessoal desproporcional e tratamento degradante ao indivíduo.[515]

Os direitos individuais relativos à intimidade e à vida privada também estão previstos em diversos dispositivos constitucionais. O art. 5°, X, integrando todos os direitos em um único articulado, prevê que *"são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação"* (BRASIL, 1998).

A atual era da informação permite moldar uma esfera da vida privada do indivíduo mais complexa, porém também mais frágil, acarretando a consequente necessidade de maior proteção, o que contrasta com a demanda atual de cada vez maior de acesso à informação. (RODOTÁ, 2018) Assim sendo, o direito ao esquecimento como um direito autônomo de personalidade através do qual o indivíduo pode excluir ou deletar as informações a seu respeito quando se tenha passado um período de tempo desde a sua coleta e utilização e, contanto que não tenham mais utilidade ou não interfiram no direito de expressão, científica, artística, literária ou jornalística [516]

O DIREITO AO ESQUECIMENTO: ANÁLISE LEGISLATIVA

Embora não esteja expressamente previsto na Constituição Federal, o direito ao esquecimento é um direito fundamental implícito, deduzido de outras normas, sejam princípios gerais e estruturantes, como é o caso da dignidade da pessoa humana, seja de direitos fundamentais mais específicos, como é o caso da privacidade, honra, imagem, nome, entre outros.[517] Destaca-se no texto constitucional, previsões nessa perspectiva: a proteção da dignidade da pessoa humana (artigo 1º, inciso III), a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas (artigo 5º, inciso inciso XI), inviolabilidade da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas (artigo 5º, inciso XII). (BRASIL, 1998)

No Brasil, as questões comerciais referentes aos dados pessoais só foram previstas com o Código de Defesa do Consumidor, que disciplinou, em seu art. 43, o direito dos consumidores ao acesso de suas próprias informações registradas nos cadastros das empresas. (BRASIL, 1990) Posteriormente, com a promulgação do Marco Civil

515 RULLI JÚNIOR, Antônio. RULLI NETO, Antônio. Direito ao esquecimento e o superinformacionismo: apontamentos no direito brasileiro dentro do contexto de sociedade da informação. *RIDB – Revista do Instituto do Direito Brasileiro*, Lisboa, ano 1, n. 1, p. 419-434, jul/dez. 2012.

516 LIMA, Cíntia Rosa Pereira de. Direito ao Esquecimento e internet: o Fundamento Legal no Direito Comunitário Europeu, no Direito Italiano e no Direito Brasileiro. *Doutrinas Essenciais de Direito Constitucional*. Vol. 8/2015, p.511-543.

517 SARLET, Ingo. Tema da Moda, Direito ao Esquecimento é anterior à internet. *Consultor Jurídico*. Disponível em: <http://www.conjur.com.br/2015-mai-22/direitos-fundamentais-tema-moda--direito-esquecimento-anterior-internet >. Acesso em 17 junho. 2019

da *Internet* que é considerado um avanço no que tange à proteção de dados pessoais; sendo a primeira lei infraconstitucional a regular a proteção de dados e prevêr a possibilidade de indenização quando ocorrer lesão em solo brasileiro. Entretanto, a sua eficácia é limitada, pois seu alcance restringe-se à jurisdição brasileira e à *internet*; não protegendo o usuário que se encontra fora da rede ou quando a lesão parta de território estrangeiro.[518]

No que tange à tutela do direito à privacidade, há o enunciado da V Jornada de Direito Civil promovido pelo Conselho da Justiça Federal/STJ, o Enunciado 404 (BRASIL) que ensina que:

> A tutela da privacidade da pessoa humana compreende os controles espacial, contextual e temporal dos próprios dados, sendo necessário seu expresso consentimento para tratamento de informações que versem especialmente o estado de saúde, a condição sexual, a origem racial ou étnica, as convicções religiosas, filosóficas e política

No mesmo sentido da jornada anterior, há o Enunciado 531 da VI Jornada de Direito Civil, (BRASIL) que trata expressamente do direito ao esquecimento:

> Os danos provocados pelas novas tecnologias de informação vêm-se acumulando nos dias atuais. O direito ao esquecimento tem sua origem histórica no campo das condenações criminais. Surge como parcela importante do direito do ex-detento à ressocialização. Não atribui a ninguém o direito de apagar fatos ou reescrever a própria história, mas apenas assegura a possibilidade de discutir o uso que é dado aos fatos pretéritos, mais especificame - te o modo e a finalidade com que são lembrados

Embora os enunciados sejam relevantes para promover o debate acerca do tema, o problema destes é que são muito vagos e não vinculantes. [519] Há ainda o Decreto nº 8.771/16 que regulamenta o Marco Civil da Internet e adota um grau de segurança e sigilo dos dados pessoais definindo diretrizes para padrões de segurança. Porém, o referido Decreto limita-se ao ciberespaço, não abrangendo totalmente os espaços onde circulam os dados pessoais.[520]

---

518 RUARO, Regina Linden; SOUZA, Fernando Inglez de. Cenários de regulação da proteção de dados pessoais e os desafios de uma tutela efetiva no ordenamento jurídico brasileiro: a internet e suas implicações na privacidade e na proteção de dados pessoais. *Interesse Público – IP*, Belo Horizonte, ano 19, n. 103, maio/jun. 2017. Disponível em: <http://www.bidforum.com.br/PDI0006.aspx?pdiCntd=247799>. Acesso em: 27 jun. 2018.

519 LIMA, Cíntia Rosa Pereira de. Direito ao Esquecimento e internet: o Fundamento Legal no Direito Comunitário Europeu, no Direito Italiano e no Direito Brasileiro. *Doutrinas Essenciais de Direito Constitucional*. Vol. 8/2015, p.511-543.

520 RUARO, Regina Linden; SOUZA, Fernando Inglez de. Cenários de regulação da proteção de dados pessoais e os desafios de uma tutela efetiva no ordenamento jurídico brasileiro: a internet e suas implicações na privacidade e na proteção de dados pessoais. *Interesse Público – IP*, Belo Horizonte, ano 19, n. 103, maio/jun. 2017. Disponível em: <http://www.bidforum.com.br/PDI0006.aspx?pdiCntd=247799>. Acesso em: 25 jun. 2019.

No intuito de promover e oferecer maior proteção aos dados e a sua própria soberania, o Brasil instituiu no dia 14 de agosto de 2018 a Lei n° 13.709/2018, inspirada no Regulamento Geral de Proteção de Dados da União Europeia e seguindo a modelagem europeia, que passa regulamentar o uso, a proteção e a transferência de dados pessoais. O referido dispositivo passou a garantir maior controle dos cidadãos sobre suas informações pessoais e a exigir que o Poder Público e a iniciativa privada obtenham consentimento explícito para coleta e uso dos dados.

A JURISPRUDÊNCIA BRASILEIRA NO ÂMBITO DO DIREITO AO ESQUECIMENTO

No que tange às decisões jurisprudenciais no Brasil, o caso Chacina da Candelária do Recurso Especial de n° 1.334.097 RJ (BRASIL, 2012), julgado em 2013, diante do debate liberdade de imprensa *vs.* direito da personalidade, foi reconhecido o direito ao esquecimento de um acusado absolvido na participação de um grave crime ocorrido no Rio de Janeiro, condenando por dano moral um veículo de comunicação social. O direito ao esquecimento dos condenados que cumpriram integralmente a pena e dos que foram absolvidos em processo criminal foi reconhecido, pois este, além de sinalizar que esta é uma evolução cultural da sociedade, confere concretude a um ordenamento jurídico que prioriza o direito à esperança, em absoluta sintonia com a presunção legal e constitucional de regenerabilidade da pessoa humana.

Por outro lado, em outro caso conhecido, o Recurso Especial n°1.593.873 a 3° Turma do Supremo Tribunal de Justiça (BRASIL, 2016a) decidiu por não existir fundamento normativo para imputar aos provedores de busca a obrigação de implementar o direito ao esquecimento. Também em outro caso notório, o caso Aida Curi, (BRASIL, 2016b) no qual a jovem de 18 anos foi brutalmente assassinada há 60 anos, prevaleceu o entendimento de que há valor jornalístico e histórico na reportagem, cujo formato não consubstanciaria abuso de direito, segue o teor:

> Tese de Repercussão Geral – Tema 786: Não é possível, com base no denominado direito a esquecimento, ainda não reconhecido ou demarcado no âmbito civil por norma alguma do ordenamento jurídico brasileiro, limitar o direito fundamental à liberdade de expressão por censura ou exigência de autorização prévia. Tampouco existe direito subjetivo a indenização pela só lembrança de fatos pretéritos

É possível perceber que as decisões no direito pátrio são pouco previsíveis e o conteúdo ainda não é pacificado entre as cortes superiores, dando margem a diversas interpretações diferentes e decisões contraditórios. A construção legal existente, em especial a constitucional ao garantir o direito à vida privada e à intimidade é muito

ampla, e suas lacunas dão margem à fragilização de liberdades civis, gerando grande insegurança jurídica nessa área;[521] como é possível notar pelos julgados acima.

CONSIDERAÇÕES FINAIS

Na era da sociedade da informação, torna-se cada vez mais difícil distinguir quais informações pessoais o indivíduo estaria realmente disposto a compartilhar, principalmente levando em consideração que até as informações aparentemente mais singelas podem, uma vez integradas a outras, provocar dano ao interessado. A privacidade no contexto da sociedade pós-moderna, deve ser analisada de uma forma a atender os paradoxos do seu tempo. Atualmente, na era da informação permite-se moldar uma esfera privada mais rica, porém mais frágil, acarretando na necessidade de maior proteção. O aumento do controle contrasta com demanda cada vez maior de acesso à informação. (RODOTÁ, 2008)

Fato é que mesmo quando os consumidores não pagam diretamente aos provedores de conteúdo, sabe-se que a sua visitação e exposição à publicidade configura fonte de receita para os *sites*, sendo possível inferir que há, portanto, uma relação de consumo.[522] No âmbito da sociedade da informação, a proteção dos dados pessoais difere-se da visão tradicional do direito à privacidade. Portanto, ainda que se considere a *Internet* um espaço público, sem um dono específico, não é possível se admitir como legítima a divulgação de dados, mensagens ou demais informações particulares a terceiros não autorizados.[523]

Na esfera da proteção da privacidade, um dos maiores desafios atuais é a segurança dos usuários da internet e os meios empregados para efetivá-la. A *internet* e suas diversas facetas transcendem às noções de jurisdição e território, também dentro do contexto de proteger a privacidade de informações, é preciso estabelecer regras o tanto quanto possível precisas de veiculação de dados pessoais por meio da *Internet*, haja vista que seu acesso é franqueado a todo o mundo, e, por diversas vezes, o seu autor não é descoberto. O ambiente virtual carece de uma regulação que o atinja por completo, ademais o próprio anonimato na rede também surja como empecilho a uma

521 RUARO, Regina Linden; SOUZA, Fernando Inglez de. Cenários de regulação da proteção de dados pessoais e os desafios de uma tutela efetiva no ordenamento jurídico brasileiro: a internet e suas implicações na privacidade e na proteção de dados pessoais. *Interesse Público – IP*, Belo Horizonte, ano 19, n. 103, maio/jun. 2017. Disponível em: <http://www.bidforum.com.br/PDI0006.aspx?pdiCntd=247799>. Acesso em: 25 jun. 2019.

522 VERONESE, Alexandre. MELO, Noemy. A Proposta Brasileira de Proteção de Dados Pessoais em Comparação ao Novo Regulamento Europeu. *Revista de Direito Civil Contemporâneo* | vol. 14/2018 | p. 71 - 99 | Jan - Mar / 2018 DTR\2018\10349

523 CARVALHO, Ana Paula Gambogi. O Consumidor e o Direito à Autodeterminação Informacional: considerações sobre os bancos de dados eletrônicos. *Doutrinas Essenciais de Responsabilidade Civil*. Vol.8, p. 343-392, Out/2011.

tutela dos dados pessoais e da privacidade, pois a impossibilidade de identificação do usuário serve como incentivo a ilícitos cibernéticos diante da ideia de impunidade.[524]

A necessidade de proteção se faz cada vez mais presente na medida em que o amplo desenvolvimento tecnológico, em especial no ambiente virtual, como a *Internet*, permite troca constante de inúmeras informações. A ciência jurídica, como é de sua característica legislativa, apresenta enorme dificuldade em acompanhar referida evolução, principalmente diante da rapidez das mudanças.[525] É fundamental ressaltar que investir em tecnologias da informação e comunicação perpassa pela segurança da informação, inclusive no que tange à proteção de dados e à privacidade. Assim sendo, o Estado, enquanto garantidor de direitos dos indivíduos, deve intervir para a garantia e defesa dos direitos fundamentais de seus cidadãos.[526]

A despeito do avanço tecnológico e das facilidades da vida moderna, não se pode admitir o uso desenfreado de informações sigilosas, ou que, ao menos, deveriam receber este tratamento, com o único fim de captação de consumidores, aferição de lucros ou prospecção de clientes. A rede mundial de computadores, ao mesmo tempo em que trouxe infinidade de novas possibilidades, exigiu do Estado atuação mais contundente, com vista a evitar o uso indevido, ou para fins ilícitos, dos dados pessoais disponibilizados na rede. O direito à proteção de dados não se limita à proteção a personalidade humana. A proteção de dados visa permitir gama maior de relações ou, de outra parte, evitar que se criem barreiras para a fruição de todos os direitos e garantias, sendo fonte de fomento para igualdade social.[527]

O cidadão brasileiro fica à mercê de uma constante violação de sua privacidade e de seus dados pessoais e também prejuízo de cunho extrapatrimonial. A ausência de um controle preventivo nesta ceara, em especial a inexistência de uma autoridade reguladora, fiscalizador e sancionadora em proteção de dados pessoais, encoraja práticas abusivas. Na lógica atual de que informação é poder, inclusive sobre pessoas.[528]

---

524 RUARO, Regina Linden; SOUZA, Fernando Inglez de. Cenários de regulação da proteção de dados pessoais e os desafios de uma tutela efetiva no ordenamento jurídico brasileiro: a internet e suas implicações na privacidade e na proteção de dados pessoais. *Interesse Público – IP*, Belo Horizonte, ano 19, n. 103, maio/jun. 2017. Disponível em: <http://www.bidforum.com.br/PDI0006.aspx?pdiCntd=247799>. Acesso em: 24 jun. 2019.

525 *Idem*

526 RUARO, Regina Linden; SOUZA, Fernando Inglez de. Cenários de regulação da proteção de dados pessoais e os desafios de uma tutela efetiva no ordenamento jurídico brasileiro: a internet e suas implicações na privacidade e na proteção de dados pessoais. *Interesse Público – IP*, Belo Horizonte, ano 19, n. 103, maio/jun. 2017. Disponível em: <http://www.bidforum.com.br/PDI0006.aspx?pdiCntd=247799>. Acesso em: 24 jun. 2019.

527 ROTUNDO, Rafael Pinheiro. *Proteção de Dados*. Revista de Direito Privado | vol. 74/2017 | p. 133 - 158 | Fev / 2017 | DTR\2017\80.

528 RUARO, Regina Linden; SOUZA, Fernando Inglez de. Cenários de regulação da proteção de dados pessoais e os desafios de uma tutela efetiva no ordenamento jurídico brasileiro: a internet e suas implicações na privacidade e na proteção de dados pessoais. *Interesse Público – IP*, Belo Horizonte, ano 19, n. 103, maio/jun. 2017. Disponível em: <http://www.bidforum.com.br/PDI0006.aspx?pdiCntd=247799>. Acesso em: 24 jun. 2019.

A promulgação da Lei Geral da Proteção de Dados Pessoas surgiu no Brasil representando um grande avanço na tutela jurídica dos indivíduos em relação a sua intimidade e privacidade, direitos assegurados constitucionalmente. A Lei de Proteção de Dados Pessoais – Lei n° 13.709/2018 –, que passa regulamentar o uso, a proteção e a transferência de dados pessoais, obriga os detentores dos dados a oferecer ao usuário de opções para visualizar, corrigir e excluir os seus dados constantes na rede. Nota-se que a legislação brasileira se inspirou em muito na legislação europeia acerca do tema, até mesmo na previsão de um órgão regulador, a Autoridade Nacional de Proteção de Dados (ANPD) – que ainda não existe no Brasil.

Na era da sociedade da informação, é cada vez mais difícil distinguir quais informações pessoais o indivíduo estaria realmente disposto a compartilhar, principalmente levando em consideração que até as informações aparentemente mais singelas podem, uma vez integradas a outras, provocar dano ao interessado. Na era da informação permite-se moldar uma esfera privada mais rica, porém mais frágil, acarretando na necessidade de maior proteção. Desse modo, o aumento do controle contrasta com demanda cada vez maior de acesso à informação. (RODOTÁ, 2008)

No âmbito da sociedade da informação, a proteção dos dados pessoais difere-se da visão tradicional do direito à privacidade. Portanto, ainda que se considere a *Internet* um espaço público, sem um dono específico, não é possível se admitir como legítima a divulgação de dados, mensagens ou demais informações particulares a terceiros não autorizados.[529]

Na esfera da proteção da privacidade, um dos maiores desafios atuais é a segurança dos usuários da internet e os meios empregados para efetivá-la. A *internet* e suas diversas facetas transcendem às noções de jurisdição e território, também é preciso estabelecer regras o tanto quanto possível precisas de veiculação de dados pessoais por meio da *Internet*, haja vista que seu acesso é franqueado a todo o mundo, e, por diversas vezes, o seu autor não é descoberto. O ambiente virtual carece de uma regulação que o atinja por completo, ademais o próprio anonimato na rede também surja como empecilho a uma tutela dos dados pessoais e da privacidade, pois a impossibilidade de identific ção do usuário serve como incentivo a ilícitos cibernéticos diante da ideia de impunidade.[530]

A despeito do avanço tecnológico e das facilidades da vida moderna, não se pode admitir o uso desenfreado de informações sigilosas, ou que, ao menos,

529 CARVALHO, Ana Paula Gambogi. O Consumidor e o Direito à Autodeterminação Informacional: considerações sobre os bancos de dados eletrônicos. *Doutrinas Essenciais de Responsabilidade Civil*. Vol.8, p. 343-392, Out/2011.

530 RUARO, Regina Linden; SOUZA, Fernando Inglez de. Cenários de regulação da proteção de dados pessoais e os desafios de uma tutela efetiva no ordenamento jurídico brasileiro: a internet e suas implicações na privacidade e na proteção de dados pessoais. *Interesse Público – IP*, Belo Horizonte, ano 19, n. 103, maio/jun. 2017. Disponível em: <http://www.bidforum.com.br/PDI0006.aspx?pdiCntd=247799>. Acesso em: 25 jun. 2019.

deveriam receber este tratamento, com o único fim de captação de consumidores, aferição de lucros ou prospecção de clientes. A rede mundial de computadores, ao mesmo tempo em que trouxe infinidade de novas possibilidades, exigiu do Estado atuação mais contundente, com vista a evitar o uso indevido, ou para fins ilícitos, dos dados pessoais disponibilizados na rede. A proteção de dados visa permitir gama maior de relações ou, de outra parte, evitar que se criem barreiras para a fruição de todos os direitos e garantias, sendo fonte de fomento para igualdade social.[531]

A necessidade de proteção se faz cada vez mais presente na medida em que o amplo desenvolvimento tecnológico, em especial no ambiente virtual, como a *Internet*, permite troca constante de inúmeras informações. A ciência jurídica, como é de sua característica legislativa, apresenta enorme dificuldade em acompanhar referida evolução, principalmente diante da rapidez das mudanças.[532]

É fundamental ressaltar que investir em tecnologias da informação e comunicação perpassa pela segurança da informação, inclusive no que tange à proteção de dados e à privacidade. Assim sendo, o Estado, como garantidor de direitos dos indivíduos interviu para a garantia e defesa dos direitos fundamentais de seus cidadãos, com a promulgação da Lei nº 13.709/2018 que passou regulamentar o tratamento dos dados pessoais na *Internet*. Haja vista que a lei é bem recente, ainda não há o que se falar em eficácia ou não da proteção dos direitos dos proprietários dos dados que circulam pela rede, o que se espera é a adequação de todos os sistemas até a data prevista na legislação para que haja maior tutela em relação aos dados.

Referências

BRASIL. **ACÓRDÃO PROCESSO C-131/12.** < http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=556072> cesso em: 23.jun.2019.

BRASIL. **Código de Defesa do Consumidor**. Lei 8.078 de 11 de Setembro de 1990. Brasília, Senado Federal, 1990. Disponível em <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm > Acesso em: 11 jun. 2019.

BRASIL. Constituição Federal (1988). **Constituição da República Federativa do Brasil**. Brasília, DF, Senado Federal, 1998. Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm > Acesso em 26 junho.2019.

BRASIL. **RECURSO ESPECIAL DE N° 1.334.097-2012 RJ**. Acesso em: <https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=31006510&num_registro=201201449107&data=20130910&tipo=5&formato=PDF > em 20.jun.2019.

531 ROTUNDO, Rafael Pinheiro. *Proteção de Dados*. Revista de Direito Privado | vol. 74/2017 | p. 133 - 158 | Fev / 2017 | DTR\2017\80.

532 *Idem*

BRASIL. **Recurso Especial** nº 1.593.873-2016a – SP. Disponível em: <https://ww2.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ATC?seq=66956815&tipo=51&nreg=201600796181&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20161117&formato=PDF&salvar=false > Acesso em: 24.06.2019

BRASIL. **TESE DE REPERCUSSÃO GERAL 786-2016b**: Acesso em: <http://www.stf.jus.br/portal/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5091603&numeroProcesso=1010606&classeProcesso=RE&numeroTema=786 > em 27.maio 2019.

BAUMAN, Zygmunt. **Danos colaterais: desigualdades numa era global**. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

COSTA JÚNIOR, Paulo José. **O direito de estar só***:* tutela penal da intimidade. 4. ed. São Paulo: Ed. Revista dos Tribunais, 2007.

EFING, Antônio Carlos. **Fundamentos do Direito das Relações de Consumo**. 2ª edição, Editora Juruá, 2011.

RODOTÁ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo.** 25. ed. São Paulo: Malheiros, 2006.

CONSELHO DA JUSTIÇA FEDERAL**. Enunciado 404**. Disponível em: <http://www.cjf.jus.br/enunciados/enunciado/208 >. Acesso em: 26.jun.2019.

CONSELHO DA JUSTIÇA FEDERAL**. Enunciado 531**. Disponível em: < http://www.cjf.jus.br/enunciados/enunciado/142 >. Acesso em: 26.jun.2019.

DOTTI, René Ariel. **A liberdade e o direito à intimidade**. Disponível em: < https://www2.senado.leg.br/bdsf/bitstream/handle/id/181214/000369546.pdf?sequence=3 >. Acesso em: 26.jun. 2019.

UNIÃO EUROPEIA. **Temos sempre de apagar os dados pessoais a pedido de uma pessoa?**. Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/do-we-always-have-delete-personal-data-if-person-asks_pt >. Acesso em: 15 junho 2019

UNIÃO EUROPEIA. **Regulamentos, diretivas e outros atos legislativos**. Disponível em: < https://europa.eu/european-union/eu-law/legal-acts_pt#diretivas > Acesso em: 15.jun.2019.

RUARO, Regina Linden; SOUZA, Fernando Inglez de. **Cenários de regulação da proteção de dados pessoais e os desafios de uma tutela efetiva no ordenamento jurídico brasileiro: a internet e suas implicações na privacidade e na proteção**

de dados pessoais. Interesse Público – IP, Belo Horizonte, ano 19, n. 103, maio/jun. 2017. Disponível em: <http://www.bidforum.com.br/PDI0006.aspx?pdiCntd=247799 >. Acesso em: 27 jun. 2019.

SARLET, Ingo. **Tema da Moda, Direito ao Esquecimento é anterior à internet**. Consultor Jurídico. Disponível em: <http://www.conjur.com.br/2015-mai-22/direitos-fundamentais-tema-moda-direito-esquecimento-anterior-internet >. Acesso em 17 junho. 2019.

BLUM, Renato M. S. Opice. GDPR – General Data Protection Regulation: Destaques da Regra Europeia e seus Refl xos no Brasil. **Revista dos Tribunais** | vol. 994/2018 | Ago / 2018, DTR/2018/17961.

CARVALHO, Ana Paula Gambogi. O Consumidor e o Direito à Autodeterminação Informacional: considerações sobre os bancos de dados eletrônicos. **Doutrinas Essenciais de Responsabilidade Civil**. Vol.8, p. 343-392, Out/2011.

CHEHAB, Gustavo Carvalho. O direito ao Esquecimento na Sociedade da Informação. **Doutrinas Essenciais de Direito Constitucional**. Vol. 8/2015, p. 563-596. Ago/2015.

JORGE, Maykon Cristiano; IOCOHAMA, Celso Hiroshi. A tutela inibitória como meio de efetivação do direito ao esquecimento e proteção da dignidade da pessoa humana. **Revista Brasileira de Direito Processual – RBDPro**, Belo Horizonte, ano 24, n. 95, p.203-226, jul./set.2016.

LIMA, Cíntia Rosa Pereira de. Direito ao Esquecimento e internet: o Fundamento Legal no Direito Comunitário Europeu, no Direito Italiano e no Direito Brasileiro. **Doutrinas Essenciais de Direito Constitucional**. Vol. 8/2015, p.511-543.

MARTINS, Sérgio Ludovico. Critérios para identificação do núcleo indevassável do direito de imagem, partindo da análise de recentes decisões judiciais. **Revista de Direito Privado**, vol. 74/2017, p. 93-115, fev. 2017.

PEREIRA, Flávio Henrique Unes; VELOSO JR., Joelson. "Marco Civil da Internet": a Gestão de Informações Públicas pelo Particular e o Papel do Estado". **Interesse Público – IP**, Belo Horizonte, ano 16, n.88, p.69-77, nov./dez. 2014

RAMOS, André de Carvalho. Direito ao Esquecimento e o Controle Indireto dos Bancos de Dados de Consumo. **Revista de Direito do Consumidor**. Vol 104/2016, p. 131-147, Mar- Abr/ 2016.

ROTUNDO, Rafael Pinheiro. Proteção de Dados. **Revista de Direito Privado** | vol. 74/2017 | p. 133 - 158 | Fev / 2017 | DTR\2017\80.

RULLI JÚNIOR, Antônio. RULLI NETO, Antônio. Direito ao esquecimento e o superinformacionismo: apontamentos no direito brasileiro dentro do contexto de sociedade da informação. **RIDB – Revista do Instituto do Direito Brasileiro**, Lisboa, ano 1,

n. 1, p. 419-434, jul/dez. 2012.

VERONESE, Alexandre. MELO, Noemy. A Proposta Brasileira de Proteção de Dados Pessoais em Comparação ao Novo Regulamento Europeu**. Revista de Direito Civil Contemporâneo**, vol. 14/2018, p. 71 – 99, Jan - Mar / 2018 DTR\2018\10349.

GERAÇÕES DE LEIS DE PROTEÇÃO DE DADOS: UM PANORAMA

Eixo Temático: A nova lei brasileira de proteção de dados pessoais (LGPD) e o GDPR europeu

Autores:
Taynara Arceno
Assessora de Juiz de Direito. Mestranda em Direito pela UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS. Bolsista CAPES/PROEX. Graduada em Direito pela UNISINOS.

Fernada Cantali
Advogada. Doutoranda em Direito pela UNISINOS. Mestre em Direito pela PUCRS. LLM em Direito Empresarial pelo CEU Law School. Professora de Direito Empresarial e de Direito da Propriedade Intelectual da UNISINOS e da ESMAFE – Escola Superior da Magistratura Federal. UNISINOS – UNIVERSIDADE DO VALE DO RIO DOS SINOS.

RESUMO
Este trabalho tem como objetivo abordar a categorização geracional de leis de proteção de dados proposta por Viktor Mayer-Schönberger, que classificou este grupo de legislações em quatro gerações: as primeiras surgiram na década de 70 e as últimas na década de 90. O que se pretende é demostrar como a construção legislativa acompanhou as transformações tecnológicas e, consequentemente, as transformações da privacidade. É fato que o direito precisou adequar-se com a revolução tecnológica a fim de promover a segurança e proteção à privacidade dos cidadãos. Com o aumento do fluxo informacional, a privacidade passou a se relacionar diretamente com os dados pessoais, deixando de se configurar como o direito de ser deixado só para um efetivo controle sobre as informações pessoais. Portanto, é possível afirmar que as legislações promulgadas com o intuito de proteger a intimidade e privacidade do cidadão, tornaram-se gradativamente obsoletas com o avanço da internet. Pensando nesse contexto, o presente trabalho faz um resgate histórico das legislações sobre proteção de dados, visando responder o seguinte questionamento: o fato de se viver uma quinta geração de proteção de dados significa que se atingiu a maturidade sobre o tema? Avançando no conceito elaborado por Mayer-Schönberger, é possível afirmar que com a vigência do Regulamento Geral sobre Proteção de Dados, se vive uma quinta geração de lei, tendo em vista que o Regulamento revoga de forma completa a Diretiva 95/46 – UE, e se traduz como uma nova era na proteção dos dados pessoais. É possível concluir que nesse momento se pode falar sobre uma maturidade legislativa, tão somente. No que se refere a maturidade de interpretação de lei, maturidade fática comportamental tanto dos encarregados de proteção de dados quanto dos titulares, cumprimento integral às normas de proteção e consciência de que a proteção de dados é um direito fundamental a ser respeitado, ainda se está no início do percurso.

INTRODUÇÃO

O respeito e a proteção da privacidade são as bases fundamentais para o desenvolvimento da dignidade humana, e nas sociedades democráticas, pode ser considerada uma prioridade. Nos últimos anos, experimenta-se uma revolução tecnológica da informação, que, com o passar dos tempos, proporcionou a criação de dispositivos inteligentes, e, dentre eles, destaca-se principalmente o surgimento da Internet. Com o advento desta, o conceito da vida cotidiana se transformou, a vida

em sociedade se transformou. A forma como as pessoas realizam suas atividades mais básicas, como realizam suas compras online e utilizam seus cartões de crédito e como se comportam dentro das redes sociais, levam a troca de um enorme fluxo de dados pessoais, tanto no setor privado quanto no setor público.

Nesse contexto, a temática da privacidade passa a se estruturar em torno da informação, e em consequência disso, em torno dos dados pessoais. A questão dos dados pessoais mantém um nexo de causalidade com a disciplina da privacidade, da qual é uma espécie de herdeira, uma vez que a atualiza e a impõe características próprias. As garantias que inicialmente eram relacionadas à privacidade passam a ser vistas, sob a ótica da proteção de dados, de uma maneira mais abrangente, por meio do qual outros interesses devem ser considerados, compreendendo as inúmeras formas de controle possíveis com a manipulação de dados pessoais (Danilo Doneda, 2006, p. 204).

Dentro desse cenário, o objetivo desse artigo é demonstrar como as legislações sobre privacidade/proteção de dados que surgiram ao da história, lidaram com essas questões. Trabalhar-se-á com a evolução proposta em 1997, por Viktor Mayer-Schönberger (professor de Governança e Regulação da Internet no Instituto da Internet de Oxford, da Universidade de Oxford), que vislumbra quatro diferentes gerações de leis de proteção de dados, sendo que as primeiras leis que abordaram a matéria, ainda que de forma indireta, surgiram na década de 1970. Dessa forma, após discorrer sobre cada geração de leis, ainda que de forma concisa, pretende-se responder o seguinte questionamento: O fato de já se estar na quinta geração de leis de proteção de dados representa maturidade sobre o tema? O assunto do trabalho se justifica pela atualidade e pela relevância teórico-prática da matéria.

O que efetivamente são os dados pessoais?

Importante mencionar o que significam os dados pessoais no contexto da era moderna. Para tanto, se extrairá o conceito exposto no Regulamento Europeu 2016/679, uma vez que é o conceito mais rico em detalhes em termos de legislação, que traz a seguinte definição:

> «Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identifi ável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificado , como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular (UE, 2018).

Conforme o elucidado, conclui-se que os dados pessoais de um cidadão podem ser: o nome e sobrenome; o endereço de uma residência; um endereço de correio eletrônico como nome.apelido@empresa.com; o número de um cartão de identificação; dados de localização (por exemplo, a função de dados de localização num telemóvel); um endereço IP (protocolo de internet); testemunhos de conexão (cookies); o identificador de publicidade do seu telefone; os dados detidos por um hospital ou médico, que permitam identificar uma pessoa de forma inequívoca (Comissão Europeia, 2018)

O titular desses dados é a pessoa singular, que no Brasil também é chamada de pessoa natural, isto é, pode ser considerada a "dona" ou "proprietária" desses dados. Além disso, importante mencionar que existe uma subcategoria dentro do conceito de dados pessoais, que são os chamados dados sensíveis. Estes, por sua vez, são aqueles dados pessoais que revelem a origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas dados genéticos, biométricos, dados relacionados com a saúde e dados relativos a orientação sexual das pessoas (UE, 2018).

A primeira geração de leis de proteção de dados: O impulso necessário

As preocupações com a disciplina da proteção de dados iniciaram-se com os impulsos tecnocráticos dentro da administração pública, que seguiram o pós-guerra na década de 1960, com o incremento da informática. No que se refere a uma construção doutrinária, o autor Alan Westin escreveu a obra *"Privacy and freedom"*, justamente como uma forma de resposta a esses projetos criados, que levou a discussão em torno da privacidade para um outro nível, propondo um modelo de definição fundamentado na autodeterminação informativa.

As primeiras legislações para a tutela dos dados pessoais surgiram na década de 1970, quando foram utilizadas como modelo a compreensão da extensa difusão da imprensa e dos serviços públicos. Conforme os ensinamentos de José Adércio Leite Sampaio (1998, p. 490), elas apresentavam as seguintes características:

> a) tratava-se de uma legislação garantista, situada na linha histórica das declarações de direito; b) pretensamente ampla, única e uniforme para todas as situações; c) cujo instrumento jurídico principal se firmava na autorização, no suposto de ser possível controlar todos os sistemas tecnológicos de coleta e de processamento de dados, a partir de uma necessária autorização previa para seu funcionamento, acompanhada de um controle a posteriori por parte de um órgão institucional; e d) de aplicação restrita às pessoas físicas.

Entre as legislações precursoras, estava a Lei do Land Hesse Alemão, que é o primeiro texto de proteção de dados. Após, surge a Lei Sueca em 1973, seguida pelo Privacy Act em 1974. Ainda, a lei da República Federal Alemã de 1977, a Lei

Dinamarquesa de 1978 e a Lei Austríaca de 1978. Mayer-Schönberger (1997, p. 221-223) propõe que estas legislações são da "primeira geração" de leis de proteção de dados, pela sua estrutura, abordagem e linguagem, uma vez que representam respostas diretas aos bancos de dados nacionais centralizados.

O autor afirma que a maioria das normas de proteção de dados de primeira geração não se concentra em proteger a privacidade individual de cada um. Ao invés disso, elas se concentram na atividade de processamento de dados na sociedade. Com a redução do custo para adquirir computadores, a tecnologia do processamento de dados se tornou uma ferramenta poderosa na mão de grandes empresas e, até mesmo, nas mãos do próprio governo. Portanto, as legislações de primeira geração visavam controlar o uso dos dados, evitando que a sociedade vivesse em uma vigilância total por um Big Brother eletrônico (Mayer-Schönberger, 1997, p. 223).

A estrutura gramática dessas leis e sua estrutura estavam relacionadas objetivamente aos bancos de dados, e não a privacidade, desde deus princípios genéricos até os regimes de autorização e de modalidades de tratamento de dados, sem que se fosse prevista a participação do cidadão neste processo. Justamente por esse motivo, foram estabelecidos os primeiros comissários de proteção de dados pessoais (Mayer-Schönberger, 1997, p. 224).

A segunda geração de leis de proteção de dados e a privacidade individual

No final da década de 1970 surgiu a segunda geração de leis sobre a matéria. Na segunda geração, a proteção se concentrou nos direitos individuais de privacidade do cidadão. Debates em torno do direito de ser deixado só e o direito de delimitar o próprio espaço íntimo, foram trazidos de volta a pauta. Neste momento, a proteção de dados estava explicitamente ligada ao direito à privacidade e era vista como o direito de afastar a sociedade de assuntos pessoais (Mayer-Schönberger, 1997, p. 226).

Pode-se dizer que o primeiro exemplo dessa geração de leis, foi a lei francesa *Informatique et Libertées,* de 1978, além disso, a lei austríaca, também de 1978, e as constituições portuguesa e espanhola também traziam essa perspectiva de proteção de dados juntamente com a privacidade individual, por mais que a lei específica de proteção de dados desses países surgisse somente anos mais tarde (Danilo Doneda, 2006, p. 209). Dessa maneira, criou-se um sistema que permite que o cidadão possa identificar o uso indevido de suas informações pessoais e requerer a sua tutela.

Na segunda geração de leis, os indivíduos obtiveram uma palavra no processo. O consentimento era, geralmente, uma pré-condição para o processamento de dados. Os direitos individuais estabelecidos nessas legislações delegaram o poder de decisão para o cidadão, que tem direito de escolher quais dados pessoais poderiam ser usados

e para quais fins. Por exemplo, o §7º e §33 da antiga lei Norueguesa de Proteção de Dados, delegava aos indivíduos o direito de recusar o processamento de seus dados para fins de marketing direto e pesquisa de mercado (Mayer-Schönberger, 1997, p. 227).

Entretanto, na vida real, o indivíduo raramente teve a oportunidade de participar dessas decisões, sob pena de excluir-se da sociedade, o que acarretou uma mudança de perspectiva e o surgimento da terceira geração de leis, na década de 1980.

A terceira geração de leis sobre proteção de dados e a autodeterminação informativa

Esse conjunto de leis apresentava uma sofisticaç o na tutela dos dados pessoais, que continuava sendo concentrada no cidadão, contudo, passou a abranger mais do que a liberdade de fornecer ou não seus dados pessoais, preocupando-se, também, em garantir a efetividade dessa liberdade. A partir dessas legislações, a questão da proteção dos dados pessoais era vista de uma maneira mais complexa, levando em consideração que permite, além da participação do indivíduo na sociedade, que seja também analisado o contexto no qual lhe for solicitado a revelação de seus dados, estabelecendo meios de proteção para situações em que sua liberdade de decidir é limitada por eventuais condicionantes. Dessa maneira, se estaria proporcionando o pleno exercício da autodeterminação informativa (Danilo Doneda, 2006, p.211).

Para Pérez Luño (1996, p. 44), a autodeterminação informativa é uma construção da doutrina e jurisprudência germânica que se equivale à liberdade informática, com uma importância indispensável para a sociedade contemporânea. A função da autodeterminação é garantir aos indivíduos direitos de informação, acesso e controle dos dados que lhe pertencem. Essa faculdade não é intersubjetiva, mas sim uma faculdade que reflete nas suas relações com os demais cidadãos e com o poder público. Em suma, refere-se a liberdade do sujeito para determinar se deseja tornar públicas informações a seu respeito, assim como a quem, e, em qual ocasião.

O marco normativo da expressão "autodeterminação informativa" é a decisão proferida pelo Tribunal Constitucional Alemão, na data de 15 de setembro de 1983 (*informationelle selbstestimmung*), que consistia no direito do cidadão de controlar a coleta, a titularidade, o tratamento e a transmissão de dados relativos à sua própria pessoa. Na referida decisão do tribunal alemão, se afirmou "O direito básico garante a capacidade do indivíduo de decidir, em geral, por si mesmo, a liberação e o uso de seus próprios dados pessoais" (Mayer-Schönberger, 1997, p. 229).

Ainda, a decisão judicial não apenas vinculou explicitamente a proteção de dados a uma disposição constitucional, mas também, o direito à autodeterminação

informativa. Além disso, profundas mudanças aconteceram em toda a estrutura da lei federal de proteção de dados da Alemanha, o tribunal declarou que todas as fases do processamento da informação, desde a coleta até a transmissão, estão sujeitas às limitações constitucionais. Consequentemente, os direitos de participação do indivíduo precisam ser estendidos a todos os estágios de processamento (Mayer-Schönberger, 1997, p. 229).

Se inserem nessa categoria algumas alterações legislativas nos Estados Alemães, em decorrência da decisão do Tribunal Constitucional, a Emenda Geral à Lei Federal Alemã de Proteção de Dados (1990), a Emenda de 1986 da Lei Austríaca de proteção de dados, a extensão dos direitos de participação individual na Lei Norueguesa de Proteção de Dados, e a adoção de uma disposição constitucional nos Países Baixos para garantir a proteção dos dados pessoais.

Contudo, a autodeterminação informativa era privilégio daquelas poucas pessoas que estavam dispostas a encarar os custos econômicos e sociais decorrentes do exercício de tais prerrogativas. A grande maioria das pessoas temiam o risco financeiro de interpor ações judiciais ou temiam o incômodo em participações e aparições em tribunais (Mayer-Schönberger, 1997, p. 244).

Pensando nesse caráter exclusivo, surgiu uma quarta geração de leis de proteção de dados caracterizadas pela preocupação em suprir as desvantagens do enfoque individual existente até então.

A quarta geração de leis de proteção de dados e a resposta Europeia

Nas legislações de quarta geração, busca-se enfocar o problema integral da informação, haja vista que se presume que a tutela dos dados pessoais não pode ser baseada simplesmente na escolha individual de cada cidadão. Por isso, são necessárias ferramentas que elevem o padrão coletivo de proteção (Danilo Doneda, 2011, p. 98).

Uma das características dessas leis, é que procuram fortalecer a posição do cidadão frente às entidades que coletam e processam seus dados. A técnica para que isso aconteça está no reconhecimento do desequilíbrio entre as partes e posterior tentativa de correção da desigualdade por meio de duas abordagens distintas, sendo a primeiras delas, conforme o já mencionado, uma tentativa de impor equilíbrio entre as partes, reforçando a posição do indivíduo em face poderosas instituições de coletas de dados, e a segunda se encontra na própria redução do papel da decisão individual na autodeterminação informativa. Isso acontece porque parte-se do pressuposto de que certas modalidades de tratamento de dados precisam de uma proteção máxima, não podendo ser obtida exclusivamente por meio de uma decisão individual, como ocorre, por exemplo com os dados sensíveis. Outra característica dessa nova geração é

a disseminação de das autoridades independentes para atuação da lei e o surgimento de normativas conexas, como forma específica para determinados setores de processamento de dados, como por exemplo, setor da saúde e de crédito ao consumo (Danilo Doneda, 2006, p.213).

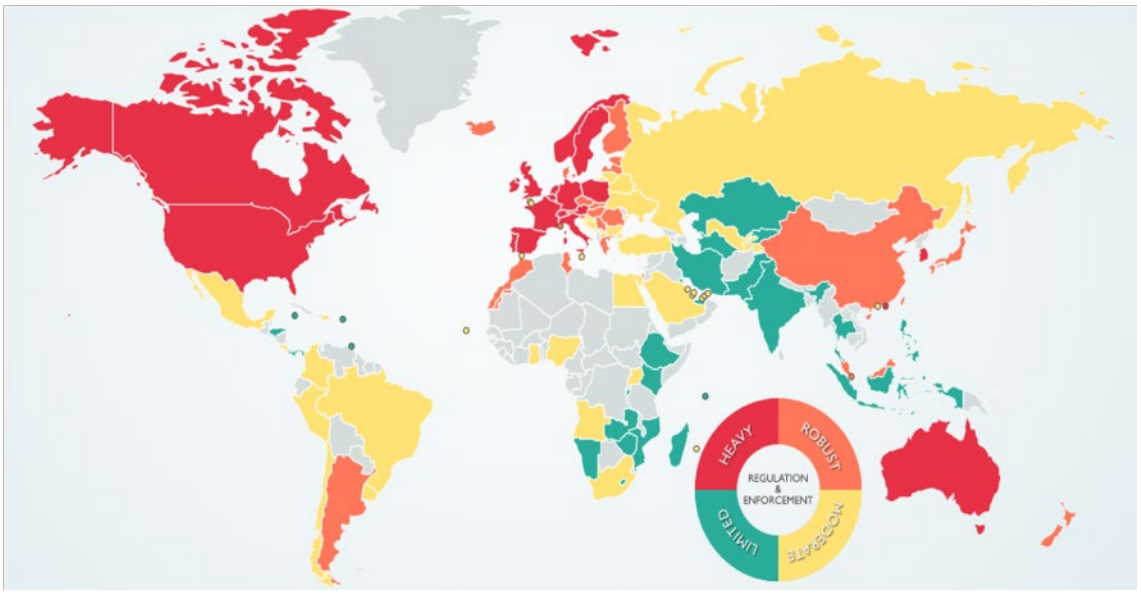
É possível afirmar que tal modelo de proteção de dados pessoais foi representado pelos países europeus que integraram dentro de seus ordenamentos a Diretiva 95/46 da União Europeia. A Diretiva buscou unificar os termos de proteção de dados em todos os Estados-membros da UE, além de obrigar que todos os Estados a incorporassem no seu âmbito jurídico interno. Com o advento da Diretiva 95/46/CE, os países da Europa passaram a estabelecer agências, comissões, ou, pelo menos, um departamento, de natureza fiscal, com a finalidade de exercer funções administrativas, consultivas, sancionatórias e outras. Posteriormente, foi editada a Diretiva 97/66/CE, que dizia respeito sobre o tratamento de dados pessoais no setor das telecomunicações.

Além disso, importante referir que a Carta dos Direitos Fundamentais da União Europeia, em seu art. 8º, estabelece que "Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito". Estabelece ainda que esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento do cidadão interessado, ou com outro fundamento legítimo previsto em lei. "Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação". Ainda, dispõe que tais regras, para o seu efetivo cumprimento ficam sujeitas a fiscalização por parte de uma autoridade independente (Conselho da Europa, 2000).

Importante referir também que existe um modelo Norte Americano de proteção de dados, mas esse modelo não se assemelha ao Europeu, tendo em conta que os Estados Unidos não possui uma lei geral e unific da sobre proteção de dados, aplicável a toda e qualquer atividade de processamento de dados. A opção feita pelos EUA foi regulamentar cada setor de maneira específica, cabendo a cada Estado ditar suas regras. Assim, existe uma legislação para o setor médico, outra para o setor de seguros, outra para o de consumo e assim por diante.

Em tempos atuais, cerca de 120 países e jurisdições independentes possuem leis de privacidade/proteção de dados pessoais mantidos por setores públicos e privados. Ademais, cerca de 40 países e jurisdições possuem, ao menos, iniciativas de leis pendentes. Na maioria dos países, existe uma comissão independente de proteção que supervisiona e aplica as leis. Grande parte deles também possuem isenções específicas para a mídia (David Banisar, 2018). A figura abaixo mostra quais países possuem legislação específicas para a proteção de dados pessoais

Leis de Proteção de Dados ao redor do mundo



Fonte: DLA PIPER, 2019.

Dentre os países da América do Sul que possuem legislação sobre proteção de dados, se destacam a Argentina, o Uruguai e também o Brasil (comentado posteriormente). Na Argentina, a Lei de Proteção de Dados Pessoas nº 25.326 a (PDPL), promulgada em outubro de 2000, fornece uma proteção ampla aos dados pessoais, seguindo o padrão de proteção da Espanha. Na data de 30 de junho de 2003, a Comissão Europeia reconheceu que a Argentina concede um nível adequado de proteção de dados pessoais, estando em conformidade com a Diretiva de Proteção de dados da UE – 95/46. O Uruguai, por sua vez, iniciou a regulamentação da matéria em 2004, com a Lei nº 17.838, que tratava da restrição de dados para informações comerciais, além de estabelecer o *habeas data*. No ano de 2008 essa proteção foi expandida com a promulgação da Lei nº 18.331, tratando especificamente da proteção de dados pessoais e da ação de habeas data. Sobre a legislação brasileira se abordará com maior riqueza de detalhes nos tópicos posteriores.

Por isso, surge a classificação em gerações de leis de proteção de dados, proposta por Viktor Meyer-Schönberger, que é consideravelmente aceita pela doutrina jurídica mundial. Como norma de quarta e última geração proposta pelo autor, tem-se como grande exemplo, a Diretiva 95/46 da União Europeia, e suas posteriores atualizações nos anos de 1997 (setor de telecomunicações) e 2002 (setor das comunicações eletrônicas). Essa Diretiva inaugurou um marco regulatório de extrema importância no direito comunitário, sendo possível afirmar que era o principal instrumento de proteção de dados vigente até então.

A continuidade da evolução legislativa: Uma quinta geração (?)

A Diretiva 95/46 CE permaneceu vigente e aplicável por 20 anos e, em que pese fosse revolucionária para o seu tempo, estava pouco a prova do futuro. A diretiva existente já não se adequava aos avanços tecnológicos dos últimos anos, sendo necessário que uma nova regulamentação cobrisse as lacunas legislativas criadas pelo surgimento das mídias sociais, *big data*, e um mundo cada vez mais digital.

Após cinco anos intensos de debate, o texto do Regulamento Geral sobre Proteção de Dados (RGPD), foi aprovado pelo Parlamento Europeu na data de 27 de abril de 2016 e buscou tutelar a proteção de dados levando em consideração o uso da internet nos últimos 20 anos.

Analisando as evoluções das leis relativas a proteção de dados proposta por Viktor Mayer-Schönberger, é possível concluir que o Regulamento Geral sobre Proteção de Dados inaugura uma nova geração de legislações sobre o tema, levando-se em consideração que se apresenta como uma nova era na proteção dos dados pessoais.

José Luis Piñar Mañas (2017, p.16) discorre que o novo regulamento causou uma reviravolta em relação a situação anterior, entretanto, a maioria dos princípios e fundamentos do novo regulamento seguem sendo os mesmos da diretiva antecedente. O novo regulamento introduz, às vezes de forma explícita e, outras vezes, de forma subjetiva, um novo modelo de proteção de dados para a Europa, um modelo que passa da gestão dos dados ao uso responsável da informação e essa é a mais profunda mudança que o regulamento vai impor.

Outra importante característica do RGPD é que ele cria um regime jurídico único em todos os vinte e oito países membros da União Europeia, diferentemente da Diretiva 95/46, que determinava a internalização/transposição dos valores apontados pela Diretiva em uma legislação nacional, o que, consequentemente, poderia ser diferente de um país para o outro.

Além disso, a atuação do RGPD recai sobre todas as empresas e banco de dados que tratem informações pessoais dentro da União Europeia, assim como fora dela. Isso signific que grandes empresas detentoras de dados como o Facebook e Google, se tratarem dados de cidadãos europeus, o que, evidentemente, vai acontecer, terão que se adequar às determinações que o RGPD estabelece.

Nesse sentido, aduz Stefano Rodotà (2015):

> Deve projetar-se também sobre os novos "Senhores da Informação" que, por meio das gigantescas coletas de dados, governam as nossas vidas. Em face de tudo isso, a palavra "privacy" evoca não apenas uma necessidade de intimidade, mas sintetiza as liberdades que nos pertencem no mundo novo onde vivemos. O próprio modo de ser desses sujeitos – chamados Amazon ou Apple, Google ou Microsoft, Facebook ou Yahoo! – mostra-nos uma

> presença de oportunidade para a liberdade e a democracia e de um poder soberano exercido sem controle sobre a vida de todos.

Na linha de pensamento do autor, essas empresas controlam o modo de vida das pessoas de tal modo que as regras constritivas não são mais suficientes, sendo necessária a criação de garantias constitucionais para os direitos da rede.

Consoante o artigo 1º do RGPD, estabeleceram-se "regras relativas à proteção das pessoas singulares, no que quis respeito ao tratamento de dados pessoais e a livre circulação desses dados" (UE, 2016). Assim, busca-se tutelar as garantias e direitos fundamentais em perfeita harmonia com o disposto no artigo 8º da Carta de Direitos Fundamentais da União Europeia, que reconhece a proteção de dados como um direito fundamental em toda sua extensão.

Muito inspirada no Regulamento Europeu, a Lei Geral de Proteção Dados (LGPD), sancionada sob o número 13.709, de 14 de agosto de 2018, também representou um marco legislativo para o Brasil, que em momento anterior a promulgação da lei, não continha norma específica sobre a proteção dos dados pessoais. O objetivo da LGPD é promover garantias para o cidadão na proteção de seus dados, e, ao mesmo tempo, fornecer bases para o desenvolvimento da economia da informação, regida nos vetores da confianç , segurança e valor. Além disso, LGPD está estruturada em cinco eixos principais no que diz respeito a proteção do titular dos dados, quais sejam: I) unidade e generalização da Lei; II) legitimação para o tratamento de dados; III) princípios e direitos do titular; IV) obrigações dos agentes de tratamento de dados e; V) responsabilização dos agentes (Laura Schertel; Danilo Doneda, 2018, p. 46).

Existe uma discussão no que se refere a Autoridade Independente de Controle. A Diretiva 95/46/CE, conforme o já mencionado, prescrevia o modelo de autoridade de proteção de dados totalmente independente, ainda que a questão da independência seja implícita. Em contrapartida, o Regulamento Europeu estabeleceu expressamente as garantias de independência das autoridades de controle. No Brasil, a implementação da autoridade independente de controle se deu de forma diversa. Inicialmente, houve veto a criação da Autoridade Nacional de Proteção de Dados – ANPD. Contudo, após diversas manifestações a favor da autoridade de controle, uma vez que sem a existência do órgão seria praticamente impossível colocar em prática as disposições da LGPD, foi editada a Medida Provisória n.º 869, de 27 de dezembro de 2018, recentemente transformada em Lei pelo Congresso Nacional. Todavia, apesar da criação da ANPD, o modelo brasileiro não possui as garantias estruturais que se fazem presentes no Regulamento Europeu, haja vista que a autoridade brasileira não será independente em suas garantias, mas sim, será um órgão da administração pública federal, integrante da Presidência da República (Laura Schertel; Danilo Doneda, 2018, p. 45).

Entretanto, em que pese a existência de problemáticas envolvendo tanto o RGPD quanto a LGPD, ambas as normas representam um significativo avanço legislativo em matéria de proteção de dados. Já que o fluxo de dados pessoais só tende a aumentar, especialmente em razão do avanço da indústria 4.0, inteligência artificial e internet das coisas, essas legislações permitem que o cidadão titular desses dados tenha controle sobre esse fluxo, de forma que não se impeça o avanço tecnológico, garantido efetiva proteção e confiança desses dados.

Afinal, atingiu-se a maturidade sobre o tema?

Diante de todo o exposto até aqui, e levando-se em consideração que atualmente se vive uma quinta geração de leis sobre proteção de dados, é possível afirmar que se atingiu uma maturidade legislativa sobre o tema. A evolução normativa teve início na década de 1970 e, atualmente, pode ser representada pelo Regulamento Europeu sobre proteção de dados, que trouxe inovações em diversos aspectos, especialmente no que se refere ao seu âmbito de aplicação. Entretanto, é possível concluir que, nesse momento, se pode falar sobre uma maturidade legislativa, tão somente. No que se refere a maturidade de interpretação de lei, maturidade fática comportamental tanto dos encarregados de proteção de dados quanto dos titulares dos dados, cumprimento integral às normas de proteção, consciência de que a proteção de dados é um direito fundamental a ser respeitado, ainda se está no início do percurso.

REFERÊNCIAS

BANISAR, David. National comprehensive data protection/privacy laws and bills 2018. Disponível em: https://ssrn.com/abstract=1951416. [Data da consulta: 05 de maio de 2019]

COMISSÃO EUROPEIA, O que são dados pessoais?, Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_pt. [Data da consulta: 06 de maio de 2019]

CONSELHO DA EUROPA. Carta dos Direitos Fundamentais da União Europeia. Disponível em: http://www.europarl.europa.eu/charter/pdf/text_pt.pdf. [Data da consulta: 06 de maio de 2019].

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico Journal of Law. Disponível em: http://editora.unoesc.e du.br/index.php/espacojuridico/article/view/1315/658. [Data da consulta: 20 de maio de 2019].

DONEDA, Danilo, "*Da privacidade à proteção de dados pessoais*". Renovar, Rio de Janeiro, 2006.

DLA PIPER, DATA PROTECTION LAWS OF THE WORLD. Disponível em: https://www.dlapiperdataprotection.com/index.html?t=world-map&c=BR, [Data da Consulta: 25 de maio de 2019].

MÃNAS, José Luis Piñar, "Hacia um nuevo modelo eropeo de protección de datos". *Reglamento general de protección de datos: hacia um nuevo modelo europeo de privacidade*, coord. José Luis Piñar Manas, Reus, Madrid, 2017.

MEYER-SCHÖNBERGER, Viktor, "General development of data protection in Europe", *Technology and privacy: the new landscape,* coord. Phillip Agre, Marc Rotenberg, MIT Press, Cambridge, 1997.

PÉREZ LUÑO, Antonio Enrique, "*Manual de informática y derechos*", Ariel, Barcelona, 1996.

RODOTÀ, Stefano, Por que é necessária uma Carta de Direitos da Internet?, **Civilistica.com**, Rio de Janeiro, nº 2, jul.-dez. 2015. Disponível em: <http://civilistica.com/porque-e-necessaria-uma-carta-de-direitos-da-internet, [Data da consulta: 20 de maio de 2019].

SAMPAIO, José Adercio Leite, *"Direito à intimidade e à vida privada: uma visão jurídica de sexualidade, da família, da comunicação e informações pessoais, da vida e da morte"*, Del Rey, Belo Horizonte, 1998.

SCHERTEL MENDES, Laura; DONEDA, Danilo, "Refl xões gerais sobre a nova lei de proteção de dados", *Revista do Direito do Consumido*r, v.120, 2018.

UNIÃO EUROPEIA. Regulamento (UE) 679/2016 do Parlamento Europeu e do Conselho de 27 de abril de 2016, Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e a livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento geral sobre a proteção de dados), Jornal Oficial da União Europeia, [S.I.], 4 maio. 2018, l 119/1. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN. [Data da consulta: 20 de maio de 2019].

A GDPR E SUA INFLUÊNCIA NO ORDENAMENTO JURÍDICO BRASILEIRO

Eixo Temático: A nova lei brasileira de proteção de dados pessoais (LGPD) e o GDPR

Autores:
Nicolas Addor
Mestre em Direito pela Pontifícia Universidade Católica do Paraná (PUCPR). Professor do Curso de Direito da UNIFACEAR-PR. Especialista em Direito Constitucional pela Academia Brasileira de Direito Constitucional. Pós-graduando em Direito da Tecnologia na PUC-Minas Gerais.

Cinthia Obladen de Almendra Freitas
Doutora em Informática. Professora Titular da Pontifícia Universidade Católica do Paraná. Professora Permanente do Programa de Pós-Graduação em Direito Econômico e Socioambiental da PUCPR.

Miriam Olivia Knopik Ferraz
Doutoranda em Direito Econômico e Socioambiental da PUCPR. Professora do Curso de Direito da UNIFACEAR – PR. Especialista em Direito Constitucional pela Academia Brasileira de Direito Constitucional. Pós-graduanda em Direito da Tecnologia na PUC-Minas Gerais. Mestre em Direito pelo Programa de Mestrado e Doutorado em Direito Econômico e Socioambiental da PUCPR.

ABSTRACT
Privacy and protection of personal data are not new topics. This article analyzes the effects that General Data Protection Regulation (GDPR), promulgated by the European Union, brought into the Brazilian legal system, with an analysis of Brazilian General Data Protection Act (Act 13.709/2018, abbreviation 'LGPD' in Brazilian's Portuguese). The article contextualizes the privacy in contemporary society and the personal data leak scandals of Facebook users. We present an overview about GDPR and relation between this legal regulation and the personal data and processing personal data. The Brazilian overview is based on Constitution of the Federative Republic of Brazil (1988), Consumer Code (1990), Brazilian Civil Rights Framework for the Internet (2014), and Brazilian General Data Protection Act (2018). The hypothesis of this work is that the GDPR influenced the legal argumentation in the LGPD, which is confi med by deductive method of research. It is argued that the both, GDPR and LGPD, are positive for the UE and Brazil, giving more reliability to the use of personal data and providing security to the international market to negotiate with Brazilian companies. In both GDPR and LGPD, it is possible to find five main objects: a) the creation of a state supervisory authority for data processing; b) the delimitation of what is legally relevant to the handling of personal data whether digital format or not; c) description of rights and guarantees of the data subject; d) the definition of penalties in case of an offense against the rights; the legitimation of the fundamental right of privacy in digital media as a branch of the right to privacy; e) the forecasting of accountability of data processing agents. Thus, both the European regulation and Brazilian law must keep in mind that legal compliance is not sufficien to encompass and enforce such legal texts, since the intersection of law and information technology has never been so close. Only with the Law and the Technology united will it be possible to walk in the full sense of data protection and privacy without ambiguities or inaccuracies.

Keywords: Privacy; Personal Data; General Data Protection Regulation (GDPR); Brazilian General Data Protection Act (LGPD); Fundamental Rights.

1. Introdução

A 4ª. Revolução Industrial e a necessidade de os Estados darem uma resposta rápida e eficiente à sociedade fez com que o Poder Público enfrentasse o tema da proteção da privacidade. A atuação considerada modelo nesse processo foi a promulgação, em 2016, da *General Data Protection Regulation* (GDPR) na União Europeia.

Privacidade e proteção de dados pessoais não são temas novos, visto que já em 1995, a União Europeia propôs a unificação normativa referente à proteção de dados no bloco. Entretanto, apenas em 2012 houve a proposta de uma lei que padronizasse a norma nos diversos Estados-parte, sendo somente aprovada em 2016. A legislação previu que a comunidade europeia tivesse o prazo de dois anos (até 2018) para que se ajustar às exigências. Curiosamente, o termo final ocorreu coincidentemente com um grande escândalo de dados pessoais envolvendo a rede social *Facebook* e a empresa de tratamento de dados *Cambridge Analytica*.[533]

Em síntese, o escândalo ocorreu em meio à descoberta de um esquema de coleta, venda e uso indevido de dados de cerca de 50 milhões de usuários estadunidenses do *Facebook*, realizados pela *Cambridge Analytica* a fim de montar uma espécie de perfil pessoal contendo traços de personalidade objetivando formar opiniões e direcionar votos para as necessidades das eleições que ocorreram em 2016 nos Estados Unidos (RONCOLATO, 2018). Ou seja, explorou-se a capacidade de influencia , por meio de algoritmos, a tomada de decisão do usuário da Internet mediante o conhecimento do modo de uso e perfil na Internet.

O artigo apresenta uma visão exploratória da GDPR sobre o ordenamento jurídico brasileiro (LGPD) relativo à proteção de dados pessoais. É preciso ressalvar, não obstante, que as investigações e soluções propostas que são encontradas nas diferentes jurisdições devem ser removidas de seu contexto conceitual e retiradas de seus entendimentos doutrinários nacionais para que possam ser vistas essencialmente a sua função, como uma tentativa de satisfazer uma necessidade legal específica (ZWEIGERT; KÖTZ, 1996, p. 44). Nesse sentido, a visão trazida neste artigo sobre as leis, brasileira e europeia, permite estabelecer um panorama de interseção entre os dois ordenamentos.

2. BREVE EXPLANAÇÃO DO GDPR[534]

A reforma normativa feita na União Europeia com a introdução do GDPR trouxe importantes e positivas mudanças na proteção de dados para os cidadãos na Europa.

533 Disponível em: <https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html>. Acesso em: 09 jun. 2019.

534 Toda e qualquer informação sobre o GDPR pode ser encontrada em: <https://eugdpr.org/>.

Entre elas, a caracterização do direito à proteção dos dados pessoais como um direito fundamental (art. 1º, § 2º) introduziu positivamente o bloco econômico no cenário do espaço digital. Sobre sua incidência territorial, a legislação prevê que a sua aplicação ocorrerá aos usuários residentes no território da União Europeia, mesmo que a coleta de dados sobre cidadãos europeus ocorra fora da EU (art. 3º, § 2º).

GDPR tem competência para regular o tratamento de dados pessoais efetuado por empresários ou empresas no exercício de atividades comerciais. Tal ressalva é feita, de maneira transparente, na explanação de motivos da lei europeia: "o presente regulamento não se aplica ao tratamento de dados pessoais efetuado por pessoas singulares no exercício de atividades exclusivamente pessoais ou domésticas e, portanto, sem qualquer ligação com uma atividade profissional ou comercial." [535]

Para o GDPR, dados pessoais significa uma "informação relativa a uma pessoa singular identificada ou identificável", ou seja, qualquer informação relacionada a uma pessoa que possa ser identificada direta e indiretamente por meio de um nome, número de identificação, identificadores digitais, localização, identidade genética, mental, econômica, cultural, social, fisiológica e física. [536]

Quando as empresas necessitarem do consentimento do titular dos dados, elas deverão, por lei, solicitar e indicar de maneira transparente o escopo do uso dos dados. Além disso, o consentimento deverá refletir a vontade do titular de forma inequívoca, impedindo interpretações dúbias quanto ao acordo firmando entre o titular e o receptor dos dados. Pretende-se impedir que as empresas de conteúdo digital mantenham brechas contratuais nos extensos contratos de adesão que notoriamente pouco são lidos por quem se cadastra para fazer uso de um aplicativo ou serviço *online* pela primeira vez (art. 4º inciso 11 e art. 7º, GPDR).

Tal proteção chama atenção pelo fato de que, na Europa Continental, condena-se largamente o tráfego de dados de consumidores por acreditarem que se trata de uma séria e potencial violação dos direitos de privacidade do consumidor se os empresários e corpo comercial puderem comprar as informações sobre as preferências, gostos e características dos titulares dos dados (WHITMAN, 2004, p.1192). Isso também explica a proibição de tratamento de dados pessoais que revelem a origem racial, étnica, as opiniões políticas, convicções religiosas, filiação sindical, convicções filosóficas dados genéticos, biométricos, dados relativos à saúde e orientação sexual de uma pessoa, com algumas ressalvas legais (art. 9º, GDPR).

Nos artigos 12 a 14 da GDPR, o texto normativo garante ao usuário o direito de receber informações claras e compreensíveis no que diz respeito sobre quem efetua

535 18º parágrafo das considerações sobre o Regulamento 2016/769 do Parlamento Europeu e do Conselho.

536 Artigo 4º, § 1º, GDPR.

o tratamento dos dados pessoais, quais são tais dados e quais serão os fins desse tratamento.

O artigo 15 dispõe sobre o direito do titular de dados de obter do responsável o acesso aos seus dados pessoais e as informações concernentes às finalidades do tratamento, as categorias dos dados pessoais, os destinatários a quem os dados serão divulgados, o prazo de conservação das informações, o direito de apresentar reclamação a uma autoridade e a existência de *"automated decision-making"*.

Em importante previsão, o artigo 22 garante ao usuário de Internet o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente por decisões automatizadas, incluindo a definição de perfis que o afete significativamente, inclusive na esfera jurídica. O texto assevera, contudo, que essa garantia não protege se: a) as decisões automatizadas forem necessárias para a celebração ou execução de um contrato entre o titular e o responsável pelo tratamento de dados; b) for autorizada pelo ordenamento da UE ou de algum Estado-Membro, salvaguardados os direitos do titular das informações e; c) houver consentimento explícito do titular.

O direito à explicação sobre todas as decisões tomadas por sistemas algorítmicos automatizados ou que aplique técnicas computacionais, a exemplo de Aprendizagem de Máquina ou Mineração de Dados, não carece de preciosismo técnico e terminológico visto ser amplo para justamente englobar as técnicas atuais e vindouras. GDPR traz a obrigatoriedade que os titulares dos dados recebam as explicações necessárias, tais como a lógica envolvida e as consequências que podem ocorrer com o uso dos sistemas automatizados de tomada de decisão. Porém, ainda cabem dúvidas sobre o que seria e como se procederia o exercício do direito à informação, nem o que seria juridicamente relevante para a validade da GDPR sobre a tomada de decisões baseadas em algoritmos e técnicas computacionais (WATCHER; MITTELSTADT; FLORIDI, 2017, p.96).

O regulamento também traz o "direito a ser esquecido", ou seja, o direito de obter do responsável dos dados a obrigação de apagar os dados pessoais da maneira mais célere possível. Para Kuner (2012, p.25), tal direito aparenta ser uma versão de um direito já existente. Tecnicamente deve-se ter em conta que o custo computacional pode ser elevado para a efetiva eliminação de dados ou mesmo deve-se respeitar o tempo legal de guarda por tipos de documentos e seus dados. Tem também, o titular, o direito de retificar e corrigir dados maneira célere (artigo 16, GDPR)

Trata-se, na realidade, de uma legítima requisição para balancear o poder sobre os dados pessoais, visto que a coleta de dados pessoais na Internet está disseminada e sem controle, ficando a propriedade sobre os dados mitigada pela ampla capacidade de armazenamento dos provedores de aplicação ou de acesso (LIMA, 2013, p.281).

No artigo 20 há também a previsão do direito de portabilidade de dados, que permite o direito de transmissão de dados pessoais entre um prestador de serviço e outro, mediante solicitação do titular, não podendo o responsável impedir de qualquer

modo tal pedido de transmissão. Já nos artigos 33 e 34 do GPDR, quando ocorrer perda ou roubo de dados pessoais e o ato ilícito prejudicar o proprietário dos dados, a empresa será obrigada a informar a invasão de maneira célere, sob pena de multa.

A legislação europeia também garante uma proteção especial às crianças, visto que toda informação direcionada ao público infantil deverá ser adaptada para uma linguagem clara e simples, de fácil compreensão. Previu-se também que a oferta direta de serviços digitais somente pode ser feita de maneira direta caso a criança (o texto normativo utiliza tal termo) tenha no mínimo dezesseis anos, caso contrário, a oferta deverá ser aceita apenas com o consentimento dos responsáveis legais (art. 8º do GPDR).

O artigo 30 regula os registros de atividades de tratamento, ou seja, a manutenção dos processos e sistemas de segurança da informação (SI). O artigo 40 determina para os Estados-Membros, as autoridades de controle, o Comitê Europeu para a Proteção de Dados e a Comissão Europeia a obrigatoriedade de elaboração de códigos de conduta para a aplicação do GDPR. O regulamento determina ainda a criação de políticas para a certificação em matéria de proteção de dados com o objetivo de comprovar a conformidade da empresa de tratamento de dados com o regulamento. No entanto, apesar da exigência de certificações (ISSO 27001 e 27002, ITIL e outros), a sua adesão pelos responsáveis pelo tratamento das informações digitais é voluntária.

O GDPR explicita também sobre o processo de transferência internacional de dados entre organizações e outros Estados (artigo 44), a qual somente poderá ser realizada se as condições "forem respeitadas pelo responsável pelo tratamento e pelo subcontratante, inclusivamente no que diz respeito às transferências ulteriores de dados pessoais do país terceiro ou da organização internacional para outro país terceiro ou outra organização internacional".

E, finalmente, nos artigos 55 a 58 do GDPR, sistematiza-se a fundação de uma entidade pública que tenha independência para atuar sobre a proteção de dados, ordenando, para tanto, que os seus dirigentes sejam independentes, com um processo de escolha transparente, estabilidade e período de mandato fixo de no mínimo 4 anos. Tais entidades dos Estados, como principais atribuições, deverão monitorar e fazer aplicar de forma correta o GDPR, promover políticas de conscientização da população, aconselhar os Poderes Públicos quanto a sua especialidade, prestar informações, criar normas para o setor regulado, receber reclamações, conduzir investigações e sancionar.

Por todos estes elementos normativos, o GDPR é marco legal mundial na proteção de dados pessoais e tutela da privacidade e direitos fundamentais, visto que o preâmbulo 2 e 13 do GDPR apontam como objetivo: contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união econômica, para o progresso econômico e social, a consolidação e a convergência das economias no nível do mercado interno e para o bem-estar das pessoas físicas.

3. A PROTEÇÃO JURÍDICA EXISTENTE NO BRASIL ATÉ 2018

Uma das primeiras legislações específicas sobre a proteção de dados pessoais foi a Lei nº 12.737/2012[537], conhecida como Lei "Carolina Dieckmann"[538], a qual acrescentou ao artigo 154-A ao Código Penal, tipificando o crime de "invasão de dispositivo informático". Tal crime dispõe que a invasão de dispositivo informático alheio, mediante violação, para obter, adulterar ou destruir dados sem autorização do titular do dispositivo tem como consequência uma pena de três meses a um ano e multa.

Nacionalmente, a proteção de dados no Brasil ganhou relevância com a Lei nº 12.965/2014[539], conhecida como "Marco Civil da Internet", a qual estabelece princípios, direitos e deveres para o uso da Internet no Brasil, bem como prevê as diretrizes para a atuação dos entes federativos na proteção, difusão e acessibilidade da rede mundial de computadores. Para o recorte metodológico proposto nesse artigo, analisa-se somente a norma no que tange à proteção de dados pessoais na Internet.

Disciplinou-se na lei brasileira oito princípios para o uso da Internet (art. 3º): a) a garantia da liberdade de expressão; b) proteção da privacidade; c) a proteção dos dados pessoais; d) a preservação da neutralidade da rede; e) a preservação da estabilidade, segurança e funcionalidade da internet; f) a responsabilização dos agentes de acordo com suas atividades; g) a garantia da natureza participativa da rede; h) a liberdade dos modelos de negócios promovidos na Internet.

Além disso, garantiu-se ao usuário, quanto à proteção de seus dados, a inviolabilidade de sua intimidade e vida privada; o sigilo do fluxo de suas comunicações via Internet; proteção e sigilo das suas comunicações privadas armazenadas; a previsão de informações claras e completas nos contratos de prestação de serviços; o não fornecimento a terceiros de informações pessoais, salvo se consentido; e a transparência contratual quanto ao uso, tratamento e armazenamento de dados pessoais (art. 7º).

No artigo 14, prevê-se que "na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet". No artigo 16, veda-se a guarda de registros de acesso à Internet sem consentimento do titular e de dados pessoais que sejam excessivos em relação à finalidade consentida. Tais medidas tem fundamento

537 Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 09 jun. 2019.

538 O que chamou atenção sobre a Lei Carolina Dieckmann é que a mobilização do Congresso Nacional para a promulgação da lei teve como causa a ampla influência da mídia na construção legislativa, demonstrando que o poder da comunicação existente com os inúmeros meios digitais é presente. (CALEFFI, 2015, p.119).

539 Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 09 jun. 2019.

técnico e jurídico de modo a não violar a privacidade nem ir além do consentido por meio de técnicas computacionais, incluindo-se o tratamento de dados pessoais.

Contudo, Marco Civil da Internet, sobre a óptica da proteção de captação e armazenamento de dados pessoais, não solucionou e tampouco esgotou o tema, não trazendo efeitos práticos. A legislação trouxe discussões acerca de temas previstos na Constituição Federal, Código Civil e Código de Defesa do Consumidor, que já asseguravam o direito à privacidade e intimidade, aplicáveis às informações pessoais digitais ou não (CUNHA; LIMA, 2015, p.109).

O Código de Defesa do Consumidor (CDC)[540], por exemplo, já assegurava em 1990, em seu artigo 43, o acesso a dados pessoais que estiverem em cadastros, registros ou fichas arquivadas. Outrossim, o instrumento do *Habeas Data* genericamente pode ser utilizado como um meio processual legítimo para a obtenção e correção de informações pessoais na seara digital. De modo complementar, o Mandado de Segurança constitui outro remédio constitucional que possibilita a obtenção e correção de informações pessoais digitais. Do mesmo modo, Machado (2015, p.44) concorda que o panorama do ordenamento jurídico pátrio era insatisfatório para uma efetiva tutela da privacidade, tratando especificamente da privacidade informacional, visto que os instrumentos jurídicos até então não tratavam especificamente da tutela de dados pessoais. A autora afirma que a proteção da privacidade informacional possui um caráter muito mais específico do que outros desdobramentos do direto da personalidade. Principalmente, se aos dados pessoais forem incluídos os dados pessoais sensíveis, tutelados tanto no GDPR quanto na atual LGPD.

4. OS IMPACTOS DO GDPR NA LGPD[541]

Tem-se em mente que as noções e as concepções do Direito Europeu são, obviamente, diferentes do entendimento do ordenamento jurídico brasileiro, uma vez que existem contextos históricos, padrões econômicos, costumes, idiomas e sistemas jurídicos diferentes. Isso exposto, é necessário trazer a ideia central da proteção de dados pessoais tanto na GDPR quanto na LGPD, ou seja, a proteção da privacidade; cabendo questionar: sob a óptica de James Q. Whitman (2004, p.1154): Se a privacidade é uma prerrogativa humana universal que emerge como um direito fundamental, por que ela possui concepções diferentes para sistemas jurídicos distintos?

Whitman (2004, p.1157-1171) compreende que, na legislação americana, a proteção à privacidade é menor do que se comparado com o contexto da EU. Na Europa

540 Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em: 09 jun. 2019.

541 O texto legal da LGPD está disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 09 jun. 2019.

continental, a proteção à privacidade é uma forma de proteção do direito ao respeito e à dignidade humana (direito à imagem, ao nome, à reputação e à autodeterminação informativa). O principal "inimigo" à privacidade na concepção europeia é a mídia ou qualquer outro agente que possa ameaçar a divulgação de dados. Na Europa, há uma preocupação em garantir um tratamento à proteção da pessoa em relação aos demais.

O contexto brasileiro para a proteção da privacidade é um pouco sutil e delicado comparado com ordenamentos estrangeiros. Observada a Constituição Federal de 1988, nota-se que há uma abrangência na preservação da vida privada do cidadão, assegurando a intimidade, a vida privada, a honra e imagem das pessoas e o direito a indenização caso ocorra sua violação (art. 5º, inciso X, CF/88)[542]. Porém, desde de 2012, tramitava um projeto de lei destinado especificamente à proteção de dados pessoais na Internet, o qual após um processo histórico legislativo complexo, foi sancionado em 14 de agosto de 2018, estabelecendo o que se conhece atualmente como Lei Geral de Proteção de Dados (LGPD). Coincidentemente a lei foi aprovada pelo corpo legislativo na mesma época que emergiu a problemática da exposição de dados com a crise *Cambridge Analytica/Facebook*.

O que se constatou, e que é apresentado neste artigo, é que a lei brasileira foi inspirada largamente na GDPR, estabelecendo princípios, diretivas, obrigações, direitos e instituindo novas entidades para a proteção de dados.

A LGPD define que "dado pessoal" é "informação relacionada a pessoa natural identificada ou identifi ável" (art. 5º, inciso I). Além disso, define também "dado pessoal sensível": "dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiaçã a sindicato ou a organização de caráter religioso, filosófic ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico" (art. 5º, inciso II). Ambos importantíssimos tanto do ponto de vista jurídico quanto tecnológico, pois 'dado' é o objeto foco da LGPD e do tratamento de dados.

Os arts. 7º e 8º tratam do tratamento e do consentimento pelo titular, afirmando que é vedado o uso sem tal requisito. Este ponto demonstra a influência da GDPR na LGPD, frente aos requisitos aplicados ao tratamento de dados pessoais. O tratamento de dados a que se refere a LGPD tem foco na boa-fé e na especificação da finalidade, dos limites, na prestação de contas, na garantia da segurança por meio de técnicas e medidas de segurança, bem como na transparência e direito de acesso por parte dos titulares. O GDPR também pontua a liberdade de escolha do titular frente ao consentimento.

No art. 9º, a LGPD afirma que o titular tem o direito ao acesso facilitado às informações sobre o tratamento de seus dados, sendo que o GDPR também preza pela transparência de tais informações, desde o consentimento até a revogação deste,

542 Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao-compilado.htm>. Acesso em: 09 jun. 2019.

cabendo ao agente oferecer as informações de modo claro e de fácil acesso. Sem esquecer o legítimo interesse, pautado na LGPD no artigo 10, sendo que o GDPR impõe restrições à atuação tanto do sujeito que realiza tratamento de dados quanto do Estado.

Nos artigos 15 e 16, a LGPD prevê as hipóteses, aparentemente não exaustivas, do término de tratamento de dados pessoais, devendo os dados tratados serem eliminados, contudo, podendo ser mantidos, por exemplo, para cumprimento de obrigação legal do responsável ou uso exclusivo do responsável desde que anonimizados. O preâmbulo 39 do GDPR pontua a limitação e imposição de prazos ao tratamento de dados, vinculado diretamente com a finalidade de tal procedimento. O GDPR se diferencia da LGPD no que tange a vinculação dos prazos à necessidade do processo, de modo que a limitação de tempo obriga o controlador a realizar a eliminação ou a revisão dos dados coletados, sendo os prazos determinados de acordo com a finalidade do tratamento.

O artigo 18 da LGPD aponta extensivamente os direitos dos titulares dos dados, desde o direito de confirmar a existência de algum tratamento até a revogação do consentimento, passando pelo acesso, correção, anonimização, bloqueio ou eliminação e portabilidade. O GDPR expressa nos artigos 12 a 15, 22 e 34 os direitos dos titulares de dados. Nos aritogs 16 e 17, o GDPR explicita o direito de retificação e o direito de ser esquecido, aqui relacionado diretamente com os direitos fundamentais e os Direitos Humanos.

Quanto ao consentimento, a LGPD assentiu que o indivíduo possui o poder de exercer de maneira absoluta o que lhe diz respeito. Ademais, "não se está tratando do consentimento negocial, mas sim de consentimento para tratamento de dados pessoais, que é bem mais específico do que aquele concedido para a celebração de contratos, por exemplo" (MACHADO, 2015, p.55-67); isso porque ele não possui uma natureza negocial, mas é um direito diretamente ligado à personalidade. Bioni (2019, p. 136) afirma que o consentimento permanece, ao longo das gerações[543] de leis de proteção de dados, como o "elemento nuclear da estratégia regulatória da privacidade informacional", de modo a "... apostar no indivíduo como um ser capaz, racional e hábil para controlar as suas informações pessoais". O autor então pondera que há que se balancear soluções que, "... por um lado, empoderem o titular dos dados pessoais, e, por outro lado, não deixem apenas sobre seus ombros a proteção de suas informações pessoais" (BIONI, 2019, p. 137).

Tal qual na GDPR (artigos 24, 25, 26, 30, 40 a 43), a LGPD prevê a manutenção dos registros das operações de tratamento de dados pessoais (artigo 37), sendo que o controlador elaborará relatório de impacto à proteção de dados pessoais (artigo

543 O autor aponta que existem quatro gerações de leis de proteção de dados pessoais. Ver: BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2ª. ed. Rio de Janeiro: Forense, 2019. p. 114-117.

38), medida esta estritamente técnica que visa a mitigação dos riscos jurídicos e tecnológicos, de modo que o operador do tratamento de dados responde civilmente por qualquer dano causado, em violação à legislação protetiva de dados pessoais (artigo 42), cabendo a adoção de programas de governança em privacidade (artigo 50). Há que se pensar na proteção de dados desde a concepção do tratamento (*privacy by design*), respeitando o que a Segurança da Informação (SI) recomenda e preconiza (ISO 27001, 27002 e ITIL).

É compreensível que a efetividade do direito à privacidade depende de uma ação positiva por parte da Administração Pública, tendo o dever de implementar medidas administrativas e legislativas (MACHADO, 2015, p.62). Mas, se por um lado é necessário o exercício do poder regulatório por parte do Poder Público para a efetividade dos direitos informacionais, de outro, deve-se estabelecer os meios formais e materiais de maneira correta para garantir duas noções elementares à nova instituição: segurança jurídica e transparência.

Finalmente, o que se percebe é que, diferentemente da legislação europeia, a legislação brasileira é muito mais vasta e, consequentemente, prolixa no que se refere à proteção da privacidade e de dados pessoais. Emerge-se, assim, uma questão para refl xão: é realmente necessária uma abordagem legiferante tão repetitiva? Ao se estar em um momento em que se adota um novo modelo de interpretação constitucional, afastando-se de um modelo de regras aplicáveis mediante subsunção e se amparando num modelo em que há "o resgate de valores, a distinção qualitativa entre princípios e regras, a centralidade dos direitos fundamentais e a reaproximação entre o Direito e a ética" (BARROSO; BARCELLOS, 2003, p.174), a disposição repetitiva sobre o tema força o entendimento que o operador do direito brasileiro não consegue interpretar lógica e sistematicamente o ordenamento jurídico, devendo a lei "facilitar" a prática interpretativa.

O movimento global de proteção de dados pessoais é premente no mundo. Em ambos, GDPR e LGPD, é possível encontrar 05 (cinco) objetos principais: a) a criação de uma autoridade estatal supervisora do tratamento de dados; b) a delimitação sobre o que é relevante juridicamente quanto ao manuseio de dados pessoais seja me formato digital ou não; c) a descrição de direitos e garantias do titular de dados; d) a tipificação de penas em caso de ofensa à direitos; a legitimação do direito fundamental da privacidade em meio digital como um ramo do direito à privacidade; e) a previsão de responsabilização dos agentes de tratamento de dados.

5. Considerações Finais

É sabido que o respeito à privacidade e à proteção de dados pessoais devem ser compreendidos como elementares para o desenvolvimento e sustentabilidade de uma sociedade democrática, bem como para o exercício de incontáveis direitos fundamentais. Fato é que na era digital o comportamento individual transformou-se numa conduta conjunta à comunidade, com os efeitos de um ato realizado na sociedade em rede ultrapassando a esfera da intimidade (LIMA, 2013, p.281). Portanto, a proteção jurídica ao tratamento de dados pessoais adveio em momento oportuno, não somente pelas constantes notícias de invasão de bases de dados, uso indevido de informações privadas e perquirições ilegais do governo no mundo digital, mas também pela necessidade de uma resposta do Estado à nova realidade digital. GDPR e LGPD são necessários para o atendimento legal efetivo dos novos serviços e atividades econômicas que surgem constantemente. Dessa maneira, o artigo trouxe uma breve explanação do GDPR, frente a sua importância no meio digital, bem como assentiu sua influência sobre o ordenamento jurídico pátrio. Assim, tanto o regulamento europeu quanto a lei brasileira, precisam ter em mente que o *compliance* jurídico não é sufi iente para englobar e fazer cumprir tais textos legais, uma vez que a interseção do Direito e da Informática nunca estiveram tão próximos. Somente com o Direito e a Tecnologia unidos será possível caminhar no plano sentido de proteção de dados e privacidade sem ambiguidades, inexatidões.

REFERÊNCIAS

BARROSO, Luís Roberto; BARCELLOS, Ana Paula. O começo da história: a nova interpretação constitucional e o papel dos princípios do direito brasileiro. **Revista de Direito Administrativo.** Rio de Janeiro, v. 232, p.141-176, abr./jun. 2003.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2ª. ed. Rio de Janeiro: Forense, 2019.

CALEFFI, Renata. **Estratégias políticas de comunicação:** o papel do telejornal na construção legislativa brasileira (Lei Carolina Dieckmann, Lei Seca e Projeto de Emenda Constitucional para redução da maioridade penal). 126 f. Dissertação (Mestrado em Comunicação) – UFPR, 2015.

CUNHA, Renata Silva. LIMA, Marco Antônio. Captação de dados pessoais e a ótica do marco civil da internet. **Revista FMU Direito,** São Paulo, v.29, n.43, p.102-112, 2015.

KUNER, Christopher. The European Commission's Proposed Data Protection Regulation: a Copernican revolution in European data protection law. **Bloomberg**

BNA Privacy and Security Law Report, p. 1-27, fev. 2012.

LIMA, Erike Noleta Kirk Palma. Direito ao esquecimento: discussão europeia e sua repercussão no Brasil. **Revista de Informação Legislativa.** v.50, n.199, p.271-283, jul./set. 2013.

MACHADO, Joana de Moares Souza. A tutela da privacidade no controle de dados pessoais no direito brasileiro. **Arquivo Jurídico.** Teresina, v.2, n.2, p.,43-65, jul./dez. 2015.

RONCOLATO, Murilo. **O uso ilegal de dados do Facebook pela Cambridge Analytica e o que há de novo.** Disponível em: <https://www.nexojornal.com.br/expresso/2018/03/19/O-uso-ilegal-de-dados-do-Facebook-pela-Cambridge-Analytica.-E-o-que-há-de-novo>. Acesso em: 09 jun. 2019.

WATCHER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a right to explanation of automated decision-making does not exist in the Genereal Data Protection Regulation. **International Data Privacy Law.** Oxford, v.7, n. 2, p. 76-99, 2017.

WHITMAN, James Q. The two western cultures of privacy: dignity versus liberty. **The Yale Law Journal**, n.113, p. 1192, 2004.

ZWEIGERT, Konrad; KÖTZ, Hein. **An introduction to Comparative Law.** 3. ed. OXFORD: Oxford University Press, 1996.

AS GARANTIAS DE INDEPENDÊNCIA DAS AUTORIDADES DE PROTEÇÃO DE DADOS: VISÃO COMPARADA ENTRE O REGULAMENTO DA UNIÃO EUROPEIA E A LGPD

Eixo temático: A nova lei brasileira de proteção de dados pessoais (LGPD) E O GDPR europeu

Autor:
Mártin M. Szinvelski
Advogado. Mestrando em Direito Público
Programa de Pós-Graduação em Direito da Universidade do Vale do Rio dos Sinos (CAPES 6)
Bolsista do Conselho de Aperfeiçoamento de Pessoal em Nível Superior/
Programa de Excelência Acadêmica (CAPES/PROEX).
Membro do Grupo de Pesquisa CNPq *Estado, Administração Pública e Novas Tecnologias*, Coordenado pela Profa. Dra. Têmis Limberger.
E-mail: martin_ms@live.com.

RESUMO
Qual o modelo de Autoridade Nacional de Proteção de Dados (ANPD) adequado à realidade brasileira? Essa situação-problema, exigente do ponto de vista da resposta, mas de simples formulação, leva em conta a recente incorporação na *Lei Geral de Proteção de Dados* (Lei n.º 13.709/2018) do modelo de ANPD vinculado à Presidência da República que, todavia, resguarda autonomia técnica ao órgão da administração federal criado. Debate-se a necessidade de uma estruturação em forma de *autoridade independente*, de acordo com o modelo europeu consolidado e recentemente atualizado pelo *Regulamento de Proteção de Dados da União Europeia (RGPD – UE 2016/679)*. Do ponto de vista metodológico, cumpre salientar que se emprega, no presente trabalho, a pesquisa exploratória, utilizando-se como procedimento de pesquisa a comparação legislativa. Conclui-se que a LGPD não respeita as garantias substanciais de independência da autoridade, no sentido de dotar a ANPD de autonomia funcional e política, embora respeite algumas prerrogativas formais de independência, especialmente aos membros do Conselho Diretor, à exceção garantia formal da administrativo-financeira.

I. INTRODUÇÃO

A mutação do Direito Administrativo na *era da internet* tem assumido graus de irreversibilidade[544]. Assiste-se, do ponto de vista da proteção dos dados pessoais,

544 Ressalta Pinãr Mañas, que "(...) cuando hablamos de las posibilidades que ofrece el uso de nuevas tecnologías, que en gran parte giran en torno a Internet, no hablamos de ciencia ficción

a *revisão global* do sistema protetivo[545]. Ainda que inacabada, a superação da noção westfaliana do Estado tende a resultar no modelo caracterizado pela *interestatalidade em rede*, desta vez, regida pelos contornos de uma *sociedade de cunho liberal e heterárquica*[546]. Não podemos olvidar a dualidade desse *tipo* de sociedade: de um lado, o *apreço* ao desempenho econômico e social; de outro, o *preço* da busca incessante pelos melhores resultados: o esgotamento físico e intelectual do ser humano. Fator que contribui para o arranjo que se encena é a imensa carga de dados e informações transmitidas e tratadas pelos setores público e privado, que demandam proteção regulatória às organizações e aos cidadãos.

Observa-se, nessa perspectiva, a consolidação do tratamento uniforme da matéria de proteção de dados e dos instrumentos estatais por meio dos quais a proteção se viabiliza, exemplo do qual se filia o Autoridade Europeia para a Proteção de Dados (AEPD)[547] e o modelo de autoridades independentes nacionais reforçado pelo Regulamento Europeu EU 2016/679. Falta, no entanto, conforme já denunciava Amato[548], restringir e racionalizar o que se entende por *autoridade independente*, porquanto o simples fato de denominar um órgão administrativo como independente ou com *autonomia técnica*, não garante a independência preceituada pelos padrões europeus. A premissa a qual partimos é relevante na discussão do modelo de autoridade

---

ni de una realidad ajurídica que no merece la atención del administrativista. La evolución que está produciéndose es vertiginosa y, como ya he apuntado en otra ocasión, exige "repensar" el concepto mismo de Administración y en consecuencia de Derecho Administrativo. Y ello porque, como apuntaba, las relaciones entre tecnologías del conocimiento y Derecho (también Derecho Administrativo) van a alterar no pocos de los paradigmas de la asignatura". Piñar Mañas, J. L., "Administración electrónica y protección de datos personales", *Revista Jurídica da Universidade de Santiago de Compostela*, n.1, 2011, p.149. No mesmo sentido, Juarez Freitas afirma que o "[…] Direito Administrativo, sem escapatória, precisa ser reinventado, incorporando temas como a personalidade digital (mais do que "electronic personhood") e, sobretudo, revendo as categorias tradicionais da polícia administrativa, da responsabilidade civil e do dever de fundamentação. Incontendivelmente, a regulação administrativa analógica não faz mais sentido. O modelo eletrônico, por sua vez, é insuficiente". Freitas, J., "Direito Administrativo e inteligência artificial", *Revista Interesse Púbico*, n. 114, 2019, p.24.

545 Do ponto de vista formal, nota-se a substituição de regulamentações em diferentes planos, notadamente pela revogação da Diretiva 95/46 pelo Regulamento Europeu de Proteção de Dados. Substancialmente, verifica-se o estabelecimento de regras ou diretrizes que objetivam mediar o impacto das novas tecnologias no tratamento de dados pessoais e, por conseguinte, na privacidade dos cidadãos. Para Piñar Mañas, *"[…] no es difícil constatar que la privacidad se ha convertido en uno de los derechos protagonistas de la sociedad de nuestros días, y parece que va a seguir siéndolo durante no poco tempo"* Piñar Mañas, J. L., "Sociedad, innovación y privacidad", *Información Comercial Española*, n. 897, 2017, p.70.

546 Nesse contexto, uma previsão responsável indica a *internet* como mecanismo que torna perceptível o fenômeno de interconexão social e estatal, não obstante a natureza fragmentada e sem contornos unitários que se apresenta. Sobre os primeiros indícios da mutação do Estado, cfr. Palombella, G., "Il rule of law oltre lo stato", *Rivista trimestrale di diritto pubblico*, n.2, 2009, p. 325-326.

547 Observe-se o que afirma Claudio Franchini a respeito do modelo comunitário que utiliza autoridades independentes. Franchini, C., "Autonomia e independenza nell'amministrazione europea", *Diritto amministrativo*, Milano, Giuffrè, 2008, n. 1, p. 91.

548 Veja-se que: *"[l]e autorità indipendenti, o meglio, le istituzione indiscriminatamente chiamate tal, sono vittime oggi dell'inesorabile fascinio che esercitano sempre, e anche sui piu avveduti, le semplificazione unificati. Chiunque ne tratti, all'inizio lo disse che ci sono delle diversità che bisogna saper distinguere."* Amato, G. "Autorità semi-indipendenti e autorità di garanzia", *Rivista trimestrale di diritto pubblico*, n.3, 1997. p.645.

de proteção de dados previsto na legislação brasileira que, se é bem verdade não estabelece a Autoridade Nacional de Proteção de Dados (ANPD) como autoridade independente, faz surgir no *imaginário* a existência da mencionada independência. Eis, portanto, o objeto de estudo do presente artigo: refletir sobre o *modelo de garantias de independência* adotado, comparando-as com modelo que preconiza o Regulamento Europeu 2016/679/CE[549], e a possibilidade de revisão pontual da legislação pátria desiderando outorgar independência institucional a Autoridade Nacional de Proteção de Dados.

II. PANORAMA

A *Lei Geral de Proteção de Dados* (*LGPD*/Lei n.º 13.709/2018)[550] dispôs sobre o tratamento de dados pessoais com o objetivo de *"[...] proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural"*[551]. Não conferiu, todavia, autonomia ao direito à proteção de dados[552] aos moldes da Carta de Direitos Fundamentais de Nice[553]. A *Medida Provisória n.º 869*, de 27 de dezembro de 2018, recentemente transformada em lei pelo Congresso Nacional, veio a suprir a lacuna de organização administrativa relativa ao vício formal que ensejou o veto da criação da Autoridade Nacional de Proteção de Dados (ANPD). Em contraste ao modelo previsto nos dispositivos vetados, o modelo adotado não confere personalidade jurídica à autoridade nacional, traço primeiro da caracterização de uma autoridade como independente.

Tradicionalmente, as autoridades nacionais assumem a função de tornarem-se as *guardiãs* do sistema nacional de proteção de dados e adotar medidas que equilibrem o respeito do direito fundamental à vida privada e a livre circulação de dados, resultante

549 Para uma introdução a análise comparativa ver: Robledo, E.P.L, "La nueva normativa europea para la protección de los datos personales", *Derechos y libertades*, Madrid, n. 40, 2019.

550 A lei brasileira faz referência à privacidade, à autodeterminação informativa, à liberdade de expressão, à inviolabilidade da intimidade, ao desenvolvimento tecnológico e à inovação, ao desenvolvimento da personalidade como fundamentos da proteção de dados. Para além disso, prevê princípios reconhecidos no âmbito comunitário europeu e nos países em que há regulação de proteção de dados, entre os quais encontra-se a prevenção (artigo 6.º, inciso VIII) e a responsabilização (artigo 6.º, inciso X), sendo que este último é conceituado pelo legislador como sendo a *"(...) demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas"*. Lei n.º 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Data da consulta: 5 de junho de 2019.

551 Lei n.º 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Data da consulta: 5 de junho de 2019.

552 Ver, no Brasil, Doneda, D., "A proteção dos dados pessoais como um direito fundamental", *Espaço Jurídico*, n.2, 2011.

553 Carta dos direitos fundamentais da união europeia. "Jornal Oficial das Comunidades Europeias. C364, p.18-19, 18 dez. 2000". Disponível em: <http://www.europarl.europa.eu/charter/pdf/text_pt.pdf >. Data da consulta: 20 de maio de 2019.

da inovação, do desenvolvimento econômico e tecnológico. Conforme destaca Piñar Mañas, no horizonte crítico da necessidade de independência, *"[...] se presume que, faltando esa autoridad, no es posible en ningún caso considerar aceptable el marco jurídico regulador del derecho"*[554]. Há de se convir que a existência da autoridade brasileira, por si, é um avanço, levando-se em conta *a possibilidade de sua ausência*; mas o fato é o modelo sobre o qual se estrutura – vinculado ao executivo – tende a não conferir *seriedade* e *segurança* (fiabilidade institucional) ao sistema regulatório de proteção de dados pessoais no Brasil. Aliás, conforme lecionam Schertel Mendes e Doneda *"[...] sem uma autoridade central, independente e com credibilidade técnica, dificilmente será possível a aplicação consistente e harmônica da Lei em setores tão diversos como aqueles que compõe seu âmbito de aplicação"*[555].

III. AUTORIDADES INDEPENDENTES: COMPARAÇÃO ENTRE AS DISPOSIÇÕES DA UNIÃO EUROPEIA E A DA LEI BRASILEIRA DE PROTEÇÃO DE DADOS

A criação de autoridades independentes leva em conta o interesse de dotar a ação pública de certa *continuidade diretiva* e, ao mesmo tempo, conferir aparência de *neutralidade*, *objetividade* e *apoliticidade*[556]. Em regra, cuida-se do estabelecimento de uma legitimação técnica da ação dos poderes públicos em temáticas sensíveis e que demandem certa especialização[557]. No âmbito de uma *escala de independência*, o contraste entre os órgãos administrativos e os independentes residiria no fato de que os primeiros exerceriam suas competências na forma de *independência contida* e, os últimos, ocupariam a posição de pessoas jurídicas com personalidade própria, as quais passariam a exercer suas funções como centros autônomos de decisão e atuação[558], e atender, segundo La Spina, os requisitos de possuir *(i)* poder regulativo incisivo e focalizado, *(ii)* alta competência especializada e *(iii)* independência de pressões políticas ou oriundas do setor privado[559].

A definição contextualizada[560] de autoridade independente guarda relação com a ideia de ente especializado, com personalidade jurídica própria, que desempenha

554 Piñar Mañas, J. L., "Administración electrónica y protección de datos personales", *Revista Jurídica da Universidade de Santiago de Compostela*, n.1, 2011, pág.167.

555 Schertel Mendes, L.; Doneda, D. "Refl xões gerais sobre a nova lei de proteção de dados", *Revista do Direito do Consumidor*, v.120, 2018, pág. 45.

556 Anota Franchini que "[...] In teoria, questo tipo di autorità dovrebbe caratterizzarsi per la funzione di limitazione dei fattori di natura politica, burocratica ed economica che possono venire ad incidere su interessi collettivi particolarmente sensibili". Franchini, C., "Mito e realtà delle autorità indipendenti", *Impresa e Stato*, 1996, n. 35, p. 29.

557 Fernández Rojas, G., "Las administraciones independientes de regulación y supervisión en España", *Vniversitas*, n. 109, 2005.

558 Pomed Sánchez, L. A. "Fundamento y naturaleza jurídica de las administraciones independientes". Revista de Administración Pública, v.132, 1993.

559 La Spina, A., *Lo Stato Regolatore*, Il Mulino, Bolonha, 2000, p.194.

560 Manetti, M., "Autorità indipendenti: tre signifi ati per una costituzionalizzazione", *Po-*

a função de ordenação de determinado setor à margem do poder de direção e tutela tradicionalmente associados a administração central, e que goza de autonomia técnica, financeira e de pessoal[561]. Em outros termos, a independência designa um estatuto que assegura ao órgão em causa a possibilidade de agir com toda a liberdade, ao abrigo de qualquer instrução ou pressão política ou financeira. Não significa, todavia, que a autoridade está imune a controles democráticos, pelo contrário: se submete aos controles de natureza democrático e institucional (controle social, legislativo, judicial e de contas).

Ao contrário da Diretiva 95/46/CE, que tratou brevemente da autoridade de controle de proteção de dados, limitando-se a indicar que o exercício das suas funções se desenvolveria com *"total independência"*[562], o Regulamento Europeu 2016/679/CE indicou *garantias substanciais e formais de independência* das autoridades, abaixo analisadas e confrontadas com a previsão normativa brasileira[563]. A análise comparativa em questão assume relevância, em razão de que as transferências de dados pessoais com países não-integrantes da União Europeia apenas serão permitidas se existir adequação ao nível de proteção previsto no Regulamento Europeu. À independência das autoridades nacionais de proteção de dados é reserva importância na União Europeia, tanto que, em 2010, a Alemanha foi punida por submeter à tutela e controle do governo federal as autoridades de controle competentes para fisc lizar o tratamento de dados pessoais nos diferentes *Länder*[564].

---

*litica del diritto, Rivista trimestrale di cultura giuridica fondata e diretta da Stefano Rodot*à, Il Mulino, n.4, 1997, pág. 657.

561 Reigada, A. T., "Las agencias de protección de datos como administración independiente", *Las Administraciones independientes*, coords. Cristina Pauner Chulvi, Beatriz Tomás Mallén, 2009, p.27-29.

562 Veja-se que o *Considerando 117* do Regulamento reproduz a ideia que as autoridades de controle são *"[...] habilitadas a desempenhar as suas funções e a exercer os seus poderes com total independência"*. Trata-se em boa medida de uma tradução do que já dispunha o artigo 8.º, parágrafo 3.º, da Carta dos Direitos Fundamentais da União Europeia. que estabeleceu que o *"[...] cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente"* e o que, de forma semelhante, reproduz o trecho final da redação do parágrafo 2.º do artigo 16 do Tratado de Funcionamento da União Europeia (TFUE), que possui a seguinte redação a *"[...] observância dessas normas fica sujeita ao controlo de autoridades independentes"*. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho*, de 27 de abril de 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>. Acesso em 1 jun. 2019.; Carta dos direitos fundamentais da união europeia. "Jornal Oficial das Comunidades Europeias. C364, p.18-19, 18 dez. 2000". Disponível em: <http://www.europarl.europa.eu/charter/pdf/text_pt.pdf >. Data da consulta: 20 de maio de 2019. *Tratado sobre o Funcionamento da União Europeia*. Disponível em: < https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e-6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF>. Acesso em: 1 jun. 2019.

563 Laita estabelece, ainda, um importante aspecto a ser considerado no tocante à independencia das autoridades:*"[...] la Agencia es independiente funcionalmente, ya que la toma de decisiones se produce sin intromisión del poder legislativo, ejecutivo y judicial, sometiendo a su control tanto al sector público como privado. La Agencia también es independiente organizativamente, como se ha puesto de manifiesto en cuanto al nombramiento del Director de la Agencia. Además, la Agencia también es independiente jurídicamente, ya que tiene competencia para la elaboración y aprobación de sus propias instrucciones y sus actos agotan la vía administrativa"*. Laita, I. G., "Independencia y régimen jurídico de la agencia española de protección de datos". *Las Administraciones independientes*, coords. Cristina Pauner Chulvi, Beatriz Tomás Mallén, 2009, p.225.

564 Prevaleceu, no caso em debate, interpretação da Autoridade Europeia de Proteção de

Dentre as inovações do Regulamento Europeu 2016/679/CE, no aspecto das autoridades nacionais, está o incremento das denominadas *faculdades de enforcement*, no sentido de ampliar as capacidades investigatórias das autoridades, inclusive cooperação internacional com outras autoridades[565], o que é compatível com a tendência de reforço dos mecanismos de supervisão e de interconexão das organizações estatais. As competências foram, em boa parte, reproduzidas na *LGPD*, no artigo 55-J, com restrição na perspectiva da edição de normas regulamentares, qual a ANPD deverá respeitar mínima intervenção[566]. No entanto, a ausência de independência, que é o pilar da estrutura protetiva que segue a tradição europeia, inclusive como premissa para o fomento de uma cultura da "responsabilidade" e "autorregulação", poderá tornar as disposições que sugerem o reforço da supervisão *"um mero borrão no papel"*[567].

III.1 GARANTIA SUBSTANCIAL DA INDEPENDÊNCIA FUNCIONAL

Passaro é suficientemente claro ao afirmar que no âmbito das diferenças entre as garantias funcionais e estruturais, as primeiras guardam relação com *"(...) una struttura che esercita in modo pieno ed autoreferenziale una propria funzione"*[568]. Desse modo, o elemento caracterizador da independência funcional é a ausência de hierarquia e de subordinação com órgãos de outros poderes e das influências do setor privado, no sentido de dizer que se há uma função própria cominada em lei, esta será exercida sem qualquer interferência[569]. Consequência da personalidade jurídica própria, a garantia estrutura-se como figura híbrida (*formal* e *substancial)*, de modo a conferir estabilidade e confiança aos administrados de que a supervisão, regulação e aplicação de sanções no tocante à proteção de dados será conduzida de forma imune a influências de qualquer gênero. Conforme destaca Reigada, a independência desloca-se da finalidade da administração pública para se tornar um *meio* para o alcance dos objetivos estabelecidos

Dados (AEPD), que defendia uma interpretação ampla da expressão "com total independência" prevista na Diretiva 45/96, no sentido de que uma autoridade de controle deve estar isenta de qualquer influência, quer esta seja xercida por outras autoridades quer fora do quadro da Administração.

565 Lombarte, A. R. "De la «libertad informática» a la constitucionalización de nuevos derechos digitales (1978-2018)". *Revista de Derecho Político*, n.100, 2017.

566 Veja, sobre o poder normativo das agências reguladoras: Aragão, A. S., "O poder normativo das agências reguladoras independentes e o Estado democrático de Direito", *Revista de Informação Legislativa*, n. 148, 2000.

567 Cabe o registro ofertado por Franchini, no sentido de que "L'attribuzione di determinati poteri, dell'autonomia di gestione e di quella organizzatoria, di organico, finanziaria e contabile, da un lato, e la previsione di talune garanzie per i titolari degli uffici dall'altro, sono strumentali ai fini del concreto riconoscimento di una posizione di terzietà e di neutralità, poichè contribuiscono a disegnare la struttura giuridica idonea al miglior esercizio della funzione". Franchini, C., "Mito e realtà delle autorità indipendenti", *Impresa e Stato*, 1996, n. 35, p. 34.

568 Passaro, M., Le amministrazioni indipendenti, Torino, Giappichelli, 1996, p. 36.

569 Reigada, A. T., "Autoridades de control independientes". *Reglamento general de protección de datos: hacia un nuevo modelo europeo de protección de datos*, coords. José Luis Piñar Mañas, Miguel Recio Gayo, María Álvarez Caro, 2016.

pela legislação[570]. Aliás, a garantia estende-se desde a independência institucional à independência dos servidores e do Conselho Diretor[571]. No entanto, a legislação brasileira, até o presente momento, não se preocupou em estabelecer a mencionada independência funcional, seja por não garantir personalidade jurídica própria à autoridade, seja por vincular a ANPD à Presidência da República, da perspectiva de pessoal, financeira e de designação dos membros, esta última, sem controle prévio do Senado Federal.

III. 2 GARANTIA SUBSTANCIAL DA INDEPENDÊNCIA POLÍTICA

As autoridades nacionais de proteção de dados devem estar acima de qualquer suspeita de parcialidade, baseando-se na distinção entre atividade política e atividades de execução das funções estabelecidas na *LGPD*[572]. O mero risco de setores da política exercerem influência nas decisões das autoridades de controle é suficiente para impedir o exercício independente das suas funções e a caracterização da autoridade como independente. O ponto elementar da crítica em torno da criação da ANPD reside na vinculação da autoridade à Presidência da República e a possibilidade de indicação de nomes sem a sabatina do Senado Federal, *existindo possibilidade* captura política (não que isso ocorra). Note-se que, no Brasil, o intuito legislativo na concepção de agências reguladores buscou atender os requisitos de independência, relativas à ausência de subordinação hierárquica, ao mandato fixo e à estabilidade dos dirigentes, com vistas a reduzir interferências e ingerências políticas no âmbito de atuação agências[573]. Isso não significou, todavia, qualquer imunidade à contaminação política. Propõe-se, portanto, que as garantias sejam levadas a sério, não como ritos obrigatórios de

570 Reigada, A. T., "Autoridades de control independientes". *Reglamento general de protección de datos: hacia un nuevo modelo europeo de protección de datos*, coords. José Luis Piñar Mañas, Miguel Recio Gayo, María Álvarez Caro, 2016.

571 O Regulamento Europeu prevê que os *"[...] membros das autoridades de controlo não estão sujeitos a influências externas, diretas ou indiretas no desempenho das suas funções e no exercício dos seus poderes nos termos do presente regulamento, e não solicitam nem recebem instruções de outrem"*. Nesse sentido, o Tribunal de Justiça da União Europeia já decidiu que *"[...] independência exclui, designadamente, qualquer instrução e qualquer outra influência externa, sob qualquer forma, seja direta ou indireta, suscetíveis de orientar as suas decisões e que podem assim pôr em causa o cumprimento, pelas referidas autoridades, da sua função de estabelecer um justo equilíbrio entre a proteção do direito à vida privada e a livre circulação dos dados de natureza pessoal". Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho*, de 27 de abril de 2016.

572 Conforme destaca "L'indipendenza dalla politica delle autorità riguarda tanto l'esercizio delle funzioni quanto la composizione dell'autorità titolare della funzione". Griffi A. P., "Le Autorità amministrative indipendenti nell'ordinamento costituzionale: profili problematici di ieri e di oggi", *Rassegna di diritto pubblico europeo*, Napoli, Edizioni Scientifiche Italiane, 2015, pág. 16

573 Veja-se como exemplo o artigo 8, §2.º, da Lei n.º 9.472/97, que organiza os serviços de telecomunicações e a criação e funcionamento do órgão regulador – a ANATEL, dispondo que *"A natureza de autarquia especial conferida à Agência é caracterizada por independência administrativa, ausência de subordinação hierárquica, mandato fixo e estabilidade de seus dirigentes e autonomia financeira"*. Lei n.º 9.472, de 16 de julho de 1997. Dispõe sobre a organização dos serviços de telecomunicações (...). Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9472.htm>. Acesso em: 9 jun. 2019.

procedimento. Além disso, os conselheiros e diretores são indicados pelo Presidente da República e investidos no cargo após a aprovação da indicação pelo Senado Federal, que verifica o atendimento dos critérios de investidura[574]. No entanto, conforme se verá abaixo, a indicação do Diretor-Presidente e do Conselho Diretor da ANPD ocorre sem a intervenção do Senado Federal, nos termos da *alínea f do inciso III do art. 52 da Constituição da República*, cuja remissão poderia ter sido feita pela *LGPD*[575].

III. 3 GARANTIA FORMAIS DE INDEPENDÊNCIA AOS MEMBROS DA AUTORIDADE DE CONTROLE

O Regulamento Europeu é um avanço em termos de garantias formais de independência dos membros das autoridades de controle, que não estavam presentes na Diretiva 95/46/CE. As garantias formais aplicam-se aos membros da autoridade, a duração do mandato, a forma e os requisitos de nomeação, a inamovibilidade e a incompatibilidade[576]. O Regulamento estabelece que os membros das respetivas autoridades de controle serão nomeados por *procedimento transparente*, seja pelo Parlamento, pelo Governo, pelo Chefe de Estado, ou por um organismo independente incumbido da nomeação nos termos do Direito do Estado-Membro.

No Brasil, o artigo 55-D, §2.º, prevê que os *"[...] membros do Conselho Diretor serão escolhidos dentre brasileiros, de reputação ilibada, com nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados"*. Veja-se que não há sabatina no Senado Federal, como no caso da Agência Nacional do Petróleo[577] e da Agência Nacional de Telecomunicações[578] e a nomeação afigura-se como escolha do

574 Veja-se o critérios elencados pela Lei n.º 9.472/97, no artigo 23: *"Os conselheiros serão brasileiros de reputação ilibada, formação universitária e elevado conceito no campo de sua especialidade, devendo ser escolhidos pelo Presidente da República e por ele nomeados, após aprovação pelo Senado Federal, nos termos da alínea f do inciso III do art. 52 da Constituição Federal"*. Lei n.º 9.472, de 16 de julho de 1997. Dispõe sobre a organização dos serviços de telecomunicações (...). Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9472.htm>. Acesso em: 9 jun. 2019.

575 Veja-se a inovação trazida pela Lei 13.848, de 25 de junho de 2019. Dispõe sobre a gestão, a organização, o processo decisório e o controle social das agências reguladoras. Disponível em: <http://www.in.gov.br/web/dou/-/lei-n-13.848-de-25-de-junho-de-2019-173020593>. Acesso em 1.º jul.2019.

576 Reigada, A. T.,"Autoridades de control independientes". *Reglamento general de protección de datos: hacia un nuevo modelo europeo de protección de datos*, coords. José Luis Piñar Mañas, Miguel Recio Gayo, María Álvarez Caro, 2016.

577 *"Art. 11 A ANP será dirigida, em regime de colegiado, por uma Diretoria composta de um Diretor-Geral e quatro Diretores. [...] "*§ 2º Os membros da Diretoria serão nomeados pelo Presidente da República, após aprovação dos respectivos nomes pelo Senado Federal*[...]"*. Lei n.º 9.478, de 6 de agosto de 1997. Dispõe sobre a política energética nacional, as atividades relativas ao monopólio do petróleo, institui o Conselho Nacional de Política Energética e a Agência Nacional do Petróleo e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9478.htm>. Acesso em: 9 jun. 2019.

578 Lei n.º 9.472, de 16 de julho de 1997. Dispõe sobre a organização dos serviços de telecomunicações (...). Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9472.htm>. Acesso em: 9 jun. 2019.

Presidente da República – no sentido de ampla discricionariedade – no âmbito dos quatro requisitos fixad s pela lei, quais sejam: *(i)* ser brasileiro; *(ii)* ter reputação ilibada; *(iii)* possuir nível superior e *(iv)* elevado conceito no campo de especialidade do cargo que desempenhará[579]. Sustenta-se, em termos de independência da ANPD, que a indicação dos membros do Conselho fosse realizada por organismo independente ou que as investiduras nos cargos do Conselho ocorressem após da avaliação dos requisitos pela maioria qualificada dos membros do Senado; ao menos, que normas orientadoras do procedimento conferissem maior transparência à escolha dos membros, tomando como base o modelo europeu.

Outra garantia formal prevista no Regulamento Europeu (artigo 51, n.º 4) vincula-se a noção de mandato fixo e da possibilidade de afastamento do cargo somente na hipótese de falta grave ou funcional: trata-se da garantia da inamovibilidade. A *LGPD* prevê mandato de quatro anos (o mínimo, se adotarmos como parâmetro a normatização comunitária europeia) cuja perda do cargo ocorrerá nas hipóteses de *(i)* renúncia, *(ii)* condenação judicial transitada em julgado ou *(iii)* pena de demissão decorrente de processo administrativo disciplinar.

A incompatibilidade é outra garantia formal prevista no artigo 52, n.º 3 do Regulamento Europeu consiste em garantir que os *"[…] membros da autoridade de controle abstêm-se de qualquer ato incompatível com as suas funções e, durante o seu mandato, não podem desempenhar nenhuma atividade, remunerada ou não, que com elas seja incompatível"*. Trata-se de garantia que busca afirmar a integridade da atuação e blinda, em tese, a captura da atuação das autoridades por interesses privados ou escusos. Nesse sentido, o artigo 55-F da *LGPD* faz referência ao art. 6º da Lei nº 12.813[580], que disciplina o *conflito de interesses na administração pública*, e comina sanção de improbidade administrativa em caso de configuração.

III. 4 GARANTIA FORMAL DE INDEPENDÊNCIA NO FUNCIONAMENTO DA AUTORIDADE

Quanto às garantias de independência relativas ao funcionamento da autoridade nacional, deve-se levar em consideração que, se adotarmos o *standard* europeu, a

579 A preocupação com a qualidade do profissional é referida no Regulamento Europeu, conforme se destaca: "Cada membro possui as habilitações, a experiência e os conhecimentos técnicos necessários, nomeadamente no domínio da proteção de dados pessoais, ao desempenho das suas funções e ao exercício dos seus poderes".

580 Lei n.º 12.813, de 16 de maio de 2013. Dispõe sobre o conflito de interesses no exercício de cargo ou emprego do Poder Executivo federal e impedimentos posteriores ao exercício do cargo ou emprego (...). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Lei/L12813.htm>. Acesso em 12 jul. 2019.

ANPD deverá selecionar e dispor sobre seu próprio pessoal. O *Considerando 121* do Regulamento Europeu prevê que a *"[...] autoridade de controle deverá dispor do seu próprio pessoal, selecionado por si mesma ou por um organismo independente criado nos termos do direito do Estado-Membro, que deverá estar exclusivamente sujeito à orientação do membro ou membros da autoridade de controle"*. Em contraste, até a regulamentação que estruture a ANPD, esta receberá o apoio técnico e administrativo da Casa Civil da Presidência da República e os cargos em comissão e as funções de confiança da ANPD serão remanejados de outros órgãos e entidades do Poder Executivo federal. Não há aqui, qualquer autonomia de pessoal e disponibilidade de recursos humanos por parte do Conselho Diretor da autoridade, muito menos previsão de concurso público relativamente à estruturação técnica da autoridade nacional, com a criação de cargos públicos, nos termos da Constituição.

Além disso, do ponto de vista financeiro, o artigo 55-A da Lei n.º 13.709/2018 cria a ANPD *"sem aumento de despesa"*, o que significa dizer que não há autonomia financeira em relação à Presidência da República. Nesse quesito, comparando apenas as disposições, o Regulamento Europeu prevê *"[...] cada autoridade de controlo fique sujeita a um controlo financeiro que não afete a sua independência e que disponha de orçamentos anuais separados e públicos, que poderão estar integrados no orçamento geral do Estado ou nacional"*. Nesse sentido, convém dizer que Sentença do Tribunal de Justiça da União Europeia manifestou-se, em 16 de outubro de 2012, pela desnecessidade de autonomia financeira à configuração da independência financeira, podendo ela restar, do ponto de vista financeiro, vinculada às verbas orçamentárias de determinado Ministério, desde que isso não afete a independência no exercício de funções. Resta saber qual medida será adotada, no Brasil, para o resguardo da autonomia financeira da ANPD: se previsão de rubrica *orçamentária destacada* no orçamento da União ou com vinculação orçamentária a determinado Ministério. No entanto, não se deve admitir que se atribua globalmente à Presidência da República a responsabilidade pelo custeio da ANPD, mesmo com fundamento na segurança nacional.

IV. CONCLUSÕES E APERFEIÇOAMENTO INSTITUCIONAL

O surgimento das administrações independentes[581] guarda relação com a crise de legalidade, consolidada pela expressão *fuga do direito administrativo*[582]. Cabe

581 Na França, as autoridades administrativas independentes surgiram como criação importante do direito público, por influência das *independent regulatory agencies*, mesmo que, naquele país, não se tenha conferido personalidade jurídica própria. Limberger, T., *O direito à intimidade na era da informática: a necessidade de proteção dos dados pessoais*, Livraria do Advogado Editora, Porto Alegre, 2007. págs. 138-139

582 Sánchez Morón, M., "El retorno del derecho administrativo", *Revista de Administración Pública*, n. 206, 2018, págs.37-66.

rememorar que o objeto do presente artigo foi estabelecer o quadro comparativo entre o Regulamento Europeu e *LGPD* em matéria de garantias de independência da autoridade nacional de proteção de dados. Podem-se traçar as seguintes conclusões:

1. Não há independência institucional da ANPD, do ponto de vista da personalidade jurídica, dada a vinculação à Presidência da República, de modo a desautorizar a denominação de "autoridade independente", com efeitos internacionais expressivos se considerarmos o padrão europeu.
2. Não há autonomia financeira da ANPD, em razão de ter sido criada "sem aumento de despesa", o que inviabiliza o gerenciamento financeiro e de pessoal por parte dos órgãos diretivos da autoridade.
3. Do ponto de vista da nomeação do Diretor-Presidente e Conselho Diretor, não há participação do Senado Federal, tornando a estruturação dos órgãos de direção mais suscetíveis a influências políticas, não sendo afetada pela Lei 13.848, de 25 de junho de 2019.
4. Ainda do ponto de vista da nomeação de dirigentes, o procedimento de escolha dos membros não é transparente, aos moldes do preceituado pelo Regulamento Europeu.
5. Existem garantias formais do ponto de vista da inamovibilidade dos dirigentes e da necessidade do exercício sem conflito de interesses que estão de acordo com o padrão europeu.

REFERÊNCIAS

Amato, G. "Autorità semi-indipendenti e autorità di garanzia", *Rivista trimestrale di diritto pubblico*, n.3, 1997. p.645.

Aragão, A. S., "O poder normativo das agências reguladoras independentes e o Estado democrático de Direito", *Revista de Informação Legislativa*, n. 148, 2000.

Carta dos direitos fundamentais da união europeia. "Jornal Oficial das Comunidades Europeias. C364, p.18-19, 18 dez. 2000". Disponível em: <http://www.europarl.europa.eu/charter/pdf/text_pt.pdf >. Data da consulta: 20 de maio de 2019.

Doneda, D., "A proteção dos dados pessoais como um direito fundamental", *Espaço Jurídico*, n.2, 2011.

Fernández Rojas, G., "Las administraciones independientes de regulación y supervisión en España", *Vniversitas*, n. 109, 2005.

Franchini, C., "Autonomia e independenza nell'amministrazione europea", *Diritto amministrativo*, Milano, Giuffrè, 2008, n. 1, p. 91

Franchini, C., "Mito e realtà delle autorità indipendenti", *Impresa e Stato*, 1996, n. 35, p. 29.

Freitas, J., "Direito Administrativo e inteligência artificial", *Revista Interesse Púbico*, n. 114, 2019, p.24.

Griffi A. P., "Le Autorità amministrative indipendenti nell'ordinamento costituzionale: profili problematici di ieri e di oggi", *Rassegna di diritto pubblico europeo*, Napoli, Edizioni Scientifiche Italiane, 2015, pág. 16

La Spina, A., *Lo Stato Regolatore*, Il Mulino, Bolonha, 2000, p.194.

Laita, I. G., "Independencia y régimen jurídico de la agencia española de protección de datos". *Las Administraciones independientes*, coords. Cristina Pauner Chulvi, Beatriz Tomás Mallén, 2009, p.225.

Lei 13.848, de 25 de junho de 2019. Dispõe sobre a gestão, a organização, o processo decisório e o controle social das agências reguladoras. Disponível em: <http://www.in.gov.br/web/dou/-/lei-n-13.848-de-25-de-junho-de-2019-173020593>. Acesso em 1.º jul.2019.

Lei n.º 12.813, de 16 de maio de 2013. Dispõe sobre o conflito de interesses no exercício de cargo ou emprego do Poder Executivo federal e impedimentos posteriores ao exercício do cargo ou emprego (...). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Lei/L12813.htm>. Acesso em 12 jul. 2019.

Lei n.º 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Data da consulta: 5 de junho de 2019.

Lei n.º 9.472, de 16 de julho de 1997. Dispõe sobre a organização dos serviços de telecomunicações (...). Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9472.htm>. Acesso em: 9 jun. 2019.

Lei n.º 9.478, de 6 de agosto de 1997. Dispõe sobre a política energética nacional, as atividades relativas ao monopólio do petróleo, institui o Conselho Nacional de Política Energética e a Agência Nacional do Petróleo e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9478.htm>. Acesso em: 9 jun. 2019.

Limberger, T., *O direito à intimidade na era da informática: a necessidade de proteção dos dados pessoais*, Livraria do Advogado Editora, Porto Alegre, 2007. págs. 138-139.

Lombarte, A. R. "De la «libertad informática» a la constitucionalización de nuevos derechos digitales (1978-2018)". *Revista de Derecho Político*, n.100, 2017.

Manetti, M., "Autorità indipendenti: tre significati per una costituzionalizzazione", *Politica del diritto, Rivista trimestrale di cultura giuridica fondata e diretta da Stefano Rodotà*, Il Mulino, n.4, 1997, pág. 657.

Palombella, G., "Il rule of law oltre lo stato", *Rivista trimestrale di diritto pubblico*, n.2, 2009, p. 325-326.

Passaro, M., Le amministrazioni indipendenti, Torino, Giappichelli, 1996, p. 36.

Piñar Mañas, J. L., "Administración electrónica y protección de datos personales", *Revista Jurídica da Universidade de Santiago de Compostela*, n.1, 2011, p.149.

Piñar Mañas, J. L., "Sociedad, innovación y privacidad", *Información Comercial Española*, n. 897, 2017, p.70.

Pomed Sánchez, L. A. "Fundamento y naturaleza jurídica de las administraciones independientes". Revista de Administración Pública, v.132, 1993.

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>. Acesso em 1 jun. 2019.

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

Reigada, A. T. "Autoridades de control independientes". *Reglamento general de protección de datos: hacia un nuevo modelo europeo de protección de datos*, coords. José Luis Piñar Mañas, Miguel Recio Gayo, María Álvarez Caro, 2016.

Reigada, A. T., "Las agencias de protección de datos como administración independiente", *Las Administraciones independientes*, coords. Cristina Pauner Chulvi, Beatriz Tomás Mallén, 2009, p.27-29.

Robledo, E.P.L, "La nueva normativa europea para la protección de los datos personales", *Derechos y libertades*, Madrid, n. 40, 2019.

Sánchez Morón, M., "El retorno del derecho administrativo", *Revista de Administración Pública*, n. 206, 2018, págs.37-66.

Schertel Mendes, L.; Doneda, D. "Refl xões gerais sobre a nova lei de proteção de dados", *Revista do Direito do Consumidor*, v.120, 2018, pág. 45.

Tratado sobre o Funcionamento da União Europeia. Disponível em: < https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF>. Acesso em: 1 jun. 2019.

CATEGORIZANDO DADOS EM UM CONTEXTO DE BIG DATA: EM DEFESA DE UMA ABORDAGEM FUNCIONAL

Eixo temático: A nova lei brasileira de proteção de dados pessoais (LGPD) e o GDPR europeu

Autor:
Pedro Bastos Lobo Martins
Bacharel e Mestrando em Direito pela Universidade Federal de Minas Gerais

ABSTRACT
A Lei Geral de Proteção de Dados (Lei 13.708/19) traz uma ampla regulamentação para atividades de tratamento de dados no Brasil. Ao trazer uma série de definições legais para o tema, cria também categorias de dados. Mais explicitamente estão os dados pessoais, dados pessoais sensíveis e dados anônimos, mas ao longo de seu texto a lei também menciona dados pseudo-anonimizados e cria regras especiais para tratamento de dados de crianças e adolescentes.
O presente texto tem como objetivo investigar se a criação de subcategorias de dados pessoais traz consequências positivas de um ponto de vista regulatório. A hipótese inicial era de que em um contexto de Big Data essa subcategorização é inócua, tendo em vista que atividades de processamento permitem que um conjunto de dados revele mais informações dos que as inicialmente contidas por ele.
A metodologia de estudo teve como ponto de partida uma análise da categoria de dados pessoais sensíveis estabelecida pela LGPD. Questionou-se a abordagem adotada pela lei de considerar um dado como sensível se este revelasse informações relacionadas a uma lista estabelecida pela lei (orientação sexual, etnia, dados de saúde, biométricos, etc.) e as limitações que essa abordagem traz. A principal limitação encontrada foi a infl xibilidade para abarcar outros elementos que possuem alto risco de gerar discriminações, mas não estão incluídas na definiçã de dado sensível, como por exemplo dados sobre situação financeira, geolocalização, gênero do titula , entre outros.
Ainda, a depender do contexto em que se utiliza uma informação ela possui maior ou menor chance de gerar um dano ao titular. A abordagem da lei desconsidera o contexto em que se dá a atividade de tratamento e categoriza dados exclusivamente com base em seu conteúdo informacional.
Posteriormente, partindo dos problemas identificados, foi estudado como o processamento de Big Data exige uma nova compreensão de vulnerabilidade e discriminação de grupos, uma vez que técnicas de *clustering* e *profling* possibilitam que enviesamentos ocorram com grupos que fogem da tradicional compreensão de quais são os principais alvos de discriminações.
Por fim, foi proposta uma abordagem funcional para a regulamentação do tratamento de dados. Em oposição à atual abordagem que identifica um dado como sensível a partir de seu conteúdo, em uma análise funcional o centro de relevância está em como determinada atividade de tratamento utiliza-se de dados pessoais. Desta forma, essas atividades de tratamento seriam reguladas de acordo com o seu risco de causar danos e gerar discriminações, o que possibilita um estudo empírico e técnico para cada setor.

INTRODUÇÃO

A nova geração de leis de proteção de dados, mais notadamente e objeto de estudo desse texto, a Lei Geral de Proteção de Dados (Lei 13.709/18), doravante LGPD, cria diferentes deveres legais para o tratamento de dados pessoais. Para facilitar essa regulamentação categorias de dados são criadas. As mais facilmente identificadas são as de dados pessoais, dados pessoais sensíveis, e dados anonimizados[583]. No entanto, a lei ainda faz menção a dados pseudo-anonimizados[584], e dados de crianças e adolescentes[585].

Na literatura existem críticas a respeito da eficácia de se estabelecer uma categorização legal em um ambiente técnico que não se limita a essas restrições. Blume questiona se, em virtude das diferenças entre os sujeitos titulares de dados (idosos, crianças, pessoas incapazes, etc.) e as consequências disso para o exercício de direitos subjetivos, capacidade de consentir e até mesmo de interagir de maneira significativa em plataformas digitais, deveriam ser criadas outras subcategorias de dados pessoais (2015, pp. 259-260)[586].

Zarsky mostra algumas incompatibilidades entre disposições da GDPR (General Data Protection Regulation), e o atual cenário técnico de processamento de dados. O autor põe em xeque a ideia de que uma maior proteção de dados leva a uma melhoria no processamento deles e a própria efetividade de algumas disposições protetivas da GDPR (2017, pp.1001-1003)[587].

Ainda, Nissenbaum alerta para a capacidade de derivar informações relevantes a partir de "dados primitivos", de forma que usar *standards* de privacidade tradicionais para esses dados primitivos com base em seu conteúdo sem levar em conta essa possibilidade de "escalada" da informação (e.g. equiparar a proteção do histórico de compras à privacidade de uma cesta de compras no supermercado) levaria a um enfraquecimento da proteção da privacidade (2019, pp. 236-237)[588].

A partir dessas considerações iniciais, esse texto irá analisar a compatibilidade entre uma categorização de dados e uma adequada proteção de dados pessoais no cenário tecnológico atual. O ponto de partida será o estudo da categoria de dados pessoais sensíveis.

LIMITAÇÕES DE UMA CONCEITUAÇÃO LEGAL PARA DADOS SENSÍVEIS

583 Ver Art. 5º, I, II e III, da Lei 13.709/18, respectivamente.

584 Ver art. 13 §4º da Lei 13.709/18.

585 Ver art. 14 da Lei 13.709/18.

586 Blume, P. "The Data Subject", *European Data Protection Law Review,* núm. 04, 2015, págs. 258-264.

587 Zarsky, T. "Incompatible: The GDPR in the Age of Big Data", *Seton Hall Law Review, núm.* 4, 2017, págs. 995-1020.

588 Nissenbaum, H. "Contextual Integrity Up and Down the Data Food Chain", *Theoretical Inquiries in Law,* núm 01, 2019, págs. 221-256.

A categoria de dados pessoais sensíveis existe tanto na LGPD quanto na GDPR como *Special Category Data*. Ambas os regulamentos possuem a mesma definição, considerando como sensíveis dados sobre "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófic ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural"[589].

Na lei brasileira, pode-se dizer que o consentimento do titular, fornecido de *"forma específica e destacada, para finalidades específicas"*[590] é a principal base legal para o tratamento nesse caso, ao contrário das hipóteses adotadas para o tratamento de dados pessoais não sensíveis. Isso porque **a base legal do legítimo interesse não figura entre as hipóteses legais de tratamento de dados sensíveis**. Os demais fundamentos previstos para o tratamento dizem respeito majoritariamente ao cumprimento de obrigações legais, exercício regular de direito e realização de pesquisa científica e, portanto, são de incidência limitada.

Ainda, a LGPD, assim como a GDPR, adotou uma conceituação voltada para o conteúdo de determinado dado, e não de sua utilização, como foi obtido ou para que fim será empregado. Ao menos duas interpretações podem ser dadas para essa abordagem.

Primeiro, é possível interpretar que as informações elencadas como sensíveis (convicção religiosa, dado referente à saúde, etc.) possuem caráter íntimo mais forte do que outros dados pessoais (por exemplo, nome, gênero, modelo do celular). Logo, para que essas informações fossem reveladas para o controlador seria preciso da autorização do titular. Ainda, no caso de um incidente de vazamento de dados ou uso ilegal desses dados, o sujeito sofreria um dano maior por ter informações íntimas de sua vida expostas.

De acordo com essa argumentação, a proteção de dados sensíveis teria forte vinculação com proteção da privacidade sob uma ótica de privacidade como intimidade, descrita por Daniel Solove como uma abordagem que valoriza a privacidade como algo essencial para estabelecer relações. Assim, para cada relacionamento o sujeito poderia estabelecer diferentes graus de intimidade e controlar quais informações quer manter em segredo (2008, p. 34)[591]. Portanto, a lei, ao instituir o consentimento como principal base legal para o tratamento de dados sensíveis estaria justamente dando poder ao titular de escolher com quais controladores ele teria uma relação de confiança para que essas informações de sua vida sejam conhecidas. No entanto, esta abordagem de privacidade é bastante anacrônica, especialmente ao ser inserida em um contexto de proteção de dados[592].

589 Redação do art. 5º, II da Lei 13.709/18
590 Redação do art. 11, I da Lei 13.709/18
591 Solove, D. *Understanding Privacy*. Harvard University Press, Cambridge, 2008.
592 Ver, por exemplo Nissenbaum, 2019 *supra* nota 6, p. 237.

Já por uma segunda interpretação, a proteção especial conferida aos dados considerados sensíveis pela LGPD tem como fundamento não só a proteção da privacidade, mas também a observância dos princípios da finalidade e não discriminação[593].

Dados que revelem origem étnica, orientação sexual, religiosa, dados referentes à saúde, entre outros, são merecedores de uma maior proteção não por seu caráter intrinsecamente íntimo, uma vez que o exercício da privacidade não é determinado pelo conteúdo da informação[594], mas sim pelo contexto informacional como um todo, abrangendo a informação, a finalidade para qual está sendo usada e como foi obtida (Nissenbaum, 2004, pp. 118-119)[595]. Portanto, pode-se concluir que a proteção especial a dados sensíveis advém do fato de a lei atribuir a eles uma **presunção de potencial discriminatório** que cause dano ao titular, levando em conta também a finalidade daquele tratamento. Essa também é a conclusão de Danilo Doneda.

> Na verdade, deve-se ter em conta que a diferenciação conceitual dos dados sensíveis atende à uma necessidade de estabelecer uma área na qual a probabilidade de utilização discriminatória da informação é potencialmente maior – sem deixarmos de reconhecer que há situações onde tal consequência pode advir sem que sejam utilizados dados sensíveis, ou então que a utilização destes dados se preste a fins legítimos e lícitos (Doneda, 2006, p. 163)[596].

O Article 29 Working Party, órgão consultivo criado pela Diretiva 95/46 da União Europeia, considerou que a razão de se adicionar uma camada de proteção para o tratamento de dados sensíveis decorre tanto da presunção de consequências mais graves em caso de uso indevido, quanto pelo fato de as consequências decorrentes desse uso indevido poderem ser irreversíveis ou resultarem danos de longo prazo (Article 29 Working Party [A29WP], 2011, p. 4)[597].

Contudo, essa interpretação não afasta todos os problemas causados pela subcategorização de dados pessoais. Mesmo na lógica da presunção de potencial discriminatório pelo uso desses dados, as informações consideradas sensíveis sobre o titular se restringem àquelas estabelecidas pela Lei. Isto é, embora orientação sexual seja considerada uma informação sensível, um dado que identifique o gênero do titular

593 Esses princípios são expressamente previstos pela LGPD em seu art. 6º, I e IX

594 Como exemplo: a filiação partidária de um candidato à presidência da república não é uma informação privada em um debate televisivo. Entretanto, essa mesma informação merece a salvaguarda jurídica da privacidade quando seu titular solicitar um empréstimo para fins particulares. Isso porque os contextos em que essa informação é compartilhada são diferentes, assim como a finalidade para qual poderá ser usada.

595 Nissenbaum, H. "Privacy as Contextual Integrity", *Washington Law Review*, núm. 01, 2004, págs. 119-157.

596 DONEDA, D. *Da privacidade à proteção de dados pessoais*. Renovar, Rio de Janeiro, 2006.

597 Article 29 Data Protection Working Party. (2011). *Advice paper on special categories of data ("sensitive data")*. Recuperado de https://www.pdpjournals.com/docs/88417.pdf [Data de consulta: 8 de maio de 2019].

não é. Surgem aqui outras duas possibilidades. Na primeira, toma-se a definição trazida pelo art. 5º, II da LGPD como uma lista exaustiva, *numerus clausus*. A outra possibilidade seria a de considera-la uma lista exemplificativa, sendo possível incluir outras informações que causem discriminação do titular.

As duas abordagens apresentam seus problemas. Sendo a definição de dado pessoal sensível exaustiva, vários grupos vulneráveis se encontrariam excluídos da proteção, uma vez que informações como gênero, situação financeira, local de residência, embora passíveis de gerar discriminação, não estão incluídas na definição. Por outro lado, considerar como sensíveis informações não previstas pela lei geraria insegurança jurídica para os controladores, uma vez que as bases legais para o tratamento são diferentes, e até mesmo o consentimento do titular para o tratamento é avaliado de forma distinta entre dados sensíveis e não sensíveis.

A IDENTIFICAÇÃO DE GRUPOS VULNERÁVEIS NO CONTEXTO DE BIG DATA

Com um processamento de quantidades massivas de dados, ou por um termo mais popular, Big Data[598], faz cada vez menos sentido separar categorias de dados pessoais entre sensíveis e não sensíveis de acordo com seu conteúdo, como argumenta Zarsky (2016, p. 1013)[599]. Isso porque o tratamento de praticamente qualquer dado pode revelar informações sensíveis, há facilidade para os controladores burlarem categorizações específicas e novos grupos vulneráveis são formados.

Como demonstrado por Kosinski, Stillwell e Graepel, a partir de uma única variável—likes no Facebook—os pesquisadores foram capazes de inferir com 93% de acurácia o gênero dos participantes. A taxa de acerto foi ainda mais alta para a raça[600] com 95% de precisão. Orientação sexual, religiosa e política também foram inferidas com altas taxas de acerto (2013, p. 5803)[601].

É verdade que a LGPD não ignorou esse fato e estende as proteções dadas para dados sensíveis também para inferências que revelem informações sensíveis sobre o

598 O termo Big Data, embora muito utilizado, não possui uma única definição. Uma possível conceituação é proposta por Viktor Mayer-Schönberger e Kenneth Cukier: "Big data refere-se a coisas que se pode fazer em grande escala que não podem ser feitas em uma escala menor, para extrair novos insights ou criar novas formas de valor, de maneiras que mudam mercados, organizações, relacionamento entre cidadãos e governos e muito mais" (Mayer-Schönberger e Cukier, 2013, p. 6, tradução livre) Mayer-Schönberger ,V. e Cukier, K. *Big Data. A Revolution That Will Transform How We Live, Work, and Think*. Murray, Londres, 2013.

599 Zarsky, 2017 *supra* nota 5.

600 Os parâmetros considerados no estudo para gênero foram masculino e feminino, e para raça caucasiano e afro-americano.

601 Kosinski, M., Stillwell, D., Graepel, T. "Private Traits and Attributes Are Predictable from Digital Records of Human Behavior", *Proceedings of the National Academy of Sciences*, núm. 15, 2013 págs. 5802–5805.

titular, conforme o art. 11 §1º[602] da lei. Isso demonstra que o legislador começa a se atentar para as possibilidades trazidas pelo Big Data. Apesar disso, as consequências dessa nova lógica de processamento de dados apresentam outros problemas que põem em xeque um modelo de proteção ao titular baseado na categorização de dados.

Um primeiro comprometimento desse modelo é identificado por Sandra Wachter com a possibilidade de utilização pelo controlador dos chamados "*proxy data*", ou dados de proximidade[603]. Esses seriam dados que não ligam diretamente um titular a uma categoria sensível (como etnia, por exemplo) mas apenas identificam uma afinidade do titular com determinado grupo. Isso permitiria ao controlador não se submeter a obrigações legais, uma vez que poderia alegar não estar identificando uma informação sensível. A autora argumenta que isso é possível devido ao fato de que "as plataformas não necessariamente se importam se colocam os usuários com precisão em determinados grupos; em vez disso, o que importa é se o usuário se comporta de maneira semelhante ao grupo assumido para ser tratado como um membro desse grupo" (Wachter, 2019, p. 13)[604].

Ainda, como argumenta Rouvroy, em um contexto de Big Data, discriminações não são geradas intencionalmente e nem mesmo com base em categorias pré-constituídas que identificamos como vulneráveis a práticas discriminatórias (2016, p.17)[605]. Segundo a autora, em uma categorização por meio de uma lógica tradicional características comuns a um grupo são identificadas, seja pelo próprio indivíduo ou por terceiros, e com isso subsumidas em categorias pré-existentes (2016, p. 28)[606]. Já os processamentos de Big Data têm como objetivo:

> realçar categorias anteriormente desconhecidas, social e visualmente imperceptíveis, com base na análise de dados sem qualquer referência a informações pré-existentes sobre esses novos grupos ou categorias. Em processos de *clustering*, os indivíduos são colocados . . . em "categorias" socialmente e existencialmente sem significado, que são imperceptíveis (porque emergem apenas enquanto o processo se desenrola) e, na maioria das vezes, sem possibilidade de estar ciente do que está acontecendo ou de se reconhecer. (Rouvroy, 2016, p. 28).[607]

602 "Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

603 O termo "dado de proximidade" foi proposto como tradução de "proxy data".

604 Tradução livre do original "Platforms do not necessarily care whether they fully accurately place users into certain groups; rather, what matters is whether the user behaves similarly enough to the assumed group to be treated as a member of the group.". Wachter, S. "Affinit Profiling and Discrimination by Association in Online Behavioural Advertising", 2019. Disponível em SSRN:https://ssrn.com/abstract=3388639 [Data de consulta: 25 de maio de 2019].

605 Rouvroy, A. ""Of Data and Men". Fundamental Rights and Freedoms in a World of Big Data." *Council of Europe, Directorate General of Human Rights and Rule of Law.* vol. T-PD-BUR(2015)09REV, 2016, págs. 1-37.

606 Rouvroy, 2016, *supra* nota 23.

607 Tradução livre com supressão de texto do original: "highlight previously unknown, socially and visually imperceptible categories on the basis of data analysis without any reference to

Mittelstadt identifica esses grupos constituídos por meio de *clustering* como "grupos *ad hoc*", uma vez que são formados através de um agrupamento volátil, com um processamento e finalidade específicos (por exemplo, por um controlador interessado em direcionar anúncios para idosos que sofram de insônia e moram sozinhos). Esse fenômeno identificado pelo autor apresenta grande complexidade, uma vez que o próprio titular terá dificuldade para saber da existência desse grupo, que é parte dele e que pode estar sofrendo desvantagens por isso. Ainda, existe uma grande dúvida a respeito de como se daria a representação dos interesses desses grupos, por exemplo, em caso de uma tutela coletiva (2017, pp. 485-486)[608].

Espera-se que tenha sido demonstrado até aqui que existem não só desafios técnicos no caminho da efetivação de uma proteção legal que garanta que o tratamento de dados pessoais não seja usado para perpetuar ou reforçar desigualdades. Há também barreiras conceituais que redefinem práticas discriminatórias. Não se trata de negar que minorias sociais continuam sendo alvo de discriminações em um contexto de tratamento de dados[609]. No entanto, surgem também novos grupos que se tornam vítimas de discriminações podem ser criados sem necessariamente corresponder àqueles vulneráveis pela lógica tradicional[610].

Portanto, partir de uma lógica tradicional de discriminação e aplica-la em um contexto de Big Data não parece ser a melhor solução. Na parte final do texto será levantada uma alternativa à categorização dos dados pelo seu conteúdo informacional.

UMA ABORDAGEM FUNCIONAL COMO ALTERNATIVA

Ainda antes da elaboração do texto da GDPR, o Article 29 Working Party emitiu um parecer com recomendações de abordagem para a regulação de dados sensíveis, ou *special category data* (A29WP, 2011, pp. 13-15)[611]. O órgão ficou dividido entre duas principais opções para uma regulação pela GDPR.

---

pre-existing information about these new groups or categories. In clustering processes, individuals are placed by another person – which can be an automatic data processing system – into socially and existentially a-significant "categories", which are imperceptible (because they emerge only as the process unfolds), and most often without any possibility of being aware of what is happening or recognising themselves.". Rouvroy, 2016, *supra* nota 23.

608 Mittelstadt, B. "From Individual to Group Privacy in Big Data Analytics", *Philosophy & Technology*, núm. 04, 2017, págs. 475–494.

609 Como exemplo, cita-se a investigação da ProPublica, revelando o uso de um algoritmo no sistema judicial americano em que réus negros eram duas vezes mais propensos do que réus brancos a serem erroneamente classificados em grupos de maior risco de reincidência criminal. Larson, J.; Mattu, S.; Kirchner L.; Angwin, J. *How We Analyzed the COMPAS Recidivism Algorithm*. 2016, Disponível em: https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm. [Data de consulta: 24 novembro de 2018].

610 Para exemplos ver Wachter, 2019, *supra* nota 22.

611 Article 29 Data Protection Working Party, 2011, *supra* nota 15.

A primeira, que já era adotada pela Diretiva 95/46 e continuou a ser na GDPR, seria a da lista fechada de categorias de dados considerados sensíveis (dados ligados à etnia, saúde etc.). As principais vantagens encontradas são ligadas à segurança jurídica para os controladores e harmonização entre a legislação de diversos países. No entanto, o órgão reconheceu a infl xibilidade para se adaptar para novas formas de processamento de dados e diferenças culturais que podem existir entre países.

A segunda opção foi chamada de abordagem contextual e permitiria maior fl xibilidade para considerar outros dados como sensíveis levando em conta o contexto em que se realiza o tratamento de dados. Como contraponto à lista fechada, as desvantagens foram justamente a insegurança jurídica e grandes diferenças que poderiam ocorrer entre legislações nacionais.

Contudo, ambas as abordagens partem de um paradigma de categorizar o dado a partir de seu conteúdo. Na lista fechada isso é mais evidente, mas mesmo pela abordagem contextual o que se busca é expandir a proteção para outros dados que podem ser usados para identificar no titular alguma característica considerada sensível. No entanto, é justamente esse enfoque na proteção de características pessoais que tradicionalmente são consideradas como íntimas que leva a uma inadequação da proteção em um contexto de Big Data.

No processamento de Big Data utiliza-se grandes quantidades de dados e bases não estruturadas, possibilitando que, tecnicamente, eles possam ser usados para as mais diversas finalidades (Bioni, 2015, p.48)[612]. Ainda, Rouvroy alerta que em atividades de *profiling* e predição de comportamento, pouco importa os dados de um indivíduo específic, desde que seu comportamento se encaixe estatisticamente dentro do modelo designado, culminando na conclusão de que "o seu dado é tão bom quanto o do seu vizinho" (2016, p. 33)[613].

Se um titular é afetado por um processamento de dados que nem mesmo precisam se referir a ele, mas que o classificam dentro de um grupo e possibilitam sua identificação, mais adequado do que se buscar uma tutela a partir do conteúdo presumidamente discriminatório de determinados dados seria regulá-los a partir de seu uso. Temos então que a "sensibilidade" de um dado pouco teria a ver com a informação que revela, mas sim em como ele é empregado.

Esse texto não tem a presunção de resolver os problemas de discriminações que podem ser gerados por atividades de tratamento de dados e a Lei Geral de Proteção de Dados é apenas um dos primeiros passos na construção de uma cultura jurídica que

612 Bioni, B. Xeque-Mate: o tripé de proteção aos dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. GPoPAI/USP, 2015. Disponível em: http://gomaoficina.com/wp-content uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf. [Data de consulta: 29 de maio de 2019].

613 Tradução livre de "your data is as good as your neighbours". Rouvroy, 2016, *supra* nota 23.

se atente para as consequências geradas pela difusão de atividades de tratamento de dados.

No entanto, é proposto que se reconheça as mudanças trazidas por análises de Big Data e a inadequação da aplicação de uma lógica de privacidade tradicional. Como alternativa, vislumbra-se uma abordagem funcional do tratamento. Isto é, ao invés de se manter em uma lógica anacrônica de dificultar ou proibir o acesso a informações que historicamente são consideradas íntimas e ligadas a discriminações, deve-se avançar para uma análise concreta e setorial de quais informações podem ser usadas para quais finalidades.

Usando como exemplo um dado de geolocalização do titular. Na avaliação de score de crédito, seria possível debater se é ou não aceitável do uso dessa informação pelos controladores, já que ela poderia levar a discriminações com base no domicílio ou local de trabalho do sujeito. Já para uma aplicação que informa as condições climáticas com base na geolocalização esse dado é não só essencial, como também não gera nenhum risco para o titular. Assim, um mesmo dado, a depender da utilização para qual é empregado, afeta o titular de maneira distinta, mesmo que em última análise revele a mesma informação (domicílio do titular).

Claro que continuarão existindo casos controversos e de difícil solução, como uso desse dado para atribuir um perfil de consumo à determinado titular. No entanto, com uma abordagem funcional as especificidades de cada situação podem ser analisadas de maneira mais concreta e estudos empíricos que demonstram discriminações injustas (ou a ausência delas) como consequência do tratamento de alguns dados podem ser levantados.

Como último ponto, embora não seja o principal objeto do texto, é importante ressaltar que as diferentes abordagens também geram efeitos na valorização do consentimento do titular. Ao se considerar dados sensíveis em virtude de seu conteúdo, o consentimento é sobrevalorizado, a partir de uma ideia de que o titular aceita que aquelas informações íntimas de sua vida sejam conhecidas pelo controlador. Todavia, há um forte questionamento na literatura a respeito da eficácia de se confiar no consentimento do titular[614]. Por outro lado, uma regulação a partir do uso do dado tem uma menor dependência do consentimento e se volta mais para a criação de regras

614 Ver, por exemplo: Schermer,B, Custers, B. Van der Hof, S. "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection", *Ethics and Information Technology*, núm. 2. págs. 171–182. 2014; Lazaro, C; Métayer, D. "Control Over Personal Data: True Remedy or Fairy Tale?", *SCRIPTed—Journal of Law, Technology & Society*, núm. 01, págs. 03–34, 2015. e Blume, 2015 *supra* nota 4.

setoriais e uma estrutura de fiscalização para que eventuais violações não dependam apenas de ações individuais para serem coibidas.

Desta forma, regular o tratamento de dados pessoais a partir da função que cumprem em determinada atividade de processamento é mais efetivo para proteger os titulares de discriminações injustas. Ainda, menos insegurança jurídica seria gerada quando comparada à abordagem contextual, porque esta expandiria a lista de dados sensíveis baseada no conteúdo informacional daquele dado, enquanto em uma análise funcional cada setor ou atividade de tratamento teria suas próprias regras.

REFERÊNCIAS BIBLIOGRÁFICAS

Article 29 Data Protection Working Party. (2011). *Advice paper on special categories of data ("sensitive data")*. Recuperado de https://www.pdpjournals.com/docs/88417.pdf [Data de consulta: 8 de maio de 2019].

Bioni, B. Xeque-Mate: o tripé de proteção aos dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. GPoPAI/USP, 2015. Disponível em: http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf. [Data de consulta: 29 de maio de 2019].

Blume, P. "The Data Subject", *European Data Protection Law Review,* núm. 04, 2015, págs. 258-264.

Doneda, D. *Da privacidade à proteção de dados pessoais*. Renovar, Rio de Janeiro, 2006.

Kosinski, M., Stillwell, D., Graepel, T. "Private Traits and Attributes Are Predictable from Digital Records of Human Behavior", *Proceedings of the National Academy of Sciences*, núm. 15, 2013 págs. 5802–5805.

Larson, J.; Mattu, S.; Kirchner L.; Angwin, J. *How We Analyzed the COMPAS Recidivism Algorithm.* 2016, Disponível em: https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm.[Data de consulta: 24 novembro de 2018].

Lazaro, C; Métayer, D. "Control Over Personal Data: True Remedy or Fairy Tale?", *SCRIPTed—Journal of Law, Technology & Society*, núm. 01, págs. 03–34, 2015.

Mayer-Schönberger ,V. e Cukier, K. *Big Data. A Revolution That Will Transform How We Live, Work, and Think*. Murray, Londres, 2013.

Mittelstadt, B. "From Individual to Group Privacy in Big Data Analytics", *Philosophy &*

Technology, núm. 04, 2017, págs. 475–494.

Nissenbaum, H. "Privacy as Contextual Integrity", *Washington Law Review*, núm. 01, 2004, págs. 119-157.

Nissenbaum, H. "Contextual Integrity Up and Down the Data Food Chain", *Theoretical Inquiries in Law,* núm 01, 2019, págs. 221-256.

Rouvroy, A. ""Of Data and Men". Fundamental Rights and Freedoms in a World of Big Data." *Council of Europe, Directorate General of Human Rights and Rule of Law.* vol. T-PD-BUR(2015)09REV, 2016, págs. 1-37.

Schermer,B, Custers, B. Van der Hof, S. "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection", *Ethics and Information Technology*, núm. 2. págs. 171–182. 2014.

Solove, D. *Understanding Privacy*. Harvard University Press, Cambridge, 2008.

Wachter, S. "Affinit Profiling and Discrimination by Association in Online Behavioural Advertising", 2019. Disponível em SSRN:https://ssrn.com/abstract=3388639 [Data de consulta: 25 de maio de 2019].

Zarsky, T. "Incompatible: The GDPR in the Age of Big Data", *Seton Hall Law Review, núm.* 4, 2017, págs. 995-1020.

PROCESSO ELETRONICO E PROVA DIGITAL

EL DERECHO CRIPTOGRÁFICO

¿UNA RAMADA EMERGENTE DEL DERECHO INFORMÁTICO?

Eje temático: Processo Eletrónico y Prueba digital

Autor:
José Francisco Vega Sacasa
Doctor en Estudios Legales Financieros.
Miembro de FIADI

RESUMEN
Durante la celebración del Congreso Internacional de Derecho Procesal Telemático en la ciudad de Caracas, Venezuela, donde tuve la oportunidad de participar como orador, escuché por primera vez la definición del término "Derecho critográfico" o "Criptoderecho". Fue el profesor Raymond Orta, en el contexto de su exposición, quien abordó esta materia desde una acertada visión:
"Rama del derecho informático encargada del estudio de las nuevas tecnologías basadas en criptografía, aplicadas a criptoactivos, cadena de bloques (blockchain), seguridad de datos y seguridad informática".
El concepto es totalmente válido: Este proceso de disrupción tecnológica es aplicable a todos los ámbitos, incluido el Derecho. Desde el punto de vista de la epistemología jurídica, podemos interpretar que el Derecho criptográfico tiene su origen en las nuevas tecnologías aplicadas al derecho, basadas en sistemas de criptografía.
Por ejemplo, la firma electrónica es un elemento derivado de la criptografía, sin embargo, se debe analizar su regulación desde el aspecto de los algoritmos criptográficos usados para establecer una seguridad razonable, al momento de validar un documento.
De igual forma, la evidencia digital debe ser sellada digitalmente por el cálculo en bruto de los hexadecimales por la cual está compuesta, lo cual dará un resultado alfanumérico denominado Hash. El Hash que se usa para sellar los documentos digitales debe ser un algoritmo que no haya sido colisionado anteriormente o que contenga vulnerabilidades, debido a que se puede establecer la duda sobre la integridad de la evidencia digital.
En ese sentido puedo definir el Derecho criptográfico como una derivación del Derecho informático y telemático que tiene como objetivo regular las tecnologías basadas en sistemas criptográficos aplicadas a un proceso judicial, a fin de garantizar su autenticidad, credibilidad, confiabilidad y admisibilidad en materia de evidencia digital.

Derecho criptográfico: ¿Una rama emergente del derecho informático?

1. PRINCIPIOS GENERALES DEL ERECHO CRIPTOGRÁFICO

Podemos establecer que como cualquier otra rama jurídica, se parte de la base de sus principios, en el caso del derecho criptográfico podemos mencionar los siguientes:

a) Confidencialidad: La privacidad de la información es el principal objetivo de la criptografía, básicamente lo podemos resumir como la forma en que se mantiene en secreto una información determinada. Este principio lo podemos subsumir del artículo 12 de la Declaración Universal de los Derecho Humanos de 1948 que establece lo siguiente:

"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques."

b)Autenticación: Este principio hace alusión al mecanismo utilizado en la actualidad para corroborar la identidad de una persona, computadora, dispositivo electrónico o empresa. Es decir que se trata de autenticar la autoría de la información contenido en un documento digital. Esto incluye implícitamente la integridad de los datos. El principio de autenticación los podemos desarrollar de los siguientes preceptos del derecho probatorio: lealtad, probidad y veracidad de la prueba.

c) Integridad: Al referirnos al principio de integridad nos estamos remitiendo al aseguramiento de que una información en particular (archivo, dato o fichero electrónico) no haya sido alterado por personas no autorizadas o idóneas. Aquí se ataca el problema de la manipulación o modificación de un documento electrónico que a la postre puede servir como elemento de convicción digital en un proceso penal. La integridad de la prueba va arraigado al principio de mismidad de la prueba, es decir la prueba debe ser la misma desde el momento de su recolección, hasta el momento de presentación y valoración en la etapa de juicio.

2. LA CRIPTOGRAFÍA COMO MÉTODO DE PRESERVACIÓN DE LOS DOCUMENTOS DIGITALES

El proceso de análisis forense a un dispositivo informático se establece mediante los siguientes pasos:

a) Preservación: la evidencia digital, a diferencia de las demás evidencias testimoniales, documentales y físicas, debe ser tratada por un experto informático forense debido a su alto grado de volatilidad, contaminación, modificación y posibilidades de ser borrada. Debemos entender primero el concepto de la palabra evidencia digital. Según la Real Academia Española, la palabra evidencia tiene los siguientes significados:

"(Del lat. evidentĭa).

1. **f. Certeza clara y manifiesta de la que no se puede dudar.** *La evidencia de*

la derrota lo dejó aturdido.

2. f. *Der.* Prueba determinante en un proceso".

Podemos resumir que el concepto etimológico de la palabra evidencia proviene de vocablo vidente y su connotación aceptable se refiere a algo que no se pone en tela de duda para poder descubrir la verdad procesal de un hecho o pretensión dentro de un proceso judicial.

La palabra digital, en materia informática, se refiere a los números dígitos y tiene sentido debido a que los dispositivos digitales, tales como las computadoras, utilizan un sistema de números binarios que consiste en dos valores representados mediante (1) uno y (0) cero que permiten almacenar, procesar y transferir cualquier información. La combinación de estos dos valores mencionados representa en términos informático un bit.

El portal de internet www.tecnologia-informatica.com nos define bit de la siguiente forma:

*"Bit es la abreviación de **Binary Digit** (dígito binario), la cual, en términos técnicos, es la menor unidad de información de una computadora. Un bit tiene solamente un valor (que puede ser 0 o 1). Varios bits combinados entre sí dan origen a otras unidades, como "byte", "mega", "giga" y "tera".*

Una vez entendido que el bit es la unidad más pequeña de almacenamiento de la información de un dispositivo informático, debemos tener en cuenta esta característica al momento de analizar cualquier documento digital.

TABLA DE CONVERSIÓN

8 Bit = 1Byte (B)
1,024 bytes = 1 Kilobyte (KB)
1,024 Kilobyte = 1 Megabyte (MB)
1,024 megabyte = 1 Gigabyte (GB)
1,024 gigabyte = 1 Terabyte (TB)
1,024 terabyte = 1 Petabyte (PB)
1,024 petabyte = 1 Exabyte (EB)

Esta es la base medular de la etapa de preservación de la evidencia digital, debido a que cada archivo almacenado en un dispositivo telemático debe estar compuesto por cualquier unidad de almacenamiento representada en dígitos en la tabla de conversión.

Las evidencias documentales en estado de copia simple pueden ser muy sencillas de cotejar en su autenticidad con el documento original, con un simple método de observación visual por medio de un fedatario competente en el caso.

2.1 Evidencia Digital

Sin embargo, cuando nos referimos a una evidencia digital, estamos hablando de un documento intangible, es decir, que al momento de emitir una copia, no se puede cotejar a través del método de observación visual con su original, debido a sus características de volatilidad y modificación, por ende ¿cuándo analizamos si una evidencia digital es evidente?

Cualquier dispositivo electrónico y digital puede ser manipulado, por ende, deja de ser "evidente". El autor Óscar Domínguez Merino, en el libro La prueba electrónica: Validez y eficacia judicial, arguye lo siguiente:

"Y es este escenario tan manipulable y aparentemente falso donde el sector jurídico tiene un hueso duro de roer. ¿Qué es real? ¿Qué es falso? ¿Qué está manipulado y qué no? ¿Podemos creer lo que perciben nuestros sentidos? ¿Confiamos en que las máquinas están programadas para funcionar como deben? ¿Quién asegura y da validez a todo esto? Se conocen claros ejemplos de manipulaciones de teléfonos, donde el emisor no es realmente el emisor; de aparatos GPS que mandan coordenadas de una ubicación por donde jamás pasaron; de correos electrónicos enviados por emisores que jamás tuvieron email; de fotografías que muestran una escena que nunca sucedió; de vídeos que muestran una secuencia de imágenes que nunca tuvieron lugar… Manipulaciones, manipulaciones y más manipulaciones".

Presentar una evidencia digital en un proceso judicial puede resultar complejo para la parte que la aporta, debido a que la contraparte sólo debe demostrar que la evidencia ha sido manipulada y en consecuencia solicitar la nulidad de la evidencia por violación de su integridad y del principio de mismidad.

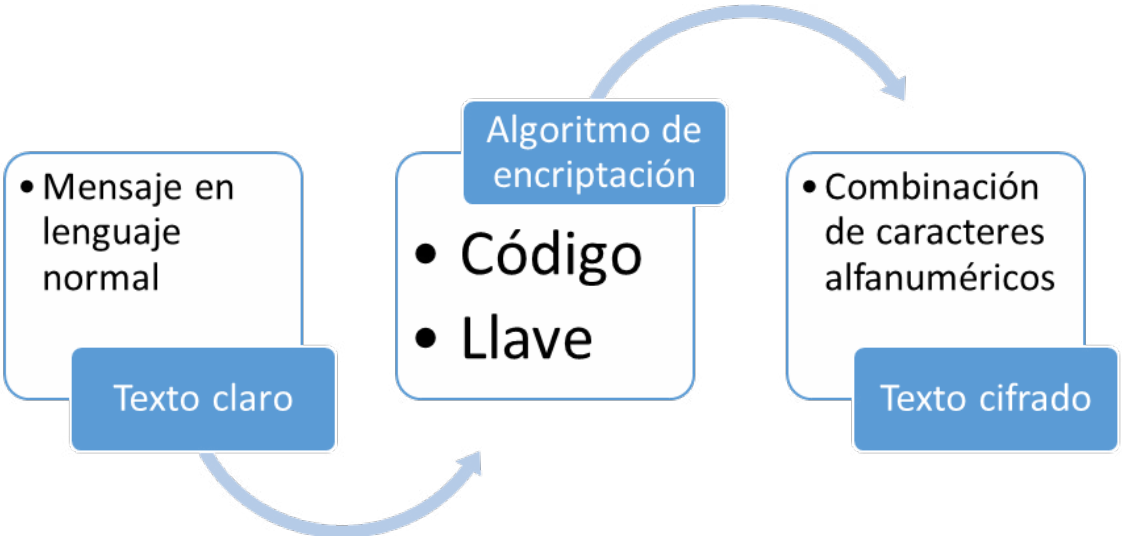
Por ejemplo, una conversación de Whatsapp o de cualquier otra aplicación de mensajería instantánea, por ningún motivo debe ser presentada únicamente impresa y cotejada por notario público, debido a que por su naturaleza es una evidencia digital, no una documental y la forma como se presenta no permite garantizar, de manera científica, que no fue adulterada.

La definición legal de Documento Electrónico la podemos encontrar en el artículo 7 de la Ley 82 de 9 de noviembre de 2012, que modifica el artículo 2, numeral 17 de la Ley 51 de 22 de julio de 2008 que establece lo siguiente:

"*Documento electrónico. Toda representación electrónica que da testimonio de un hecho, una imagen, un sonido o una idea, con independencia del soporte utilizado para su fijación."*

Para proteger la integridad de un documento electrónico o evidencia digital es necesario la aplicación de métodos criptográficos. Según el autor Óscar Manuel Lira Arteaga, en su obra Cibercriminalidad, define la criptografía como *"la ciencia que se encarga de estudiar las distintas técnicas para transformar (encriptar o cifrar) la información y hacerla irreconocible a todos aquellos usuarios o personas no autorizadas".*

Es decir que un sistema criptográfico está basado en un algoritmo fijo de encriptación en conjunto con un código, a fin de convertir un texto en lenguaje claro y proceder a cifrarlo. (Ver figura 1)



2.2 Tipologías de la criptografía

Existen dos tipos de sistemas criptográficos en virtud del sistema de llave utilizado, este puede ser divido en criptografía asimétrica y simétrica, la primera consiste en emplear el uso de dos llaves distintas para cifrar y descifrar el mensaje, es decir la persona A (el emisor) quiere enviar un mensaje codificado mediante una llave pública para que posteriormente la persona B (el receptor) lo pueda leer, descodificándolo con su llave privada.

En cambio, la criptografía simétrica consiste en utilizar una sola llave pública en la técnica de codifi ación y descodificación del mensaje. Se basa en funciones matemáticas muy simples ejecutadas sobre los símbolos del mensaje original.

Figura 2: criptografía simétrica y asimétrica

2.3 Función Hash

A través de la criptografía se deriva la función Hash que nos sirve como base medular para la protección de la integridad de un documento electrónico o evidencia digital.

El ingeniero en Telecomunicaciones Sergio Carrasco Mayans, en su artículo titulado La alegalidad o limbo legal de la prueba electrónica, define el Hash de la siguiente forma:

"En el caso de documentos electrónicos contamos con herramientas que nos van a permitir crear la huella digital del mismo o hash, una cadena alfanumérica hexadecimal generada a partir de la aplicación de un algoritmo que debe identificar de manera inequívoca dicho documento, de tal manera que el menor cambio realizado sobre el mismo sería rápidamente detectado (aunque respecto a este último factor es importante ver si el algoritmo concreto utilizado para su generación es realmente adecuado). Esto además nos permitirá realizar duplicados de dichos documentos y probar que se corresponden plenamente con el original".

Por otro lado, el ingeniero Oscar Manuel Lira Arteaga, en su obra Cibercriminalidad, define el Hash de la manera:

"Conjunto de algoritmos que utilizan una serie de operaciones matemáticas sobre el mensaje original para calcular un valor de tamaño fijo (128, 160, 256 o 512 bits), utilizando una función dispersión unidireccional (no se puede reconstruir el mensaje a partir de su compendio o huella digital) que cumple con una serie de propiedades criptográficas como son:

1. Cualquier alteración del mensaje o datos originales influye en el resultado del compendio o huella digital.

2. No es posible la reconstrucción del mensaje original a partir del compendio.

3. La probabilidad de encontrar dos mensajes con una misma huella digital es prácticamente nula."

En conclusión, podemos deducir que el Hash es un algoritmo criptográfico que al realizar las sumas de los bits datos o documentos digitales arrojará un valor matemático por medio de una cadena alfanumérica, que nos va garantizar la integridad de la evidencia digital y, en caso de modificar o alterar la evidencia digital, el valor alfanumérico cambia en su totalidad.

Los sellados de tiempo o huellas digitales de función Hash más utilizados son MD5, SHA1, SHA2.

Podemos obtener un sellado de tiempo basado en función Hash a través de distintos softwares ya sea de código abierto o cerrado. En este caso usaremos el software Hash My File de fuente abierta para demostrar el proceso de sellar un documento electrónico con un valor Hash de 256 (64 dígitos) del contenido de un dispositivo USB

de memoria ROM en la unidad (G) del puerto, con capacidad de almacenamiento de 29.2 Gygabyte (GB) que contiene 3 archivos.

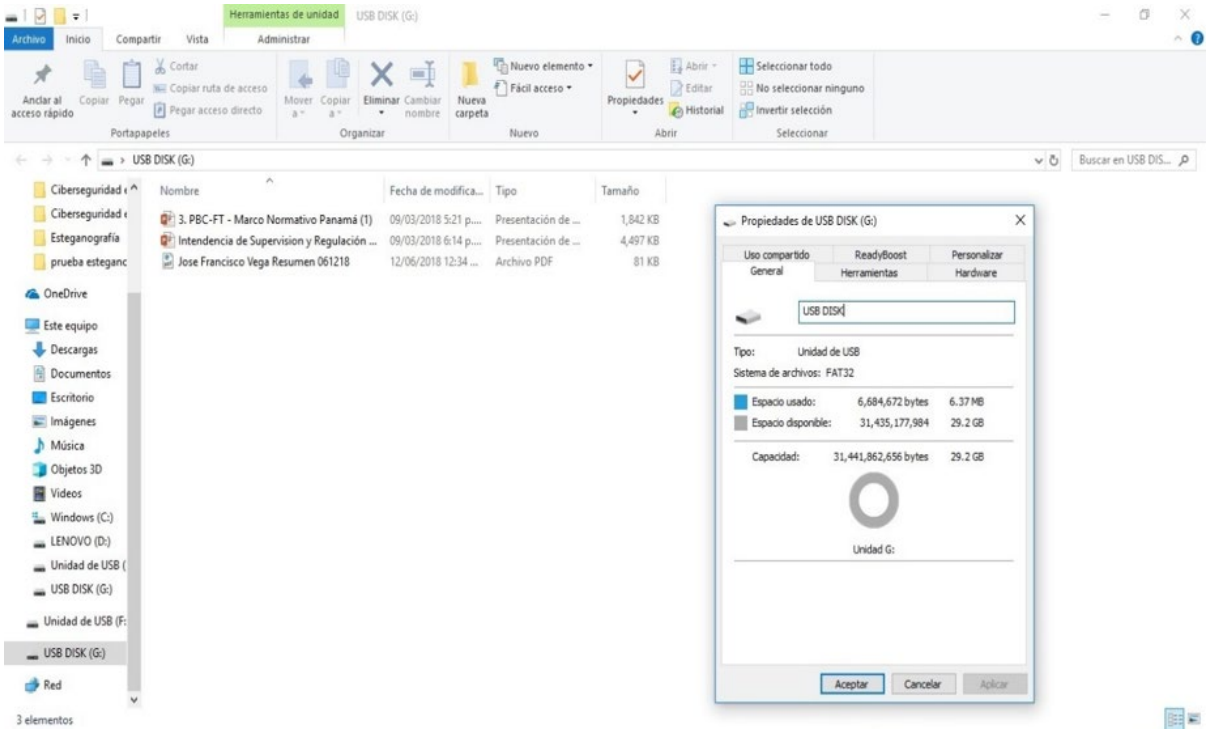


Figura 3: memoria USB de 29.2 GB, con tres archivos de contenido.

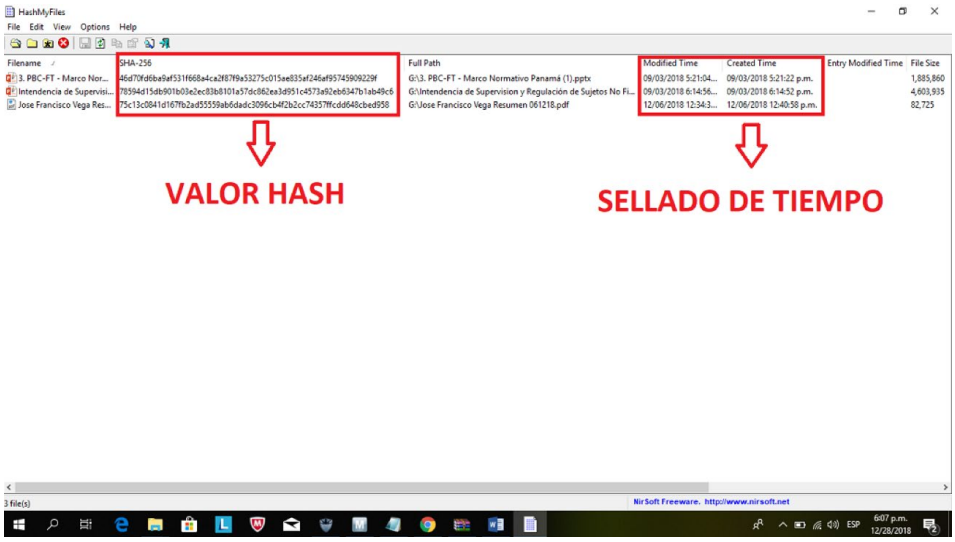


Figura 4: se muestra el valor Hash de los 3 archivos junto con el sellado de tiempo.

El fundamento legal del Hash y el sellado de tiempo se encuentra en el artículo 7 de la Ley 82 de 9 de noviembre de 2012, que modifica el artículo 2 y agrega el numeral 46 de la Ley 51 de 22 de julio de 2008 que establece lo siguiente:

46. Sellado de tiempo (Time stamping). Conjunto de datos en forma electrónica utilizados como medio para vincular inequivalente la existencia de un documento a un instante de tiempo y constatar el momento en que se ha efectuado una actuación sobre otros datos electrónicos a los que están asociados. Cuando cualquiera otra norma del ordenamiento jurídico panameño se refiera al sellado de tiempo, este servicio se encuentra comprendido en la definición de fechado electrónico.

El protocolo se sellado de tiempo también está regulado por el estándar internacional RFC 3161. Este documento hace hincapié en la aplicación del Hash tomando en cuenta las siguientes recomendaciones descritas textualmente:

"*Solo para marcar en tiempo una representación Hash del dato, es decir, una impresión de datos asociada con una resistencia a la colisión unidireccional función Hash identificada de forma única por un OID.*

Para examinar el OID del hash resistente a la colisión unidireccional función para verificar que la longitud del valor hash es consistente con el algoritmo Hash".

En relación a lo anterior podemos observar que la norma RFC 3161 hace mucho énfasis en el tema de la colisión de la función Hash, debido a que no basta sólo con sellar el documento electrónico o la evidencia digital con el valor Hash, este tiene que ser resistente a ataques contra los sistemas criptográficos que puedan penetrar y descifrar el algoritmo y por ende acabar con la integridad de la evidencia digital.

Podemos observar el Manual de Evidencias Digitales, emitido por el Ministerio de Justicia y Derechos Humanos de la República de Perú, en su página 52, anexo 1 establece lo siguiente:

"Para asegurar la integridad de la copia forense, se la auténtica ***mediante una función HASH o digesto matemático*** *(ANEXO III). Las imágenes forenses pueden realizarse mediante una computadora, un programa específico y un bloqueador de escritura, o bien, utilizando un dispositivo autónomo denominado duplicador forense.* ***EL HASH se refiere a una función o método para generar claves que representen de manera casi unívoca a un documento, registro, archivo etc.*** *Resumir un dato a través de la probabilidad, Utilizando una función hash o algoritmo hash.* ***El HASH permite darle mayor seguridad de que la evidencia digital obtenida no fue manipulada ni alterada, ya que el HASH generado es inviolable."***

3. LA CRIPTOGRAFÍA Y SUS FALENCIAS COMO MEDIO DE PRESERVACIÓN DE INTERIDAD DIGITAL

El autor Álvaro Gómez Veites nos menciona los principales ataques a los sistemas criptográficos en su obra denominada, Seguridad en Equipos Informáticos:

"Los ataques de fuerza bruta, que tratan de explorar todo el espacio posible de claves para romper un sistema criptográfico.

- *Los ataques de diccionario, que trabajan con una lista de posibles contraseñas: palabras*

de un diccionario en uno o varios idiomas, nombres comunes, nombres de localidades o accidentes geográficos, códigos postales, fechas de calendario etc.

• Los ataques contra el diseño del algoritmo.

• Los ataques contra los dispositivos hardware o las aplicaciones de software que lo implementan.

• Las distintas técnicas de criptoanálisis: criptoanálisis lineal, diferencial, técnica de análisis estadísticos de frecuencia".

Dentro de los sistemas criptográficos de función Hash que han sido colisionados podemos mencionar el MD5 de 32 caracteres alfanuméricos compuestos por 128 bit. El perito informático debe asegurarse de sellar las evidencias digitales con un valor Hash que no haya sido vulnerado, debido a que la contraparte podrá poner en tela de duda la resistencia y la integridad de la evidencia digital en caso de utilizar un sellado endeble.

En el año 2004 un grupo de expertos informáticos constituyeron el proyecto de computación distribuida MD5CRK, con el objetivo de demostrar que el Hash MD5 es inseguro frentes a los diferentes ataques a los sistemas criptográficos, incluso el algoritmo de Xiaoyun Wang y Hongbo Yu nos demuestra detalladamente en su informe cómo se puede implementar una colisión al MD5 y lograr un valor hash MD5 que se duplicado en dos documentos electrónicos diferentes.

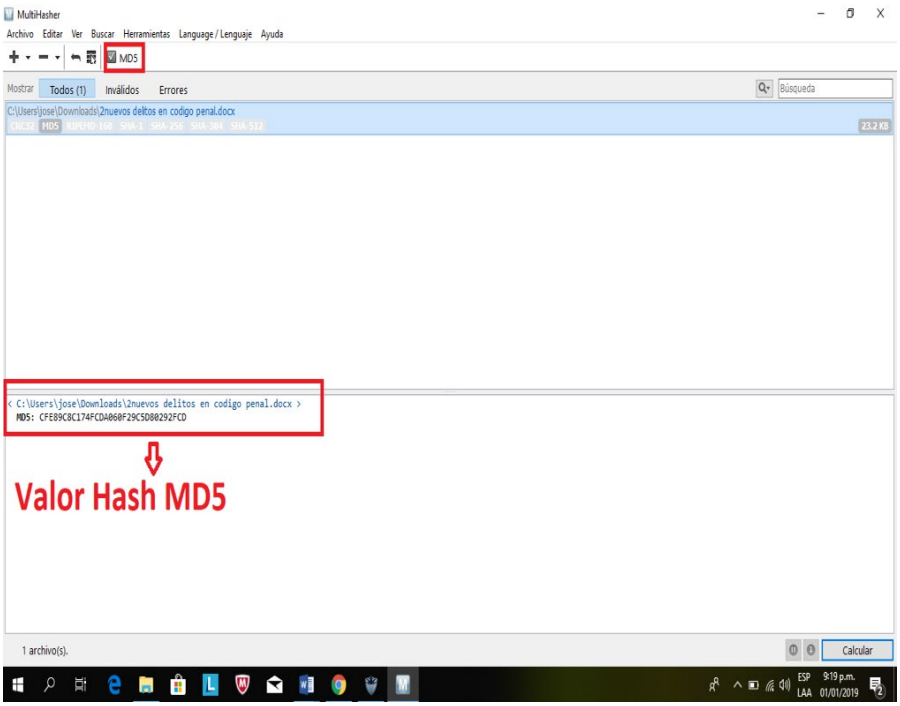


Figura 2: valor Hash MD5 de 128 bits representada típicamente como un número de 32 símbolos hexadecimales.

Incluso ya existen precedentes sobre la valorización judicial del uso del algoritmo criptográfico MD5 como método del sellado digital para proteger la integridad de la evidencia digital.

Un juez de tráfico en Australia invalidó una evidencia digital, debido a que el abogado del acusado logró demostrar que la función Hash MD5 es vulnerable y por ende no puede garantizar la integridad de la evidencia digital presentada.

En el portal web www.hispasec.com se relata de forma resumido el caso australiano:

"*Un australiano consigue anular una multa de tráfico ante la imposibilidad de las autoridades de tráfico de demostrar fehacientemente que la imagen registrada por un radar no ha sido alterada.*

Todo empezó cuando un australiano circulaba con su coche por una carretera que estaba siendo controlada con un radar que registra aquellos vehículos que circulan a una velocidad superior a la permitida. Si se sobrepasa la velocidad, automáticamente se emite una denuncia y se expide la correspondiente multa.

Hasta aquí nada destacable. Lo curioso del caso empieza cuando el abogado que representa al multado recurre la denuncia, argumentando que no se ha probado que la imagen obtenida por la cámara asociada al radar no ha sido modificada de ninguna forma.

Las autoridades australianas del tráfico responden a esta argumentación que se utiliza el algoritmo matemático MD5 para obtener una suma de control de las imágenes obtenidas por el radar. El problema radica en que no encuentran a ningún perito que demuestre ante el tribunal la validez de dicho algoritmo".

Dentro del Manual Único de Cadena de Custodia de Evidencias, emitido por el Ministerio del Poder Popular para Relaciones Interiores, Justicia y Paz, publicado Gaceta Ofic al No. 41.247 del 29 de septiembre de 2017 de la República Bolivariana de Venezuela, podemos observar en su página 36 las técnicas de embalaje secundarios referente a evidencias digitales.

"El embalaje secundario debe conglomerar las evidencias de misma naturaleza, y debe cumplir con el precintado sólo a efectos del traslado. Precintado Biológico: ADN sintético. Físico: Fleje, precinto desechable (T-RAP), sello, tiras, cinta o cordón ***Digitales: Algoritmo Hash, Código QR****."*

CONCLUSIÓN

Podemos recapitular que el derecho criptográfico es un elemento esencial en el mundo informático, debido a su técnica matemática relacionadas con los aspectos de seguridad de la información tales como la confidencialidad, la integridad de los datos, la autenticación de origen y entidad. Valiéndose principalmente de distintos métodos

de cifrado y de la funciones que generan un HASH, que sirve para verificar la integridad y autoría de una información o documento electrónico en particular que puede servir como evidencia en un proceso judicial. También debemos tener en cuenta otras funciones como la firma digital, que en gran parte de loa países tienen su legislación referente a este tema basado en sus reglamentos técnicos de cifrado asimétrico. Que a medida que los documentos y dinero efectivo se vayan desmaterializando vamos a tener una mayor necesidad de aplicar el Derecho Criptográfico.

BIBLIOGRAFIA

Arteaga, O. M. (2010). *Cibercriminalidad: Fundamentos de investigación en México.* México D.F.: Instituto Nacional de Ciencias Penales.

Barceló, R. O. (2016). *La Prueba Electrónica* . España: Juristas con Futuro .

International Organization for Standardization. (2015). *www.iso.org*. Obtenido de https://www.iso.org/standard/44406.html

Pino, D. S. (s.f.). *Manual de Manejo de Evidencias Digitales y Entornos*. OEA. Obtenido de https://www.oas.org/juridico/english/cyb_pan_manual.pdf

Real Academia Española . (s.f.). Obtenido de RAE: http://lema.rae.es/drae2001/srv/search?id=XhVdMwGHBDXX2WQEB9ll

Tecnologia & Informatica. (s.f.). Obtenido de https://tecnologia-informatica.com/que-es-el-bit-byte/

The Internet Society (. (2002). *www.rfc-editor.org*. Obtenido de https://www.rfc-editor.org/info/rfc3227

Maiorano, A. (2017). *Criptografía* . Mexico: Alfaomega Group.

MPPRIJP. (2017). *http://www.mpprijp.gob.ve*. Obtenido de http://www.mpprijp.gob.ve/wp-content/uploads/2018/05/ManualDeCustodia.pdf

ROLI, A. (s.f.). *https://www.mpfn.gob.pe/*. Obtenido de https://www.mpfn.gob.pe/Docs/0/files/manual_evidencia_digital.pd .

O SISTEMA JUDICIAL ELETRÔNICO E OS BENEFÍCIOS QUE O USO DO INSTRUMENTO DO BLOCK CHAIN PODERIA OCASIONAR NA INSTRUMENTALIZAÇÃO DOS PROCESSO E CONTRATOS

Eixos temáticos: Processo Eletrônico e Prova Digital

Autor:
João Felipe Fernandes de Souza
Graduando em Direito pela Estácio de Natal

RESUMO
O presente trabalho visa uma nova perspectiva de uso para tecnologias adaptativas, as quais já são amplamente usadas por outras esferas da nossa sociedade, tais como financeira e jornalísticas e tem enorme aceitação, além de ampla empregabilidade, bem como representam a adaptação do judiciário aos avanços que o advento das novas tecnologias proporcionou à vida cotidiana das quais o judiciário brasileiro pode se beneficiar frente as constantes mudanças que a globalização engendra as nossas vidas. O Processo Judicial Eletrônico admite a transmissão de dados de uma forma inda arcaica, que requer um intermediário, qual seja, uma empresa certificadora digital que esteja cadastrada ao judiciário, mesmo que já tenha apresentado grandes avanços, contudo, o *blockchain*, que é a ferramenta proposta à utilização na transmissão dos dados de usuários do processo judicial eletrônico. O trabalho faz uma comparação da perspectiva que o processo judicial eletrônico trouxe para o trabalho jurídico e como ele mudou, além da forma como funciona a transmissão de dados neste sistema, propõe o uso do *blockchain* como ferramenta para aumentar a celeridade e garantir a segurança jurídica em um estado de direito que notadamente sofre com vazamentos de informações ou mesmo modificação das informações originais. O *blockchain* proporcionaria, além de um avanço as bases de dados do sistema judiciário, mais segurança ao juízo competente que receberia provas com validade virtualmente incontestáveis. O trabalho foi estruturado com base em referências bibliográficas, pesquisas empíricas e observações cotidianas com o uso do sistema judicial eletrônico. A hipótese do trabalho é de que a adoção do *blockchain* como forma de transmissão de dados tornaria o judiciário mais seguro e célere, por não haver corrupção de dados digitais. Conclui-se que a utilização dessa nova tecnologia seria benéfica em várias esferas, não somente para o judiciário, como também para o erário da união e para os usuários que por vezes dependem do pagamento de precatórios ou requisitórios de pequeno valor assinados digitalmente.

INTRODUÇÃO

A globalização atingiu todas as relações humanas, inclusive e principalmente as financeiras O surgimento das *fintechs, definidas por Fernanda Yumikatori no seu trabalho de conclusão de curso, p.16 como"* Fintech é uma nova indústria financeira que aplica a tecnologia para aprimorar as atividades financeiras, *"legaltechs que o renomado site lecnews iden ica como"*. De modo geral, *lawtech* e *legaltech* são a mesma coisa. A abreviação de *Legal Technology – law* (advocacia) e *technology* (tecnologia) –, gerou o termo *lawtech*. Já a *legaltech* é uma forma prática de chamar empresas que oferecem soluções tecnológicas para assegurar a otimização de processos advocatícios. Essas empresas, em sua maioria, são startups. e *start-ups* é uma prova cabal dessa influência positiva. Os trâmites passaram a ser mais confiáveis, dotados de tecnologias como o *block chain*[1]. A *blockchain*, como é conhecida hoje, surgiu como a plataforma na qual a criptomoeda Bitcoin se baseia. A *blockchain* é um banco de dados distribuído que é usado para guardar uma lista crescente de registros, chamados de blocos, que são encadeados numa cadeia. Daí o nome em inglês, blockchain (para uma visão mais específica sobre o funcionamento da blockchain, ver Catalini & Gans, 2016; Lee, 2016; Nakamoto, 2008). Os registros guardados na blockchain podem ser transações financeiras entre duas ou mais pessoas, contratos, códigos de programação, entre vários outros itens que ficam registrados de forma permanente na blockchain. Pela natureza do protocolo criptográfico, alterar esses registros é uma tarefa muito difícil. De fato, a grande inovação da blockchain é exatamente sua capacidade de manter transações de forma segura, sem a necessidade de um intermediário de confiança entre as partes que estão transacionando. Que nada mais é do que uma tecnologia de registro distribuído que visa a descentralização como medida de segurança, o que garante que a publicidade dos fatos seja maior. O espaço do direito ampliou-se e saiu da esfera física para um mundo completamente novo, como é o da informática, um universo completamente diverso e com possiblidades ampliadas em face do universo físico, onde as barreiras são quebradas a todo momento, tendo assim novas modalidades de contratos e de obrigações.

O advento da tecnologia foi fundamental para a ressignificação das relações humanas e tornou as distâncias muito menores, os laços foram encurtados, bem como dificuldades foram sanadas, assim também não pôde deixar de acompanhar o direito, que apesar de adaptar-se após os acontecimentos, se viu forçosamente enquadrando-se em um novo conceito de relações jurídico-sociais.

A celeridade da justiça que antes fora tão criticada e ainda sofre com os entremeios da ineficiên ia dos aparatos que o Estado oferece, foi acrescida de uma velocidade enorme após a digitalização do judiciário, tornando os trâmites muito mais confiáveis e rápidos, e que podem ainda mais ser assegurados com a incrementação do instrumento do *blockchain* como forma de pagamento de precatórios ou Requisitório de Pequenos Valores, além da garantia do princípio do contraditório e da celeridade processual serem mais salvaguardados. Logo após o advento do Processo Judicial

Eletrônico, como mostram os dados do Conselho Nacional de Justiça em sua revista CNJ EM NÚMEROS. É possível salientar a eficiência resultante do modelo em cada indicador de forma separada, a partir da relação entre a taxa de congestionamento e, respectivamente, a produtividade dos magistrados (Figura 134), a produtividade dos servidores (Figura 135) e a despesa total (Figura 136). Os tribunais que mais se aproximam da linha de fronteira (linha azul nessas figuras) são os mais eficientes, e os mais distantes dessa linha, os menos eficientes. Os Tribunais de Justiça de Sergipe e de Roraima, ambos de pequeno porte, estão na fronteira de eficiência em todos os casos, enquanto o TJRJ (grande porte) apresentou o melhor desempenho nos indicadores de produtividade por magistrado e por servidor. O TJRS encontra-se na fronteira de eficiência ao considerar a despesa total por processo baixado e produtividade por servidor; o TJPR também está nessa última fronteira" em 2017 os processos sofreram um acréscimo de velocidade absurda em seus andamentos, pois para o juízo há mais possibilidades de desenvolver um trabalho mais focado.

Não menos importante, para o juízo, é mister observar a velocidade e atentar para o fato de que os contratos tem cláusulas, hoje em dia, muito mais específicas, o que dificult para o consumidor quando confir a a contratação, apertando naquele simples botão de "aceito os termos de uso", sem saber o que de fato contrata, ao que tem direito e quais seus deveres nessa relação.

1. O PROCESSO JUDICIAL ELETRÔNICO E SEU FUNCIONAMENTO FRENTE AO FUNCIONAMENTO PELA POSSIBILIDADE DO USO DO *BLOCKCHAI*N

O Processo Judicial eletrônico hoje funciona como uma base de dados receptora que necessita de um certificado digital feito por uma entidade credenciada, o proposto pelo trabalho seria transformar a certificação em forma de blockchain, o que criaria mais segurança na transmissão de dados e excluiria um intermediário que onera o judiciário. O blockchain tornaria ainda mais eficiente a transmissão de dados, e baratearia os custos dos usuários, além de gerar mais celeridade processual.

1.1 o blockchain

A princípio, é importante salientar a importância da ferramenta de descentralização que é o *block chain*, que tem como finalidade garantir cada vez mais segurança aos usuários, redistribuindo os registros de qualquer operação feita via internet. Em tese, esse processo garante que o poder da informação não permaneça somente em nas mãos de uma entidade, o que relaciona o princípio do contraditório, pois garante

que as duas partes de um processo tenham conhecimento do que se passa durante a celebração de um contrato, o *blockchain* equilibra a balança jurídica e comercial.

1.2 O funcionamento do block chain

Segundo André Salem, pesquisador do IBM Blockchain:

> "O blockchain é uma interface de negócios segura, na qual os participantes transferem itens de valor (ativos), por meio de um ledger (livro-razão) comum distribuído, do qual cada participante possui uma cópia, e que tem seu conteúdo em constante sincronia com os outros."

São elos que formam uma cadeia pela qual todos os participantes monitoram as atividades, sem que haja possibilidade de interferirem, pois não há brechas de segurança que sustentem a possibilidade de modificarem conteúdo. Logo, a mesma lógica usada em ativos e livros-razões pode ser usada em transmissão dos dados dos sistemas judiciais eletrônicos.

O *blockchain* funciona como uma cadeia de elos. Estes possuem uma área de transação e uma área de cabeçalho, como elaborou TIMOTEO PIMENTA PIRES em seu trabalho de conclusão (2016). Na área de transação estão todas as transações coletadas por aquele bloco e na área de cabeçalho estão o *hash* do cabeçalho.

2. O PROCESSO JUDICIAL ELETRÔNICO

O processo judicial eletrônico surgiu como forma de inovar as relações jurídicas no Brasil, com a lei nº 11.419, de 19 de dezembro de 2006 teve aplicabilidade eficiente tornando mais céleres os processos e garantindo publicidade maior aos usuários. Em todas as esferas do direito, seja penal, trabalhista, civil ou fazendária, houve notável aumento de agilidade nos trâmites processuais, garantia de publicidade e maior comodidade para os usuários do sistema.

Segundo o Conselho Nacional de Justiça "O Processo Judicial eletrônico (PJe) é um sistema desenvolvido pelo CNJ em parceria com os tribunais e a participação da Ordem dos Advogados do Brasil (OAB) para a automação do Judiciário."

O objetivo principal é manter um sistema de processo judicial eletrônico capaz de permitir a prática de atos processuais, assim como o acompanhamento desse processo judicial, independentemente de o processo tramitar na Justiça Federal, na Justiça dos Estados, na Justiça Militar dos Estados e na Justiça do Trabalho.

O CNJ pretende convergir os esforços dos tribunais brasileiros para a adoção de uma solução única, gratuita para os próprios tribunais e atenta para requisitos

importantes de segurança e de interoperabilidade, racionalizando gastos com elaboração e aquisição de *softwares* e permitindo o emprego desses valores financeir s e de pessoal em atividades mais dirigidas à finalidade do Judiciário: resolver os conflito

A utilização do sistema exige a certificação digital de advogados, magistrados, servidores ou partes que precisarem atuar nos novos processos.

Contudo, restam ainda algumas lacunas a serem preenchidas quando a segurança da transmissão de dados, onde o *blockchain* poderia auxiliar, pois somente o certificado de assinatura digital, que todas as partes devem ter emitidas por autoridade específica certificadora e credenci da, sugere ainda falhas. Ainda que sejam admitidas as provas por meio digital, essas provas podem ser corrompidas de acordo com o *know-how* de um usuário mal intencionado que tenha as ferramentas necessárias para deturpar as provas ou provocar falhas nessa transmissão de dados.

O processo judicial eletrônico torna mais célere o julgamento de processos de um país que culturalmente sofre de um fenômeno de hiper judicialização, entretanto, certa insegurança jurídica é gerada por essas possíveis falhas na transmissão de dados, pincipalmente no tocante as fases mais posteriores dos processos, onde ocorrem os pagamentos por expedição de alvarás.

2.1 O pagamento das causas pós fixação do juízo pela sentença

Contudo, por vezes, mesmo tendo uma eficiê cia maior no cumprimento de prazos processuais, o último e mais importante momento àquele que necessita, que é o do pagamento fixado pelo juízo, acaba por demorar, sobretudo nas causas contra a fazenda pública, pois bem como disse Cf. Renato Luis Benucci, A tecnologia aplicada ao processo judicial (p.22). Campinas, SP: Millenium, 2007:

> "O maior problema da Justiça brasileira tem sido atribuído ao descompasso entre o tempo do processo com a finalização da execução e satisfação do direito exigido e o tempo do mundo moderno globalizado. O paradigma da justiça deve ser modificado para deixar de atuar somente em tempo pretérito, em restauração do direito lesado, a fim de resgatar o direito presente, não somente com o auxílio da informática, bem como de meios alternativos de solução de conflitos em ação conjunta com o Judiciário.

Os pagamentos ainda hoje feitos por meio de precatórios com alvarás demoram a ser emitidos, influenc am diretamente na situação econômica do estado ou união e geram um desconforto enorme ao usuário do sistema judiciário, pois os documentos não gozam de tanta segurança e velocidade quanto deveriam.

A lei de precatórios ainda hoje como pode-se verificar encontra-se ineficiente em não garantir um direito no momento em que ele é devido, bem como demonstra o dispositivo de lei nº 13.463, de 6 de julho de 2017:

> "Art. 1º
> A gestão dos recursos destinados aos pagamentos decorrentes de precatórios e de Requisições de Pequeno Valor (RPV) federais será realizada pelo Poder Judiciário, que contratará, com dispensa de licitação, instituições financeiras integrantes da administração pública federal para a operacionalização da gestão dos recursos.
> Parágrafo único. Os valores correspondentes à remuneração das disponibilidades dos recursos depositados, descontada a remuneração legal devida ao beneficiário do precatório ou da RPV, constituirão receita e deverão ser recolhidos em favor do Poder Judiciário, o qual poderá destinar até 10% (dez por cento) do total para o pagamento de perícias realizadas em ação popular.
> Art. 2º Ficam cancelados os precatórios e as RPV federais expedidos e cujos valores não tenham sido levantados pelo credor e estejam depositados há mais de dois anos em instituição financeira oficia
> §1º O cancelamento de que trata o caput deste artigo será operacionalizado mensalmente pela instituição financeira oficial depositária, mediante a transferência dos valores depositados para a Conta Única do Tesouro Nacional.

O escopo da discussão trazida a tona é: seria necessário mesmo manter de forma tão arcaica o processo de pagamento dessas causas; uma nova tecnologia não poderia ajudar na obtenção de resultados superiores e mais satisfatórios, gerando leveza aos servidores do judiciário e uma aprovação maior da população em referência a este órgão que por vezes vem sendo rechaçado.

3. A EFICIÊNCIA E SEGURANÇA QUE O BLOCK CHAIN GARANTIRIA AO PROCESSO

Bem como já foi dito, o *blockchain* é uma ferramenta que possibilita a descentralização de informações e torna mais segura a cadeia de passagens das mesmas. Dados mostram que há uma redução a quantidade quase inexistente de quebra de segurança e protocolos quando usado o *blockchain* nas transações financeiras, o mesmo poderia ocorrer nos processos digitais que dependem exclusivamente da passagem de informações de um servidor para outro, em que pese, dos servidores dos usuários para o servidor dos tribunais de justiça.

3.1 A garantia do princípio da duração razoável do processo e satisfação dos usuários com a implantação de novas tecnologias

É importante reconhecer a morosidade no atendimento aos usuários dos sistemas judiciários brasileiros, ainda que tenham melhorado com as tentativas ultimamente implantadas, deixam muito a desejar a todos os usuários dos serviços.

Respeitando o princípio da tempestividade do direito, que como versa Fredie Didier:

> Bem pensadas as coisas, conquistou -se, ao longo da história, um direito à demora na solução dos conflitos. A partir do momento em que se reconhece a existência de um direito fundamental ao devido processo, está-se reconhecendo, implicitamente, o direito de que a solução do caso deve cumprir, necessariamente, uma série de atos obrigatórios, que compõem o conteúdo mínimo desse direito. A exigência do contraditório, os direitos à produção de provas e aos recursos certamente atravancam a celeridade, mas são garantias que não podem ser desconsideradas ou minimizadas. É preciso fazer o alerta, para evitar discursos autoritários, que pregam a celeridade como valor. Os processos da Inquisição poderiam ser rápidos.

4. CONCLUSÃO

Com o advento da tecnologia, e avanço das formas de obtenção de segurança e privacidade, o judiciário brasileiro há muito deveria estar se beneficiando dessas novas ferramentas, garantindo graus de satisfação muito mais elevados dos seus usuários e equidade maior a todos os usuários que por ventura não tenham equipamento mais sofisticada que os garantam maior nível de segurança. Hodiernamente, temos que acompanhar os avanços da sociedade para que os parâmetros de igualdade sejam respeitados e aquele que precisa, tenha seus direitos garantidos da forma mais célere possível, ora, não pode um indivíduo necessitado esperar o trâmite um processo que possa durar décadas, ou a expedição de um precatório que, em caso de idosos, pode dificultar até mesmo o saque após os anos que teve que esperar pelo seu recebimento. É de extrema importância atentar para o fato de que a justiça deve acompanhar os avanços benéficos da sociedade, não obstante observando as novas formas de promover o direito.

REREFÊNCIAS BIBLIOGRÁFICAS

Cf. BENUCCI, Renato Luís. A tecnologia aplicada ao processo judicial. Campinas, SP: Millenium, 2007. p 25 ss; COSTA, Marcos da; MARCACIN1, Augusto Tavares Rosa. Direito em Bits. São Paulo: Fiúza, 2004. ALMEIDA, Jorge Luiz de. Emenda constitucional n. 45/04 e responsabilidade, p. 1-28; OLIVEIRA, Luiz Flávio de. A razoável duração processo na perspectiva dos direitos humanos, p. 89-104; DE PIERI, Sueli Aparecida. Princípio da celeridade processual; Duração razoável do processo e hierarquia da normas de tratados internacionais de direitos humanos: Instituídos

pela Emenda Constitucional n. 45, p. 105-131. In: A Reforma Do Poder Judiciário. Campinas, SP: Millennium, 200

LEI Nº 11.419, DE 19 DE DEZEMBRO DE 2006

LEI Nº 13.463, DE 6 DE JULHO DE 2017

DIDIER, Fredie, Curso de Direito Processual Civil, Introdução ao Direito Processual Civil, Parte Geral e Processo de Conhecimento, 17ª Edição, Salvador, Editora Jus Podium

http://www.lecnews.com.br/blog/o-que-e-legaltech-entenda-aqui/ (30/06/2019)

http://www.cnj.jus.br/files/conteudo/arquivo/2018/09/8d9faee7812d35a58cee3d92d2df2f25.pdf (30.06.2019)

blockchain como um fator de mudança na competição e no arranjo econômico de oportunidades. irene ciccarino pontifícia universidade católica do rio de janeiro (puc-rio) (2017)

IMPACTO DA TECNOLOGIA SOBRE A JUSTIÇA

Eixo Temático: Processo Eletrônico

Autor:
Marcos da Costa
Advogado, Presidente da OAB SP nas gestões 2013 a 2015 e 2016 a 2018. É Conselheiro do Conselho Universitário da Pontifícia Universidade Católica de São Paulo

RESUMO
O artigo traz o histórico do processo de informatização do Poder Judiciário, desde o uso da tecnológica em atividades cartoriais, até seu emprego para a prática de atos processuais, sob a ótica da experiência do autor, que acompanhou todas as etapas desde a época em que os primeiros computadores foram usados para substituir as máquinas de escrever até os dias de utilização da inteligência artificial. O autor teve oportunidades de testemunhar essa evolução, não apenas como advogado, mas especialmente como dirigente da OAB, já que sua trajetória na instituição como com a presidência da primeira comissão de informática jurídica da OAB de São Paulo e, despois, da OAB Nacional, participando das discussões junto aos órgãos gestores do Poder Judiciário e junto ao Congresso Nacional brasileiro, onde apresentou, como presidente daquela Comissão paulista, dentre outros, os primeiros projetos tratando de documento eletrônico, assinatura digital e comércio eletrônico, além de participar de audiência pública sobre projeto de lei que dispunha sobre informatização do processo judicial, onde propôs a criação do diário oficial eletrônico do Poder Judiciário, adotado atualmente por todos os tribunais do país.
Essas informações são relevantes para compreensão sobre as resistências enfrentadas por questões culturais e as respectivas dificuldades financeiras, mas também os benefícios alcançados com a implantação do processo eletrônico. Uma das diversas batalhas das quais o Autor participou foi a luta pela adoção, na lei brasileira, da criptografia assimétrica como instrumento para geração de assinaturas digitais, assegurando ao documento eletrônico o mesmo valor probante do documento lavrado em papel, combatendo o discurso de que a lei não poderia engessar a tecnologia com a afirmação de que criptografia assimétrica é um algoritmo matemático e a tecnologia na verdade apenas é responsável por sua aplicação.
O Autor finaliza o trabalho expondo sobre o estágio atual da tecnologia jurídica, com a chegada da inteligência artificial. Menciona legislações estrangeiras que buscam limitar o uso dessa tecnologia, e o tratamento que já é dado sob o ângulo da ética de seus desenvolvedores. E desperta a atenção para o fato de que o Poder Judiciário brasileiro já está empregando a IA para reconhecer recursos e que está estudando outras modalidades de aplicação.

IMPACTO DA TECNOLOGIA SOBRE A JUSTIÇA

O filme Suprema se passa na década de 50 e trata da luta da igualdade de gênero empreendida, desde o tempo de brilhante estudante, pela advogada Ruth Bader Ginsburg, que depois assumiria uma cadeira na Suprema Corte Americana. Em determinado momento do filme, alguém sugere o uso de computadores para identifica , dentro do cipoal de normas americanas, aquelas numerosas que, sob os mais diferentes aspectos, impunham tratamento diferente entre homens e mulheres,

e que assim poderiam sofrer impacto de um eventual precedente do reconhecimento de inconstitucionalidade da norma da Receita Federal que estava sendo contestada por proibir desconto tributário de gastos com homens cuidadores. E a resposta foi o assombro espelhado na dúvida sobre qual mundo estaríamos criando, quando um computador é capaz de substituir o ser humano na leitura e interpretação de leis.

A tecnologia foi invadindo todas as atividades e áreas do conhecimento humano, e era inevitável que o direito também viesse a sofrer seus impactos, notadamente após a chegada dos computadores de mesa na década de 80 e, ainda mais especialmente, da popularização da internet, na década de 90.

A evolução do uso de tecnologia pela Justiça é lenta e em regra encontra resistências. Em meados da década de 80, por exemplo, quando advogados começaram a trocar a datilografia das máquinas de escrever pela digitação dos teclados de computadores, diversas iniciais foram declaradas ineptas por conta da falta de acentuação dos textos, tarefa que os sistemas informáticos de então (teclado, software de edição, driver de impressoras) não conseguiam atender.

No começo dos anos 90, o foco de atenção era o uso da tecnologia para suporte de suas atividades burocráticas, como a substituição dos fichários de anotações de andamentos processuais por fichários eletrônicos.

Na presidência de Dirceu de Mello (1998 e 1999) surgiu uma oportunidade de avanço na informatização da estrutura da Justiça Paulista. A Imprensa Oficial fez uma constatação: ao contrário do que já acontecia com os Poderes Executivo e Legislativo, o Judiciário ainda encaminhava em formato impresso, em folhas papel, seus atos para publicação no jornal ofi ial. O custo com remessa de atos processuais nas numerosas comarcas paulistas e o tratamento do papel para impressão era gigantesco, fora o tempo que isso representava. Embora a própria Imprensa Oficial tivesse se proposto a financiar uma rede privativa para que a transmissão dos atos passasse a ser eletrônica, houve imensa resistência da magistratura em permitir que isso ocorresse. Para se ter ideia da dificuldade em sua implantação, alguns juízes anulavam intimações se na publicação da decisão no Diário Oficial não fosse impressa a sua assinatura manuscrita. Só na gestão seguinte, do Presidente de Marcio Bonilha (2000 a 2001), conseguiu-se implementar a medida, mesmo assim após o novo presidente baixar ato obrigando os juízes a aceitarem a transmissão eletrônica das decisões judiciais. Um estudo realizado à época pela Imprensa Oficial mostrou que a transmissão eletrônica das decisões judiciais representou uma economia anual, em valores da época, de aproximadamente R$ 4.500.000,00, e um ganho médio em torno de 220 dias na tramitação dos processos, considerando o número médio de publicações por processo, e o tempo que transcorria do encaminhamento em papel da decisão até sua publicação.

Não havia naquele momento investimento do Poder Judiciário em informatização. Os poucos equipamentos que existiam nos fóruns eram adquiridos pessoalmente por

magistrados e serventuários. Até que em 2001, durante uma longa greve, a maior, até então, da Justiça Paulista, acontece um fato pitoresco, mas revelador da situação em que se encontrava o Tribunal de Justiça: os servidores em greve levam embora seus computadores, obrigando o presidente Marcio Bonilha a baixar ato proibindo-os de apagar os dados processuais armazenados naqueles equipamentos pessoais.

Já a época alguns Tribunais começaram a utilizar a internet para divulgar seus acórdãos, mas não a Corte paulista. Após a eleição do novo presidente do Tribunal, ocorrido no final de 2001, publiquei, como presidente da Comissão de Informática, junto com o então presidente da OAB SP, um artigo denunciando que a ausência do TJ-SP na internet significava simplesmente seu desaparecimento como paradigma do direito, posto que seria muito mais fácil a operadores e estudantes pesquisar e conhecer acórdãos de qualquer outro tribunal do país [615]. Fomos ambos chamados a conversar com o Presidente recém-eleito do Tribunal, Sergio Nigro Conceição (2002 a 2003), que disse compreender a crítica da OAB SP mas que não tinha dinheiro para investir em informática, ao que sugerimos que solicitasse esse valor dos bancos públicos que detinham os depósitos judiciais. Dai surgiu o primeiro grande investimento em informática da Corte, promovido pela Caixa Econômica de São Paulo [616].

Em 2004, uma crise no Tribunal de Justiça, presidido por Luiz Elias Tâmbara, impactou no processo de evolução da informática: a Emenda 45, que dentre outros pontos, como da criação do CNJ e CNMP, promoveu a unificação do Tribunal de Justiça com os Tribunais de Alçada. São Paulo tinha até então 3 tribunais de alçada: dois cíveis e um criminal e cada um com um sistema de informática diferente. A integração simplesmente jamais ocorreu.

Em paralelo à informatização de tarefas burocráticas do Judiciário, estava sendo promovida uma discussão mais profunda, do uso da tecnologia para a prática de atos processuais, com a troca do papel pelo meio eletrônico [617].

A substituição da manifestação de vontade expressa em papel, por aquela promovida por meio eletrônico, reclama o cumprimento de basicamente três requisitos: integridade, que é basicamente a possibilidade de identificar eventuais mudanças que o texto eletrônico possa sofrer depois de se apresentar como documento, e autoria, ou seja, a sua vinculação, como elemento imaterial, ao seu autor. O terceiro requisito, que

615 A Justiça e o comércio de informação legal, Folha de São Paulo, Tendências e Debates, 02 de janeiro de 2002.

616 http://www.saopaulo.sp.gov.br/eventos/judiciario-paulista-estara-totalmente-informatizado-ate-o-final-de-2003/3

617 Augusto Tavares Rosa Marcacini, que no país foi provavelmente quem primeiro se interessou pela questão, dentro de sua formação acadêmica de mestre e doutor em processo civil, assim define, com precisão, o conceito de documento eletrônico: "Uma seqüência de bits que, traduzida por meio de determinado programa de computador, seja representativa de um fato" (em "Direito e Informática – Uma Abordagem Jurídica sobre Criptografia", Editora orense, página 66).

nem sempre é destacado, é a acessibilidade, ou seja, a capacidade de terceiros terem acesso as informações nele inseridas[618].

No documento em papel, técnicas periciais são capazes de identificar as menores modificações que o texto tenha sofrido, de forma a permitir que eventual questionamento sobre a veracidade de seu conteúdo possa ser verificado. De outra parte, a identidade do autor de um documento em papel é comprovada por meio de sua assinatura, também conferível por meio de perícia.

Já o documento eletrônico, por ser imaterial, não apresenta, por si, os elementos que permitem aferir quer a sua titularidade, já que nenhum dado biométrico poderia vincular diretamente seu teor a determinada pessoa, quer a sua integridade, uma vez que corresponde a uma sequência de zeros e uns, cuja modificação não é detectável por meio de perícia.

Na década de 70, dois professores de Stanford, Martim Hellman e Whitfiled Diffie buscavam encontrar solução para uma questão essencial para o sigilo da informações, ou seja, das distribuição da chave criptográfica para decodificar uma mensagem criptografada. Por maiores que foram os avanços na complexidade da criptografia de mensagens, especialmente no plano militar, para evitar que pessoas desautorizadas tivessem acesso ao seu conteúdo, um ponto crítico permanecia em aberto, ou seja, como fazer com que o destinatário da mensagem tivesse acesso à chave que permitiria tornar acessível a mensagem, sem que terceiros conseguissem obter cópia dela.

Em outras palavras. A criptografia tradicional está baseada em dois métodos, um para criptografar a mensagem e o outro para decriptá-la. E em uma única chave, a mesma usada para as duas funções. O exemplo tradicionalmente apresentado e de fácil compreensão é o de Julio Cesar, que codificava as ordens para as suas tropas, substituindo cada letra do texto pela terceira letra subsequente no alfabeto. O método para criptografar a mensagem era o avanço de letras à frente do alfabeto; e o método para decriptar era retornar para letras anteriores no alfabeto; e a chave, única nos dois métodos, era o número três: três casas à frente, três casas atrás. [619]Com o avanço da criptografia, século após século, critérios mais complexos passaram a ser usados, mas sempre seguindo esse mesmo modelo: uma mesma chave cifra e decifra a mensagem. E era exatamente na dificuldade de distribuição segura dessa chave que residia o risco de quebra do sigilo criptográfico.

---

618 Não é comum a doutrina mencionar esse terceiro requisito, mas é importante notar que um documento que não permita conhecer seu conteúdo não pode ter valor judicial. No documento eletrônico, onde o uso da criptografia se torna cada vez mais comum, e essencial, é possível criptografar documentos com chaves de sigilo impedindo que terceiros, mesmo um juiz, possam ter acesso ao seu conteúdo. Verifique-se, nesse sentido, o disposto no art. 166, 2, do Código de Processo Penal de Portugal, que determina: "Artigo 166.º (Tradução, decifração e transcrição de documentos) 2 - Se o documento for dificilmente legível, é feito acompanhar de transcrição que o esclareça, e se for cifrado, é submetido a perícia destinada a obter a sua decifração.

619 Essa cifragem é conhecida como Cifra de César.

Hellman e Diffie por sua vez, inovaram e criaram um algoritmo matemático que invertia o processo. Ao invés de dois métodos, um apenas. E substituía a única chave por duas. Descobria-se a criptografia assimétrica, que, posteriormente, percebeu-se ser capaz de gerar uma "assinatura eletrônica" capaz não apenas de servir, como faz a manuscrita no papel, para vincular documentos eletrônicos a alguém, como também promover o controle de sua integridade [620].

Basicamente, o sistema trabalha com as chaves publica e privada. O que a chave privada faz, a chave pública desfaz. E vice-versa. Ambas as chaves são geradas por um algoritmo que usa elementos aleatórios que impedem que a mesma operação matemática gere um par de chaves igual ao outro [621]. Como exemplo, imagine-se uma operação que tivesse como fatores o número de série de uma CPU e do sistema operacional, a velocidade da ventoinha do equipamento, a soma dos "uns" e "zeros" de arquivos armazenados no equipamento, a hora da emissão das chaves, etc. Todos esses elementos, que são estatisticamente improváveis de se repetirem em um outro computador, serviem como fatores na operação matemática de geração das chaves. O par de chaves se torna, assim, estatisticamente único, a cada vez que é gerado, evitando que duas pessoas possam ter as mesmas chaves.

A chave privada é aquela de conhecimento único de seu titular, guardada sob proteção de senhas. Já a chave pública é de conhecimento de todos com quem ele pretenda se relacionar e muitas vezes, para conhecimento do público em geral.

Aquele que quiser passar uma informação sigilosa para outrem utiliza da chave pública do destinatário para codificá-la. E seu titular utiliza da chave privada de mesmo par, que é sigilosa, para decriptá-la. Esse sistema é muito usado, por exemplo, em operações financeiras na internet.

Por sua vez, o dono do par de chaves pode utilizá-lo para "assinar" eletronicamente um documento. Como só ele tem acesso à chave privada, sigilosa, só ele consegue acioná-la na operação matemática que irá gerar a "assinatura" eletrônica, que nada mais é do que o resultado de uma operação matemática que tem como fatores, além da chave privada, um resumo matemático dos zeros e uns que compõem a sequência binária do documento.

---

620 Sobre a história da descoberta da criptografia assimétrica, ver "O Livro dos Códigos: A Ciência do Sigilo – do antigo Egito à Criptografia Quântica" (The Code Book, no original), de Simon Singh, importante estudo sobre a evolução da criptografia até os dias atuais (Editora Record, Tradução de Jorge Calife).

621 Daniel Balparda de Carvalho esclarece: "A geração de números aleatórios é central na prática criptográfica moderna. Isto porque, por um lado, eles são necessários como ferramentas para várias tarefas na criptografia e por outro, bons números aleatórios são relativamente difíceis de conseguir." E em seguida, afirma: "Na criptografia precisa-se dos chamados números aleatórios criptograficamente fortes. É impressionante como se pode facilmente ser enganado quando se trata de gerar este tipo de número. Normalmente, quando se precisa de um número aleatório na criptografia, o inimigo não pode, nem de perto, desconfiar qual o número escolhido. Se ele possuir um meio de reproduzir o processo de geração de números e/ou limitar o espaço de procura, então o número não é adequado para usos criptográficos." (em Criptografia: Métodos e Algoritmos", Editora Express Book, página 59)

Presume-se por estatística, já que não é possível gerar o mesmo par duas vezes, que se uma chave pública validar a assinatura eletrônica do documento, é porque seu titular, que detém a chave privada, sigilosa, correspondente, foi quem a gerou. Assegura-se com isso a certeza de autoria. Ao mesmo tempo, ao se validar, com a chave pública, aquele resumo matemático denominado "assinatura eletrônica"tem-se a certeza de que o documento do qual foi extraído não sofreu modificação. Isso porque qualquer mudança na sua sequência binária modificaria seu resumo matemático, invalidando o próprio documento. Garante-se, como isso, sua integridade. Desta forma não apenas documentos eletrônicos podem ser utilizados para expressar manifestações de vontade, como também passam a servir como prova processual. Mais ainda. Atos processuais, como petições, certidões e despachos podem utilizar a mesma metodologia para sua elaboração.

Diversos países passaram a adotar leis [622], assim como a Comunidade Europeia, com diretiva de seu Parlamento [623], destinadas a assegurar ao documento eletrônico gerado com emprego da criptografia assimétrica o mesmo valor jurídico daqueles emitidos em papel com assinatura manuscrita.

No Brasil, o primeiro projeto de lei a tratar de documentos eletrônicos, o PL 1589/99, na Câmara dos Deputados, foi elaborado pela Comissão de Informática da OAB de São Paulo, a primeira em todo o país, que tive a honra de presidir.

Em 2001, o Governo Federal adotou a Medida Provisória 2.200, criando a chamada ICP – Brasil, Infra-Estrutura de Chaves Públicas do Brasil [624], que criou o sistema único de certificação digital do país, cuja existência visou a dar validade jurídica aos documentos eletrônicos.

Certificado eletrônico nada mais é do que uma declaração formulada em formato eletrônico padrão, que atesta a quem pertence a chave pública e, assim, da chave privada a ela correspondente. É como um atestado de titularidade do par de chaves, que gera e confere a assinatura digital.

O modelo adotado no Brasil pela MP 2200 é único no mundo, e foi objeto de diversas críticas nossas, a começar por conter, na sua primeira versão, a obrigação de que o par de chaves criptográficas, que serve não apenas para gerar assinaturas, mas também para criptografar mensagens e assegurar o sigilo delas, fosse fornecido pela CEPESC - Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações, que é o braço tecnológico da ABIN – Agência Brasileira de Informação, sucessora

---

622 Argentina - Ley 25.506, de 11/12/ 2001; Austrália - Electronic Transactions Act 1999; Chile - Ley 19799, de 25/03/2002; EUA – Electronic Signatures in Global and National Commerce Act , de 30/06/2000;

623 Diretiva 1999/93/CE, do Parlamento Europeu e do Conselho, de 13 de dezembro de 1999, relativa a um quadro legal comunitário para as assinaturas eletrônicas.

624 A expressão Infra-Estrutura de Chave Pública tem origem na expressão inglesa Public Key Infrastructure – PKI

do SNI – Serviço Nacional de Informação[625]. As críticas que fizemos à arapongagem institucional deram resultado e o CEPESC foi afastado da emissão das chaves criptográficas. O sistema centralizado de emissão de certificados eletrônicos, porém, permanece até os dias atuais, embora sustentado juridicamente por uma Medida Provisória que jamais foi votada pelo Parlamento, eis que teve sua vigência prorrogada indefinidamente pela disposição transitória do art. 2º, da EC 32/2001.

Em 2006, foi promulgada a Lei nº 11.419, dispondo sobre informatização do processo judicial. Tive a oportunidade de participar da audiência pública na comissão especial que analisava o respectivo projeto de lei, onde apresentei propostas para diversas alterações, muitas delas acolhidas, e dentre elas o uso da assinatura digital para a prática de atos processuais e a criação do Diário Oficial Eletrônico, idealizado junto com Augusto Marcacini na Comissão de Informática da OAB SP.

A criação do Diário Oficial Eletrônico evidencia os múltiplos efeitos que o uso da tecnologia pode gerar. O Diário Oficial do Poder Judiciário de São Paulo era até então a maior mídia impressa diária de todo o mundo, com média de 2.200 páginas diárias. Além do impacto ambiental, o diário eletrônico representou economia para as empresas paulistas, já que, como o diário em papel não era pago pelo Judiciário, seu custo era incorporado no preço das publicações obrigatórias das demonstrações financeiras no diário oficial. E ainda assegurou isonomia de tratamento processual, uma vez que o diário oficial da União, impresso em Brasília, sendo transportado fisicamente, só chegava nas Capitais no dia seguinte, e ainda mais alguns dias depois, nas comarcas mais distantes do interior.

Ainda estamos distantes de compreender os reais efeitos da aplicação da tecnologia no processo judicial. Se antes o acesso à nova jurisprudência se dava através das revistas de repositório oficial, que demoravam meses, senão anos, entre o dia do julgamento até a sua chegada ao escritório de advocacia, hoje temos possibilidade de acompanhar as decisões pela internet. Se aquelas revistas traziam apenas os principais julgados, selecionados pelos próprios magistrados, nos sites dos tribunais encontramos atualmente a base com a íntegra de todos os julgados proferidos pelas Cortes. É de se perguntar, por exemplo, se o acesso mais rápido, quase imediato, e na totalidade das decisões, causou impacto, por exemplo, sobre a velocidade de mudança da jurisprudência, e sobre a própria segurança jurídica do país.

Outras questões vão surgindo na medida em que avançamos no emprego da tecnologia. O princípio da publicidade tomou nova dimensão pois o nível de exposição de processos virtuais, em comparação com o processo em papel, que reclamava consulta individual e pessoal, levou as Cortes a estabelecer controles para evitar que robôs pudessem baixar todos os processos de todos os tribunais brasileiros para

625 Velha burocracia e novos arapongas virtuais, artigo publicado na Folha de São Paulo, painel Tendências e Debates, de 17 de julho de 2001.

armazenar e processar as informações neles contidas. A nova lei geral de proteção de dados pessoais - Lei nº 13.709, de 14 de agosto de 2018, ainda que possa não ser aplicada às bases de dados dos processos em trâmite no Judiciário, deve promover um novo nível de consciência ainda mais crítico sobre os riscos que o tratamento informatizado de informações pode gerar aos cidadãos. E, para reforçar essa proteção, foi aprovada no Senado Federal a Proposta de Emenda Constitucional 17/19, que agora aguarda tramitação da Câmara Federal, elevando, no Brasil, como já fizeram outras nações, como a espanhola[626], para o plano constitucional, o direito à autodeterminação informativa.

Estamos no limiar de um novo tempo nas relações sociais em geral e, no ambiente da Justiça, em especial, com a chegada da chamada inteligência artificial. Se na década de 50, como mencionei no início deste artigo, o uso de computadores para localizar determinadas leis sem necessidade de análise humana causou enorme espanto, a inteligência artificial tem potencial infinitamente mais impactante, ultrapassando limites da mera análise de base de dados para ingressar na capacidade de formular e responder questões inerentes à própria condição humana.

O avanço tecnológico, no entanto, é inevitável; a sua incorporação pela sociedade e o desaparecimento de uma tecnologia causado pelo surgimento de uma outra são cada vez mais céleres [627]. Da derrota do mestre russo Garry Kasparov, provavelmente o mais graduado jogador de xadrez da história, para o Deep Blue, da IBM, em 1997, fato que surpreendeu o mundo e fez as ações da IBM dispararem, para os dias atuais, o avanço da inteligência artificial é impressionante. Dialogamos hoje com máquinas que nos oferecem serviços ou negociam dívidas por telefone, imaginando que pessoas estejam do outro lado da linha, quando são computadores que se prepararam para uma conversa, considerando todas as variáveis possíveis. Serviços estão sendo realizados por sistemas de inteligência em todo o mundo [628]. Na área médica já existe o "doutor IA", aprovado pela agência americana Food and Drug Administration, uma ferramenta impulsionada pela inteligência artificial que detecta a retinopatia diabética, estudando imagens da parte posterior do olho. Em um minuto, o software produz um diagnóstico, detectando a presença ou ausência da condição, causada quando o alto nível de açúcar no sangue danifica os vasos sanguíneos da retina, o que pode levar à perda da visão.

---

626 Art. 18, 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."

627 A previsão de Ray Kurzwei, em Era das Máquinas Espirituais, editado em ____ é impressionante. Após calcular a velocidade do desenvolvimento tecnológico das últimas décadas, ele conclui que a capacidade humana estimada de 2×10^{16} cálculos por segundo (conexões neurais) será igualada por qualquer dispositivo de computação, no valor de mil dólares, por volta de 2020. E que a capacidade de computação irá dobrar a cada 12 meses ou 12 vezes por década, o que corresponde a um exponencial de 1.000 (2^{10}) a cada 10 anos.

628 https://www.echosis.com.br/3-exemplos-que-mostram-que-a-inteligencia-artificial--ja-e-realidade/

[629] Escritórios de advocacia usam a nova tecnologia em diversas atividades ligadas especialmente a leitura de documentos. As cortes superiores brasileiras desenvolveram sistemas para inicialmente tentar identifica , nos milhares de recursos que recebem, os que tratam de temas com repercussão geral; mas já são estudadas outras funções para esses sistemas [630].

Alguns países, como a França, tentam evitar essa tecnologia com leis que proíbem o uso de inteligência artificial sobre atividades jurídicas[631]. A Comunidade Europeia aprovou um código de conduta que impõe aos desenvolvedores valores como os de supervisão humana, privacidade e boa governança de dados[632]. Não há como deter a evolução tecnológica, mas há como fazer com que seja empregada para o bem-estar social.

Marcos da Costa, Advogado, Presidente da OAB SP nas gestões 2013 a 2015 e 2016 a 2018.

629 https://www.modernhealthcare.com/article/20181006/TRANSFORMATION03/181009975/ai-alone-now-making-the-diagnosis

630 "Batizado de VICTOR, a ferramenta de inteligência artificial é resultado da iniciativa do Supremo Tribunal Federal, sob a gestão da Ministra Cármen Lúcia, em conhecer e aprofundar a discussão sobre as aplicações de IA no Judiciário. Cuida-se do maior a mais complexo Projeto de IA do Poder Judiciário e, talvez, de toda a Administração Pública Brasileira". .... "VICTOR não se limitará ao seu objetivo inicial. Como toda tecnologia, seu crescimento pode se tornar exponencial e já foram colocadas em discussão diversas ideias para a ampliação de suas habilidades. O objetivo inicial é aumentar a velocidade de tramitação dos processos por meio da utilização da tecnologia para auxiliar o trabalho do Supremo Tribunal. A máquina não decide, não julga, isso é atividade humana. Está sendo treinado para atuar em camadas de organização dos processos para aumentar a eficiência e velocidade de avaliação judicial." Noticia veiculada no site do STJ em 30 de maio de 2018. - http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=380038

631 Matéria intitulada Como a França declarou 'guerra' a robôs que analisam decisões judiciais. - Em https://noticias.uol.com.br/tecnologia/noticias/redacao/2019/06/12/como-a-franca-declarou-guerra-a-robos-que-analisam-decisoes-judiciais.htm?cmpid=c um estudo realizado à época pela Imprensa Oficial opiaecol

632 https://ec.europa.eu/digital-single-market/en/news/communication-building-trust--human-centric-artificial-intelligenc

COOPERAÇÃO JURÍDICA INTERNACIONAL NA PRODUÇÃO DE PROVA DIGITAL – CASO MERCOSUL

Eixos temáticos: Processo eletrônico e prova digital

Autora:
Sabrina Rodrigues Santos
Profissão: dvogada
Categoria acadêmica: doutoranda
Instituição: Programa de Pós-Graduação Integração da América Latina Universidade de São Paulo – PROLAM/USP

RESUMO
A integração econômica através do MERCOSUL e a expanção transfronteiriça dos sistemas informáticos, impõe refl xão sobre as formas de produção da prova digital localizadas em diferentes Estados. O estudo é feito da perspectiva do direito nacional e da cooperação jurídica no bloco, e os aspectos práticos que envolvem os atos. Ao final, conclui-se pela baixa adesão dos operadores do direito aos Protocolos firmados entre os Estados artes e o conflito de normas que impede a sua utilização no Brasil

COOPERAÇÃO JURÍDICA INTERNACIONAL NA PRODUÇÃO DE PROVA DIGITAL – CASO MERCOSUL

INTRODUÇÃO

Viajantes da Apollo 11 pisaram na Lua em 20/07/1969, data essa considerada um marco na história da Humanidade por alguns fatores: a saída de seres humanos fora da órbita da terra que viajaram pelo espaço e desceram na Lua, um planeta de natureza diferente da Terra. O feito foi transmitido ao vivo em rede de televisão para todos que estivessem à frente da televisão e ficou registrado para as gerações futuras [633].

Nas últimas décadas a vida das pessoas passou a deixar cada vez mais rastros nos sistemas informatizados: biometria para votar, compartilhamento de conteúdos pessoais e profissionais por redes sociais, movimentações financeiras, trabalhar em

633 Vídeo disponibilizado pela NASA em 2009, que restaurou os vídeos da Missão Apollo 11. Disponível em <https://youtu.be/FydRSZQ7Dtg>

casa, fazer compras pela web, realizar ataques aos sistemas, contratar via internet, integrar pólos no processo eletrônico, dentre outras tantas.

Sites especializados em tecnologia de informação e comunicação noticiam a expansão dos negócios voltados a internet das coisas (IoT), Big data, softwares corporativos e datacenters na América Latina [634], tecnologias onde se pode encontrar os "rastros" e a prova digital.

O que todas essas ações têm em comum é que elas deixam rastros, ainda que sejam praticados no anonimato. E nem todos os rastros são acessíveis pelas pessoas, nem todas as ações são danosas, nem sempre se conhece a extensão do dano, nem sempre se conhece o autor do conteúdo e nem o agressor se apresenta a vítima.

Então, como obter os registros de conexão? Como saber a extensão do dano? Como identificar os agentes?

A resposta a esses questionamentos depende, muitas vezes, do acesso aos sistemas por particulares que, por sua vez, depende da autorização *munus público*. Isso porque as pessoas fruem do direito à privacidade e o acesso por terceiros depende de autorização judicial. A privacidade é um dos bens que integram os direitos à personalidade, cujas definição, natureza jurídica e elementos que os compõem variam nas legislações pátrias.

No Brasil, as pessoas fruem da garantia constitucional e infraconstitucional à privacidade [635] e, por isso, todos os dados são protegidos por lei [636]. Consequentemente, o acesso a eles somente é possível mediante ordem judicial [637].

---

634 "Tudo está na nuvem, mas onde ficam os principais servidores de internet?" Matéria publicada no site UOL em 29/06/2018. Disponível em <https://noticias.uol.com.br/tecnologia/noticias/redacao/2018/06/29/cabeca-nas-nuvens-onde-estao-os-principais-servidores-de-internet-no-mundo.htm>, acesso em 01/07/2019.

"5 inovações com Interconexão de Data Center na América Latina", conteúdo postado no site TI Inside Services em 18/01/2019, disponível em <https://tiinside.com.br/tiinside/services/18/01/2019/5-inovacoes-com-interconexao-de-data-center-na-america-latina/>. "Fortaleza ganha mais novo HUB de comunicação da América Latina", conteúdo postado em 22/04/2019 no site Canaltech, disponível em <https://canaltech.com.br/data-center/fortaleza-ganha-mais-novo-hub-de-comunicacao-da-america-latina-137581/>.

635 Constituição Federal artigos 5º XII, LVI, 136 § 1º e Código Civil artigo 21.

636 No Brasil, Lei sobre interceptação telefônica - Lei nº 9296/1996, Lei de Telecomunicações – Lei nº 9472/1997, Lei do Processo Eletrônico Lei nº 11.419/2006, Marco Civil da Internet (MCI) – Lei nº 12.965/2014, Regulamentação MCI – Decreto nº 8771/2016, Lei Geral de Proteção de Dados – Lei nº 13.709/2018.

Uma das primeiras regulamentações sobre a proteção de dados é Resolução nº 51/162 da Assembleia Geral de 16/12/1996 da CNUDMI/Uncitral sobre comécio eletrônico. Após intensos trabalhos na União Europeia, em Maio/2018, o Regulamento Geral sobre a Proteção de Dados entrou em vigor na União Europeia. Site <https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_pt> [Data da consulta: 28 de Julho de 2018]

637 Código Civil, artigo artigo 5º II.

Pois bem, considerando que a prova digital pode ser fungível, e se a parte necessitar produzi-la para certifica -se da autoria de um ilícito ou da existência de um dano? E se ela quiser saber quais bens jurídicos foram atingidos, se houve dano e quiser quantificá-los, a fim de contingencia-lo em uma possível indenização? E se ela apenas quiser documentar relação jurídica a partir de uma prova digital?

No conjunto de elementos que compõem a complexidade que envolve a produção da prova digital incluem-se a fungibilidade, a volatilidade dos registros e o armazenamento em nuvem, pois que os dados os sistemas geralmente são armazenados em países diferentes. Tanto o armazenamento e acesso, como as regras de proteção, são regidos pela lei do país onde se encontram. Isso é um complicador para a produção da prova digital, pois pode haver conflito de leis do pais solicitante e solicitado .

A conjunção dos elementos do cenário mostra-se muito interessantes ao profissional e pesquisadores do Direito, o que nos estimula a refletir sobre os benefícios da cooperação jurídica diferenciada no bloco no que tange a produção da prova digital.

O método utilizado é o interpretativo das normas e o referencial teórico a amparar as refl xões são o direito processual e direito internacional privado, em conjunto com a base legislativa processual civil nacional e normativas do bloco.

Em conclusão, pretende-se demonstrar que, na prática, os acordos no MERCOSUL ainda mostram-se insuficientes para enfrentar a fungibilidade da prova digital e, por isso, prejudica o sentimento de segurana jurídica no bloco.

1. Breves linhas sobre a produção da prova digital no Brasil, Argentina e Uruguai

O fato existe ou não existe, assim como a Terra orbita em torno do Sol. Então o que se espera ao indicar e apresentar as provas em um processo, é a aferição sobre a veracidade das alegações das partes.

O instituto da prova passou por significativas alterações ao longo do tempo

No Brasil, Amaral Santos (1952, p. 12) afirma que a prova é ato e meio que as partes e juiz têm para amparar as suas afirmações sobre um fato, ao que acrescenta-se a lição de Dinamarco (2005, p. 59), de que as afirmações podem ser verdadeiras ou falsas, por isso a necessidade da prova [638]. Em obra recente, Theodoro Junior (2018, p. 895) propõe dois conceitos para a prova no processo: "(a) um objetivo, isto é, como o instrumento ou o meio hábil, para demonstrar a existência de um fato (os documentos, as testemunhas, a perícia etc.); (b) e outro subjetivo, que é a certeza (estado psíquico) originada quanto ao fato, em virtude da produção do instrumento

638 SANTOS, Moacyr Amaral, **Prova judiciária no cível e comercial.** 1952. p. 12. DINAMARCO, **Instituições de Direito Processual**. 2005 Pp. 59

probatório. Aparece a prova, assim, como convicção formada no espírito do julgador em torno do fato demonstrado" [639].

Ou seja, a utilidade da prova foi ampliada, deixou de ser um instrumento de apuração da verdade e ter por destinatário final um juízo, para se ser um instrumento de demonstração da existência ou não de um fato ou de relação juridica, e conferir-lhes grau de certeza, que tanto dá às partes a segurança jurídica que precisam para tentar uma solução consensuada, como ao julgador chamado a dirimir a controvérsia (CPC 2015 artigos 381 I, II, III e parágrafo 5º).

Jéremmy Bentham (1971) defende que aa inversão dos ônus da prova pode ser indistintamente [640], em oposição a Jorge W. Peyrano (2008), que defende a aplicação em caso excepcional e de forma subsidiária [641].

Essa excepcionalidade é que prevalece no sistema processual brasileiro, que autoriza a inversão dos ônus de produzi-la por quem tem melhores condições de faze-lo, CPC 2015 artigo 373 parágrafos 1º, 2º e 3º.

Ainda no Brasil, a produção da prova adquiriu novos contornos. Deixou de ser contenciosa e exauriente, é permitida a realização no foro mais benéfico a sua produção, sem que isso atraia a competência para eventual ação principal e ampliou a sua utilidade, ao prever outras finalidades: i) proporcionar às partes interessadas elementos concretos úteis na formulação de um acordo, ii) verificar a existência ou não de um fato e quais são as pessoas que mantém relação com ele e, para promover uma demanda ou iii) um acordo e, iv) arrolar bens, ou ainda ter acesso a documentos, sejam tais medidas permeadas de urgência ou não (Código de Processo Civil artigos 381 II e III §§ 1º, 382 § 3º e 396).

Em especial a perícia em sistemas informatizados, a parte interessada poderá escolher o juízo onde houver melhores condições de acessibilidade ao sistema, menores custos e profissionais melhor capacitados. Nos casos em que os registros de ponto do empregado são feitos em meio digital e o funcionário não tem acesso, a declaração de horas extras pode demandar a perícia nos sistemas de ponto, a fim de aferir a veracidade das afirmações e, inclusive, apurar eventual fraude.

Na Argentina a produção da prova na esfera civel e comercial está regulamentada no *Codigo Procesal* Civil e Comercial de la Nación, nos artigos 359/404, sendo que a medida cautelar antecipada da prova, prevista no artigo 326, deve demosntrar os requisitos de fungibilidade,as dificuldades em realiza-las e mesmo os danos e prejuízos

---

639 THEODORO JUNIOR, Humberto. **Curso de direito processual civil**. Vol. I. 2018. Pp. 895.

640 **Tratado de las pruebas judiciales**. Tradução da obra original "Traité des preuves judiciaires" feita por Manuel Ossorio Florit. vol. II. Buenos Aires: EJEA, 1971.

641 **Nuevos lineamentos de las cargas probatorias dinámicas**. Buenos Aires, Rubinzal-Colzoni, 2008.

na hipótese de demora. As provas digitais localizadas fora do território poderão ser obtidas através da cooperação jurídica internacional prevista no artigo 526/529.

No Uruguai a produção da prova é regida pelo *Codigo General de Proceso, artigos 118, 137 a 147*.

2. Breves linhas sobre o MERCOSUL e seu tratamento no direito brasileiro

O Mercado Comum do Sul – MERCOSUL, foi criado com o Tratado de Assunção em 1991, firmado pelos presidentes de Argentina, Brasil, Paraguay e Uruguai, em 2006 ingressou Venezuela, suspensa por descumprimento do protocolo de adesão e por violação do Protocolo de Ushuaia, e em 2015 ingressou Bolívia. São Estados Associados Chile, Equador, Peru, Suriname, Guiana, Colômbia [642].

A produção normativa celebrada no âmbito do MERCOSUL é recepcionada e internalizada nos ordenamentos jurídicos dos Estados Partes, respeitadas as particularidades legislativas de cada um (Protocolo de Ouro Preto, artigos 38 a 40). Por isso a produção normativa do MERCOSUL não pode ser classificada como Direito Comunitário, porque não fora produzida por órgãos supranacionais e quiçá internalizada automaticamente ao direito nacional, mas é, de fato, um direito internacional público, regional, integracionista [643].

No Brasil, o repertório jurisprudencial demonstra que os tratados e acordos internacionais celebrados são recepcionados pelo ordenamento jurídico no mesmo plano de validade, efic cia e autoridade das leis ordinárias (Constituição Federal artigos 49 I, 84 VIII, 87 I). Segundo BARROSO (2015), constitucionalmente não há hierarquia entre o acordo internacional e a legislação ordinária, estando pois, sujeitos a regra geral de que a norma posterior revoga a anterior, exceção daqueles de proteção dos direitos humanos, que fruem de tratamento diferenciado no ordenamento interno, nos termos da Constituição Federal, artigo 5º, parágrafo 3º [644]. É essa a interpretação do Supremo Tribunal Federal [645].

RESEK (1997), que teve participação durante as negociações para criação do MERCOSUL é realista em suas refl xões, e atenta para o fato de sua origem de parcimônia e que, por isso, não deveríamos sonhar com o modelo europeu, fundado

642 Informações institucionais sobre o Mercados Comum do Sul – MERCOSUL, podem ser vistas em <https://www.mercosur.int/>.

643 REZEK, op. cit. p. 56. Sobre a recepção das normativas da União Europeia pelos Estados Partes, ver BARAV, Ami. Recepção da regra do direito comunitário pelas ordens jurídicas nacionais. *In* **Direito Comunitário do Mercosul**. pp. 37-51.

644 BARROSO, Luíz Roberto. Constituição e Tratados Internacionais: alguns aspectos da relação entre o Direito Internacional e Direito Interno. *In* **Panorama do Direito Internacional Privado atual e outros temas contemporâneos**. MENEZES, Wagner (orgs.). pp. 410-430.

645 STF, ADI-MC 1480-3, Min. Celso de Mello, DJ de 18.05.2001 e Rcl 2.645/SP, Rel. Ministro TEORI ALBINO ZAVASCKI, CORTE ESPECIAL, julgado em 18/11/2009, DJe 16/12/2009.

em bases muito diferentes daquelas aqui experimentadas, mas que se construísse um modelo a partir de coisas simples e, com o êxito destas, naturalmente evoluísse a integração [646].

BASSO (2007), dentre outros internacionalistas e economistas, propõe o MERCOSUL como solução para aumentar a competitividade no comércio internacional e atender as necessidades nacionais de garantia democrática [647].

O apelo da integração econômica apenas pelo viés econômico não é de bom alvitre, pois que são as pessoas físicas e jurídicas os reais atores no mercado integrado.

PEÑA (2007) acrescenta que o MERCOSUL tem como finalidades principais melhorar as condições de participação dos Estados Partes em um cenário global e regional, bem como facilitar os processos de consolidação da democracia, de coesão e transformação produtiva [648].

CARVALHO RAMOS (2008) acuradamente defende que os direitos econômicos estão imbricados com as liberdades econômicas que, por sua vez, integram o rol de Direitos Humanos. A despeito da rica doutrina e da miríade de tratados de Direitos Humanos celebrados pelos Estados Partes ou ainda cláusulas insertas em tratados não conexos, ele ressente que "a ausência de uma proteção efetiva e coerente de Direitos Humanos deslegitimam o próprio processo de integração econômica e cria um fator de desconfi nça e temos de que eventual transferência de poder do Estado aos órgãos integracionistas possa ser um fator de vulneração de direitos e erosão das garantias já conquistadas a duras penas no plano interno" [649]. Em síntese, "não e possível elaborar uma política integracionista com objetivo de atingir um mercado comum ou uma união econômica profunda, sem ao mesmo tempo, influenciar ou atingir os direitos dos indivíduos" [650].

Jeronimo Moscardo (2010), embaixador brasileiro, manifestou a preocupação de muitos agentes governamentais, pesquisadores, observadores, nacionais dos Estados Partes, todos de alguma maneira envolvidos no processo integracionista do MERCOSUL: "fala-se da necessidade de mercados e não de nações, de consumidores, e não de cidadãos. Não estaremos nos dedicando excessivamente à construção material e esquecendo a dimensão cultural-ético-institucional na arquitetura da integração? Com efeito, até o presente, a agenda internacional vinha sendo dominada basicamente pelas preocupações estratégico-militares e econômicas. O homem tem sido visto

646 REZEK, Francisco. Transcrição da conferência proferida em 19/11/1997. *In* **Direito Comunitário do Mercosul**. VENTURA, Deyse (org.). pp. 55.

647 BASSO, Maristela. "Mercosul – do passado ao futuro". *In BASSO*, **Mercosul--Mercosur.** p. 23.

648 PEÑA, Félix. "Instituciones y concertación de intereses nacionales: algunas refl xiones a la experiencia de los quince años del Mercosur". In BASSO, Maristela. **Mercosul – Mercosur – estudos em homenagem a Fernando Henrique Cardoso**. p. 9.

649 CARVALHO RAMOS, André de. **Direitos humanos na integração econômica**. p. 35.

650 CARVALHO RAMOS, André de. Op. cit. p. 34

somente como soldado ou como diplomata na área clássica da guerra e da paz, ou como consumidor de produtos e serviços na esfera da economia. O grande ausente tem sido sempre o cidadão, os problemas criados no contexto de seus valores, dos seus problemas éticos. Assim é que, ainda que não haja resolvido de maneira global suas carências de sobrevivência material, a humanidade enfrenta desafios éticos cada vez mais sérios e profundos, que resultam na impossibilidade da plena realização da pessoa humana. Daí a importância das construções institucionais e éticas" [651].

O MERCOSUL completa 28 anos de existência em 2019. Sua estrutura institucional se transformou ao longo dos anos, a economia do espaço expandiu significativamente, forma criados instrumentos para promover as liberdades de circulação de bens e fatores de produção (capital, trabalho, pessoas).

Quanto ao segurança jurídica no bloco, foi preservado o sistema de solução de controvérsias inicalmente pactuado, oTribunal Arbitral e criado o Tribunal de Permante de Recursos a partir do Protocolo de Olivos em 2004, apenas disponíveis aos Estados Partes. Aos particulares apenas cabe reclamar seus direitos nos Poderes Judiciários dos Estados Partes, que têm como instrumentos a cooperação jurídica internacional para facilitar o acesso à justiça.

3. A cooperação jurídica internacional no âmbito do MERCOSUL para a produção da prova digital

A cooperação internacional é princípio de Direito Internacional que pauta as relações dos Estados. É a cooperação jurídica internacional uma de suas espécies e integra os estudos do Direito Internacional Privado, que se assenta nos princípios de reciprocidade, auxílio mútuo, respeito, solidariedade.

A cooperação jurídica internacional compreende um arcabouço normativo de fontes internacionais (assim consideradas as fontes jurídicas recepcionadas pelo ordenamento nacional) e nacionais (Constituição Federal e legislação infraconstitucional) para proporcionar, facilitar e instrumentalizar a cooperação entre os Estados, bem como entre estes e as Organizações Internacionais, com objetivo de contribuir no acesso à justiça. A colaboração pode ser para atender medidas extrajudiciais e judiciais e se realiza através de autoridades com atribuições legais para o seu cumprimento [652].

651 MOSCARDO, Jeronimo. Integração para que? (Em busca de uma ética para a Integração Latino-Americana. *In* **Integração Latino-Americana: 50 anos de ALALC e ALADI**. Brasília: FUNAG, 2010. 108p. p. 81. Disponível em < http://www.funag.gov.br/biblioteca/dmdocuments/0803.pdf >. Acesso em 6/6/2015.

652 Sobre cooperação jurídica internacional, sugere-se estudos de CARVALO RAMOS, "Direito Internacional Privado e seus aspectos processuais: a cooperação jurídica internacional", *in* CARVALHO RAMOS, André de, e MENEZES, Wagner. **Direito Internacional Privado e a nova cooperação jurídica internacional**, BERGMAN, Eduardo Tellechea. "La Cooperación jurisdiccional internacional com especial referencia al ámbito del MERCOSUR y al derecho uruguayo", ARAÚJO,

É cediço na doutrina que a cooperação jurídica internacional impõe ao intérprete o diálogo de saberes, na medida que suas fontes são plurais - nacionais e internacionais. A coexistência em maior ou menos grau entre os Estados é que justifica o ramo do Direito Internacional, que segundo STRENGER (1996) "o direito internacional somente se torna possível quando os sistemas jurídicos particulares não se negam totalmente a coexistir dentro de um regime de vida de interpretação continuada" [653].

No MERCOSUL, os textos normativos para cooperação jurídica foram produzidos já no início da formação do bloco, a partir do ano de 1992. O esforço concentrado derivou na significativ produção legislativa, destacando-se ao presente estudo o Protocolo de Las Leñas de Cooperação e Assistência Jurisdicional em Matéria Civil, Comercial, Trabalhista e Administrativa (1992) [654], o Protocolo de Ouro Preto de Medidas Cautelares (1994) [655], Protocolo de San Luis de Assistência Jurídica Mútua em Assuntos Penais (1996) [656] .

Os pedidos de cooperação jurídica no âmbito do MERCOSUL não estão sujeitos a juízo de discricionaridade da autoridade requerida, e se esta se recusa a cumpri-la total ou parcialmente, tem o dever de informar os motivos (Protocolo de Las Leñas artigo 14, Protocolo de Ouro Preto artigo 15, Protocolo de San Luis artigo 5º).

A produção de provas digitas para instruir processos em andamento ou medidas cautelares em matérias civil, administrativa e trabalhista podem ser requeridas através de cartas rogatórias e enviadas através da autoridade central, via diplomática ou pelas partes interessadas, que neste caso precisa legalizar pela autoridade diplomática do país requerido (Protocolo de Las Leñas artigo 10 e Protocolo de Ouro Preto artigo 19). A produção de provas referentes a assuntos penais deverão ser solicitadas pelo juiz ou Ministério Público, inclusive com pedido de confiencialidade se o caso, e encaminhado pela Autoridade Central (Protocolo de San Luis artigos 4º e 10).

Nos casos de medidas cautelares de produção de provas digitais e que tramitam em cidades fronteiriças, é possível que os juízes ou tribunais têm a prerrogativa de envia-las diretamente uns aos outros sem a necessidade de legalização (Protocolo de Ouro Preto artigo 19).

Quanto aos custos com os procedimentos de produção de provas digitais em algum dos Estados Partes do MERCOSUL, as partes que por ela demandam devem ter tratamento igual aos nacionais do país rogado (Protocolo de Las Leñas, artigos 3º e 4º).

Nadia de. "Cooperação jurídica nos litígios internacionais – cartas rogatórias no Brasil e no Protocolo de Las Leñas".

653 STRENGER, Irineu. **Direito internacional privado**. pp. 37.

654 Incorporado ao ordenamento jurídico brasileiro pelo Decreto nº 2.067/1996.

655 Incorporado ao ordenamento jurídico brasileiro pelo Decreto nº 2.626/1998.

656 Incorporado ao ordenamento jurídico brasileiro pelo Decreto nº 3.468/2000.

No caso da medida cautelar de produção de prova, a parte interessada deverá arcar com os custos (Protocolo de Ouro Preto artigo 24). Da mesma forma em matéria penal, a solicitação de produção de prova digital implica em custos de perícia e gastos extraordinários decorrentes do emprego de formas ou procedimentos especiais, que deverão ser suportados pelo Estado requerente a medida (Protocolo de San Luis artigo 13).

As regras de cooperação jurídica no MERCOSUL demonstram os esforços de promover a harmonização dos procedimentos, a fim de minimizar os conflitos de leis no cumprimento dos pedidos de cooperação e contribuir para o acesso à justiça e a segurança jurídica das partes.

4. A prática na transmissão dos pedidos de cooperação jurídica no MERCOSUL

Os Protocolos de Las Leñas, de Ouro Preto e de San Luis, bem como a Convenção Interamericana sobre Exhortos ou Cartas Rogatorias de 1975 firmada no âmbito da Conferência Especializada Interamericana sobre Direito Internacional Privado (CIDIP) já foram incorporados pelos Estados Partes e são a base dos pedidos de acolhimento e tramitação dos pedidos de produção de provas digitais, dentre outros.

Essas normativas estão presentes nas informações prestadas nos portais dos Ministérios da Justiça do Brasil, Argentina, Paraguai e Uruguai para a solicitação de cumprimentos de cartas rogatórias de produção de provas, que em geral reescreveram os conteúdos e procedimentos especiais que demandam a produção das mesmas, inclusive a responsabilidade por eventuais custos.

De outro lado, os portais dos tribunais da Argentina, Brasil, Paraguai e Uruguai apresentam muitos de seus serviços já informatizados. Mas apenas o Brasil implementou a nível nacional o processo judicial eletrônico [657]. Argentina [658], Paraguay [659] e Uruguai [660] apenas iniciaram a informatização do processo judicial, ainda em estágio inicial.

Não obstante isso, as cartas rogatórias ainda são expedidas em meio físico e encaminhadas, em geral, por suas autoridades centrais.

No Brasil, o Ministério da Justiça, por sua Coordenação-Geral de Cooperação Jurídica Internacional – DRCI, processa, envia e recebe pedidos de produção de provas, encaminhando-as a justiça federal para cumprimento. Na prática, o procedimento requerido demora de 06 a 09 meses para o cumprimento e devolução.

---

657 Lei nº 11.419/2006 – Lei do Processo Eletrônico.

658 Ley 26.685/2011. Autoriza o uso de expedientes electrónicos.

659 Acordada N°1107/2016 - Corte Suprema de Justicia. Aprova os trámites judiciales electrónicos.

660 Ley Nº 18.237/2007. Autoriza o expediente electrónico em todos os promovidos perante o Poder Judiciário.

Da analisa de jurisprudência do Supremo Tribunal Federal e do Superior Tribunal de Justiça, verifica-se que ambos reconhecem os que os tratados e convenções internacionais têm caráter normativo quando incorporados ao sistema jurídico brasileiro e, por isso, têm eficácia de lei ordinária e força normativa. Ainda, o Superior Tribunal de Justiça já se manifestou positivamente ao cumprimento de pedidos de cooperação internacional entre autoridades congêneres [661], assim como os Tribunais Regionais Federais das 3ª e 4ª Regiões, reconhecem que os pedidos de cooperação sem conteúdos decisórios podem ser encaminhados para processamento diretamente na justiça federal [662].

Todos os Estados Partes do MERCOSUL em geral procedem da mesma forma envio dos pedidos pela autoridade central e, eventualmente, pela via diplomática, a despeito dos Protocolos de Las Leñas e de Ouro Preto autorizarem o envio das cartas rogatórias pelas partes interessadas e este último protocolo autorizar os juizes de fronteira requerer o cumprimento de medidas cautelares.

BERGMAN informa que o governo do Uruguai emprega os modos postal, facsímile e correio eletrônico para adiantar os pedidos de cooperação junto às Autoridades Centrais dos Estados Partes do MERCOSUL. E que não é raro as próprias partes interessadas completam a cadeia de legalização e encaminham a carta rogatória ao país rogante, com o auxílio de profissional habilitado a tal fim. Ainda, que ao largo da fronteira de Argentina e Uruguai começaram a ocorrer esse tipo de

---

661 AgInt na CR 11.165/EX, CR 4841-EX, AgRg na CR 3162-CH, STJ - Rcl 2645-SP, STF - PET 5946.

662 Decisão Em Habeas Corpus: "(...) Vê-se que o legislador federal atribuiu à Advocacia-Geral da União o cumprimento de pedidos passivos de auxílio direto (mutual legal assistance). E o fez apenas por uma razão: por estar presente o interesse da União no atendimento a demandas estrangeiras, tenham ou não base convencional. Somente a existência de interesse federal é apta para justificar a atuação da Advocacia de Estado mantida pelos cofres da União, no atendimento a uma demanda estrangeira. De fato, segundo o art. Iº da Lei Complementar 73/1993, a Advocacia-Geral da União é a instituição que representa a União judicial e extrajudicialmente.O artigo 34 do novo CPC vai na mesma linha e diz competir "ao juízo federal do lugar em que deva ser executada a medida apreciar pedido de auxílio direto passivo que demande prestação de atividade jurisdicional". Embora encartada na legislação civil, esta é seguramente uma regra de cunho geral, que se aplica indistintamente a todos os pedidos de cooperação internacional de índole passiva.Por sua vez, o art. 965 do CPC/2015 não destoa dessa diretriz, ao estabelecer que o "cumprimento de decisão estrangeira far-se-á perante o juízo federal competente, a requerimento da parte, conforme as normas estabelecidas para o cumprimento de decisão nacional." (destacou-se). Assim já decidiu o E. STJ ((STJ, HC 18.307/MT, Rei. Ministro Hamilton Carvalhido, 6a Turma, julgado em 18/04/2002, DJ 10/03/2003, p. 313))" ((TRF4, HC 5061277-84.2017.4.04.0000, OITAVA TURMA, Relator LEANDRO PAULSEN, juntado aos autos em 06/11/2017)).

PROCESSUAL PENAL. MANDADO DE SEGURANÇA CONTRA ATO JUDICIAL. TRÁFICO TRANSNACIONAL DE DROGAS. PEDIDO DE COOPERAÇÃO JUDICIÁRIA. OITIVA DE TESTEMUNHAS. AUXÍLIO JURÍDICO DIRETO. DESNECESSIDADE DE EXEQUATUR, AINDA QUE O PEDIDO TENHA SIDO DESIGNADO COMO "CARTA ROGATÓRIA". SEGURANÇA CONCEDIDA. (TRF 3ª Região, PRIMEIRA SEÇÃO, MS - MANDADO DE SEGURANÇA - 331305 - 0015491-42.2011.4.03.0000, Rel. DESEMBARGADOR FEDERAL COTRIM GUIMARÃES, julgado em 17/11/2011, e-DJF3 Judicial 1 DATA:24/11/2011).

comunicação, "aun cuando una adecuada de limitación de la profundidad de tales zonas y consecuentemente de los tribunales que por razón de lugar están em condiciones de emplear la modalidad, habrá de impulsar su desarrollo" [663].

Das pesquisas empreendidas no fórum das justiças comum e federal na cidade de Foz do Iguaçu no ano de 2018, conclui-se que não os juízes de fronteira não têm diálogo para o cumprimento de cartas rogatórias de forma direta, como previsto no artigo 19 do Protocolo de Ouro Preto. Nas cidades de Iguazu na Argentina e na Ciudad del Este no Paraguai verificou-se que também não é utilizada a modalidade de forma direta.

No Brasil, a produção da prova digital no exterior é regida pelo Código de Processo Civil (artigos 26 a 34). E o cumprimento de carta rogatória para o mesmo fim é regido pela Constituição Federal (artigos 105 I i, 109 X).

Verifica-se o conflito entre o Protocolo de Ouro Preto de Medidas Cautelares e o Código de Processo Civil, que não permite o diáologo entre juízes para a realização da prova digital em cidades de fronteira com o Brasil. Pesquisas de jurisprudência nos portais do Tribunal Regional da Quarta Região e do Superior Tribunal de Justiça, mostrou-se que não há respostas para busca de julgamento sobre esse assunto.

CONCLUSÕES

O acesso à justiça somente é possível às pessoas se o Estado promover uma rede de instrumentos legais, relacionamentos institucionais e recursos adequados à sua consecução.

No mercado integrado economicamente acrescenta-se a necessidade da cooperação jurídica e de aprofundamento das relações institucionais entre os Poderes Judicários e os demais operadores do direito, a fim de proporcionar a compreensão do direito internacional disponível e a importância da sua utilização na rotina forense.

Verificou-se que os Protocolos de Las Leñas, Ouro Preto e San Luis firmados no âmbito do MERCOSUL apresentam-se como instrumentos jurídicos valiosos no acesso à justiça neste mercado econômico ampliado.

No caso do Brasil, no entanto, o flagrante conflito entre o Código de Processo Civil (2015) e o Protocolo de Ouro Preto sobre Medidas Cautelares (1994) e a ausência de uma solução ou de julgados sobre o tema até o presente, mostra a baixa adesão dos operadores do direito em detrimento dos benefícios que o Protocolo traz para a vida real.

As perspectivas de Basso, Carvalho Ramos e Moscardo, mostram que os direitos humanos, ainda não é tratado com relevância nas negociações no MERCOSUL e

663 BERGMAN, Eduardo Tellechea. "La cooperación jurisdiccional internacional com especial referencia al ámbito del Mercosur y al derecho uruguayo. pp. 364-367

mesmo no trato da economia do bloco. Daí concluir que a relativização dos direitos humanos e o alijamento da sociedade civil no processo de integração no MERCOSUL, prejudica o sentimento de segurança jurídica pelas populações.

REFERÊNCIAS

BARROSO, Luíz Roberto. "Constituição e Tratados Internacionais: alguns aspectos da relação entre o Direito Internacional e Direito Interno". *In* **Panorama do Direito Internacional Privado atual e outros temas contemporâneos**. MENEZES, Wagner (orgs.). pp. 410-430.

BASSO, Maristela. "Mercosul – do passado ao futuro". *In BASSO*, **Mercosul-Mercosur: estudos em homenagem a Fernando Henrique Cardoso.** BASSO, Maristela (org.). São Paulo: Editora Atlas, 2007. pp. 23-35.

BERGMAN, Eduardo Tellechea. "La Cooperación jurisdiccional internacional com especial referencia al ámbito del MERCOSUR y al derecho uruguayo". DECITA: derecho del comercio Internacional. Nº 4, Buenos Aires, 2005. pp. 359-395

CARVALHO RAMOS, André de. **Direitos Humanos na integração econômica – Análise comparativa da proteção de direitos humanos e conflitos jurisdicionais na União Européia e Mercosul**. Rio de Janeiro: Renovar, 2008.

DINAMARCO, Cândido Rangel. **Instituições de Direito Processual**. 2005.

MERCOSUL. Disponível em <http://www.mercosul.gov.br/index.php/saiba-mais-sobre-o-mercosul>. Acesso em 06/06/2019.

MOSCARDO, Jeronimo. "Interação para que? (Em busca de uma ética para a Integração Latino-Americana". *In* **Integração Latino-Americana: 50 anos de ALALC e ALADI**. Brasília: FUNAG, 2010. 108p. p. 81. Disponível em < http://www.funag.gov.br/biblioteca/dmdocuments/0803.pdf >. Acesso em 6/6/2019.

PEÑA, Félix. "Instituciones y concertación de intereses nacionales: algunas refl xiones a la experiencia de los quince años del Mercosur". *In* BASSO, Maristela. **Mercosul – Mercosur – estudos em homenagem a Fernando Henrique Cardoso.** São Paulo: Atlas, 2007. pp. 10-22.

REZEK, Francisco. "Transcrição da conferência proferida em 19/11/1997". *In* **Direito comunitário no Mercosul**. VENTURA, Deyse de Freitas Lima (org.). Porto Alegre:

Livraria do Advogado, 1997. pp. 52-61.

SANTOS, Moacyr Amaral, **Prova judiciária no cível e comercial.** 1952.

STRENGER, Irineu. **Direito internacional privado**. 3ª ed.aum. São Paulo: Editora LTr, 1996.

THEODORO JÚNIOR, Humberto. **Curso de direito processual civil**. Vol. I 59ª ed. rev.atual.ampl. 2018. Rio de Janeiro: Forense, 2018. pp. 895-968.

EL PROCESO ELECTRÓNICO EN ARGENTINA

Eje tematico: Proceso Electrónico, Firma, Mediación, Acceso

Autores:
Bibiana Luz Clara
Abogada y Mediadora, Vicepresidente de FIADI, Doctoranda de la Universidad de Salamanca

ABSTRACT
Nos encontramos frente a fuertes cambios tecnológicos que afectan todas las áreas de nuestra vida. La justicia es una de ellas, y por ello es necesario adaptar el proceso judicial a su versión electrónica, buscando la simplificación de las tramitaciones y la eficaci , a través de acciones concretas para lograrlo, de las cuales hablaremos a continuación, respecto de su implementación en la Argentina.

INTRODUCCIÓN

En la República Argentina el procedimiento civil y comercial ha ido cambiando de la versión papel a su nuevo formato electrónico, si bien aún no totalmente, pues se requiere la reforma del código de rito, para su implementación total. Dicha reforma se encuentra en curso, habiéndose elaborado los correspondientes anteproyectos de ley en tal sentido, tanto a nivel nacional como provincial, los que se encuentran en estudio para su aprobación, si bien en la provincia de Buenos Aires, ya la ley 14142[664], lo había modificado permitiendo la confección de cédulas electrónicas de oficio o por impulso de parte.

El cambio del procedimiento a su versión electrónica comenzó con la aprobación del sistema de presentaciones y notificacione electrónicas en 2012, mediante la Res. SCBA. 1827/12, para luego ir incrementando la virtualización, ya que la tarea jurídica es una actividad con costumbres muy tradicionales, que genera una fuerte resistencia a los cambios. Pero como la tecnología avanza de todas maneras, a pesar de quien sea, se fue implementando la virtualización, de acuerdo a un cronograma progresivo,[665] hasta llegar al envío de los escritos electrónicos firmados digitalmente mediante el sistema de firma digital[666]. Para ello se otorga a los letrados matriculados,

664 Reglamentado su uso por la AC. SCBA 3540/11.

665 - 2 de marzo del 2015: todas las dependencias administrativas y jurisdiccionales de la Suprema Corte de Justicia y órganos del fuero Civil y Comercial, Contencioso Administrativo, de Familia, del Trabajo y Justicia de Paz.
- 4 de mayo del 2015: Para los entes públicos Provinciales.
- 1 de Julio de 2015: Para los entes públicos del Estado Nacional.
- 1 de septiembre de 2015: Para las municipalidades.
- 1 de febrero de 2016: Letrados y Auxiliares de la Justicia.

666 La Suprema Corte de Justicia en Acuerdo 3886/18 resolvió aprobar el "Reglamento para las

un dispositivo denominado token, que contiene el certificado de firma digital, que consta de un par de claves de criptografía asimétrica, una clave publica y una clave privada. La primera de ellas la tiene el certific dor licenciado, que en este sistema depende de la Corte, para poder ser verificada en su autenticidad. La clave privada queda en poder y bajo absoluto control del firmante, en este caso los abogados de la matricula, quienes para poder utilizarla deben descargar los controladores - drivers- al ordenador que van a utilizar para enviar documentos escaneados, notificaciones, oficios y escritos electrónicos firmados digitalmente.

El sistema de firma digital, asegura la integridad de los documentos digitales[667] que viajan encriptados, autoría, autenticidad y no repudio, cualidades que identifican a la firma digital, también conocida como firma electrónica avanzada. La ley de firma digital la equiparó a la firma manuscrita, y el nuevo Codigo Civil y Comercial indica en su artículo 288[668] que todos los documentos electrónicos para ser considerados válidos deben estar firmados digitalmente, con lo cual ésta se vuelve un requisito ineludible

Nuestra ley 25506[669] de firma digital fue sancionada en 2001, luego reglamentada en 2002[670], aunque el uso efectivo del sistema empezó, como vemos bastante tiempo después, y ha sufrido recientemente algunos cambios, con la finalidad de optimizar los sistemas y recursos.

Los cambios indicados han permitido reducir sensiblemente los tiempos de las tramitaciones, en las cuales las notificaciones implicaban un sesenta por ciento del tiempo que demanda la gestión y resolución de una causa, ya que desde la primera presentación se debe constituir domicilio electrónico[671], por cada letrado, al cual serán enviadas las notificaciones electrónicas.

La constitución del domicilio electrónico, y el uso del dispositivo criptográfico de firma digital para las presentaciones electrónicas es obligatorio para los abogados, desde el año 2016.

---

presentaciones por medios electrónicos" como Anexo Único, y que se aplicará en forma obligatoria a todos los procesos en los que rija el régimen de escritos previsto en el Libro I, Título III, Capítulo II del Código Procesal Civil y Comercial de la Provincia (v Decreto Ley Nº 7425/68, Leyes Nº 11.653, 12.008, 13.928, modificatorias y complementarias.

667 La ley 25506 define en su art. 6 al documento digital: "Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura".

668 ARTICULO 288.- Firma. La firma prueba la autoría de la declaración de voluntad expresada en el texto al cual corresponde. Debe consistir en el nombre del firmante o en un signo. En los instrumentos generados por medios electrónicos, el requisito de la firma de una persona queda satisfecho si se utiliza una firma digital, que asegure indubitablemente la autoría e integridad del instrumento.

669 Que actualizada se puede visitar en http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-999/70749/texact.htm accedida 14/7/2019.

670 Mediante el decreto 2628/2002 http://www.saij.gob.ar/2628-nacional-decreto-reglamentario-ley-25506-sobre-firmadigital-dn20022002628-2002-12-19/123456789-0abc-826-2002-2002soterce accedido 12/7/2019.

671 EL domicilio electrónico debe ser único para cada letrado.

Otra mejora ha consistido en reducir la cantidad de personas que todos los días debían concurrir a los tribunales, y todo este cambio se encuadra en el marco del "Programa Justicia 2020[672] y Justicia Abierta", que el gobierno nacional lleva delante con la finalidad de cumplir con la agenda 2030 y los Objetivos de Desarrollo Sostenible de las Naciones Unidas. El programa fue premiado por la OCDE[673], como uno de los casos mas innovadores del mundo de Gobierno Abierto.

Se trata de una plataforma digital del Ministerio de Justicia y Derechos Humanos de la Nación, República Argentina, que funciona a través de la participación ciudadana, constituyendo un espacio de dialogo para construir y debatir propuestas para la mejora del servicio de justicia, promoviendo políticas de transparencia y participación ciudadana, en sus diversos ejes.

INICIO DEL PROCEDIMIENTO

El procedimiento se inicia con la presentación de la planilla de receptoría[674] aun en formato papel, donde se indican las partes, la materia, y si corresponde el pedido de sorteo de mediador, ya que desde mediados de los años noventa en la ciudad de Buenos Aires[675], y desde mayo de 2012 en la provincia de Buenos Aires, se instrumentó el sistema de mediación prejudicial obligatoria[676], con la finalidad de sacar del ámbito de los tribunales un gran número de causas, que podrían ser solucionadas en una instancia previa con la ayuda de un mediador.

Con el mismo formulario de ingreso de datos, con el que siempre se iniciaron los expedientes por receptoría general, se solicita, sea llenado un nuevo casillero, el pedido de sorteo de mediador para la causa.

Se identifica con un número de código, según la materia de que se trate, y siempre que se encuentre dentro de las que pueden ser llevadas a mediación por no estar comprometido el orden público, se procede al sorteo del juzgado interviniente y del mediador. De todos modos, existe un listado de materias que pueden presentarse a mediación.

EL sistema se estructuró primero con la necesidad de la formación de mediadores, que debieron cursar y aprobar un curso de posgrado de dos años de duración, el que fue dictado por los colegios de abogados y las universidades. Luego de aprobado el mismo, quienes desean matricularse deben rendir un examen ante el Ministerio de

672 https://www.justicia2020.gob.ar/

673 Organización para la Cooperación y el Desarrollo Económicos.

674 Planilla Inforec, que se presenta en papel y luego se informatiza.

675 Mediante la sanción de la Ley de Mediación y Conciliación 24.573, en 1995 http://www.cpacf.org.ar/lmp.php?sec=lmp_mediacion accedido 12/7/2019

676 Mediante la ley 13591 http://www.gob.gba.gov.ar/legislacion/legislacion/l-13951.html accedido 14/7/2019

Justicia, que es el organismo encargado de otorgar las matrículas, cuyo número es limitado, ya que se ha fijado un cupo para el listado de integrantes mediadores

Cada cierto tiempo se llama a quienes estén interesados en presentarse a rendir examen, para integrar el listado de mediadores prejudiciales, a quienes luego de aprobado se otorga un carnet habilitante. Así se van cubriendo las vacantes que siempre se producen, por algunos mediadores que se alejan de la profesión por distintos motivos.[677]

El sistema sufrió en un comienzo, los embates de quienes sintieron, que la mediación prejudicial obligatoria, iba contra los principios de la mediación que por esencia es voluntaria. Este punto en general es refutado, indicándose que lo único que es obligatorio, es presentarse a la primera audiencia de mediación, y que si no se desea continuar en la misma se puede pedir el cierre de dicha instancia para continuar con el proceso judicial ante el juez que ya se encuentra designado. Sólo se debe acompañar el acta de cierre de la mediación como prueba de su realización, y el juzgado dará curso a la continuación de las actuaciones. Si las partes en algún momento durante el proceso, quisieran intentar un acuerdo, podrán solicitar la reapertura de la mediación, presentando un escrito en tal sentido.

Otros criticaron el sistema con otro argumento, viendo en la mediación prejudicial una traba al libre acceso a la justicia, indicando que encarecería los costos del proceso, ya que al mediador deben pagarle las partes, en base a una escala de honorarios fijada por ley, escala que a poco de fijada fue reducida[678], justamente para evitar agravar los gastos.

Para llevar adelante el procedimiento de mediación se elaboró un software de gestión que se denomina "Mediare"[679], y que permite el ingreso de los expedientes, mediante un código de barras que carga automáticamente los datos de las partes, sus letrados y materia y juzgado designado.

El sistema también permite la realización de notificaciones, pero no su envío electrónico, sino aun papel ya que se envían a los domicilios reales de los requeridos, los que a ese momento no han constituido domicilio electrónico.

EL sistema permite cargar las audiencias, e indicar quienes se encuentran presentes en ellas, en tiempo real, realizar las actas, ya sea de la audiencia o de cierre de la mediación, con o sin acuerdo, y enviarlas instantáneamente al Ministerio de Justicia, quien lleva el control del sistema, y realiza la estadística de las causas en trámite, y los resultados obtenidos.

677 Jubilación; renuncia al listado de mediadores; muerte; traslado a otra jurisdicción; enfermedad, etc.

678 Decreto 43/2019 articulo 31. https://colabdol.com.ar/wp/archivos/639 accedido 14/7/2019.

679 Que se puede acceder en el sitio http://www.mediaciones-ba.org.ar/

Desde la plataforma mediare se pueden descargar modelos de actas, de convenio de confiden ialidad, de cedulas de notificación, y dispone de un código QR que aparece en el acta de cierre para su identificación.

Las actas aún se suscriben con firma ológrafa, pues no se ha incorporado todavía la firma digital en las mismas, ni su envío electrónico al juez de la causa para su conocimiento y homologación. Lograr el cumplimiento de este punto sería de suma importancia para la virtualización total del sistema de mediación prejudicial.

Pasados todos estos años desde su instrumentación, el sistema ha logrado resolver más de treinta por ciento de las causas que se inician y que de otro modo estarían engrosando el número de expedientes en trámite en los tribunales, con lo cual se ha logrado agilizar la tramitación, y resolución de los mismos fortaleciendo el acceso a la justicia y dando una respuesta más acorde a los justiciables.

Otro de los avances que el Programa de Justicia 2020 promueve, es el de cambiar el sistema de escritura por el de la oralidad en el procedimiento, la fijación de audiencias de conciliación previo a la fijación de la apertura a prueba, donde en un importante numero de casos se logran acuerdos, ya que las audiencias son atendidas personalmente por el juez de la causa, quien presenta a las partes la situación de la misma, escucha sus propuestas, y si no se logra llegar a un acuerdo, se decide que pruebas son conducentes y cuales no entre las ofrecidas con la demanda, y en consecuencia se desisten o se proveen para su producción. Una vez producidas las pruebas informativas, y periciales, se fija una audiencia donde declaran los testigos y las partes. Dicha audiencia puede ser filmada y grabada para su posterior estudio, y se pasarán los autos para dictar sentencia.

Los expedientes electrónicos pueden ser visualizados desde una mesa virtual[680], a la cual se ingresa mediante un usuario y contraseña, y que se puso en funcionamiento aún antes de la implementación del sistema de envío de presentaciones electrónicas con firma digital. Actualmente a las consultas de los expedientes y su estado, se puede acceder también mediante el dispositivo criptográfico token, por medio del portal de notificaciones de la Suprema Corte de la provincia de Buenos Aires.

Como vemos se han hecho ya muchos cambios en busca de la eficacia procesal, y muchos aguardan aún por materializarse, a fin de apaciguar el descontento de la sociedad sobre la prestación del servicio de justicia, y su falta de transparencia.

CONCLUSIÓN

La necesidad de facilitar el acceso a la justicia y de lograr la eficacia en los procesos judiciales, ha llevado a tomar distintas medidas como hemos comentado,

680 MEV : https://mev.scba.gov.ar

con la finalidad de acortar los tiempos, favorecer las posibilidades de llegar a acuerdos que pongan fin a los litigios de manera de mantener las relaciones y fomentar una cultura de paz, para lo cual la mediación es una herramienta de enorme utilidad.

Basados en estas prioridades se ha instrumentado el expediente electrónico, a fin de asegurar una tramitación rápida que haciendo uso de las herramientas digitales, que la tecnología pone hoy a disposición de la justicia.

Mucho es todavía lo que queda por hacer, ya que las posibilidades tecnológicas todos los días nos plantean oportunidades insospechadas, aun así, los avances realizados son concretos y se advierten mejoras importantes en la gestión, que se traducen en beneficios para una sociedad mas justa para todos

JURIMETRIA E JUSTIÇA PREDITIVA

PROMETEA: JUSTICIA DIGITAL AL SERVICIO DE LA COMUNIDAD[681]

Eje Temático: Jurimetría y Justicia predictiva

Autor:
María Paula Castellanos Peña
Estudiante de quinto semestre de la Facultad de Derecho, estudiante investigadora adscritas al Semillero de Derecho y Tecnología en la Sociedad de la Información (DITSI), vinculada al Grupo de Investigación Doctor Angélico Iuris Et Realitas Categoría C de la facultad de Derecho de la Universidad Santo Tomás, Sede Villavicencio. mariacastellanosp@usantotomas.edu.co

RESUMEN
La noción de inteligencia artificial nace en una reunión celebrada en el verano de 1956 en Dartmouth (USA) donde participaron los mayores exponentes y conocedores del área. En dicha reunión, J. McCarthy, M. Minsky, N. Rochester y C. E. Shannon redactaron una propuesta en la que aparece por primera vez el término «inteligencia artificial». Es necesario reconocer que tras la evolución misma del término, la IA tuvo una primera clasificación, es así como se reconocerá la inteligencia artificial fuerte, y débil. Para efectos de la presente propuesta, así como del proyecto en posterioridad, nos referiremos a la noción de inteligencia artificial fuerte, toda vez que la misma se caracteriza por considerar que un ordenador puede tener mente o estados mentales, y que, por tanto, le será posible construir uno con todas las capacidades propias de la mente humana. En ese orden de ideas, se concluirá que el ordenador será capaz de razonar, imaginar, entre otras cosas.
Por otra parte, el desarrollo propiamente científico de la IA ha distinguido unos temas específicos que componen a la misma, tales son: resolución de problemas y búsqueda, representación del conocimiento y sistemas basados en el conocimiento, aprendizaje automático y la inteligencia artificial distribuida. Es de interés para el desarrollo del presente proyecto, reconocer cuál o cuáles de los temas se identifican o evidencian en el caso de Prometea; para lograr tales efectos será pertinente realizar un estudio específico de la herramienta y reconocer las causas o finalidades que sostiene la acción de implementar a la misma en la rama judicial, y a su vez, a una de las altas y más renombradas cortes de Colombia. Partiendo de dichas premisas enunciativas y conceptuales, resultará inclusiva tomar el curso investigativo mediante el método cualitativo la reciente incursión de IA en la rama judicial (Corte Constitucional), teniendo en cuenta elementos como: la igualdad, transparencia, celeridad, entre otros; todo con el fin de establecer la eficacia de la herramienta denominada "Prometea" en el ordenamiento interno, más específicamente en el judicial, y de arrojarse un resultado positivo de la premisa anterior, la viabilidad de una extensión de Prometea a los procesos de selección de tutelas de la Corte Suprema de Justicia y el Consejo de Estado. Para alcanzar dichos objetivos será necesario un estudio y análisis completo de la herramienta "Prometea", reconocer su importancia y funcionamiento, así como el propósito de la misma (hablando a largo plazo).
Es así como en el transcurso de la investigación, se hará manifiesta la importancia respectiva al impacto social que podría ocasionar la IA en el ordenamiento jurídico colombiano, reconociendo los pilares y ejes fundamentales para el funcionamiento correcto de un Estado, abordando a profundidad las prácticas que se han llevado a cabo (hablando de inteligencia artificial) para evaluar los elementos que permiten distanciarlas de las acciones humanas, así como el rol que cumplirá el programador y el operador judicial en clave del desarrollo de Prometea y la imperatividad de que los mismos posean principios y ética.

681 Artículo para participar como ponente en el XXIII Congreso Iberoamericano de Derecho e Informática a realizarse del 01 al 04 de Octubre del 2019 en la ciudad de San Pablo – Brasil. Artículo enmarcado en el proyecto institucional "Inteligencia Artificial al servicio de la justicia" de la Universidad Santo Tomás, Sede Villavicencio.

ABSTRACT
The notion of artificial intelligence was born in a meeting held in the summer of 1956 in Dartmouth (USA) where the greatest exponents and connoisseurs of the area participated. At that meeting, J. McCarthy, M. Minsky, N. Rochester and C. E. Shannon wrote a proposal in which the term "artificial intelligence" appears for the first time. It is necessary to recognize that after the evolution of the term, AI had a first classification, this is how strong and weak artificial intelligence will be recognized. For the purposes of this proposal, as well as the project later, we will refer to the notion of strong artificial intelligence, since it is characterized by considering that a computer can have a mind or mental states, and therefore it will be possible to build one with all the capabilities of the human mind. In that order of ideas, it will be concluded that the computer will be able to reason, imagine, among other things.
On the other hand, the proper scientific development of AI has distinguished specific issues that comprise it, such as: problem solving and search, knowledge representation and knowledge-based systems, machine learning and distributed artificial intelligence. It is of interest for the development of this project, to recognize which or which of the issues are identified or evidenced in the case of Prometea; To achieve these effects, it will be pertinent to carry out a specific study of the tool and recognize the causes or purposes that support the action to implement it in the judicial branch, and in turn, to one of the highest and most renowned courts in Colombia. Based on these enunciative and conceptual premises, it will be inclusive to take the investigative course through the qualitative method the recent incursion of AI in the judicial branch (Constitutional Court), taking into account elements such as: equality, transparency, speed, among others; all in order to establish the effectiveness of the tool called "Prometea" in the internal system, more specifically in the judicial system, and to throw a positive result of the previous premise, the viability of an extension of Prometea to the selection processes of Guardians of the Supreme Court of Justice and the Council of State. In order to achieve these objectives, a full study and analysis of the "Prometea" tool will be necessary, recognizing its importance and functioning, as well as the purpose of it (speaking in the long term).
Thus, in the course of the investigation, the importance of the social impact that AI could cause in the Colombian legal system will be manifested, recognizing the fundamental pillars and axes for the proper functioning of a State, addressing in depth the practices that They have been carried out (speaking of artificial intelligence) to evaluate the elements that allow them to distance them from human actions, as well as the role that the programmer and the judicial operator will play in the key to Prometea's development and the imperative that they have principles and ethics.

JUSTIFICACIÓN

Pensar en los procesos administración de justicia en el siglo XXI necesariamente nos lleva a reconocer la IA como una herramienta fundamental en la expectativa de prosperidad y desarrollo de un país como Colombia.

El presente proyecto partirá de la idea de proveer el entendimiento de lo que hoy día se conoce como Inteligencia Artificial (IA) así como su reciente inmersión en el ordenamiento jurídico colombiano. La descripción del proyecto se enfocará en el vínculo concerniente al acceso y administración de justicia y la inteligencia artificial; asimismo, resultará imperativo conocer la estructura de la inteligencia artificial que abarca las instituciones y mecanismos que la componen, así como los requisitos establecidos para que un objeto/maquina se denomine con IA.

Por otra parte, se analizará mediante un método cualitativo, la reciente incursión de IA en la rama judicial (Corte Constitucional), teniendo en cuenta elementos como: la igualdad, transparencia, celeridad, entre otros; todo con el fin de establecer la eficacia de la herramienta denominada "Prometea" en el ordenamiento interno,

más específicamente en el judicial, y de arrojarse un resultado positivo de la premisa anterior, la viabilidad de una extensión de Prometea a los procesos de selección de tutelas de la Corte Suprema de Justicia y el Consejo de Estado. Para alcanzar dichos objetivos será necesario un estudio y análisis completo de la herramienta "Prometea", reconocer su importancia y funcionamiento, así como el propósito de la misma (hablando a largo plazo). Para ello, se procurará establecer una comunicación con los órganos que principalmente la han desarrollado e incorporado. Tales serán: La universidad del Rosario (como creadora de la herramienta), la Corte Constitucional (para entender el porqué de la incorporación de la inteligencia artificial en la rama judicial), el Ministerio de las TICS (para brindar un concepto a gran escala de lo que significaría la incorporación de la IA en Colombia), entre otros conocedores de la IA en sentido amplio.

Finalmente, el proyecto dará la importancia respectiva al impacto social que podría ocasionar la IA en el ordenamiento jurídico colombiano, reconociendo los pilares y ejes fundamentales de la filosofía humanista, abordando a profundidad las prácticas que se han llevado a cabo (hablando de inteligencia artificial) para evaluar los elementos que permiten distanciarlas de las acciones humanas y la dimensión del ser en cuanto a temas de equidad y justicia, así como el rol que cumplirá el programador y el operador judicial en clave del desarrollo de Prometea y la imperatividad de que los mismos posean principios y ética.

OBJETIVOS

General

1. Analizar cómo la implementación de Prometea (IA) ha servido a la administración de justicia en Colombia.

Específico

1. Enunciar las principales instituciones y mecanismos de IA en la administración de justicia.
2. Analizar caso particular de Prometea IA y su inclusión en la Corte Constitucional.
3. Establecer los desafíos de la IA en la administración de justicia y la posible extensión del modelo Prometea a otras altas cortes.

MARCO TEÓRICO

Para el presente proyecto, será de vital importancia el despliegue de un marco teórico mediante el cual se desarrollará ésta investigación sobre inteligencia artificial y su relación con la justicia para entender y analizar de una forma pertinente todos los desafíos y velos arraigados a la inclusión de la IA en la práctica judicial colombiana. En consecuencia de lo anterior, es imperativo la enunciación de algunos conceptos generales tales como: inteligencia, justicia, humanidad, inteligencia artificial, corte constitucional, acceso a la justicia y celeridad en la administración de justicia (entendiendo la relación con la temática pretendida, así como la relación entre los mismos conceptos).

1. Inteligencia

Para poder enmarcar y entender la Inteligencia Artificial (IA), es necesario entender de antemano el concepto de inteligencia. Pues para llegar a una IA conectada a la justicia es imperativo conocer qué es exactamente la inteligencia y así poder recrearla y enlazarla al medio jurista que queremos. Según Piaget, la inteligencia es la adaptación al medio que nos rodea. Para ello es necesario tener un equilibrio entre los mecanismos de asimilación y acomodación (Piaget, 1947). Siguiendo esta línea, otro reconocido autor respecto de estudios sobre la inteligencia, definió la misma como aquella "Capacidad para pensar y para desarrollar el pensamiento abstracto, como capacidad de aprendizaje, como manipulación, procesamiento, representación de símbolos, capacidad para adaptarse a situaciones nuevas, o para solucionar problemas" (Mayer, 1983). Así mismo, encontramos que la inteligencia también puede ser entendida según Gardner como una "habilidad para resolver problemas o para elaborar productos que son de importancia en un contexto cultural o en una comunidad determinada" (Gardner, 1983).

Entendiendo así que la inteligencia puede ser entendida como un proceso de adaptación al contexto y las maneras en las que el sujeto se acoplará a sus variaciones. Teniendo un precedente, un problema o novedad y el proceso inteligente para acoplarse a dicho problema o novedad y poderlo(a) resolver.

2. Justicia

El presente concepto ha sido desarrollado a lo largo de la historia por filósofos y doctrinantes, encontrando una constante de confundir justicia con derecho, sin embargo; se tratan de dos conceptos que si bien tienen una relación directa; hacen referencia a dos cosas diferentes. Entenderemos el concepto de derecho que expuso Kelsen al expresar "el derecho es una ordenación normativa del comportamiento

humano, es un sistema de normas que regulan el comportamiento" (Kelsen, 1934). Ahora bien, respecto del concepto de justicia, Aristóteles la expone como la virtud por excelencia. Para Santo Tomás, la justicia es "el hábito por el cual el hombre le da a cada uno lo que le es propio mediante una voluntad constante y perpetua" (Aquino, 1485). También Kelsen expresa respecto de la justicia: "La justicia es para mí aquello cuya protección puede florecer la ciencia y junto con la ciencia, la verdad y la sinceridad. Es la justicia de la libertad, la justicia de la paz, la justicia de la democracia, la justicia de la tolerancia" (Kelsen, 1934). Ulpiano la expresaría como la constante y perpetua voluntad de darle a cada quién lo que le corresponde, John Rawls la ve como equidad y Cicerón como un hábito del alma. Es así pues como tenemos una variedad de posiciones y pensamientos respecto de qué es la justicia. Concepto el cual podríamos entender como aquella que nos permite decidir dentro del margen correcto y perfectamente equitativo para poder darle a cada quien lo que le corresponde.

3. Inteligencia Artificial

La inteligencia artificial (IA) ha venido abriéndose campo durante las últimas décadas. Es una defini ión amplia la que la abarca, tiene por objeto el estudio del comportamiento inteligente en las máquinas. Dicho comportamiento supone percibir, razonar, aprender, comunicarse y actuar en entornos complejos (Nilsson, 2001, pp. 1). Según la RAE, la IA es la disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico. Para lograr entender si una máquina posee IA, Alan Turing dispuso el llamado Test de Turing en 1950 para lograr resolver dicha incertidumbre el examen evaluará las capacidades de: reconocimiento del lenguaje natural, razonamiento, aprendizaje y representación del conocimiento. Una vez superadas de manera satisfactoria estas capacidades; la máquina será catalogada como una máquina de IA.

Los objetivos de la IA se sintetizan en poder alcanzar el aprendizaje y razonamiento de la mente humana y poder llegar a superarla, logrando dar respuestas y facilitando todas las áreas del conocimiento o desempeño que el hombre llegue a necesitar. Lograr éste nivel de raciocinio y aprendizaje será el determinante de la IA y su máxima expresión.

Se han distinguido cuatro tipos de IA según Stuart Russell y Peter Norving: los sistemas que piensan como humanos, estos realizan actividades como resolución de problemas, toma de decisiones y aprendizaje mediante la automatización de actividades. Los sistemas que actúan como humanos, los cuales imitan el comportamiento humano, a manera de ejemplo podemos observar la robótica. Los sistemas que piensan

racionalmente, los cuales serían los sistemas expertos. Éstos tratan de tratan de imitar el pensamiento humano. Y por último; los sistemas que actúan racionalmente, los cuales vendrían a ser a manera de ejemplo los agentes inteligentes (Russell y Norving, 2009, p.2).

4. Corte Constitucional

La Corte Constitucional creada con la presente carta política de 1991 es descrita por su página principal como un organismo perteneciente a la rama judicial del Poder Público y se le confía la guarda de la integridad y supremacía de la Carta Política. Sus funciones, descritas en el artículo 241 de la Constitución, consisten en decidir sobre las demandas de constitucionalidad que promuevan los ciudadanos contra las leyes, los decretos con fuerza de ley dictados por el Gobierno y los actos legislativos reformatorios de la Constitución; resolver sobre la constitucionalidad de la convocatoria a un referendo o a una Asamblea Constituyente para reformar la Constitución; decidir sobre la constitucionalidad de los referendos sobre leyes, las consultas populares y los plebiscitos del orden nacional; ejercer el control constitucional sobre los decretos legislativos dictados por el Gobierno al amparo de los estados de excepción; decidir definitivamente acerca de las objeciones por inconstitucionalidad que el Gobierno formule contra proyectos de ley y de manera integral y previa respecto a los proyectos de ley estatutaria aprobados por el Congreso; resolver acerca de las excusas para asistir a las citaciones realizadas por el Congreso en los términos del artículo 137 de la Carta; decidir sobre la exequibilidad de los tratados internacionales suscritos por el Estado colombiano y de las leyes que los aprueben y revisar las decisiones judiciales relacionadas con la acción de tutela de los derechos constitucionales prevista en el artículo 86 de la Constitución.

5. Acceso a la justicia

Según el ministerio de justicia el acceso a la justicia es una pieza fundamental del Estado Social de Derecho por la relación intrínseca que tiene con la reducción de la pobreza y el crecimiento inclusivo. El acceso a la justicia abarca cada aspecto de la cotidianidad, incluyendo la salud, el empleo, la educación, la vivienda y el emprendimiento. Además, en la sentencia T-283/13, se estableció concepto sobre el derecho de acceso a la administración de justicia, definiendo lo siguiente: "El derecho a la administración de justicia ha sido definido por la jurisprudencia constitucional como la posibilidad reconocida a todas las personas residentes en Colombia de poder acudir en condiciones de igualdad ante los jueces y tribunales de justicia, para propugnar por

la integridad del orden jurídico y por la debida protección o el restablecimiento de sus derechos e intereses legítimos, con estricta sujeción a los procedimientos previamente establecidos y con plena observancia de las garantías sustanciales y procedimentales previstas en las leyes. Aquella prerrogativa de la que gozan las personas, naturales o jurídicas, de exigir justicia, impone a las autoridades públicas, como titulares del poder coercitivo del Estado y garantes de todos los derechos ciudadanos, distintas obligaciones para que dicho servicio público y derecho sea real y efectivo".

6. Celeridad en la administración de justicia

De conformidad con la ley 270 de 1996, la celeridad en la administración de justicia debe ser pronta, cumplida y eficaz en la solución de fondo de los asuntos que se sometan a su conocimiento. Los términos procesales serán perentorios y de estricto cumplimiento por parte de los funcionarios judiciales. Su violación injustificada constituye causal de mala conducta, sin perjuicio de las sanciones penales a que haya lugar. Lo mismo se aplicará respecto de los titulares de la función disciplinaria. Asimismo, la Corte Constitucional en sentencia C-826-13 expresó sobre el principio de celeridad lo siguiente: "En cuanto al principio de celeridad, la jurisprudencia de esta Sala ha sostenido que éste implica para los funcionarios públicos el objetivo de otorgar agilidad al cumplimiento de sus tareas, funciones y obligaciones públicas, hasta que logren alcanzar sus deberes básicos con la mayor prontitud, y que de esta manera su gestión se preste oportunamente cubriendo las necesidades y solicitudes de los destinatarios y usuarios, esto es, de la comunidad en general. Igualmente ha señalado esta Corporación, que este principio tiene su fundamento en el artículo 2º de la Constitución Política, en el cual se señala que las autoridades de la Nación tienen la obligación de proteger la vida, honra, bienes, creencias y demás derechos y libertades de los ciudadanos, al igual que asegurar el cumplimiento de los deberes sociales del Estado y de los particulares, lo cual encuentra desarrollo en artículo 209 Superior al declarar que la función administrativa está al servicio de los intereses generales entre los que se destaca el de la celeridad en el cumplimiento de las funciones y obligaciones de la administración pública". Con este precedente, podremos ver a lo largo de éste proyecto cómo la IA ayudará a la celeridad en la administración de justicia, facilitando los diversos procesos que la justicia necesita para hacerse efectiva y célere.

MARCO METODOLÓGICO

Para llevar a cabo el proceso de investigación se realizará una metodología con enfoque cualitativo, que es entendido por el Maestro Roberto Hernández Sampieri en la sexta edición de su libro Metodología de la investigación como un enfoque:

> …Guiado por áreas o temas significativos de investigación. Sin embargo, en lugar de que la claridad sobre las preguntas de investigación e hipótesis preceda a la recolección y el análisis de los datos (como en la mayoría de los estudios cuantitativos), los estudios cualitativos pueden desarrollar preguntas e hipótesis antes, durante o después de la recolección y el análisis de los datos.

Asimismo, el maestro Sampieri asevera que "La acción indagatoria se mueve de manera dinámica en ambos sentidos: entre los hechos y su interpretación, y resulta un proceso más bien "circular" en el que la secuencia no siempre es la misma, pues varía con cada estudio." (Sampieri, 2014, p: 7). Teniendo en cuenta el contenido de la cita en mención, la adopción del enfoque cualitativo permitirá una adecuada interpretación de los hechos y de las normas inmersas en el ordenamiento jurídico Colombiano.

BIBLIOGRAFÍA/REFERENCIAS

Aquino, S., (1485), Yon B, L (s.f) La Justicia de acuerdo a Santo Tomás de Aquino (ensayo). Recuperado de: http://www.eleutheria.ufm.edu/articulos/050921_01_lajusticia.htm#_ftn3

Congreso de Colombia. (15 de marzo de 1996) Estatutaria de la Administración de Justicia. [Ley 270 de 1996]. Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/ley_0270_1996.html

Corte Constitucional (s/f). La Corte. Corte Constitucional. Recuperado de http://www.corteconstitucional.gov.co/lacorte/

Corte Constitucional, (2013) D-9623 [MP Luis Ernesto Vargas Silva].

Corte Constitucional, (2013) T- 3.567.368. [MP Jorge Ignacio Pretelt Chaljub].

Editorial, (2018). El mundo de Sophia: La primer robot humanoide con inteligencia artificial avanzada estuvo en Colombia esta semana. El Tiempo. Recuperado de https://www.eltiempo.com/opinion/editorial/el-mundo-de-sophia-robot-con-inteligencia-artificial-en-medellin-25035

Gardner, H. (1983). Frames of Mind. The Theory of Multiple Intelligences. Nueva

York, Basic Books. (Versión castellana (2001). Estructuras de la Mente. La Teoría de las Inteligencias Múltiples. México, FCE).

Guber, R. (2007). La etnografía Método, campo y refl xividad. (Norma, Ed.) (p. 140). Bogotá, Buenos Aires, Caracas. Recuperado de: http://www.arte.unicen.edu.ar/secretarias/academica/catedra/dinamica/unidad5/complementaria/etno_guber.pdf

Hernández, F., Boulat, P., (2015). Inteligencia Artificial y Derecho. Problemas y perspectivas. Noticias Jurídicas. Recuperado de http://noticias.juridicas.com/conocimiento/articulos-doctrinales/10061-inteligencia-artificial-y-derecho-problemas-y-perspectivas/

Kelsen, H., (1934). Reine Rechtslehre (2° ed. 1960). Traducción al español de la segunda edición por Roberto Vernengo: Teoría pura del derecho, Porrúa-UNAM, México, D. F., 1991.

Mayer, R., (1983). Pensamiento, Resolución de Problemas y Cognición. (Trad. Graziela Baravalle). Serie Cognición y Desarrollo Humano. Paidós.

Nilsson, J., (2001). Inteligencia Artificial: Una nueva síntesis. Madrid. McGra -Hill.

Piaget, J., (1947), Psicología de la Inteligencia.

Real Academia Española y Asociación de Academias de la Lengua Española (2014). «Diccionario». Diccionario de la lengua española (23.ª edición). Madrid: Espasa. ISBN 978-84-670-4189-7.

Rivanedeira, J. (2019). Prometea, inteligencia artificial para la revisión de tutelas en la Corte Constitucional. Mayo 08, 2019, de Ámbito Jurídico. Sitio web: https://www.ambitojuridico.com/noticias/informe/constitucional-y-derechos-humanos/prometea-inteligencia-artificial-para-l

Russell, Stuart J.; Norvig, Peter Norvig (2009). Artificial intelligence: a modern approach (en inglés) (3.ª edición). Upper Saddle River, N.J.: Prentice Hall. ISBN 0-13-604259-7.

Sampieri, H. Roberto. (2014). Metodología de la Investigación. México D.F.: McGraw-Hill.

Torra, V. (2011). La inteligencia artificial. Mayo 08, 2019, de Instituto de Investigación en Inteligencia Artific al (CSIC) Sitio web: http://www.fgcsic.es/lychnos/es_es/

articulos/inteligencia_artificia

Vargas, S., (2019). La inteligencia artificial, a la conquista del universo / Opinión. El Tiempo. Recuperado de https://www.eltiempo.com/vida/ciencia/inteligencia-artificial-a-la-conquista-del-univers -columna-de-santiago-vargas-344136

LA JUSTICIA PREDICTIVA: ENTRE MITO Y REALIDAD

Eje tematico: Justicia Predictiva, Bases de datos, algoritmos, Datos Abiertos

Autores:
Audilio Gonzalez
Docteur en droit et Informatique. Profesor. Université Paul-Valéry. Montpellier. Francia. Institut Méditerranéen des Sciences de l'Information et de la Communication (IMSIC) Université de Toulon, Aix-Marseille Université - audilio.gonzales@univ-montp3.fr

Ana María Sanabria Clavijo
Secretaria general de VisuaLEX (http://visualex.org). Asociada del Bufete Fernando Sanabria y Abogados Asociados. Colombia

RESUMEN
Nuestro artículo está dividido en cuatro partes fundamentales, empezando por un breve recuento histórico de la evolución de la Justicia Predictiva; para demostrarles que la este tipo de predicción jurisprudencial no es un fenómeno reciente como se podría pensar, pues esta noción fue planteada hace más de dos siglos en Francia por Condorcet en su Ensayo sobre la aplicación del análisis de la probabilidad de decisiones tomadas por pluralidad de votos de 1785. En los Estados Unidos, Loevinger, Kort y Lawlor fueron los primeros en haber formulado la idea de anticipar un resultado los litigios basados en decisiones judiciales anteriores.
Haremos referencia en la segunda parte a las definiciones y los elementos funcionales: datos, open data y algoritmos que hacen parte de la noción de la justicia predictiva. en una tercera parte traeremos a colación ejemplos actuales de dispositivos de justicia predictiva para terminar con la elaboración de una síntesis sobre las ventajas y los límites de este tipo de justicia.

ABSTRACT
Our article is divided into four fundamental parts, beginning with a brief historical account of Predictive Justice evolution; demonstrating that this type of jurisprudential prediction is not a recent phenomenon as you might think; this notion was raised more than two centuries ago in France by Condorcet in his Essay "Application of Probability Analysis on Decisions Made by Plural Vows in 1785." In the United States, Loevinger, Kort and Lawlor were the first to formulate the idea of anticipating the outcome of disputes based on previous judicial decisions. The second section, will mention the definitions and predective justice functional elements: data, open data and algorithms,. In a third section, we will bring up current examples of predictive justice devices. And finall , we will summarize the advantages and limits of this type of justice."

La Justicia Predictiva: entre mito y realidad

"El día que la inteligencia artificial se desarrolle por completo podría significar el fin de la raza humana. Funcionará por sí sola y se rediseñado cada vez más rápido. Los seres humanos, limitados por la lenta evolución biológica, no podrán competir con ella y serán superados. "
Stephen Hawking

"Nadie lo expresa de esta manera pero creo que la inteligencia artificial es casi una

disciplina de humanidades. Es en realidad un intento de entender la inteligencia y la razón humanas".
Sebastian Thrun, escritor y profesor de inteligencia artificial en la Universidad de Stanford

"Debemos abordar, individual y colectivamente, las cuestiones morales y éticas planteadas por la investigación de vanguardia en inteligencia artificial y biotecnología, lo que permitirá la extensión de nuevas formas de vida, como los bebés de diseño y la extracción de memoria".
Klaus Schwab, fundador de Foro Económico Mundial

INTRODUCCION

Nuestro artículo está dividido en cinco partes fundamentales: empezando por un breve recuento histórico de la evolución de la Justicia Predictiva (1). Haremos referencia en la segunda parte a las definiciones y los elementos funcionales (2). Luego mostramos cómo los datos, open data y algoritmos que hacen parte de la noción de la justicia predictiva (3). enseguida traemos a colación ejemplos actuales de dispositivos de justicia predictiva (4) y para terminar elaboramos una síntesis sobre las ventajas y los límites de este tipo de justicia (5).

1. Breve Resumen Histórico de la Justicia Predictiva

La predicción jurisprudencial no es un fenómeno reciente como se podría pensar, pues esta noción fue planteada hace más de dos siglos[682] en Francia por Condorcet[683] en su Ensayo sobre la aplicación del análisis de la probabilidad de decisiones tomadas por pluralidad de votos de 1785. En los Estados Unidos, Loevinger, Kort y Lawlor fueron los primeros en haber formulado la idea de anticipar un resultado los litigios basados en decisiones judiciales anteriores. El Profesor Norteamericano Holmes propuso el concepto de predicción al vaticinar en una conferencia en Boston (Estados Unidos) en 1709 lo siguiente [...]: "lo que yo entiendo por Derecho, es decir con la Ley, son las profecías de lo que decidirán concretamente los tribunales" [...].[684]

En 1837, el matemático Simon-Denis Poisson publicó un importante tratado titulado "*Recherches sur la probabilité des jugements en matière criminelle et en matière civile*" ("Investigaciones sobre la probabilidad en los juicios en materia civil y criminal"). Este estudio es el tercer intento importante de aplicar el cálculo de probabilidad a la

682 Barbin Evelyne, Marec Yannick. Les *recherches sur la probabilité des jugements* de Simon-Denis Poisson. In: Histoire & Mesure, 1987 volume 2 - n°2. Varia. pp. 39-58. DOI : https://doi.org/10.3406/hism.1987.1311 www.persee.fr/doc/hism_0982-1783_1987_num_2_2_1311

683 CONDORCET, Essai sur l'application de l'analyse à la probabilité des décisions rendues à la pluralité des voix, Paris, Imprimerie Royale, 1785.

684 Guillaume ZAMBRANO. Precedents et predictions jurisprudentielles a l'ere des big data : parier sur le resultat (probable) d'un proces. 2015. https://hal.archives-ouvertes.fr/hal-01496098

evaluación de los procedimientos judiciales. Laplace[685] en su Ensayo filosófic sobre las probabilidades de 1814, busco calcular la probabilidad de que la decisión de un juicio sea correcta.

Loevinger, propuso la creación de una nueva ciencia "jurimétrica" definida como "la aplicación del método científico al estudio del derecho", cuya finalidad era el "cálculo de las probabilidades de las decisiones judiciales"[686]. Lee Loevinger lanzó el término "jurimetría" y subrayó la importancia de los métodos científicos y estadísticos para los abogados. Vio una serie de posibilidades para utilizar estas aplicaciones en la ley. El sostenía que el conocimiento de la ley podía obtenerse mediante la observación, en lugar de la especulación. La jurimetría prometía agrandar las ventanas en la casa de la ley, para que los que están dentro puedan ver hacia fuera, y abrir las puertas con el fin que los que están fuera puedan entrar. La voluntad de Loevinger fue aplicar métodos científicos a la le , pero no recibió un apoyo unánime[687].

Jurimétrica, según Loevinger es "el estudio empírico de la forma, el significado y la pragmática (y las relaciones entre ellas) de las demandas y autorizaciones que emanan de las organizaciones estatales con la ayuda de modelos matemáticos, utilizando asi el individualismo metodológico como paradigma básico para la *explicación y la predicción* del comportamiento humano"[688].

Kort[689] realizó un estudio en 1957, que tenía por objeto "demostrar que, al menos en un ámbito de la revisión judicial, es posible tomar algunas decisiones, identificar los elementos de hecho que influyeron en las decisiones, obtener valores numéricos de estos elementos utilizando una fórmula y, a continuación, predecir correctamente las decisiones de los casos restantes en el ámbito especificado.

Nagel[690] en este artículo, usando operaciones aritméticas y algebraicas bien conocidas, sigue las variables clave de anteriores para determinar la probabilidad de un juicio para un litigante en un nuevo caso. Nagel y Lawlor han desarrollado métodos para analizar jurisprudencia con el fin de predecir las decisiones; todo depende del contenido o de los hechos, análisis de las decisiones.

Los tres dirigieron su atención a las decisiones de la Corte Suprema de los Estados Unidos como un todo, partiendo todos del mismo punto: Los tres hacen uso de las computadoras. Aunque, Lawlor aplicó su tecnología a los jueces individuales. Loevinger ha reconocido que la esperanza del éxito de la predicción del derecho se basa en el desarrollo de métodos eficaces de análisis de contenido. En los métodos de

685 LAPLACE, *"Essai philosophique sur les probabilités"*. Paris, réédition Bourgeois, 1986.

686 Lee LOEVINGER, « Jurimetrics - The Next Step Forward », Minnesota Law Journal, 1949

687 PALIWALA, A. *A History of Legal Informatics*. Prensas Universitarias de Zaragoza. 2010, 288 pags.

688 Ob. cit. pag. 150

689 KORT, F. (1957). Predicting Supreme Court Decisions Mathematically: A Quantitative Analysis of the "Right to Counsel" Cases. *American Political Science Review, 51*(1), 1-12. doi:10.2307/1951767

690 Stuart NAGEL, « Using simple calculations to predict judicial decisions », American Behavioral Scientist , Décembre 1960, n° 4(4), p. 1.

Kort, las ponderaciones se basan en hechos individuales en los que aparentemente se basa el tribunal para llegar a su decisión. La suma de estas ponderaciones da el peso de los hechos en un caso. Kort encontró que cuando el peso de todos los hechos en un caso excede un valor umbral identificable, el caso usualmente va en una dirección, pero cuando cae por debajo de ese valor, usualmente va en la otra dirección. El método de Nagel también emplea una técnica de ponderación[691].

Para desvirtuar el juicio erróneo sobre la novedad de la Justicia Predictiva, haremos un breve recuento histórico de la transformación del derecho frente a las innovaciones introducidas por la tecnología, con el fin de demostrar que la predicción jurisprudencial no es una demostración incipiente de Inteligencia Artificial (AI) sino un avance secuencial de la misma.

En la evolución de la derecho predictivo podemos distinguir varias etapas a saber: una fase inicial, una fase de automatización y, por último, una fase de apoyo a la decisión; para evidenciar porque el desarrollo de la justicia predictiva se encuentra en la última fase. En la *fase inicial*, durante el primer período de innovación, surgieron las primeras bases de datos. Estos progresos se erigieron en torno a motores de búsqueda incipientes, los cuales permitieron examinar la presencia de una palabra específica en un texto o en los metadatos del texto. La segunda etapa, denominada *fase de automatización*, corresponde a la ejecución expedita de operaciones básicas para el abogado, como la redacción de prácticas estandarizadas (estatutos, contratos, formularios) o la vinculación a través de plataformas construidas para este fin. La última etapa, que creemos tal vez la actual, se presenta bajo el nombre de "*apoyo a la decisión*", pues esta se fundamenta en tecnologías desplegadas por industrias avanzadas y la utilización informática. Poseyendo un excesivo impacto en la sociedad, puesto que simula el núcleo de la acción humana: la elección de resoluciones o juicios. La justicia predictiva es claramente parte de este último paso.

2. Definiciones de Justicia Predictiva y Su Relación con la Inteligencia Artificial (IA)

A continuación, les expondremos múltiples enunciaciones encontradas sobre la conceptualización de Justicia Predictiva por seis diferentes literatos del tema, con el fin de forjar una noción más rigurosa sobre lo que se debe entender como tal. Para concluir este acápite, mostraremos cual es nuestra visión sobre esta innovación tecnológica y su relación con la Inteligencia Artificial (IA).

691 Lawlor, Reed C. "What Computers Can Do: Analysis and Prediction of Judicial Decisions." *erican Bar Association Journal* 49, no. 4 (1963): 337-44. http://www.jstor.org/stable/25722338.

La justicia predictiva, llamada por Frédéric Rouvière "la versión moderna de la bola de cristal"[692], consiste en predecir, como sabemos, la solución dada a un conflicto basado en la informática.

En el reporte sobre el Open Data en Francia del 2017 p. 24 precisa que " la justicia predictiva consiste, "en el desarrollo de algoritmos basados en un gran número de decisiones judiciales ya dictadas, en extraer información útil de las decisiones para proponer probabilidades de resultado de un litigio".

La Justicia Predictiva, se define como el "conjunto de instrumentos desarrollados a través del análisis de grandes masas de datos de la justicia que proponen, a partir de un cálculo de probabilidades, de predecir tanto como sea posible el resultado de un litigio".[693]

Desde un punto de vista funcional la Justicia Predictiva, se puede definir como el "uso de algoritmos que permiten calcular el éxito de un proceso dentro de una jurisdicción, el monto de las indemnizaciones que es posible obtener y de identificar los argumentos de hecho y derecho que serán susceptibles de influir en la decisión jurisdiccional futura"[694].

La definició tomada de B. Dondero, "Un conjunto de instrumentos desarrollados a través del análisis de grandes cantidades de datos de justicia que incluyen, en particular sobre la base de un cálculo de probabilidad, para predecir el resultado de un litigio en la medida de lo posible"[695].

En nuestro concepto, se debe entender la Justicia Predictiva, como el análisis de grandes cantidades de decisiones judiciales por un software de inteligencia artificial con el fin de hacer predicciones sobre el resultado de ciertos tipos de litigios especializados.

El término "predictivo" utilizado por las empresas de tecnología jurídica proviene de un ámbito de la ciencia (principalmente de la estadística) que permite predecir los resultados futuros a través del análisis inductivo. Este razonamiento identifica las correlaciones entre las variables de ingreso de datos (criterios establecidos en la legislación, los hechos del caso y el raciocinio) y datos de salida (juicio formal). Las correlaciones que se consideran relevantes admiten crear modelos que, cuando se utilizan con nuevos datos de entrada (es decir, nuevos hechos descritos), producen una predicción de la decisión.

Durante mucho tiempo, la noción de Inteligencia Artificial (de ahora en adelante IA) fue discutida dentro de la comunidad científica sin ningún consenso pleno sobre

692 F. ROUVIÈRE, professeur à l'université d'Aix-Marseille, *« La justice prédictive, version moderne de la boule de cristal », RTD Civ., 2017, p. 527.*

693 Observar el reporte del profesor Loïc CADIET de la universidad Panthéon-Sorbonne *"l'Open data des décisions de justice. Mission d'étude et de préfigurattion sur l'ouverture du public des décisions de justice"* mayo 2017. pag. 24. http://www.justice.gouv.fr/publication/open_data_rapport.pdf

694 ob. cit. pag 10

695 *« Justice prédictive : la fin de l'aléa judiciaire ?* » Recueil Dalloz 2017, p.5

su significa o, solo fue hasta 1956 en la Conferencia de Dartmouth, donde por primera vez, el matemático y profesor estadounidense John McCarthy, dio una definición certera de lo que era este campo de estudio estableciéndola como «la ciencia e ingenio de hacer máquinas inteligentes, especialmente programas de cómputo inteligentes».

Partiendo de esta definición y viendo la evolución que esta ciencia ha tenido durante los años podríamos decir que la IA, tiene como propósito el análisis y la investigación de la comprensión, discernimiento, percepción, solución de conflictos y toma de resoluciones de la conducta humana, para que, una vez analizados estos comportamientos; sean imitados y desarrollados por un ordenador o máquina; atribuyéndole a estos últimos, conductas y/o actividades mentales humanas para incluso a optimizar dichas capacidades ya existentes en cada individuo analizado.

Como puede inferirse de la definición de IA dada anteriormente, su relación con la Justicia Predictiva es muy estrecha, pues esta última busca resolver un problema y tomar una decisión jurídica mediante el análisis de casos similares en cuanto a los hechos, "*ratio decidendi*" y decisiones de sentencias ya ejecutoriadas. Estos estudios se realizan a través de un algoritmo manejado por un programa u ordenador preestablecido.

3. Elementos de la Justicia Predictiva: Datos y las Bases de Datos, el Open Data y los Algoritmos

Los elementos principales de la justicia predictiva son esencialmente tres: Datos y las bases de datos, el open data y los algoritmos.

3.1 Datos y Bases de Datos

Definición de bases de datos. A efectos de la Directiva 96/9/CE del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos, "tendrán la consideración de «base de datos» las recopilaciones de obras, de datos o de otros elementos independientes dispuestos de manera sistemática o metódica y accesibles individualmente por medios electrónicos o de otra forma".[696]

Estos artículos de ley requieren la publicación en datos abiertos (datos disponibles de manera gratuita, modificables y transferibles) de todas las decisiones judiciales y administrativas, después de la anonimización, a partir de la fecha de vigencia de los decretos. correspondiente solicitud.

Características de las bases de datos. Esto aumenta drásticamente el tamaño de la base de datos a la que pueden acceder las herramientas de justicia predictiva, permitiéndoles

696 Consultar en línea: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELE-X%3A31996L0009

proporcionar estadísticas cada vez más precisas y una visión general de la posición de un juez o jurisdicción en litigios muy graves, específico.

3.2 Open Data. De inición de datos abiertos

Este término, hace referencia a la posibilidad de consulta y reutilización por el público de las de bases de datos estructuradas para su descarga.

Estos datos pueden ser reutilizados de manera gratuita, siempre y cuando se observen las condiciones de la licencia específic , que puede en concreto, convenir o impedir los fines establecidos de reutilización.

El Open data o datos abiertos, no deben confundirse con la información pública unitaria disponible en sitios web, puesto que en esta última situación no se puede descargar toda la base de datos sino una parte de ella.

Por último, a veces existe confusión entre los datos (en sentido estricto, datos abiertos) y sus métodos de procesamiento (machine learning, data science, etc) para diferentes objetivos (motores de búsqueda, asistencia en la redacción de documentos, análisis de casos, tendencias del derecho, la predicción de las decisiones jurisprudenciales, etc.) lo cual implica que se deba tener muy claro su conceptualización para evitar esta desorientación.

Los Datos Abiertos son datos cuyo acceso es totalmente público y gratuito, así como su explotación y reutilización. Estos datos ofrecen muchas oportunidades para expandir el conocimiento humano y crear nuevos productos y servicios de calidad. Descubra una definición completa y ejemplos concretos de cómo utilizar Open Data.

3.2.1 Datos abiertos: definición estandarizada

El término Datos Abiertos se refiere a los datos a los que cualquier persona puede acceder, usar o compartir. Los criterios esenciales de Open Data son la disponibilidad, reutilización y distribución, y la participación universal. Esta es la definición dada por la Open Knowledge Foundation en 2005.

Disponibilidad y acceso: Los datos deben ser plenamente accesibles a un coste razonable de reproducción. Preferiblemente, deben poder descargarse de Internet. La forma debe ser cómoda y modificable.

Reutilización y redistribución: Los datos deben proporcionarse en condiciones que permitan su reutilización y redistribución, incluida la mezcla con otros conjuntos de datos.

Participación universal: Todos deben poder utilizar, reutilizar y redistribuir los datos. No debe haber discriminación en cuanto a la finalidad del uso, ni contra individuos o

grupos. Por ejemplo, las restricciones no comerciales que impiden el uso comercial, o las restricciones de uso en ciertas áreas, no son compatibles con los datos abiertos.

Estos tres criterios son la esencia de los Datos Abiertos, ya que permiten la interoperabilidad. La interoperabilidad se refiere a la capacidad de diferentes empresas o sistemas para trabajar juntos. En este caso, la interoperabilidad es la capacidad de mezclar diferentes conjuntos de datos.

3.2.2 Interoperabilidad, la esencia de los datos abiertos

Esta interoperabilidad es importante porque permite que diferentes componentes trabajen juntos. Esto es lo que hace posible crear sistemas grandes y complejos. Sin interoperabilidad, esto simplemente no es posible. Un ejemplo es el mito de la Torre de Babel. En esta leyenda, la imposible comunicación impide completamente la construcción de la torre.

En el caso de los datos, la puesta en común se basa en la posibilidad de mezclarlos libremente. Esta interoperabilidad es esencial para cosechar los beneficios de la apertura. Entonces es posible desarrollar más y mejores productos y servicios.

3.2.3 Los datos abiertos legales

En Europa existe el sitio http://eucases.eu/legalopendata.html que reagrupa las experiencias de Open data Legal.

En Francia la Ley de la República Digital No. 2016-1321, de 7 de octubre de 2016, prevé la apertura de los datos de las decisiones judiciales. El 25 de enero de 2017, Jean-Jacques Urvoas estimó que la aplicación debería durar varios años "de 12 a 24 meses para las decisiones civiles de los tribunales de apelación; de 24 a 36 meses para las decisiones penales; y extenderse a un período de 3 a 8 años para las decisiones en primera instancia". en Francia existe el site de Open Data que pone a disposition la legislacion y un numero importante de bases de datos jurisprudenciales a disposición de los ciudadanos en formato XML.

El 15 de septiembre de 2016, el DILA y la Asociación de Derecho Abierto lanzaron un breve programa sobre la apertura de datos de jurisprudencia en colaboración con Etalab, el Ministerio de Justicia, el Tribunal de Casación, el Tribunal de Cuentas, el Conseil d'État, el Colegio de Abogados de París, la CNIL y el INPI1.

La adopción de los artículos 20 y 21 de la Ley para una República Digital de 7 de octubre de 20162, que prevé la apertura masiva de los datos de la jurisprudencia en un futuro próximo, ha creado un clima de emulación y ha planteado muchas cuestiones que han sido abordadas por el DILA y la asociación Open Law, con el fin de estimular

desde el principio una dinámica de colaboración en la construcción de futuros modelos de difusión de sentencias.

3.3 Algoritmos

Los algoritmos son una secuencia finita de reglas formales, es decir, operaciones lógicas e instrucciones, que hacen posible obtener un resultado de la entrada inicial de información. Esta secuencia puede formar parte de un proceso de ejecución automatizado y basarse en modelos diseñados a través del *machine learning* [697].

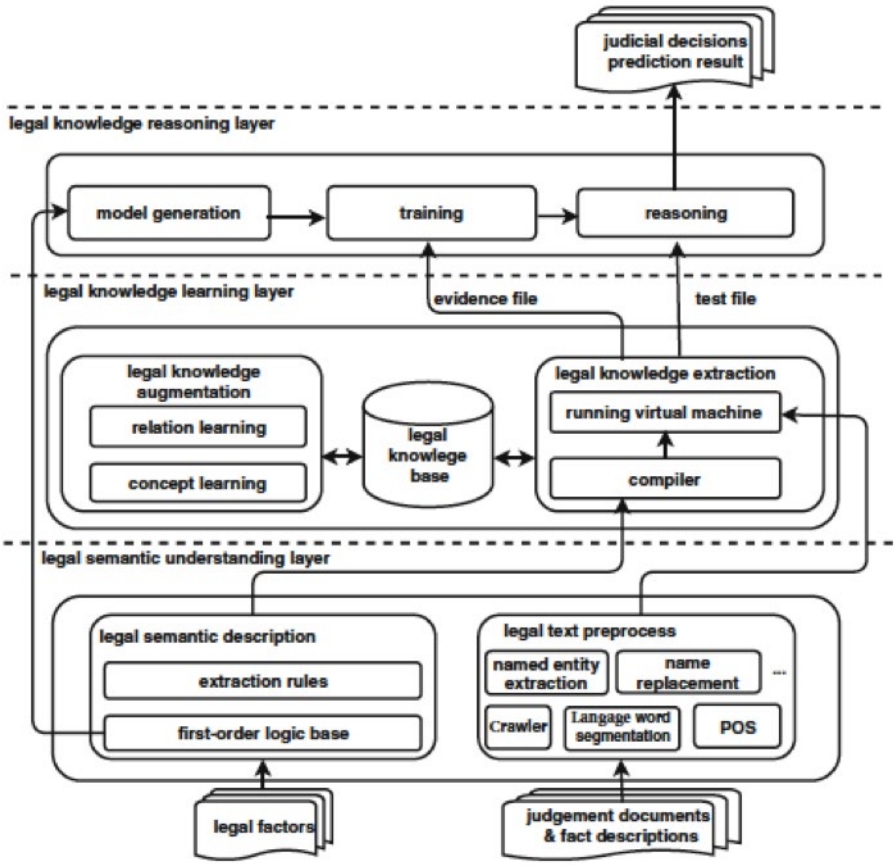


Figure 1. Marco de computación cognitiva para predecir las decisiones judiciales. https://doi.org/10.1007/s11265-018-1429-9. Jiajing Li et al. (2018)[698]

697 El aprendizaje automático (o machine learning, por su nombre en inglés) permite construir un modelo matemático a partir de los datos, incorporando un gran número de variables que no se conocen de antemano. Los parámetros son configurados gradualmente durante la "fase de aprendizaje", la cual utiliza conjuntos de datos de formación para encontrar y clasificar los enlaces. Los diferentes métodos de aprendizaje automáticos son elegidos por los diseñadores dependiendo de la naturaleza de las tareas a realizar. Estos métodos se suelen clasificar en tres categorías: Aprendizaje supervisado (humano), aprendizaje no supervisado y aprendizaje de refuerzo. Estas tres categorías agrupan diferentes métodos, entre los que se incluyen los métodos de redes, aprendizaje profundo (deep learning), etc.

698 Li, Jiajing, Guoying Zhang, Longxue Yu, et Tao Meng. « Research and Design on Cognitive Computing Framework for Predicting Judicial Decisions ». *Journal of Signal Processing Systems*, 10 décembre 2018. https://doi.org/10.1007/s11265-018-1429-9.

En la justicia predictiva, entre los algoritmos más usados para el procesamiento de la información está el análisis regresivo[699], estableciendo múltiples relaciones entre las variables, además de la minería de datos[700], para el procesamiento de datos no estructurados. Dentro de los instrumentos del tipo hallados en el comercio están la IBM Waston, herramientas open-source, como Google y Microsoft CNTK TensorFLow.

Estos modelos predictivos al usar estos tipos de algoritmos -principalmente de regresión- deben realizar un análisis que se divide en tres etapas, las cuales están asociadas y corresponden a las respuestas de las siguientes tres preguntas:

> *1 - "¿Qué pasó?* "Debido a la adquisición de gran volumen de datos, es decir, al aditamento de metadatos que detallan las particularidades de la disputa en un documento, soluciones predictivas justicia son primeros formidables motores de búsqueda semánticos e inteligentes, muy superior a la generación anterior. Gracias a ellos, el profesional puede, entre otros, ordenar la información en función de su significado o sus características específicas.
>
> *2 - "¿Qué pasará?* Como nunca hay dos disputas perfectamente idénticas, el desafío es comprender el impacto de un factor o una combinación de factores (análisis multivariado) en la sentencia. Aquí es donde entran en juego los algoritmos de *machine learning*, capaces de cruzar observaciones para crear modelos predictivos complejos. Al aplicar estos modelos a las características de una disputa, es posible evaluar las probabilidades de resolución.
>
> *3 - "¿Cómo optimizarlo*? La tecnología tiene como propósito valorar y contrastar múltiples estrategias, lo cual faculta al usuario de dicha innovación a escoger su preferencia de dichas creaciones; para lograr mayores posibilidades de éxito, siendo estas determinadas por la estadística según las particularidades del caso[701].

4. Ejemplos de Utilización de la Justicia Predictiva

699 El examen de regresión lineal está siendo considerablemente aplicado para modelar la correlación estructural entre una variable respuesta o dependiente y una o un conjunto de predictores o variables independientes o explicativas. Usualmente, se emplea este prototipo para conjeturar, tan exactamente como sea viable, los alcances de la variable respuesta frente a observaciones futuras de las variables explicativas. Estos esquemas terminan siendo de fácil edificac ón y comprensión razón por la cual termina siendo uno de los predilectos a la hora de realizar este análisis. Este método, no obstante, obedece al desempeño de unos hipotéticos o circunstancias sobre sus bases de cimentación, estableciendo únicamente su utilización a escenarios donde estas condiciones se realicen.

700 Datamining (minería de datos), es el conjunto de métodos y tecnologías que acceden a examinar enormes bases de datos, de manera automática o semiautomática, con el propósito de hallar estándares repetitivos, normas o tendencias que expongan el comportamiento de los datos en un contexto señalado. Fundamentalmente, el datamining nace para pretender asistir en la comprensión del contenido de un repositorio de datos. Con esta finalidad, la minería de datos hace uso de conocimientos estadísticos y, en ciertos momentos también, de algoritmos de búsqueda allegados a la Inteligencia Artificial y a las redes neurológicas

701 Gide la justice prédictive. https://blog.predictice.com/guide-ultime-de-la-justice-predictive

En la Actualidad, el desarrollo de la tecnología ha creado grandes avances en materia de Justicia Predictiva, no solamente en países desarrollados -tecnológicamente hablando-, sino que vemos que esta tendencia ha generado un revuelo a nivel mundial.

4.1 Cyberjusitice laboratory - "corte virtual" (canadá)

El laboratorio de Ciberjusticia fue creado en 2010 por los profesores Karim Benyekhlef (Universidad de Montreal) y Fabien Gélinas (Universidad McGill), con el fin de generar "un centro para el pensamiento y la creatividad, donde los procesos de justicia se modelan y se vuelven a imaginar. Específicamente, el Laboratorio analiza el impacto de las tecnologías en la justicia y desarrolla herramientas tecnológicas concretas que se adaptan a la realidad de los sistemas de justicia."[702]

Dentro del laboratorio de Ciberjusticia, existe un proyecto que vale la pena resaltar, se denomina "Corte Virtual". Esta es una plataforma es altamente modular y configurable rápidamente para que se pueda modelar en muy poco tiempo la mayoría de las funciones esenciales de una cadena de justicia penal, civil o administrativa.

4.2 COMPAS (Estados Unidos)

Compas[703] es una plataforma creada por la empresa americana Northpointe es utilizada por la Policía de Nueva York, para "evaluar los riesgos" que representa una persona para la seguridad de la ciudad; este programa encuentra su sustento en algoritmos que analizan el estatus socioeconómico, laboral, familiar, antecedentes personales y familiares, delitos del vecindario y otros componentes para conseguir un pronóstico del peligro criminal del sujeto, ya sea en una escala de "bajo" a "alto" , con juicios concretos o porcentajes.

702 Mirar : https://www.cyberjustice.ca/en/parle-3/la-solution-cyberjustice/

703 Examinar: http://www.northpointeinc.com/fil_s/downloads/Risk-Needs-Assessment.pdf

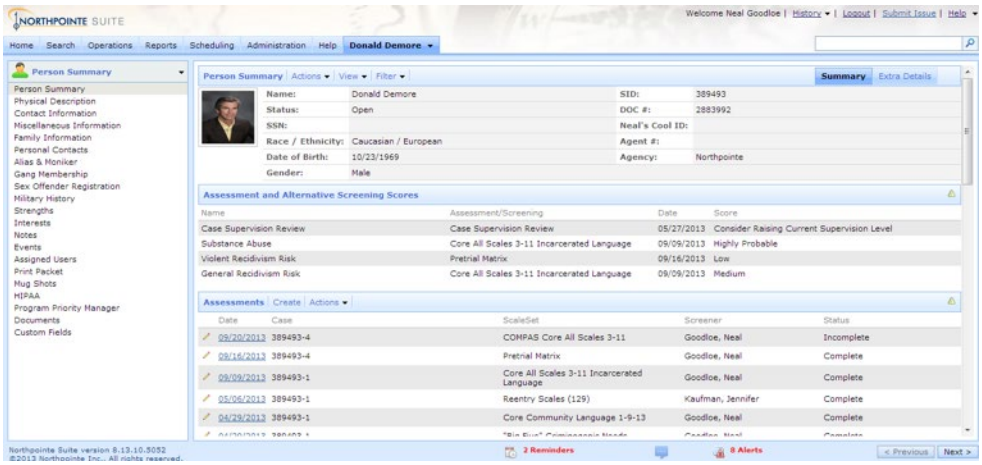


Figura 2. Pantalla de resumen de evaluación e historial de casos

En el escrito, divulgado el 23 de mayo de 2016[704] por ProPublica[705], se expusieron potenciales discriminaciones raciales en el algoritmo COMPAS. Este estudio, extracto los puntajes del algoritmo para de más de 10,000 individuos arrestados por conductas punibles, en el condado de Broward (Florida) y la probabilidad de repetición de esa u otra conducta ilícita dentro de dos años siguientes. Según los investigadores, el sesgo en las puntuaciones de riesgo penal es matemáticamente inevitable" publicado el 30 de diciembre de 2016 »[706].

4.3 Predictice (Francia)

Es un software que ayuda a predecir jurisprudencialmente una decisión basado en algoritmos que permiten pronosticar cómo el juez del caso en concreto va a fallar basado en las sentencias ya existentes.

1. Un juez debe fallar en un caso de despido por mala conducta grave a raíz de los insultos pronunciados por un empleado ebrio contra su superior.
2. El magistrado entra en el motor de búsqueda del software los principales criterios del juicio.
3. el software analiza la jurisprudencia en pocos segundos y proporciona al juez los resultados de procedimientos anteriores similares (más indemnización y daños y perjuicios, si los hubiere).

704 Considerar: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal--sentencing

705 ProPublica es una sala de prensa independiente, sin fines de lucro, que produce periodismo de investigación con fuerza moral. Para exponer los abusos de poder y las traiciones de la confianza pública por parte del gobierno, las empresas y otras instituciones, utilizando la fuerza moral del periodismo de investigación para impulsar la reforma a través de la atención sostenida de la mala conducta. Ver https://www.propublica.org/about/

706 Valorar:https://www.propublica.org/article/bias-in-criminal-risk-scores-is-mathematically-inevitable-researchers-say

4. La decisión final queda a discreción del magistrado

El software: Utiliza millones de decisiones judiciales anónimas. No se utiliza en el derecho penal.

En la gráfica 5 se presenta el funcionamiento del software "Justice prédicitive" a través de un ejemplo con un caso concreto:

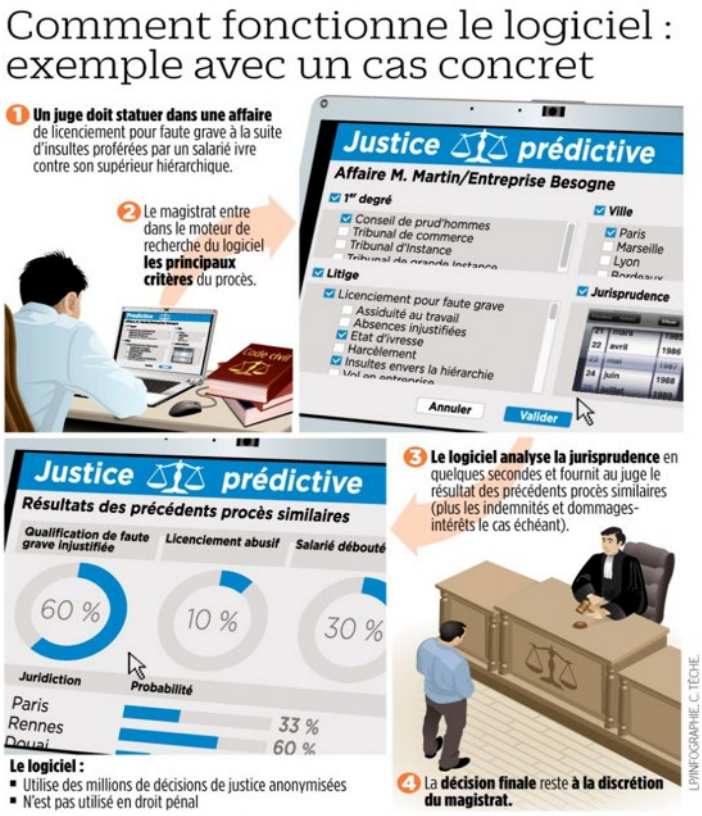


Figura 5. Gráfico de barras de evaluación

Este sistema fue probado por los Tribunales de Apelación de Rennes y Douai además del Colegio de Abogados de Lille. Sus promotores sostienen que este sistema puede "poner fin a una justicia que era impredecible, aleatoria y dispar en todo el país y avanzar hacia algo un poco más lógico, científico o, al menos, un poco más controlable ".[707]

En colaboración con el Ministerio de Justicia, unos diez magistrados de los tribunales de apelación de Douai y Rennes han acordado, a título experimental, utilizarlo durante varios meses. Xavier Ronsin, primer presidente del Tribunal de Apelación de Rennes, emitió su veredicto[708] en octubre 2017, mediante comunicación conjunta con la Cancillería el 9 de octubre de 2017 sobre el uso del programa Predictice.

707 Examinar: https://predictice.com/

708 Observar:https://www.dalloz-actualite.fr/interview/l-utilisation-de-l-outil-predictice--decoit-cour-d-appel-de-rennes

En su análisis, el uso de la herramienta Predictice decepciona al Tribunal de Apelación de Rennes.

El software *Predictice* "sólo está interesado en la parte operativa de una decisión judicial. El algoritmo no sabe cómo leer todas las sutilezas de la motivación, especialmente cuando la decisión es compleja. Sin embargo, por ejemplo, en la apelación, el sistema puede muy bien confirmar parte de la decisión de los primeros jueces y el software no podrá decir qué elementos se confirman y de qué manera. No hay que olvidar que una decisión judicial es una obra intelectual completa y a menudo compleja".

4.4 Siarelis (Colombia)

La Delegatura para los Procedimientos Mercantiles de la Superintendencia de Sociedades cuenta con un programa asistente con bases de Inteligencia Artificial para la Resolución de Litigios Societarios denominado: Siarelis[709].

Dicho software, fue realizado por un equipo multidisciplinario -de juristas expertos en derecho comercial e ingenieros de la Corporación anteriormente mencionada-, inspirado en el programa canadiense de Cyberjustice Laboratory de la Universidad de Montreal (Canadá).

Figura 6. Interfaz del Programa Siarelis

De acuerdo con esta entidad, el proyecto le hace unas interpelaciones al juez y a su grupo; sobre los elementos fácticos del asunto materia de estudio, para inmediatamente después de unos segundos darle su decisión. Pero su función no cesa ahí, pues asimismo expone los fallos más distinguidos para asuntos análogos ya ocurridos.

709 Consultar: https://www.supersociedades.gov.co/delegatura_mercantiles/Paginas/siarelis.aspx

Siarelis, además puede enlazarse con los procedimientos privados de la Supersociedades asistiendo al juez y redactando bosquejos de autos y sentencias. Igualmente, los usuarios de la Delegatura para los Procedimientos Mercantiles conseguirán hacerle preguntas al sistema desde la página web de la institución.

Al consultar este programa nos damos cuenta, que realmente no cuenta con las especific ciones otorgadas por sus creadores, pues se trata de una base de datos primitiva, la cual, al seleccionar el usuario dentro de los 5 ámbitos de estudio del derecho societario su tema de interés, lo que despliega son un número X preguntas para que el usuario responda "si o no" a cada una de las interrogaciones con la finalidad de otorgar una posible resolución que le sirva para justificar su respuesta.

Vemos que este programa, no cumple los presupuestos expuestos por sus desarrolladores, por dos razones principalmente, la primera, es que no se puede considerar un programa basado en inteligencia artificial, pues este olvida mencionar cuales son los algoritmos utilizados para su funcionamiento, y creemos que no los utiliza, pues el método adoptado para ubicar al usuario en razón a su escogencia, es un motor de búsqueda simple sobre un tema muy específico, orientado por el esquema pregunta- respuesta.

La segunda razón es que el software utiliza únicamente las resoluciones expedidas por dicha corporación lo que limita el desarrollo y la eficiencia de la máquina, pues no versa sobre un *corpus iuris complejo*, como generalmente se utilizan en grandes programas de justicia predictiva europeos o americanos para diversificar su posible solución al caso en concreto. Aunque este programa no cumpla con los propósitos enunciados, no debe pensarse, que este avance no es un adelanto para Latinoamérica en temas relacionados con Inteligencia Artificial (IA) y visualización; pues estos ámbitos en la aplicación del Derecho, no han sido desarrollados en la misma magnitud que en Europa, India o Estados Unidos.

4.5 Prometea (Argentina)

Es un sistema producto de la labor de un equipo interdisciplinario del Ministerio Público Fiscal de la Ciudad de Buenos Aires, abanderado por Luis Cevasco y Juan G. Corvalán, en unión con especialistas en Inteligencia Artificial. Su presentación oficial es el 22 de noviembre 2018 según lo anunciado en el site https://innovacionyderecho.com.ar/prometea/.

"Entendemos la inteligencia artificial como la capacidad de analizar datos con mucha velocidad y proponer respuestas. No es la idea de este tipo de programas reemplazar a funcionarios judiciales y abogados. Es fundamental que atrás de Prometea siempre haya una persona de carne y hueso que, con su inteligencia natural,

y no artificial, defina si la propuesta del sistema es adecuada o no", aclararon Cevasco y Corbalán[710]. El programa es gobernado enteramente por IA que funciona de la siguiente manera: "llega un expediente a dictaminar, que no ha sido analizado por ninguna persona. Se carga entonces el número de expediente a la inteligencia artificial Prometea, y en pocos segundos después pasa todo lo que se detalla a continuación. El sistema de IA busca la carátula en la página del Tribunal Superior de Justicia de la Ciudad de Buenos Aires, lo asocia con otro número y luego va a la página del Poder Judicial de la Ciudad Autónoma de Buenos Aires. Busca y lee las sentencias de primera y segunda instancia, luego analiza más de 1400 dictámenes, para finalmente emitir la predicción. En concreto nos dice que detecta un modelo determinado para resolver el expediente y nos ofrece la posibilidad de completar algunos datos para imprimir o enviar a revisar el dictamen con base en ese modelo ."[711]

4.6 SAJ Insights (Brasil)

SAJ Insights es una solución esencial de apoyo a la decisión en todos los ámbitos de la organización en niveles operativo, táctico y estratégico. Además de los análisis descriptivos y de diagnóstico, la solución propone análisis predictivos y prescriptivos con un alto nivel de sofisticación matemática y computacional, presentando un escenario actual confiable y tendencias para el futuro.

La capa más sofisticada de SAJ Insights se centra en el análisis predictivo y prescriptivo. Con la aplicación de técnicas avanzadas de minería de datos, pudimos crear algoritmos que indican las predicciones con un alto nivel de confianza. Con la aplicación de técnicas avanzadas de minería de datos, pudimos crear algoritmos que indican las predicciones con un alto nivel de confianza.

El análisis prescriptivo representa el elemento humano de la solución, donde los análisis son interpretados y devueltos a la institución en forma de propuestas de mejora de sus procedimientos, formación, nuevas normas y acciones de intervención directa. El análisis prescriptivo representa el elemento humano de la solución, donde los análisis son interpretados y devueltos a la institución en forma de propuestas para mejorar sus procedimientos, capacidades, nuevas regulaciones y acciones de intervención directa.

En la etapa de modelado y análisis Modelado y análisis se utilizarán métodos de aprendizaje supervisados y no supervisados. En algunos casos, el objetivo del análisis será realizar un estudio exploratorio para entender la relación existente en

710 Revisar:http://www.noticiasurbanas.com.ar/noticias/la-justicia-portena-incorporo-a--prometea-una-inteligencia-artificial

711 Verifica ::http://thomsonreuterslatam.com/2017/10/la-primera-inteligencia-artificial-predictiva-al-servicio-de-la-justicia-prometea/

un conjunto de variables. En otros casos, el propósito del análisis será realizar un estudio exploratorio para entender la relación existente en un conjunto de variables. Se desarrollarán algoritmos sofisticados para sugerir soluciones a los tomadores de decisiones (magistrados, fiscales, promotores).

4.7 Convex Legal Analytics, de Softplan (Brasil)

Convex Legal Analytics, de Softplan, Creada y desarrollada por Softplan, empresa líder en transformación digital, analítica e Inteligencia Artificial (IA) para el ecosistema de la justicia, Convex Legal Analytics es el resultado de años de experiencia y conocimiento especializado de la justicia brasileña.

Convex Legal Analytics reúne en una sola plataforma una visión completa y detallada de todos los procesos legales, históricos y en curso de una organización, con un análisis diagnóstico que permite, en otra capa, centrarse en el análisis predictivo y prescriptivo. A partir de estos datos, se construyen escenarios futuros basados en el comportamiento de los procesos en curso.

5. Alcances y Límites de la Justicia Predictiva

En palabras de Antoine Garapon, la justicia predictiva es una "revolución cognitiva", que aporta conocimientos no solo jurídicos sino también desafíos a las formas actuales de justicia, el derecho y su práctica. Se sueña secretamente con un mundo en el que, "las relaciones sociales ya no estén formadas por la política y el derecho, sino por la propia tecnología"[712]. Tecnología que será, portadora de la fantasía de la precisión aritmética de la solución y del fin de la incertidumbre judicial, que daría paso a una especie de zumo ex machina. La actitud a adoptar respecto de la justicia predictiva sería, por tanto, la misma que el que tuvo para fax, teléfono o Internet.

5.1 Los alcances de la justicia predictiva

La justicia predictiva puede tener un impacto real en la toma de decisiones judiciales y proporcionar las probabilidades de éxito de un procedimiento, promoviendo la resolución alternativa de conflictos y aliviando la congestión de los tribunales (Caso posible de Prometea de Argentina). Frente al riesgo de formato de la justicia señalado por los críticos de los algoritmos, el magistrado afirma el sentido común del juez: "La justicia robótica es una fantasía, siempre seguirá siendo humana".

712 *GARAPON, A. « Les enjeux de la Justice prédictive », JCPG, 2017, N°1-2, p. 47.* http://ihej.org/wp-content/uploads/2017/01/Justice_predictive.pdf

Por lo tanto, apoyamos la tesis del profesor Garapon quien entiende que la justicia predictiva ayudará a lograr "un nivel de realidad que antes era inaccesible. No sólo la producción completa se vuelve transparente, sino también el detalle, juez por juez, argumento por argumento, parte por parte. (...). La justicia predictiva también altera la función ordenadora del tiempo porque introduce ab initio, si no la solución, al menos una solución muy probable. (...). La justicia predictiva aumenta el presente".[713]

La justicia predictiva como lo advierte el Sr. Jean-Claude Marin, procurador general de la Corte de Casación "permitiría así desarrollar estrategias jurídicas y judiciales eficaces, determinar la duración probable de un procedimiento o el importe medio de la indemnización, o incluso animar a las personas a evitar recurrir a los tribunales favoreciendo métodos alternativos de resolución de litigios cuyo resultado sería "sin sorpresa", previsible"[714].

Sin embargo, si la justicia predictiva puede responder a una demanda social vinculada a un deseo de previsibilidad de la decisión judicial y, por lo tanto, a una mayor confianza en la institución judicial en sentido amplio, ignora la dimensión humana que a menudo es irreductible a la frialdad de la ecuación matemática.

El considerable aumento del número de decisiones disponibles en el contexto de la aplicación de los artículos 20 y 21 de la Ley de 7 de octubre de 2016 para una república digital en Francia podría, por lo tanto, promover significativamente el desarrollo de aplicaciones y software de justicia predictiva. Dada la enorme cantidad de datos potenciales que se pueden encontrar en la jurisprudencia, esta perspectiva sería tanto científica como socialmente significativa. Una de esas técnicas que podría aplicarse es la técnica conceptual para trabajar con grandes bases de datos descrita anteriormente. En general, en esta técnica se calcula la probabilidad de que cada documento sea relevante para un determinado concepto. Por lo tanto, la técnica podría ser una ayuda tanto en la selección de los casos adecuados como en el procedimiento de codificación de los factores. Esta aplicación es innovadora, pero sobre la base de estudios piloto parece prometedora. El tipo de conocimiento creado de esta manera también puede ser utilizado como insumo en los sistemas legales de apoyo a la toma de decisiones.

5.2 Los límites de la Justicia predictiva

Buscando una objetividad en nuestro análisis de la justicia predictiva haremos referencia a los postulados doctrinales sobre el tema en un primer aparte y luego

713 Antoine GARAPON, op. cit. 10

714 Ver su intervención en el sitio internet de La Corte de Casación francesa que se ha intersado en temas desde hace muchos años y que ha organizado varios coloquios sobre el tema : https://www.courdecassation.fr/publications_26/prises_parole_2039/discours_2202/marin_procureur_7116/justice_predictive_38599.html

citando los autores de los proyectos así como la evaluación de los usuarios de los software de justicia predictiva.

5.2.1 Límites según los postulados doctrinales

En el reporte sobre el Open Data en Francia en 2017 p. 24 precisa que "el término "predictivo", frecuentemente utilizado en referencia al inglés, puede efectivamente ser discutido: los tratamientos algorítmicos a los que se refiere determinan las probabilidades del resultado de una controversia más de lo que predicen el resultado del caso, e incluso más, siempre que se cumplan ciertas condiciones. La noción de "previsibilidad" podría sustituirse ventajosamente por la de "previsibilidad" o "probabilidad", que describe con mayor precisión los resultados producidos por estos tratamientos. En cualquier caso, la eficaci de estas herramientas depende de la cantidad de datos disponibles. Cuanto más importante sea esto último, mejor será la calidad de las previsiones propuestas." [715]

Bruno Dondero, profesor de la Facultad de Derecho de la Sorbona, se muestra cauteloso. "Hay tantas variables en una decisión... No estoy seguro de que estos programas puedan tenerlos en cuenta todos".

5.2.2 Límites de algunos de los proyectos de justicia predictiva existentes

En el caso del sistema de "Predictive" de Francia, que fue evaluado por 10 magistrados del Tribunal de Apelación de Rennes, Xavier Ronsin, primer presidente del Tribunal de Apelación de Rennes al preguntarle sobre ¿Qué futuro para la justicia predictiva? ha respondido : "Todavía estamos lejos de la fantasía de la "*justicia de los botones*". El resultado de este experimento permite afirmar que el papel consultivo del abogado es insustituible y que el del juez que decide un caso concreto es igualmente insustituible. La justicia predictiva permitiría, antes de un juicio, dar una idea de las desviaciones de la indemnización media concedida. Pero la inteligencia artificial tendrá que basarse en datos abiertos y, por lo tanto, resolver los problemas de anonimato que la acompañan y que pueden impedir que estos productos se conviertan en realidad."

Respecto de los temas para los que es y será utilizado Prometea de Argentina, Corvalán advirtió: "*Prometea no va a trabajar sobre expedientes complejos, porque no va a tener con qué comparar, sino que su tarea es predecir sobre expedientes donde la Justicia ya tiene algo dicho. De esta manera, permite que la persona pueda destinar su tiempo a los casos complejos y*

715 Ver *"l'Open data des décisions de justice. Mission d'étude et de préfigurattion sur l'ouverture du public des décisions de justice"* mayo 2017. pag. 24

evitar que se transforme en un autómata que solo controla números de expedientes y errores en algún párrafo"[716].

CONCLUSIONES

Al aclarar que la predicción jurisprudencial no está delineada para computarizar la justicia, debemos mostrar cual es su verdadera función principal; esta consiste únicamente en suministrar un instrumento de asistencia a la decisión para los profesionales del derecho, buscando así una contribución al rendimiento y la transparencia del servicio público de la justicia.

Es trascendental aclarar que esta innovación jurídica, no pretende sustituir al operador legal en su labor de juzgamiento e investigación, sino por el contrario, este instrumento le permitirá perfeccionar su trabajo al emplear un programa que le patrocine comprender mejor los sucesos fácticos y los elementos propios del caso, el cual será consecuencia del análisis de una serie de datos, extraordinariamente superlativo a la compilación y procesamiento de datos realizado por el cerebro del abogado quien realizará la tarea.

Por lo tanto, la tecnología de justicia predictiva es esencialmente un apoyo para la decisión de los profesionales legales; lo que hace posible ajustar de manera inteligente el asesoramiento y la estrategia al superar el conocimiento práctico e irreparablemente básico del profesional.

Consideramos que es necesario regular el uso de las nuevas herramientas de justicia llamadas "predictivas" y que es indispensable darle un marco jurídico a este tipo de dispositivos. Pensamos que se debe regular sobre estos puntos de la justicia predictiva:

- la promulgación de una obligación de transparencia de los algoritmos;
- la aplicación de mecanismos de control fl xibles por parte de las autoridades públicas; y
- la adopción de un sistema de certificación de la calidad por un organismo independiente.

Para concluir pensamos como lo afirma Jean-Marc Sauvé, vice-presidente del consejo de estado de Francia "La justicia predictiva se acerca rápidamente, pero hay que reconocer que todavía no es plenamente operativa y segura. Pero las cosas podrían cambiar rápidamente. Por lo tanto, es ahora cuando debemos refl xionar sobre las oportunidades y los riesgos implicados, así como sobre las condiciones imperativas para su desarrollo"[717].

716 Mirar:http://www.noticiasurbanas.com.ar/noticias/la-justicia-portena-incorporo-a-prometea--una-inteligencia-artificial

717 Intervención de Jean-Marc Sauvé, vice-présidente del Consejo de Estado. Coloquio organizado

BIBLIOGRAFÍA

BARBIN, E., & MAREC, Y. (1987). Les recherches sur la probabilité des jugements de Simon-Denis Poisson. *Histoire & Mesure*, *2*(2), 39-58. https://doi.org/10.3406/hism.1987.1311

BARRAUD, B. (2017). Un algorithme capable de prédire les décisions des juges: vers une robotisation de la justice? *Les Cahiers de la justice*, (1), 121–139.

BARTHE, E. (2017). L'intelligence artificielle et le droit. *I2D–Information, données & documents*, *54*(2), 23–24.

BONNET, J., & TÜRK, P. (2017). Le numérique: un défi pour le droit constitutionnel. *Les Nouveaux Cahiers du Conseil constitutionnel*, (4), 13–24.

FREZAL, S. (2017). Outils prédictifs: contresens et dérives. *Esprit*, (2), 28–32.

GARAPON, A. « Les *enjeux de la Justice prédictive », JCPG, 2017, N°1-2, p. 47*. http://ihej.org/wp-content/uploads/2017/01/Justice_predictive.pdf

GARAPON, A., & LASSÈGUE, J. (2018). *Justice digitale: révolution graphique et rupture anthropologique*. Presses Universitaires de France.

Guide de la Justice Prédictive (1).pdf. (s. d.).

KORT, F. (1957). Predicting Supreme Court Decisions Mathematically: A Quantitative Analysis of the "Right to Counsel" Cases. *The American Political Science Review, 51*(1), 1-12. doi:10.2307/1951767

LI, JIAJING, GUOYING ZHANG, LONGXUE YU, ET TAO MENG. (2018) « Research and Design on Cognitive Computing Framework for Predicting Judicial Decisions ». *Journal of Signal Processing Systems*, 10 décembre 2018. https://doi.org/10.1007/s11265-018-1429-9

LAWLOR, R. (1963). What Computers Can Do: Analysis and Prediction of Judicial Decisions. *American Bar Association Journal, 49*(4), 337-344. Retrieved from http://www.jstor.org/stable/25722338

NAGEL, S. *Using simple calculations to predict judicial decisions*, American Behavioral

con motivo del bicentenario del Colegio de Abogados en el Consejo de Estado y el Tribunal de Casación "Justicia predictiva" el 12 de febrero de 2018. http://www.conseil-etat.fr/content/download/126837/1283810/version/1/file/2018-02-12_Justice%20pr%C3%A9dictive.pd

Scientist , Décembre 1960, n° 4(4), p. 24-28

NGOMPÉ, G. T., HARISPE, S., ZAMBRANO, G., MONTMAIN, J., & MUSSARD, S. (2017). Reconnaissance de sections et d'entités dans les décisions de justice: application des modèles probabilistes hmm et crf. In *Extraction et Gestion des Connaissances-EGC 2017*.

open_data_rapport.pdf. (s. d.).

ROUVIÈRE, Frédéric. (2017). La justice prédictive, version moderne de la boule de cristal. *RTD Civ., 2017, p. 527*.

SAYN, I. (2017). Les états généraux de la recherche sur le droit et la justice. In *Les* États *généraux de la recherche sur le droit et la justice*.

SAYN, I. (2018). Connaître la production des juridictions ou predire les decisions de justice?

SAYN, I. (s. d.). Les états généraux de la recherche sur le droit et la justice, 6.

VÉTOIS, J., & LISCOUËT, M. (2018). Vivre dans un monde sous algorithmes. *Terminal*.

ONTOLOGÍAS JURÍDICAS: TECNOLOGÍAS PARA LA REUTILIZACIÓN Y LA INTEROPERABILIDAD ENTRE FUENTES HETEROGÉNEAS DE CONOCIMIENTO DEL ÁMBITO JURÍDICO

Eje temático: Jurimetria e Justiça Preditiva

Legal Ontologies: technologies to support reuse and interoperability between heterogeneous sources of legal knowledge

Autores:
Yarina Amoroso Fernández
Universidad de las Ciencias Informáticas. La Habana, Cuba, yarina@uci.cu

Eliober Cleger Despaigne
Universidad de las Ciencias Informáticas. La Habana, Cuba, ecleger@uci.cu

Ayrat Faridovich Hasyanov
Universidad Federal de Kazán, República Tartaristán, Federación Rusa, ak@it.kfu.ru

Carlos Rafael Rodríguez
Universidad de las Ciencias Informáticas. La Habana, Cuba, crodriguezr@uci.cu

RESUMEN
Aunque las ontologías legales son todavía jóvenes respecto a las ontologías en sí mismas, se pueden referenciar más de 30 años de evolución en el campo de la ingeniería ontológica. Teniendo en cuenta la variedad de criterios acerca de las ontologías jurídicas, en el presente trabajo se realiza una actualización del estado del arte con énfasis en la contribución de las ontologías jurídicas, la reutilización del conocimiento compartido en el dominio jurídico, así como a la interoperabilidad entre fuentes heterogéneas de las aplicaciones desarrolladas en el marco de la informática jurídica. Se caracterizan las ontologías jurídicas, y se enumeran ejemplos que contribuyen al reúso y la interoperabilidad. Por último, se establece la idea de crear una ontología o conjunto de ontologías que posibiliten la interoperabilidad entre las fuentes de datos de la Fiscalía General de la República y Los Tribunales Populares Cubanos.

Palabras claves: Ontología, ontología jurídica, reutilización, interoperabilidad

ABSTRACT
Although legal ontologies are still young compared to ontologies themselves, more than 30 years of evolution in the field of ontological engineering can be referenced. Considering the diversity of criteria regarding legal ontologies, this paper updates the state of the art with emphasis on the contribution of legal ontologies in terms of shared knowledge reuse in the legal domain, as well as the interoperability between heterogeneous sources of applications developed within the scope of legal informatics. Legal ontologies are also characterized, and some examples which contribute to reuse and interoperability are listed. Finally, it is stated the idea of creating an ontology or set of ontologies that enable interoperability between the data sources of the Attorney General's Office and the Cuban Popular Courts.

Keywords: *Ontology, legal ontology, reuse, interoperability*

I. INTRODUCCIÓN

Desde principios de los años 90, las ontologías se han convertido en un tema de investigación de gran interés para varias comunidades de científicos de la Inteligencia Artificial, incluyendo la ingeniería del conocimiento, el procesamiento del lenguaje natural y la representación del conocimiento (Studer, Benjamins, & Fensel, 1998, p. 183). En la actualidad, la ontología se presenta al menos en dos modalidades principales: la comprensión filosófic tradicional de la ontología ha sido complementada recientemente por una nueva comprensión basada en la informática y las ciencias de la computación.

La ingeniería ontológica tiene varios orígenes. En el trabajo "A Cognitive Science Perspective on Legal Ontologies" se han identifi ado cinco, y las cinco todavía juegan un papel importante en la ingeniería ontológica. La ontología filosófic se centra en la "realidad"; la ciencia de la información en la terminología sistemática; la inteligencia artificial (IA) en el conocimiento terminológico y la gestión de la información a nivel semántico (Breuker & Hoekstra, 2010, p. 69).

A partir de esta visión general de las raíces de las ontologías, se hace comprensible por qué existen una variedad tan grande de tipos de ontologías, y que hay tan poco acuerdo sobre lo que son o deberían ser las ontologías. En primer lugar, los objetivos difieren considerablemente. Algunos están orientados al razonamiento; la mayoría son para la gestión y recuperación de información, enparticular para aplicaciones Web semántica. En segundo lugar, está la perspectiva de la reutilización. Las ontologías más abstractas y generales (core, superiores o fundacionales) se suponen aplicables a casi cualquier dominio. La ontología filosó ca ha sido a menudo la principal fuente de inspiración (por ejemplo, DOLCE, SUMO). Las ontologías fundacionales capturan algunos grupos de conceptos que son típicos de algún campo de acción, como la medicina o el derecho, lo que las hace reutilizables para las ontologías de dominio de dicho campo. En tercer lugar, existe una amplia gama de formalismos en los que se basan las ontologías (por ejemplo, OWL-DL, Topic Maps, RDFS) hasta el formalismo de intercambio (KIF, CommonLogic), y los lenguajes de especificación

conceptual (UML, CML). Cuarto, las ontologías difieren mucho en los detalles de la representación. Algunas no son más que estructuras de términos de clase y subclase, mientras que otras tienen especificaciones complejas (estructuradas) de propiedades y relaciones (Breuker & Hoekstra, 2010, p. 73).

Esto también explica la amplia tipología de ontologías jurídicas en términos de granularidad, grado de formalidad, metodologías de desarrollo y fuentes de conocimiento para la extracción de conceptos y términos (Casanovas, Sartor, Biasiotti, & Fernández-Barrera, 2010, p. 1). Parafraseando la expresión de Deborah McGuiness para referirse a la madurez del campo de la ingeniería ontológica se puede decir que hoy en día las ontologías jurídicas han alcanzado la mayoría de edad. (McGuinness, 2003). Aunque las ontologías legales son todavía jóvenes respecto a las ontologías en sí mismas, se pueden referenciar más de 30 años de evolución en el campo de la ingeniería ontológica. Teniendo en cuenta la variedad de criterios acerca de las ontologías jurídicas, en el presente trabajo se realiza una actualización del estado del arte con énfasis en la contribución de las ontologías jurídicas la reutilización del conocimiento compartido en el dominio jurídico, así como a la interoperabilidad entre fuentes heterogéneas de las aplicaciones desarrolladas en el marco de la informática jurídica. En la sección Antecedentes de las definiciones de ontología jurídica se realiza un breve análisis cronológico de las diferentes definiciones de ontología transitando hasta la ontología jurídica, asumiendo por último una propia definición del término. En una segunda sección se caracterizan las ontologías jurídicas, y se enumeran ejemplos que contribuyen al reúso y la interoperabilidad. Por último, se establece la idea de crear una ontología o conjunto de ontologías que posibiliten la interoperabilidad entre las fuentes de datos de la Fiscalía General de la República y Los Tribunales Populares Cubanos.

II. MATERIALES Y MÉTODOS

Se realizó una revisión bibliográfica de los antecedentes de las ontologías jurídicas a partir del método histórico lógico y el análisis y la síntesis de la bibliografía recopilada. Ello posibilitó el arribar a las conclusiones, así como encontrar posibles campos de acción en los que aportar al Derecho desde la informática.

1. Antecedentes de las definiciones de ontología jurídica

La ontología filosófic adopta muchas formas, desde la metafísica de Aristóteles hasta la teoría de objetos de Alexius Meinong. El término *"ontología"* fue acuñado en 1613, independientemente, por dos filósof s, Rudolf Göckel (Goclenius), en su

Lexicon philosophicum y Jacob Lorhard (Lorhardus), en su Theatrum philosophicum. Su primera aparición en inglés según lo registrado por la Diaconía Ecuménica aparece en el diccionario de Bailey de 1721, que define la ontología como "un registro de la existencia en abstracto" (Smith & Welty, 2001, p. 3).

McCarthy afirmó ya en 1980 que los desarrolladores de sistemas inteligentes basados en la lógica deben primero "listar todo lo que existe, construyendo una ontología de nuestro mundo". La mayoría de los esfuerzos de la IA en el campo de la lógica se centraron en capturar información sobre el mundo que fuera compatible con la perspectiva del sentido común humano, y estos esfuerzos estuvieron estrechamente relacionados con la investigación sobre el tema del razonamiento de sentido común.

En 1993, el uso del término "ontología" ya estaba bastante extendido en cada uno de estos subcampos de la informática. Aunque a menudo se le atribuye el inicio de su uso en estos campos, la contribución de Tom Gruber en 1993 fue en realidad la de hacer el primer intento de definición creíble del término. Pero su definición, *"una ontología es una especificación de una conceptualización"*, dejó espacio para demasiadas interpretaciones, y a pesar de un intento de clarificar y formalizar aún más la definición de Guarino, continuaron proliferando nuevos significados del término "ontología". Welty, Lehmann, Gruninger y Uschold reportaron en 1999 sobre un amplio espectro de artefactos de información (catálogo, conjunto de archivos de texto, glosario, tesauro, colección de taxonomías, conjunto de restricciones de lógica general) que en algún momento habían sido clasificados como ontologías (Smith & elty, 2001, pp. 4–6).

Durante este período, también vale la pena destacar la definición de Rudi Studer y otros que consideran que una ontología es *"una especificación formal y explícita de una conceptualización compartida"* (Studer et al., 1998, p. 184). Se puede apreciar que en esta definic ón los autores incorporan los términos "formal, explícito y compartido", haciendo una distinción en su definición con respecto a la dada por om Gruber.

En Cuba la Dra. Marta I. Blaquier Ascaño en su trabajo "OnProc: Una Ontología para el Proceso Jurídico" plantea que *"una ontología es una descripción formal explícita de conceptos en un dominio de discurso"* - las clases - las propiedades de cada concepto que describen las funcionalidades y los atributos del concepto - los slots, algunas veces llamados roles o propiedades - y las restricciones sobre los slots - las facetas, algunas veces llamadas restricciones sobre los roles.

Kevin D. Ashley definió el término "ontología" como *"una especificación explícita, formal y general de una conceptualización de las propiedades de los objetos y las relaciones entre ellos en un dominio determinado"*. (Ashley, 2010, p. 99)

Las ontologías jurídicas, si bien son el resultado de los nuevos desarrollos de las TICs y de la necesidad de introducir el conocimiento jurídico en la Web Semántica, haciéndola accesible y utilizable, están relacionadas con algunas preocupaciones tradicionales de los abogados y académicos del derecho. Por un lado, los lenguajes y

métodos de la ingeniería ontológica proporcionan una nueva forma de expresar ideas que tradicionalmente han formado parte del pensamiento jurídico (la idea de que los conceptos jurídicos tienen una estructura y están vinculados entre sí) y, por otro lado, permiten una reevaluación crítica del pensamiento jurídico y su incorporación en diferentes prácticas jurídicas.

El debate en la investigación ontológica sobre el objeto de las ontologías y su relación con el conocimiento científico y de sentido común, ha sido amplio. Se han propuesto ontologías jurídicas como *"modelos conceptuales para las más diversas aplicaciones jurídicas, como la recuperación de información, los marcos de interoperabilidad y el planteamiento de inferencias, entre otras"*. (Casanovas et al., 2010, p. 1)

Teóricamente, las *ontologías legales son esenciales para representar, procesar y recuperar la información legal, y pueden mejorar la web legal semántica*. Existen varios enfoques en la aplicación de la ontología jurídica, como el modelado de documentos, las perspectivas lingüísticas, la recuperación de información (RI), el aspecto computacional, el razonamiento basado en casos y el razonamiento jurídico. (Thammaboosadee, Kiattisin, Darakorn, & Watanapa, 2017, p. 2)

Valentina Leone y otros aportan una definición similar: *Las ontologías jurídicas proporcionan una representación estructurada de los conceptos jurídicos y sus interconexiones*. Estas ontologías son entonces explotadas para apoyar la extracción de información y la respuesta a consultas en el ámbito legal. (Leone, Caro, & Villata, 2018)

Teniendo en cuenta los puntos de vista expuestos anteriormente, la *"ontología jurídica"* en nuestra opinión *es una representación explícita y estructurada de conceptos jurídicos compartidos, así como de sus interconexiones y restricciones* acorde a modelos de conocimiento que están detrás de los documentos y actos de comunicación concretos en el dominio del Derecho. *Su objetivo fundamental es la formalización del conocimiento del dominio para dar soporte a los diversos enfoques tecnológicos existentes en el campo de la jurisprudencia*.

En las últimas tres décadas, ha habido una tendencia a abarcar también los conceptos de sentido común ocultos detrás de los fundamentos de los conceptos legales, utilizando fundamentalmente ontologías generales/top/upper/foundational/core (Breuker & Hoekstra, 2010, pp. 79–80; Hauser, 2006). Ello ha generado el reto para los investigadores de cómo incluir los datos empíricos de la ciencia cognitiva en el análisis para el desarrollo de dichas ontologías.

2. Rol y uso de las ontologías jurídicas con énfasis en la reutilización y la interoperabilidad

Existen diferentes tipos de ontologías. Si bien todos comparten -hasta cierto punto- la idea subyacente de captar explícitamente el conocimiento estático sobre

algún dominio, también varían considerablemente. La mayoría de los investigadores están de acuerdo en que es útil distinguir entre diferentes niveles de generalidad de las ontologías:

- Las ontologías de dominio capturan el conocimiento válido para un tipo particular de dominio (por ejemplo, electrónico, médico, mecánico y legal).
- Las ontologías genéricas son válidas en varios dominios. Las ontologías genéricas también se conocen como superteorías y como ontologías generales o fundacionales (core).
- Las ontologías de aplicación contienen todo el conocimiento necesario para modelar un dominio en particular (normalmente una combinación de ontologías de dominio y de método).
- Las ontologías representativas no se comprometen con ningún dominio en particular. Estas ontologías proporcionan entidades de representación sin indicar lo que debería estar representado. Una ontología representativa bien conocida es la Frame Ontology, que define conceptos como frames, slots y las restricciones sobre los slots que permiten expresar el conocimiento de una manera orientada a objetos o basada en frames.
- Las ontologías de métodos y tareas, modelan el conocimiento dinámico y proporcionan términos específicos para tareas particulares (por ejemplo, "hipótesis" pertenece a la ontología de la tarea de diagnóstico), y términos específicos para PSM (método de solución de problemas por sus siglas en inglés) (por ejemplo, "estado correcto" pertenece a la ontología del método de propuesta y revisión) (Studer et al., 1998, p. 186).

Por su parte Andre Valente propuso cinco usos o roles principales para las ontologías en IA y el Derecho. (Valente, 2005, p. 69)

a) Organización y estructuración la información: ontologías como herramientas para describir objetos o fenómenos en el dominio de interés. La ontología desempeña así el papel de vocabulario, respondiendo a dos preguntas principales: a) ¿qué términos pueden utilizarse? (léxico); y b) ¿qué oraciones *válidas* se pueden expresar (gramática)?

b) Razonamiento y resolución de problemas: ontología como estructura de la base de conocimientos. Presente en los numerosos sistemas expertos y sistemas de toma de decisiones desarrollados en la IA y el Derecho.

c) Indexación y búsqueda semántica: ontología como índice semántico de información, que permite la búsqueda semántica de contenidos. Hay una necesidad clave de organizar y encontrar los documentos u otros artefactos producidos en la actividad jurídica. Las ontologías pueden utilizarse para ir más allá de las palabras clave.

d) Integración e interoperabilidad de la semántica: ontologías para apoyar las aplicaciones en el intercambio electrónico de información. La ontología aquí funciona como un interlenguaje, definiendo un vocabulario (restringido) utilizado en el intercambio de información.

e) Comprensión del dominio: ontologías para proporcionar una visión de lo que es un dominio - tratar de dar sentido a la variedad de conocimientos en ese dominio. La ontología aquí funciona como un mapa que especifica qué tipos de conocimiento pueden ser identificados en el dominio. Conocidas como ontologías generales o fundacionales (core ontologies).

Pompeau Casanovas y otros en su trabajo "Introducción: Teoría y Metodología en Ingeniería de Ontología Jurídica" (Casanovas et al., 2010, p. 1) nos ofrecen una clasificación variada de las ontologías jurídicas que considero integral y ampliamente utilizada por la comunidad científica

- En términos de granularidad (de dominio específico vs. core-general
- Grado de formalidad (altamente axiomatizado vs. lexicales o con orientación al lenguaje).
- metodologías de desarrollo (top-down vs. bottom-up y middle-out)
- fuentes de conocimiento para la extracción de conceptos y términos (fuentes legales oficiales vs. entrevistas con xpertos legales y trabajo etnográfico

La diversidad de esta clasificación se debe al hecho de que las ontologías jurídicas se diferencian de las ontologías en otros campos de la práctica, como la medicina o la ingeniería, en que tienen que abarcar una amplia gama de conceptos (principalmente) de sentido común que forman parte del mundo físico, abstracto, mental y social. Los dominios jurídicos comparten nociones complejas y variadas de normas y responsabilidad, pero además de este "núcleo" legal, un dominio jurídico se refiere a algún mundo de actividades sociales. Este núcleo normativo ha sido tradicionalmente objeto de estudio en la teoría jurídica (Benjamins, Casanovas, Breuker, & Gangemi, 2005, p. 10).

Hasta 2010, se habían completado más de sesenta ontologías jurídicas. Véase la tabla en "Introducción: Teoría y Metodología en Ingeniería en Ontología Jurídica: Experiencias y orientaciones futuras" de Pompeu Casanovas y otros (2010, pp. 5–8), que reproduce la actualización de treinta y tres de ellas por (Breuker, Casanovas, Klein, & Francesconi, 2009, pp. 12–14), basada en la tabla original de André Valente de 2005.

Esta tabla muestra ciertamente la fuerza y dinamismo del dominio. Sin embargo, pocas de estas ontologías han superado la etapa de prototipos avanzados y refinados, incluso escalables y listos para su reutilización. Esto es coherente con las encuestas industriales sobre la Web Semántica cf. (Cardoso, 2007) en las que las aplicaciones

legales son casi invisibles. Tal vez LKIF-core y el amplio uso de ontologías de alto nivel o generales como DOLCE+ y SUMO en el dominio legal son excepciones parciales (Casanovas et al., 2010, p. 4). Por su parte Breuker resalta el uso de LRI–Core y FOLaw esta última suministra un modelo global y extensible dentro del cual puede establecerse correspondencia entre datos pertenecientes a diversos dominios y permitir la integración de estos, formalizando dentro de la ley el conocimiento de sentido común.

En Cuba a nivel de trabajo de diploma en la Universidad de las Ciencias Informáticas en el 2016 se planteó la realización de una ontología para el Código Civil (CC) de Cuba que posibilita la reutilización, interoperabilidad y recuperación del conocimiento representado. OntoLex, resultó ser una ontología cuyo domino concurre en el Código Civil de la República de Cuba con el objetivo de estandarizar la legislación".

Un trabajo de mayor envergadura lo constituye OnProc. El dominio de la ontología OnProc es el proceso jurídico y tiene como propósito ser un instrumento en la automatización de estos procesos y de la recuperación de información sobre los mismos. OnProc tiene un carácter mixto, ha sido concebida como una ontología general para el proceso jurídico y además es dependiente de la legislación, en este caso del Derecho Procesal cubano. En su primera capa OnProc ofrece las categorías: Proceso, Ocurrencia, Rol y Agente.

III. DISCUSIÓN DE LOS RESULTADOS

A partir de la bibliografía consultada queda evidenciada la fertilidad para realizar investigaciones en el campo de la ontología jurídica. Entre los principales retos identificados: (1) Incluir el sentido común asociado a la práctica jurídica entre los conceptos que formarán parte de la ontología. (2): lograr que la ontología o conjunto de ontologías desarrolladas constituyan realmente una estructura que posibilite la reutilización y la interoperabilidad entre fuentes heterogéneas del conocimiento en el dominio jurídico. (3) Elegir un enfoque de desarrollo de la ontología (o la combinación de ellos) que posibilite combinar el conocimiento adquirido a través de la práctica jurídica con la teoría existente. (4) Lograr que los sistemas para el razonamiento basado en casos con base ontológica obtengan la aceptación esperada por sus desarrolladores en la comunidad de juristas, sin intentar sustituir el intelecto necesario para el desarrollo de la actividad jurídica. A partir de estas cuatro tareas, se puede decir que en el ámbito jurídico cubano existen aún grandes posibilidades de aplicar la ingeniería ontológica. A continuación, un ejemplo de ello:

En el sector jurídico cubano la Fiscalía General de la República y Los Tribunales Populares Cubanos manejan documentos llamados actos de resolución de conflictos (sentencias, arbitrajes o mediaciones, etc.) de gran importancia para la labor de abogados, fiscales y jueces. Los decisores en este sector necesitan considerar las relaciones entre los diferentes actos, lo que podría prevenir la violación de los pasos en el proceso judicial, así como la omisión de los actos necesarios para la toma de decisiones. En estas instituciones, no existe un modelo que permita la reutilización del conocimiento del dominio y contribuya a la interoperabilidad entre fuentes heterogéneas de conocimiento. Asimismo, el manejo expedito de los datos asociados a la documentación legal se ha convertido en una necesidad cuyas soluciones aún soportan la introducción de mejoras.

Nuestro objetivo es desarrollar un modelo de grafo de propiedad basado en ontologías jurídicas para la representación de actos de resolución de conflictos, que facilite la reutilización e interoperabilidad entre fuentes heterogéneas de conocimiento en el ámbito jurídico.

IV. CONCLUSIONES

Las investigaciones en ingeniería de ontología jurídica están impulsadas principalmente por la necesidad de desarrollar nuevas aplicaciones informáticas para satisfacer las demandas de los profesionales del derecho y los ciudadanos, en un marco caracterizado por un desarrollo tecnológico acelerado. Por ello a pesar de la diversidad de teorías asociada a la definición del término ontología, existe consenso en que su principal función es lograr un lenguaje (representación estructurada) del conocimiento asociado a determinado dominio entendible tanto por el hombre como por las tecnologías de la IA. Los cuatro retos identificados por los autores del presente trabajo no tienen la intención de ser absolutos, hay espacio en este campo para novedosas soluciones y enfoques. La propuesta realizada requiere de mayor profundización y contraste con las actuales tendencias en el desarrollo de soluciones informáticas basadas en ontologías jurídicas. No obstante, la materialización del tema podría constituir un paso de avance en el aporte de las ciencias informáticas a nuestro desarrollo social.

V. REFERENCIAS BIBLIOGRÁFICAS

Ascaño, M. I. B. OnProc: Una Ontología para el Proceso Jurídico http://www.biblioci encias.cu/gsdl/collect/eventos/import/Onproc_ontologia_proceso_juridico.pdf

Ashley, K. D. (2010). The Case-Based Reasoning Approach: Ontologies for Analogical Legal Argument. In Approaches to Legal Ontologies (Series 1, pp. 99–115). Springer Science & Business Media, Dordrecht. https://doi.org/10.1007/978-94-007-0120-5_6

Benjamins, V. R., Casanovas, P., Breuker, J., & Gangemi, A. (2005). Law and the Semantic Web, an introduction. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (LNCS 3369, pp. 1–17). New York: Springer-Verlag Berlin Heidelberg. https://doi.org/10.1007/978-3-540-32253-5_1

Breuker, J., Casanovas, P., Klein, M. C. A., & Francesconi, E. (2009). The flood, the channels and the dykes: Managing legal information in a globalized and digital world. In Frontiers in Artificial Intelligence and Applications 188 (1) (pp. 3–18). Amsterdam: IOS Press. https://doi.org/10.3233/978-1-58603-942-4-3

Breuker, J., & Hoekstra, R. (2010). A Cognitive Science Perspective on Legal Ontologies. In Approaches to Legal Ontologies, Law, Governance and Technology (Series 1, pp. 69–81). Springer Science & Business Media, Dordrecht. https://doi.org/10.1007/978-94-007-0120-5_4

Cardoso, J. (2007). The Semantic Web Vision: Where Are We? IEEE Intelligent Systems, 22(5), 84–88. https://doi.org/10.1109/mis.2007.4338499

Casanovas, P., Sartor, G., Biasiotti, M. A., & Fernández-Barrera, M. (2010). Introduction: Theory and Methodology in Legal Ontology Engineering: Experiences and Future Directions. In Approaches to Legal Ontologies (Series 1, pp. 1–14). Springer Science & Business Media, Dordrecht. https://doi.org/10.1007/978-94-007-0120-5_1

Hauser, M. D. (2006). Moral Minds: The Nature of Right and Wrong. Harper Perennial. New York: HarperCollins. https://doi.org/10.1007/s11024-007-9080-9

Leone, V., Caro, L. Di, & Villata, S. (2018). Legal ontologies and how to choose them: The investigationt tool. In Proceedings of the ISWC 2018 Posters & Demonstrations, Industry and Blue Sky Ideas Tracks co-located with 17th International Semantic Web Conference. (Vol. 2180). Retrieved from http://ceur-ws.org/Vol-2180/paper-36.pdf

McGuinness, D. L. (2003). Ontologies Come of Age. In Spinning the semantic web: Bringing the world wide web to its full potential. The MIT Press. https://doi.org/10.7551/mitpress/6412.003.0008

Smith, B., & Welty, C. (2001). Ontology: Towards A New Synthesis. In International

Conference on Formal Ontology in Information Systems (FOIS) (pp. 3–9). https://doi.org/10.1145/505168.505201

Studer, R., Benjamins, V. R., & Fensel, D. (1998). Knowledge Engineering: Principles and methods. Data and Knowledge Engineering, 25(1–2), 161–197. https://doi.org/10.1016/S0169-023X(97)00056-6

Thammaboosadee, S., Kiattisin, S., Darakorn, S., & Watanapa, B. (2017). Sentence identification system based on criminal law ontology. International Review of Law, Computers and Technology, 1–15. https://doi.org/10.1080/13600869.2017.1304615

Valente, A. (2005). Types and roles of legal ontologies. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (LNCS 3369, pp. 65–76). New York. https://doi.org/10.1007/978-3-540-32253-5_5

PRESENTACIÓN DEL LIBRO "EL DERECHO DE LAS TIC EN IBEROAMÉRICA"

En la tarde del segundo día del Congreso se realizó el lanzamiento y presentación pública del libro "El Derecho de las TIC en Iberoamérica", una obra colectiva de 1327 páginas en la que se dieron cita por invitación 74 co-autores, profesores y expertos, tanto miembros como no de FIADI, superando incluso los límites de la Federación con aportes extra regionales provenientes de Francia, Italia y Finlandia.

Organizado por la Directiva actual de la Institución bajo la dirección de su Presidente Marcelo Bauzá Reilly, y editado por La Ley Uruguay del Grupo Thomson Reuters, hicieron uso de la palabra Juliana Mayumi O. Ono, Directora de Contenidos y Operaciones Editoriales de Thomson Reuters Brasil, y el propio y citado Presidente de FIADI y Director de la obra.

Señalando los aspectos más importantes, la primera de las nombradas resaltó el trabajo mancomunado de ambas casas editoriales, la uruguaya y la brasileña, para poder arribar al 23º. CIDI con una obra de tamaña enjundia y esmerada calidad de presentación, como la editada y presentada.

Por su parte el Director de la obra refirió a la estructura básica de la misma, consistente en dos partes diferentes que terminan por darle la riqueza final esperada. La primera parte compuesta por 34 capítulos desarrollados a partir de un plan de materias tendiente a la completitud (al estilo de los Manuales), en el tratamiento de las principales áreas del Derecho Informático y la Informática Jurídica. Mientras que la segunda parte se abre en 35 contribuciones especiales, volcadas hacia temas siempre pertinentes a las enunciadas disciplinas, pero si se quiere más específicos y en buena medida librados al interés del autor por desarrollar un análisis focal y concentrado de cierto asunto de su especialidad. El resultado final es una obra de ricas facetas tanto por sus contenidos como por el número y calidad de los autores intervinientes. Donde quedan tratadas las principales cuestiones que enfilan, histórica y sobre todo actualmente, el impacto de lo digital sobre el Derecho. Un esfuerzo de esos que difícilmente puedan encontrarse antecedentes comparativos de altura similar al día actual, cuanto menos en la vasta región hispanoparlante que incluye el espacio brasileño con varios co-autores de este país (algunos que escribieron sus textos en idioma español y otros en idioma portugués).

El presentador culminó su oratoria augurándole a la obra un promisorio futuro de servicio, tanto para la enseñanza en las Universidades de las disciplinas conectadas, como para la Asesoría y la Cultura Jurídica en general, desde el momento que se trata de un Libro cuya lectura y consulta resultarán provechosas, podría caber decir ineludibles, para quienes atienden o asumen los retos jurídicos e informáticos de la sociedad digital.