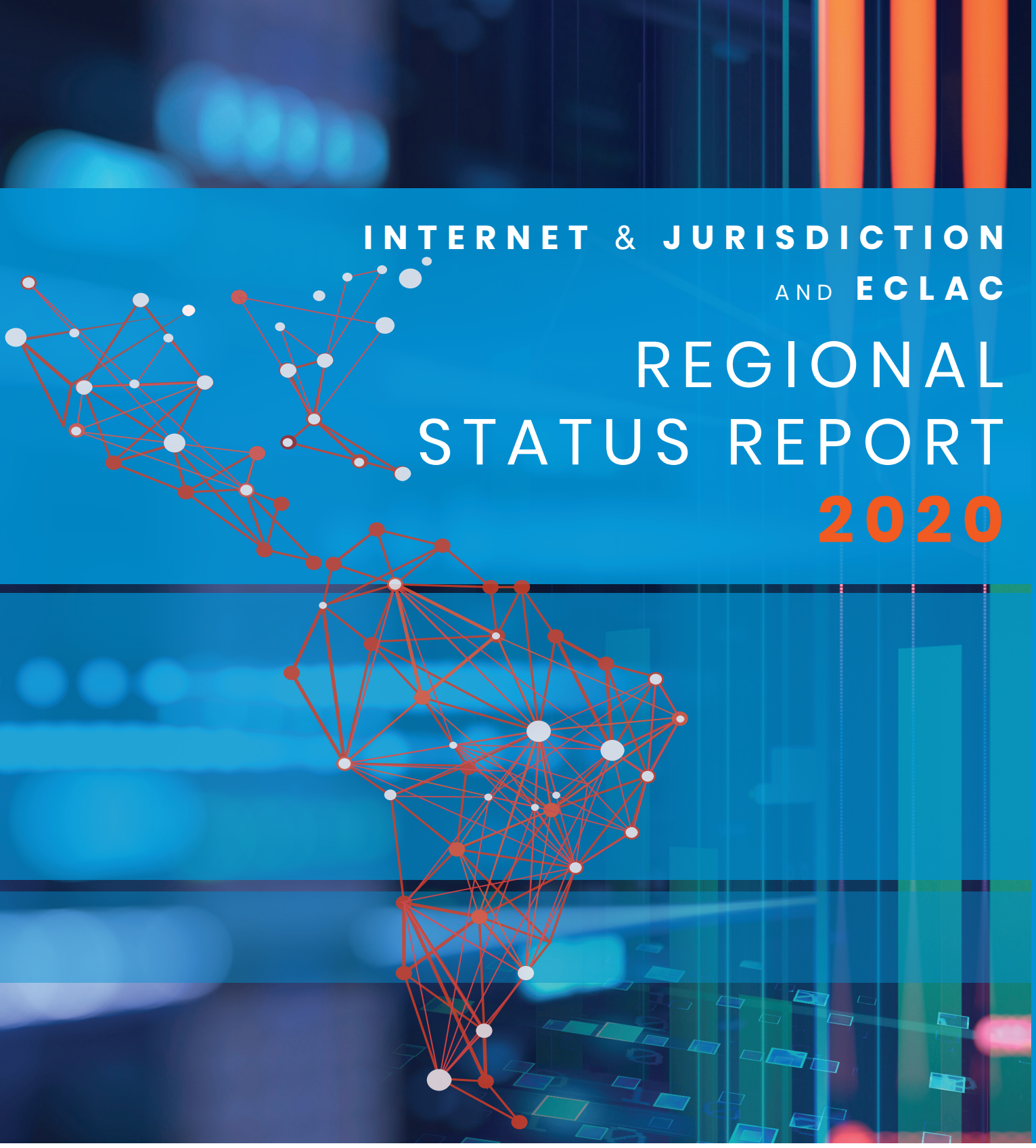


INTERNET & JURISDICTION AND ECLAC

REGIONAL STATUS REPORT 2020

UNITED NATIONS

ECLAC

INTERNET & JURISDICTION POLICY NETWORK

german cooperation

DEUTSCHE ZUSAMMENARBEIT

Thank you for your interest in this ECLAC publication

Please register if you would like to receive information on our editorial products and activities. When you register, you may specify your particular areas of interest and you will gain access to our products in other formats.

Register

UNITED NATIONS

ECLAC

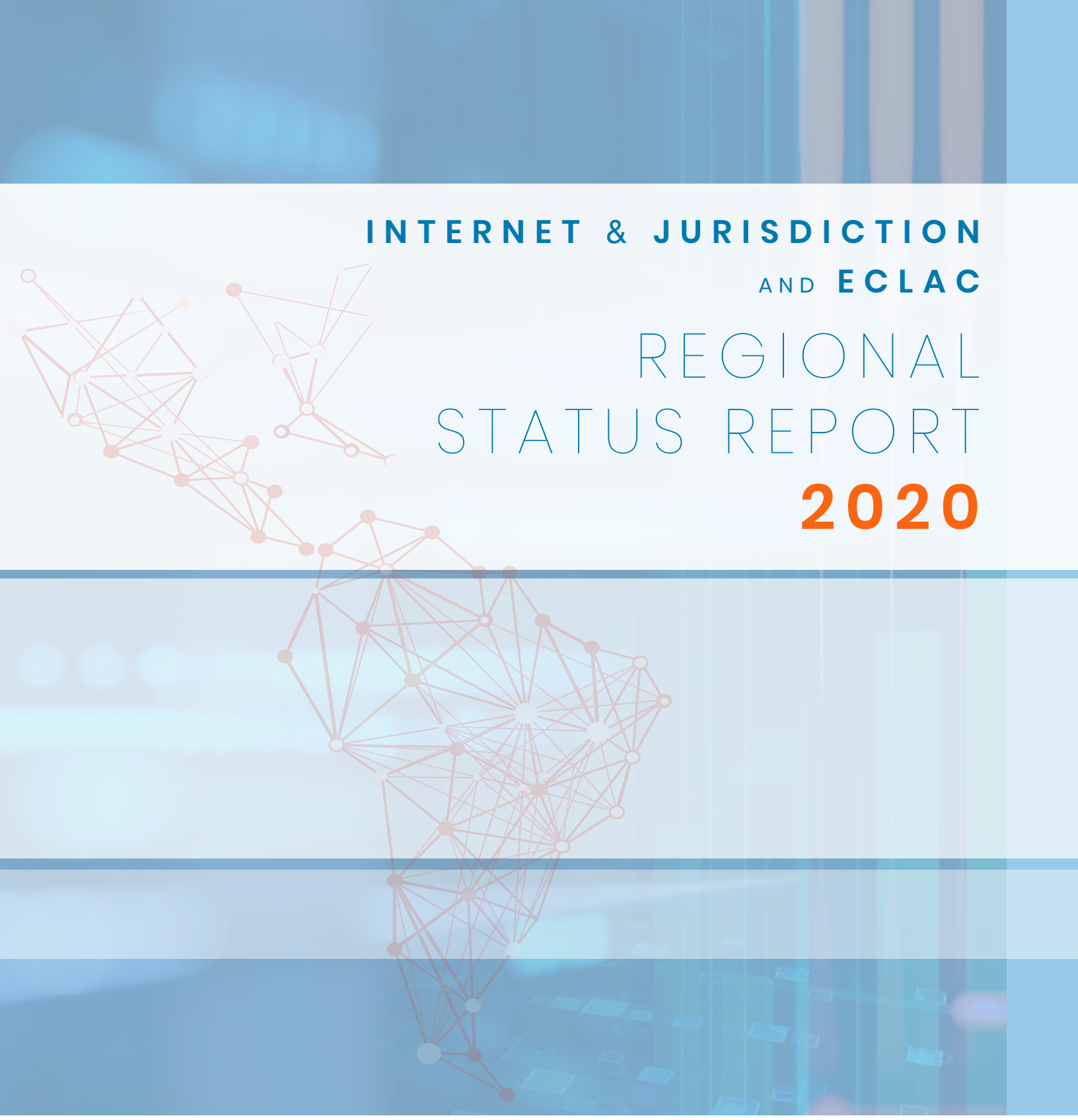
www.cepal.org/en/publications

facebook.com/publicacionesdelacepal

www.cepal.org/apps

INTERNET & JURISDICTION AND ECLAC

REGIONAL STATUS REPORT 2020



UNITED NATIONS

ECLAC

INTERNET & JURISDICTION POLICY NETWORK

german cooperation
DEUTSCHE ZUSAMMENARBEIT

This report was commissioned by the Secretariat of the Internet & Jurisdiction Policy Network (I&JPN) and the United Nations Economic Commission for Latin America and the Caribbean (ECLAC), and was authored by Carlos Affonso Souza.

The report represents the author's best endeavour to map the current ecosystem and trends in Latin America and the Caribbean on the basis of desk research and stakeholder surveys and interviews. The completeness of the information cannot be guaranteed, however, as this report constitutes a first regional baseline with regard to the state of jurisdiction over the Internet.

ECLAC and the I&JPN Secretariat are grateful for the financial and institutional support of the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ), acting on behalf of the German Federal Ministry for Economic Cooperation and Development (BMZ), which enabled this report to be produced.

The views expressed in this document are those of the authors and do not necessarily reflect the views of the I&JPN Secretariat, ECLAC, I&JPN stakeholders or the financial supporters of the report.

United Nations publication
LC/TS.2020/141
Distribution: L

Printed at United Nations, Santiago
S.19-01092

Internet & Jurisdiction Policy Network publication

This publication should be cited as: Economic Commission for Latin America and the Caribbean (ECLAC)/Internet & Jurisdiction Policy Network (I&JPN), *Internet & Jurisdiction and ECLAC Regional Status Report* 2020 (LC/TS.2020/141), Santiago, 2020.

CONTENTS

ACKNOWLEDGEMENTS

This report was commissioned by the Secretariat of the Internet & Jurisdiction Policy Network (I&JPN) and the Economic Commission for Latin America and the Caribbean (ECLAC).

The production of this report was made possible by financial support provided by the German Agency for International Cooperation (GIZ), acting on behalf of the German Federal Ministry for Economic Cooperation and Development (BMZ), and by ECLAC.

AUTHORSHIP TEAM:

AUTHOR:

Professor Carlos Affonso de Souza
Rio de Janeiro State University (UERJ)
Director
Institute for Technology & Society (ITS Rio)

RESEARCH ASSISTANCE:

Christian Perrone
Ph.D. candidate - Fulbright scholar
Senior Researcher
Institute for Technology & Society (ITS Rio)

Giovana Carneiro
Junior Researcher
Institute for Technology & Society (ITS Rio)

PROJECT COORDINATION (I&JPN):

Martin Hullin
Director of Operations and Knowledge Partnerships
Secretariat of the Internet & Jurisdiction Policy Network

PROJECT TEAM (I&JPN):

Bertrand de La Chapelle
Executive Director
Secretariat of the Internet & Jurisdiction Policy Network

Paul Fehlinger
Deputy Executive Director
Secretariat of the Internet & Jurisdiction Policy Network

PROJECT TEAM (ECLAC):

Edwin Fernando Rojas
Division of Production, Productivity and Management
Economic Commission for Latin America and the Caribbean

Alexis Arancibia
Consultant
Economic Commission for Latin America and the Caribbean

Alonso Zúñiga Irigoin
Consultant
Economic Commission for Latin America and the Caribbean

PRODUCTION:

Economic Commission for Latin America and the Caribbean

Secretariat of the Internet & Jurisdiction Policy Network

EDITING:

Sophie Tomlinson
Manager, Communications and Outreach
Secretariat of the Internet & Jurisdiction Policy Network

DESIGN AND LAYOUT:

Economic Commission for Latin America and the Caribbean

We greatly appreciate the time and contributions of all survey respondents and interviewees. Without their valuable insights, this report could not have been produced.

Mauricio Agudelo
Coordinator of the Digital Agenda
Development Bank of Latin America (CAF)
Colombia

Pablo Bello
Head of Private Messaging Policy, LATAM
Facebook
Brazil

Daniel Cavalcanti
Coordinator
Ministry of Science, Technology, Innovations and Communications
Secretariat of Digital Government
Brazil

María Angélica Chinchilla Medina
Director of Telecommunications Evolution and Market
Ministry of Science, Technology and Telecommunications (MICITT)
Costa Rica

José Clastornik
President of the Fundación para la Innovación Digital de Uruguay
Former Executive Director
Agency for the Development of Electronic Government and the Information and Knowledge Society (AGESIC)
Uruguay

Pelayo Covarrubias
President
País Digital Foundation
Chile

Agustina Del Campo
Director
Centre for Studies on Freedom of Expression and Access to Information (CELE)
Argentina

César Díaz
Engineer
Uruguay

Lester García
Head of Connectivity Policy LATAM
Facebook
Mexico

Raúl Echeberría
Executive Director
Latin American Internet Association (ALAI)
Uruguay

Alexandre Fernandes Barbosa
Manager
Regional Centre of Studies for the Development of the Information Society (CETIC.br)
Brazilian Network Information Centre (NIC.br)
Brazil

Matías Fernández Díaz
Senior Manager (Public Affairs)
Mercado Libre
Argentina

Gustavo Gómez
Executive Director
Latin American Observatory on Regulation, Media and Convergence (OBSERVACOM)
Uruguay

José Juan Haro
Chief Wholesale and Public Affairs Officer
Telefónica
Spain

Héctor Huici
Former Secretary
Information and Communication Technologies Secretariat
Argentina

Erick Iriarte
Partner
Iriarte & Asociados (IALaw)
Peru

Juan Jung
Former Coordinator
Latin American Telecommunications Research Centre (cet.la)
Uruguay

Yacine Khelladi
Regional Coordinator, Latin America and the Caribbean
Alliance for Affordable Internet (A4AI)
Dominican Republic

Juan Carlos Lara
Content Director
Derechos Digitales
Chile

Carolina Limbatto
Head of Americas
Cullen International
Belgium

Omar de León Boccia
Executive Director
Teleconsult
Uruguay

Lilia Liu
Executive Director
Lilia Liu & Associates (LLASO)
Panama

Maryleana Méndez
Secretary General
Inter-American Association of Telecommunication Enterprises (ASIET)
Uruguay

Oscar Messano
President
High Technology Training Centre for Latin America and the Caribbean (CCATLAT)
Argentina

César Moliné Rodríguez
Director of Cybersecurity, Electronic Commerce and Digital Signature
Dominican Telecommunications Institute (INDOTEL)
Dominican Republic

Gonzalo Navarro
Executive Director
Latin American Internet Association (ALAI)
Uruguay

Rodrigo de la Parra
Vice President, Stakeholder Engagement & Managing Director - Latin America & Caribbean
Internet Corporation for Assigned Names and Numbers (ICANN)
Mexico

Sissi de la Peña
Digital Commerce and International Organizations Manager
Latin American Internet Association (ALAI)
Mexico

Eric Ramírez
Director
Secretariat of Innovation, Government of El Salvador
El Salvador

Rodrigo Ramírez Pino
President
Chilean Chamber of Digital Infrastructure (IDICAM)
Chile

María Eunises Rivas Robleto
Executive Secretary
Nicaraguan Council of Science and Technology (CONICYT)
Nicaragua

Beatriz Rodríguez
President
Internet Society – Uruguay Chapter (ISOCUY)
Uruguay

Jorge Romo
National Digital Strategy Coordination Office (CEDN)
Office of the President of the Republic
Mexico

Eduardo Salido
Public Affairs and Policy Manager for Latin America
Telefónica
Spain

Andrés Sastre
Regional Director for the Southern Cone
Inter-American Association of Telecommunication Enterprises (ASIET)
Uruguay

Thiago Luís Sombra
Partner
Mattos Filho, Veiga Filho, Marrey Jr. e Quiroga Advogados
Brazil

Paloma Szerman
Senior Regulatory Policy Manager
GSMA Latin America
Argentina

Fernanda Teixeira Souza Domingos
Federal Prosecutor
Federal Prosecution Service
Brazil

Berioska Torres
Under-Secretary
Office of the Under-Secretary for the Information Society and e-Government
Ministry of Telecommunications and the Information Society (MINTEL)
Ecuador

Paloma Villa Mateos
Public Policy Manager
Telefónica
Spain

Juan Manuel Wilches Durán
Telecommunications and Digital Transformation Consultant
Colombia

Cristina Zubillaga
Senior Consultant
Former Deputy Executive Director
Agency for the Development of Electronic Government and the Information and Knowledge Society (AGESIC)
Uruguay

PREFACE

ALICIA BÁRCENA
Executive Secretary
Economic Commission for Latin America and the Caribbean (ECLAC)

As Latin America and the Caribbean battles the most severe health and humanitarian crisis in a century, the inequalities that pervade the region have been laid bare. Just as the coronavirus disease (COVID-19) pandemic has revealed the consequences of unequal access to health care, a high-quality education system and economic opportunities, the stark digital divide has also become more evident. Over 60% of individuals in the region have an Internet connection, but there are marked inequalities in connectivity by income, rural and urban areas and ethnicity, among other factors. In some countries, the connectivity gap between the richest and poorest quintiles is as wide as 60 percentage points. To weather the crisis and build back better, it is essential that steps be taken to move towards universal connectivity and provide greater access to digital tools. This will only be possible with strong normative frameworks.

The COVID-19 pandemic amplifies the need for greater coordination to ensure policy coherence among the countries of the region on issues such as cross-border data transfers, regulatory harmonization, privacy and data security. The deployment of technologies that require the rapid transfer of large amounts of new data among numerous actors to control the spread of COVID-19 calls for common standards and legal interoperability. The increased importance of remote working and distance learning initiatives requires secure connectivity solutions to ensure no one is left behind.

As the technical secretariat of the Ministerial Conference on the Information Society in Latin America and the Caribbean, the Economic Commission for Latin America and the Caribbean (ECLAC) has been working in coordination with government stakeholders and observer representatives from academia, industry, the technical community and multilateral organizations to prepare a regional digital agenda, prioritizing issues related to the digital development of our region for over 15 years. As we develop the 2020–2022 digital agenda for Latin America and the Caribbean (eLAC2022), one of the highest priority initiatives is the creation of a regional digital market. The regional digital market seeks to strengthen the digital integration of Latin America and the Caribbean, taking advantage of the geographical proximity and similar interests of the region's countries.

This pioneering report is the first comprehensive mapping of its kind in Latin America and the Caribbean and provides a robust evidence base that will support the development of eLAC2022. The report identifies and addresses key trends in the rapidly growing regional digital policy field and charts the path to be followed. This vital contribution to the policy debate will shed light on some of the challenges we face and opportunities we can seize to bring us closer to a more integrated and harmonized regional digital market.

PRESENTATION

Bertrand de La Chapelle
Executive Director
Paul Fehlinger
Deputy Executive Director
Secretariat of the Internet & Jurisdiction Policy Network

The digital transformation of economies, governments and societies in Latin America and the Caribbean is sharply accelerating in 2020, further catalysed by the COVID-19 pandemic. With the growth of cross-border services and data flows, the need for more legal interoperability and coordination rises. Uncoordinated action of a wide range of actors and initiatives risk hampering the digitalization. To provide an indispensable mapping and analysis of the regional ecosystem in Latin America and the Caribbean, the Internet & Jurisdiction Policy Network in coordination with the United Nations Economic Commission for Latin America and the Caribbean (ECLAC) created this first *Internet & Jurisdiction and ECLAC Regional Status Report 2020*. It is a regional edition of the groundbreaking *Internet & Jurisdiction Global Status Report 2019*. The Report builds on the unique methodology of the Internet & Jurisdiction Policy Network to mutualize knowledge of key regional stakeholders from states, companies, technical operators, international organizations, academia and civil society through interviews and surveys and make their voices heard.

A key message of the Regional Status Report is that more policy coherence is needed to build a thriving and integrated regional digital ecosystem. By laying out key trends with regard to the handling of legal challenges on the continent, the Report is intended to allow policymakers and shapers to enhance their understanding of the myriad of fast-paced developments to enable evidence-based policy innovation and advance legal interoperability in cyberspace. Bridging the fields of the digital economy, security and human rights, the Report sheds light on the changing technological and regulatory landscape in the region. It provides the most up-to-date overview of the plurality of national and private policy initiatives, as well as jurisprudence that sets the rules for online interactions, digital services and data flows. The Report reveals the latest trends on key topics ranging from start-ups, artificial intelligence, the Internet of Things, expression and privacy to the role of intermediaries. Moreover, it showcases the geographic extension and impact of national measures from the region, as well as the influence of public and private regulatory measures from outside of it.

This important mapping for policymakers and decision makers, was created thanks to the strong partnership between the Internet & Jurisdiction Policy Network and ECLAC under the five-year Memorandum of Understanding signed in 2019. The Regional Status Report is an important milestone in the efforts of the Internet & Jurisdiction Policy Network to map the global cross-border legal ecosystem to help develop better policies and solutions. We therefore hope that it can contribute to fostering coordination on cross-border legal challenges and digital cooperation in Latin America and the Caribbean, and beyond.

METHOD

The method chosen to prepare this report was shaped by the need to arrive at a comprehensive understanding of a highly complex and dynamic ecosystem, one that comprises multiple actors, initiatives and trends across the policy silos of the digital economy, human rights and security.

This prompted the adoption of a flexible, qualitative research design that allowed the research questions to be explored in depth. By using the multifaceted research method first adopted for the production of the pioneering *Internet & Jurisdiction Global Status Report 2019*, the present report was able to incorporate an unprecedented and innovative large-scale collaborative contribution and review process in the Latin America and Caribbean region.

This process leveraged the combined expertise of the key stakeholders engaged in the Internet & Jurisdiction Policy Network and ECLAC and beyond through semi-structured interviews, peer review feedback and data collection procedures, combined with detailed and extensive desk research.

The desk research

The desk research employed conventional legal research methods and consisted primarily of a comprehensive study and analysis of relevant case law, legislation and other regulatory initiatives, and the literature, including books, journal articles, published conference papers and industry publications. This was supplemented with a detailed study of a variety of valuable reports and other materials from a range of bodies over recent years.

The desk research benefited greatly from publications produced by ECLAC and the Internet & Jurisdiction Policy Network's wide-ranging collection of relevant material available in the I&J Retrospect Database. This open access database is the flagship information resource of the Internet & Jurisdiction Policy Network, documenting policy developments, judicial decisions, international agreements and other material reflecting jurisdictional tensions on the cross-border Internet. This important collection provided up-to-date insights into current major trends, attitudes, developments and initiatives. The material in the Retrospect Database also provided important insights into current legal and technical approaches to solutions, as well as into what this report calls "overarching trends".

The stakeholder survey

The first method for obtaining stakeholder input was the utilization of an online survey made up of 15 questions on a variety of topics relevant to the research questions. In considering how best to gather survey data to inform the research questions, great care was taken to design questions that could be answered by any of the relevant stakeholders. This ensured that all survey participants were exposed to the same set of questions. The Internet & Jurisdiction Policy Network Secretariat and ECLAC identified survey participants representing all of I&JPN's stakeholder groups, namely academia, civil society, governments, international organizations, Internet platforms and the technical community, and participants were specifically selected to ensure geographical diversity within the Latin America and Caribbean region. Furthermore, the selection of the survey participants was purposive, in that they were specifically targeted in consideration of their considerable expertise and knowledge. In total, input was received from over 40 survey participants during a period running from the fourth quarter of 2019 to the second quarter of 2020. Participants provided their views in a personal capacity rather than as representatives of any specific organization, and all the input from the surveys has been used without attribution. The expert input gleaned from the survey was invaluable. In addition to highlighting major topical trends, approaches to solutions, overarching trends and widely held concerns in the ecosystem, the survey results helped provide both context and a more nuanced understanding of the operating environments facing civil society, governments, international organizations, Internet platforms and the technical community. Survey results are used throughout the report to show, in figures, the concerns and attitudes of the stakeholder ecosystem surveyed. In addition, the comments of the stakeholders surveyed have been used to highlight particularly important arguments, observations and concerns.

Stakeholder interviews

Semi-structured interviews were held across a broad range of stakeholders to complement the insights gained from the survey responses and desk research. As with the surveys, great care was taken to ensure inclusiveness and diversity, with a geographically diverse array of stakeholders

representing academia, civil society, governments, international organizations, Internet platforms and the technical community being selected for interview. These stakeholders were identified from both within and beyond the Internet & Jurisdiction Policy Network and ECLAC.

Each interview lasted over 30 minutes on average. The interviews were conducted in confidence and were not recorded. Detailed notes were collated, however, and observations were documented in a structured manner, facilitating cross-referencing and detailed analysis. The semi-structured interviews allowed for considerable flexibility and catered for supplementary questions based on discussions with the interviewee. Combined with the confidentiality guarantee, this provided an environment in which interviewed stakeholders could highlight matters that were important to them within the general topics discussed. In many cases, the interviewees could also provide perspectives, insights and information that might otherwise have been inaccessible to the researchers. Indeed, part of the purpose of the interviews was to make up for regional and topical gaps in the desk research. In total, over 30 interviews were carried out from the fourth quarter of 2019 to the second quarter of 2020. As with the survey, the stakeholders interviewed provided their views in a personal capacity rather than as representatives of any specific organization, and all input from the interviews has been used without attribution. Like the comments elicited through the survey, again, those made by the stakeholders interviewed were vital and have been used throughout the report to highlight particularly important arguments, observations and concerns.

Limitations of the study

A research study of this nature carries certain limitations. First, the scope of the report is defined by the mandate of the Internet & Jurisdiction Policy Network and ECLAC. Thus, this is not a regional status report about the Internet generally, but focuses specifically on cross-border legal issues in relation to the Internet. Second, despite the steps outlined above, there are bound to be gaps. The statistical relevance of exploratory research that relied in part on a limited number of survey participants and interviewed stakeholders should not be overstated. In addition, most forms of desk research may involve biases that are difficult to eliminate entirely, whatever efforts are made to do so.

In the light of the above, this report represents the compilers' best effort at producing a broad-brush yet comprehensive overview and documentation of past, current and emerging trends, relevant actors and proposed solutions to the major cross-border legal policy challenges facing our connected society as of 1 June 2020. As such, it is a timely snapshot of the policy environment and provides a first regional baseline for future studies in the Latin America and Caribbean region.

EXECUTIVE SUMMARY

The *Internet & Jurisdiction and ECLAC Regional Status Report 2020* is the region's first comprehensive exercise in mapping the different policy trends relating to the transborder nature of the Internet and the way this affects different actors such as governments, companies and civil society.

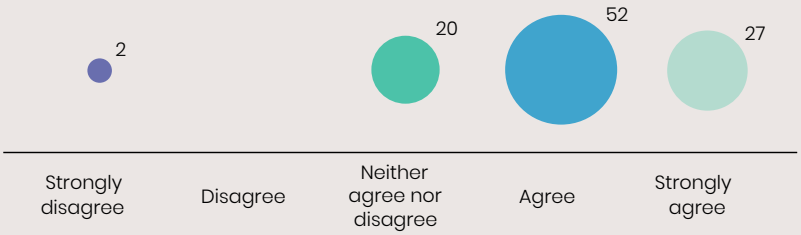
How might differing regional and national regulations create barriers to cross-border e-commerce and investment in digital markets? What economic and social benefits might be attained by harmonizing legal frameworks throughout the region? A better understanding of this situation is vital to efforts to foster investor confidence, promote innovation and economic diversification, create greater trust in e-commerce and boost a market of more than 600 million people, while opening up an array of opportunities for businesses, most particularly small and medium-sized enterprises.

At the same time, uncoordinated action by a wide range of actors and initiatives risks hampering the digitalization of economies, governments and societies. It is to help policymakers navigate the challenges ahead that the Internet & Jurisdiction Policy Network, in coordination with the Economic Commission for Latin America and the Caribbean (ECLAC), is presenting this report.

The report aims to: (i) map and consolidate information relevant to Latin America and the Caribbean and the regional digital market; (ii) create and strengthen regional contributor networks; and (iii) develop capacity-building for stakeholders on cross-border legal topics associated with the digital transformation.

In surveys and interviews conducted for the report with leading experts in the region, 78% of respondents agreed that Internet-related cross-border legal challenges would become increasingly acute in the next three years. At the same time, 73.17% of the stakeholders interviewed agreed or strongly agreed that coordination was required to address cross-border legal challenges, while 60.98% believed that the institutions needed to tackle those challenges were still not in place.

Will Internet-related cross-border legal challenges become increasingly acute in the next three years?



Source: Internet & Jurisdiction Policy Network and Economic Commission for Latin America and the Caribbean (ECLAC).

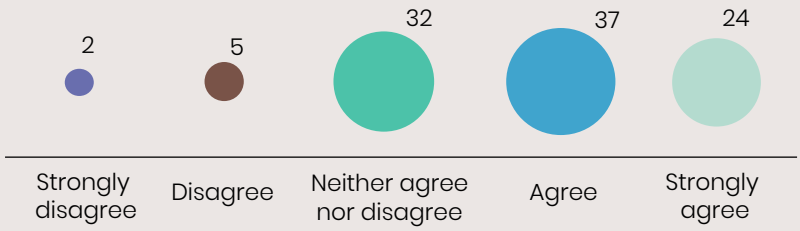
In an effort to analyse trends that are unique to the region, the report investigates how a changing technological landscape is empowering the idea of transnational activities as an emerging new dynamic that not only involves big multinational companies but is also setting the stage for regional start-ups to grow rapidly.

The report identifies how regional and national regulatory frameworks might be inspired by foreign initiatives, especially those arising in the United States and the European Union. This is the case with the European Union General Data Protection Regulation (GDPR), which has sparked a number of legislative changes in Latin America and the Caribbean. Is there room for cross-fertilization, or is this mere replication?

As major Internet companies try to adapt to the changing expectations of governments and the general public, involving increasing demands for greater responsibility, a plurality of norms is making the region ripe for jurisdictional conflicts, testing the limits of enforceability and the reach of national laws.

This report organizes the major topical trends in Latin America and the Caribbean into three groups: expression, security and the economy. There is no lack of trends that are unique to the region, although others are also present on a global scale.

One of the most pressing trends in the area of expression is the way the fight against disinformation and so-called fake news has been leading many countries to adopt new rules that might have impacts extending far beyond their borders. A substantial majority (60.98%) of the stakeholders interviewed agreed or strongly agreed that the cross-border nature of the Internet facilitated foreign interference with the democratic process. Cases in which automated social media accounts created abroad end up playing a role in a country's elections are not uncommon in the region.



Does the cross-border nature of the Internet facilitate foreign interference with the democratic process?

Source: Internet & Jurisdiction Policy Network and Economic Commission for Latin America and the Caribbean (ECLAC).

The same demand for cooperation among countries to address jurisdictional challenges has surfaced in the region during investigations into corruption scandals. To secure evidence located in different countries, law enforcement agencies in Latin America and the Caribbean are pressing for more cooperation, which should create the conditions for standardization of cross-border data transfers in the region.

Coordination is crucial if a digital single market is to be created in Latin America and the Caribbean. A topic that came clearly to the fore in the interviews and surveys conducted for the report were the economic effects of a regional approach to issues such as the spread of financial technology (fintech) in the region. Stakeholders expressed considerable support for innovative regulatory solutions, with 82.92% agreeing or strongly agreeing that the deployment of innovative frameworks such as regulatory sandboxes helped foster economic growth.

The report also highlights the way significant approaches to cross-border Internet dilemmas in Latin America and the Caribbean might come from legislation or from the development of technological tools such as geo-blocking and content filtering, with all the controversies such resources might bring.

The *Internet & Jurisdiction and ECLAC Regional Status Report 2020* is intended to supply tools for evidence-based policy innovation and to provide all stakeholders with the information they need to develop frameworks and policy standards for the digital society in Latin America and the Caribbean. The report contains the following major observations:

Major transversal aspects of trends and solutions: overarching trends

- **Connectivity is on the rise.** A number of countries in the region are experiencing a significant increase in the numbers of the digitally included, but bridging the digital divide and tackling structural socioeconomic inequalities are still major challenges for development and innovation.
- **The landscape is changing.** The romanticized technological euphoria of the past has given way to a "techlash", triggered by concerns about disinformation, hate speech and cybercrime (with a recent period of technology intensity in response to the COVID-19 pandemic and as part of the fight against it). Transnational interactions are an emerging new dynamic, the influence of multinational companies is strong and the entrepreneurial environment of regional start-ups is growing.
- **Foreign regulatory initiatives have influenced regional and national proposals.** There is an increasing appetite for regulating cyberspace, as the proliferation of initiatives attests; but are these legislative and judicial inspirations useful cross-fertilization or mere imitation?
- **Concerns about external influence and increasing normative plurality are appearing.** Rules are being set for —and by— large and well-established international actors, and the role of company norms is increasing as their terms of service attain "constitutional" status for the digital spaces they control.
- **The role of territoriality/sovereignty in a global network is increasingly being called into question.** National laws are increasingly extraterritorial in reach, but this is bringing challenges of enforceability.
- **Intermediaries are expected to play new roles.** Private operators are being asked to bear increasing responsibilities; intermediaries have been called upon to provide the main support in administrative and judicial investigations; transparency is vital to enhance trust, but implementation varies; there is a growing concern with due process in content moderation activities.

Major topical trends in Latin America and the Caribbean

Expression:

- Fake news and disinformation campaigns are triggering calls for regulatory action;
- Governments are imposing stricter rules for content moderation and removal on online platforms;
- The non-consensual distribution of sexually explicit media ("revenge porn") knows no borders and can perpetuate harm;
- The Google Spain case at the European Court of Justice (ECJ) has sparked a regional debate about the "right to be forgotten": while experts recognize this right as global in scope, the regional experience with amnesty laws and the notion of a "right to remember" have created a backlash against the enforcement of a general right to be forgotten;
- Defamation cases are triggering debates about the cross-border effects of protecting a person's reputation. Moreover, defamation is both a civil and a criminal offence in many countries of the region, raising additional questions about how the protection of reputation might restrict freedom of expression (e.g., for journalists and bloggers).

Security:

- There is a growing need and aspiration for coordination in cybersecurity efforts to deal with widespread incidents in the region;
- Cross-border corruption cases in the Latin America and Caribbean region have prompted a sophisticated debate over multi-jurisdictional investigation practices;
- The challenges involved in accessing digital evidence across multiple jurisdictions mean there is a need to review current investigation practices in the region;
- Regional stakeholders do not advocate overhaul of the mutual legal assistance (MLA) system, but rather support its adaptation to the digital age; however, law enforcement agencies in the region are increasingly seeking access to user data outside the MLA treaty structure;
- Regional stakeholders agree that the Budapest Convention is a step in the right direction when it comes to facilitating cross-border investigations, but that it does not fully solve the problems of the MLA system;
- Stakeholders reaffirm that "back doors" would undermine trust in encrypted systems;
- Countries in the region have yet to fully adapt their legislation to the demands of fighting cybercrime;
- Mutual recognition of digital IDs would be a positive driver of regional and economic integration, not least for a digital single market.

The economy:

- Inspired by the GDPR, countries in Latin America and the Caribbean are creating or improving national data protection regulations;
- Half the countries in the region have a specific data protection regulation, but there is room for improvement and coordination to achieve a truly region-wide framework for data protection;
- Regional initiatives are fostering standardization of cross-border data transfers;
- There is demand for the creation of a digital single market in the region;
- Stakeholders indicated that areas such as consumer and data protection, digital payments and tax regimes were vital to the creation of a region-wide digital single market;
- The region has a strong consumer rights culture, providing a useful basis for the creation of a digital single market;
- Choice of law and choice of forum clauses tend to be frowned upon in e-commerce because of national consumer protection standards;
- The Internet of Things (IoT) knows no borders and requires standardization, but stakeholders are divided on the need for specific regulations for IoT;
- There are a number of challenges and opportunities for smart cities in the region;
- Smart farming enlarges the set of international players and is a natural move for the region;
- Digital payment developments in the region coexist with an unbanked population, low penetration of international credit cards, an enduring cash culture and foreign exchange volatility;
- Fintech is revolutionizing financial services in the region, but faces disparate regulatory treatment at the national level;
- Cross-border jurisdictional issues are increasingly impacting the activities of fintech companies in the region;
- Stakeholders have shown great enthusiasm for the adoption of innovative regulatory solutions, such as regulatory sandboxes;
- Blockchain and cryptocurrencies are viewed as enablers of cross-border trade (but also crime).

Major approaches to cross-border Internet dilemmas in Latin America and the Caribbean: legal trends

- States are increasingly resorting to an "effects doctrine" in asserting jurisdiction;
- The assertion of geographically far-reaching jurisdiction may not lead to actual enforcement;
- Higher courts in the region have so far refrained from decisions with a global reach;
- National courts are increasingly issuing platforms with take-down, stay-down and stay-up orders for content posted online;
- In addition to civil liability, countries are increasingly resorting to administrative sanctions to enforce compliance with sectoral norms;
- Companies' terms of service interact with national laws, reinforcing or contradicting provisions regulating user behaviour;
- The impact of the controversial update to the European Copyright Directive is already being felt in the region;
- Online marketplaces are deploying dispute resolution systems as governments push for co-regulation of the sale of counterfeit goods;
- In the interests of consumer protection, courts in the region tend not to uphold choice of forum and choice of law clauses in international platforms' terms of service.

Major approaches to cross-border Internet dilemmas in Latin America and the Caribbean: tools

- The use of personal data to map and control the COVID-19 pandemic will consolidate the discussion about geolocation technologies in the region;
- Geo-blocking and geo-pricing are raising antitrust and consumer and data protection concerns;
- Content filtering is on the rise as countries fight hate speech and disinformation;
- App blocking, once a last resort, is now common practice, with the potential for major impacts across borders;
- DNS blocking is being ordered by some governments, but is not a widespread practice;
- Internet shutdowns are not common, but can happen at times of social unrest;
- Mandatory data localization has been adopted in some countries for various reasons, but it raises serious concerns among stakeholders.

INTRODUCTION

WHY A REGIONAL STATUS REPORT?

The present report is the first regional version of the pioneering *Internet & Jurisdiction Global Status Report 2019* that the Internet & Jurisdiction Policy Network launched at the United Nations Internet Governance Forum in Berlin in November 2019, providing for the first time a global baseline for the cross-border ecosystem of Internet jurisdiction. This regional report is based on the proven methodology of the global report of 2019.

The objectives of the *Internet & Jurisdiction and ECLAC Regional Status Report* 2020 are as follows:

- Mapping and consolidation of information relevant to the Latin America and Caribbean region and the regional digital market. The report provides, for the first time, a comprehensive regional overview and documentation of past, current and emerging trends, significant actors and proposed solutions to the major cross-border jurisdictional policy challenges that stakeholders are facing in Latin America and the Caribbean.
- Investigation of the most salient trends and policy challenges of the digital society and economy. The report expands in particular upon the findings and issues encompassed by the three programmes of the Internet & Jurisdiction Policy Network, namely cross-border access to user data, cross-border content restrictions, and domain suspensions. The report also examines the most important emerging issues and debates, including topics such as the Internet of Things, digital trade and blockchains, in order to map these upcoming policy challenges.
- Creation and strengthening of regional contributor networks. The report provides a consolidated basis for capacity-building through knowledge sharing and the facilitation of well-informed decision-making, using an innovative large-scale collaborative contribution and review process to create a regional contributor network and leverage the combined expertise of engaged stakeholders through structured interviews and data collection efforts.
- Capacity-building for major stakeholders on cross-border legal topics associated with the digital transformation. This comprehensive overview and analysis of trends and initiatives provides decision makers with an interpretation of the highly complex and often technical substantive issues involved and contributes to the development of a much-needed common taxonomy for the policy ecosystem. The report aims to help mitigate acute jurisdictional conflicts, support the development of concrete operational solutions and equip policy actors with the information they need to avoid losing the benefits of the open, interoperable cross-border Internet.

This document should serve practitioners as a roadmap to some of the most pressing issues surrounding policymaking and the cross-border nature of the Internet in Latin America and the Caribbean.

A. The Internet: a rapidly evolving regulatory landscape

For over two decades, there has been a discussion about whether and how the Internet can be regulated. Before agreement is reached on these questions, though, it is important to reflect on what regulating the Internet actually means. Regulation comes in many different forms, and a State-imposed law is not the only way in which behaviour might be stimulated or discouraged. Lawrence Lessig suggested back in 1999 that the regulatory tug-of-war could be more complex when

what was at issue was how technology impacted human behaviour. Legal rules were not going to be the sole source of regulation. Instead, they would have to contend with competing forces such as the market and its economic logic, social constraints and, lastly, the technology itself, whose architecture might either allow or prevent a particular type of behaviour.[1]

The scenario depicted by Lessig reveals that changes in culture, market forces or technological architecture could be more effective than legislative changes in shaping human relations and behaviour. For the future of Internet regulation to be understood, then, the analysis should include but not be limited to State action.

States unquestionably play an important role by setting the legal rules, but they also have a coordinating role, promoting digital inclusion and literacy in a given society and aligning market incentives. Yet the State alone cannot fully control Internet regulation or the end results.

On the topic of disinformation, for instance, it has become increasingly clear that the economic incentives of the monetization models implemented by platforms may impact the types of content developed for online distribution.[2] The characteristics and criteria of curation algorithms also influence the consumption or otherwise of controversial, disputed or even polarizing speech on social networks.[3] Media literacy and social etiquette likewise play a role.[4] All these factors play as much of a part in curbing the spread of disinformation as legal rules, and sometimes even more.

To take another example, the protection of intellectual property online has advanced greatly because of a market shift. The traditional procedure of tracking down repeat offenders —whether those who post copyrighted material or those who constantly access it— and then shutting down their accounts, serving them with fines or, in some instances, even jailing them has its limits. The advent of streaming platforms for video and music, though, has had a great impact, and consumption of pirated content online has plummeted.[5]

Just when consumers have begun to acquire new habits, though, the multitude of streaming platforms has ended up creating new economic constraints, making it more expensive for users to access all the content they desire. Some see this as the beginning of a new phase of widespread illegal access to copyrighted online content.[6]

In Latin America and the Caribbean, where resources for law enforcement and general oversight are scarce, it is even more important that legal rules take into consideration and benefit from the different forces at play in regulating the Internet. This report, then, draws upon knowledge of trends involving all four areas: legal rules, economic incentives, social norms and technology. The idea is to extract insights from their interaction and highlight how the four points of the tug-of-war impact cross-border regulation.

B. Competing interests are difficult to reconcile across borders

At a basic level, the purpose of regulating the Internet is to counter abuse, protect individual rights and safeguard innovation and the digital economy, particularly market access. From the standpoint of the region, however, there are other dimensions to be considered.

1 L. Lessig, "The Law of Horse; what CyberLaw might teach", *Harvard Law Review*, vol. 113, No. 501 [online] https:// cyber.law.harvard.edu/works/lessig/finalhls.pdf.
2 V. Bakir and A. Mcstay, "Fake news and the economy of emotions: problems, causes, solutions", *Digital Journalism*, vol. 6, No. 2, 2018 [online] https://www.tandfonline.com/doi/full/10.1080/21670811.2017.1345645.
3 S. Bradshaw, "Disinformation optimized: gaming search engine algorithms to amplify junk news", Internet Policy *Review*, vol. 8, No. 4, 2019.
4 F. Saurwein and C. Spencer-Smith, "Combating disinformation on social media: multilevel governance and distributed accountability in Europe", *Digital Journalism*, vol. 8, 2020.
5 M. Freixo Nunes, "On-demand music streaming and its effects on music piracy", Dissertation, International Master of Science in Management, Universidade Católica Portuguesa, 2018.
6 See Intelligencer, "Piracy is Back", 26 June, 2109 [online] https://nymag.com/intelligencer/2019/06/piracy-is-back.html.

Despite perceived commonalities, Latin America and the Caribbean is very diverse in terms of size, economic development and even social and cultural roots. This diversity makes for complicated alignments of interests. There are many different national, subnational and subregional connections and alliances, and all of these are influenced by extraregional interests as well, be they those of major countries and regions such as the United States, Europe or China, or of multinational corporations and organizations that bring pressure to bear on national and regional decision makers, quite apart from the rivalries that have been fostered by an environment that is more competitive than cooperative.

All this provides a difficult backdrop for the resolution of cross-border legal dilemmas. On the one hand, different and even contradictory standards exist in the region, some of them intrinsic to individual countries' sense of identity or legal order or rationale. On the other hand, pressure from different interest groups may lead to the transplantation of legal concepts and inadequate or inappropriate implementation of legal solutions.

This context becomes particularly challenging in the absence of any international arrangement that can provide clear guidance, coordinate action and solve contradictions. In a quest for efficacy, and despite the clash of interests, several States have taken it upon themselves to solve Internet problems unilaterally. This has taken the form of assertions of sovereignty over cyberspace, extraterritorial application of national legislation, and even administrative and judicial decisions with global reach (all topics explored in this report). The result may be more potential for clashes, more competition between States and even the exacerbation of differences in States' reach and capacity unless these challenges are addressed through cooperation and coordination.

C. Companies, governments and individuals are increasingly concerned about abuses online

There is growing concern over online abuses (disinformation, hate speech, harassment, cybercrime, hacking, privacy violations and fraud, among others). The general feeling is that the rapid rise in connectivity has been accompanied by opportunities for unethical and illegal behaviour online.

This view is strengthened by a perception that the borderless nature of cyberspace makes it more difficult to police, hinders investigations and restricts the scope of government action. State regulation seems porous and incapable by itself of encompassing or properly responding to activities that impact citizens' lives and property.

The stakeholders surveyed noted that there were at least three different dimensions to such concerns: (i) individuals acting alone or in coordination can cause a great deal of harm without at any time being physically present in a country, making it truer than ever that crime and fraud do not stop at borders; (ii) international companies are under pressure to take action and do not always feel compelled to observe the specificities of national regulations, particularly when local requirements run counter to the legal obligations of their place of incorporation; and (iii) foreign influence in different shapes and degrees impacts both the substance of local legal responses and their ability to achieve their objectives, with power imbalances between countries potentially rendering domestic action less than optimal.

Furthermore, international scandals such as the Snowden revelations,[7] Cambridge Analytica[8] and the Panama Papers[9] have shown the extent to which situations arising in one country may impact the very fabric of another country's political order. The legal tools available do not or cannot address the challenges fully.

[7] See L. M. Austin, "Lawful Illegality: What Snowden Has Taught us about the Legal Infrastructure of the Surveillance State", April 2014 [online] https://ssrn.com/abstract=2524653.

[8] See F. González and others, "Global Reactions to the Cambridge Analytica Scandal: A Cross-Language Social Media Study", 2019 [online] https://www.researchgate.net/publication/333066944_Global_Reactions_to_the_Cambridge_Analytica_Scandal_A_Cross-Language_Social_Media_Study.

[9] See L. J. Trautman, "Following the Money: Lessons from the Panama Papers, Part 1: Tip of the Iceberg", *Penn State Law Review*, vol. 807, 12 May 2017 [online] https://ssrn.com/abstract=2783503.

Some of the stakeholders interviewed pointed out that such international incidents had often been accompanied by domestic upheaval. One expert noted that many governments had capitalized on these emotional responses, resorting to the criminal law and criminalization of online behaviour with varying degrees of success. Another mentioned the tendency to extend the reach of national laws, either by applying them extraterritorially or by creating an artificial form of localization, particularly when seeking access to data for criminal investigations or for national security purposes.

D. Addressing cross-border jurisdictional challenges is critical to build trust in a global network

The global nature of the Internet is part and parcel of how cyberspace has been architected. The "world" in the "world wide web" ("www") is not there by chance. The logical layer of the Internet is borderless by design. Yet the international world order is structured on a very different principle, with the sovereign equality of States making the nation State and its geographical territory the primary centre of regulation.[10] Differing approaches and even priorities are to be expected. Regulation tends, then, not to be constant or uniform.

Handling the coexistence of such heterogeneous laws and regulatory methods as they apply to the cross-border Internet is one of the greatest policy challenges of the twenty-first century. Scalable and coherent policy solutions cannot be developed without a comprehensive understanding of this highly complex and dynamic ecosystem, comprising multiple actors, initiatives and trends across the policy silos of the digital economy, human rights and security.

This paradox of local primary regulation and global space (cyberspace), coupled with the multiplicity of actors, tends to lead naturally to fragmentation. Two phenomena may impact the Internet as it currently is. The first is the tendency for it to splinter, recreating the borders of the physical world in cyberspace. The second are the efforts by national institutions to exert extraterritorial sway in an attempt to regulate the global Internet from a unilateral, national standpoint. Both dynamics undermine the usefulness of and trust in the global Internet.

The Latin America and Caribbean region's history of fighting against colonization and the resulting emergence of the international principle of non-intervention tend to reinforce both phenomena: splintering and efforts to extend the reach of national legislation extraterritorially. However, differences in size, power and administrative efficiency have meant varying degrees of success.

In any event, the experts surveyed noted the tendency of countries in the region to regulate the Internet and affirm their sovereignty over cyberspace. This seems to be particularly true when it comes to data, with claims being made regarding data sovereignty and data localization (as discussed in section V.B.6) and with extraterritorial applications of data protection legislation (as analysed in section IV.C.6).

To advance the regional debate about the design and application of online legislation and to catalyse the development of a shared framework, it is important for stakeholders to engage in ongoing dialogues that help identify the challenges and foster coordination of different initiatives and policy proposals. Obtaining high-quality information through relevant research and documentation is vital to support decision-making processes and stimulate evidence-based policy innovation. This report presents the current state of the discussion and ongoing trends, providing the basis for a much-needed reflection on how to properly address the coordination aspect of jurisdiction and cross-border concerns.

[10] M. Ketteman, *The Normative Order of the Internet: A Theory of Rule and Regulation Online*, Oxford University Press, 2020 [online] https://www.hans-bredow-institut.de/uploads/media/default/cms/media/ijp5yvb_Kettemann_The-Normative-Order-of-the-Internet.pdf.

From the standpoint of the region, digital integration is unquestionably an opportunity. It is an indispensable part of the effort to diversify regional economies. There is evidence of the enormous potential for intraregional trade to move in the direction of a more knowledge-intensive export basket. In 2018, 54% of intraregional exports by value consisted of high-, medium- and low-technology manufactures.[11] At the same time, the rapid growth of cross-border e-commerce provides major opportunities for small and medium-sized enterprises (SMEs) to trade internationally.

An estimated 155.5 million people in Latin America bought goods and services online in 2019, a substantial 22% increase on the 126.8 million who did so in 2016. However, the average annual number of online transactions per capita in Latin America in 2016 was the lowest in the world, at only 9.2 per year.[12]

The region has made significant progress with legislation concerning the Internet. In 2017, more than 80% of the countries in Latin America and the Caribbean had some type of legislation on electronic transactions and electronic signatures, and 90% had regulations on intellectual property.

These figures highlight the importance of promoting a harmonized legal and regulatory framework to help eliminate the barriers to cross-border e-commerce and investment in digital markets. The harmonization of policy frameworks throughout the region could create significant economic and social benefits, potentially leading to increased investor confidence and more foreign direct investment, the promotion of innovation and economic diversification. It could also foster confidence in e-commerce and boost a market of more than 600 million people, while opening up an array of opportunities for businesses, including small and medium-sized enterprises in particular.

E. Coordination is needed to address this overlooked challenge

Countries in the region are becoming more and more aware of the international dimension of the challenges brought by the Internet. It has become clear that the global nature of the world wide web is a source both of strength, providing many social and economic opportunities, and of a number of the difficulties associated with it, particularly the interplay between local action and international impact and vice versa.

National government structures, however, seem insufficient on their own to deal with many of the issues brought by the Internet. With the efficacy of State action thus called into question, notions of sovereignty and non-interference seem to take on different connotations.

This perception is heightened by the relative power and potential impact of the countries of Latin America and the Caribbean. Interviewees spoke of an impression that not all States can have the same influence on the way the Internet is regulated or the way they and their citizens are affected by its structure and governance arrangements.

1. The need for multi-stakeholder dialogue in the region

The international community has long recognized the need for multi-stakeholder dialogue to discuss Internet governance. The Internet Governance Forum (IGF) is the pre-eminent platform for such dialogue. However, the 2020 Report of the United Nations Secretary-General's High-level Panel on Digital Cooperation has identified challenges and gaps in the existing digital cooperation arrangements and proposed three possible architectures for such cooperation on a global scale.[13] The current mechanisms of Internet governance decision-making are thus undergoing improvement.

[11] Economic Commission for Latin America and the Caribbean (ECLAC), *International Trade Outlook for Latin America and the Caribbean, 2018* (LC/PUB.2018/20-P), Santiago, 2018.
[12] Statista, *E-commerce in Latin America* [online] https://www.statista.com/study/14764/e-commerce-in-latin-america-statista-dossier/.
[13] United Nations, *The Age of Digital Interdependence. Report of the UN Secretary-General's High-level Panel on Digital Cooperation*, 2020, pp. 22-29 [online] https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-for-web.pdf.

The first Latin American and Caribbean Internet Governance Forum (LACIGF) was held in 2008 on the initiative of the Association for Progressive Communications (APC), the Latin American and Caribbean Internet Addresses Registry (LACNIC) and the Information Network for the Third Sector (RITS). Between May 2019 and July 2020, the LACIGF Programme Committee conducted a review of LACIGF in order to shape concrete proposals for developing and assessing action points to improve the forums.[14] Stakeholders have mentioned LACIGF as providing an important opportunity for collective problem mapping and the development of common public policies, even in the absence of binding decisions. It is also important to ensure that these coordination mechanisms provide for diversity and include youth, women and indigenous people while increasing the subregional representation of Latin America and the Caribbean. At the national level, not all Latin America and Caribbean countries have an active agenda for Internet governance-related topics. Taking national IGF initiatives (national and regional IGF initiatives (NRIs)) as a starting point for analysis, the first national Internet governance event was held in Brazil in 2011. At the time of writing, national IGF events in the Latin America and Caribbean region are hosted in Argentina, Barbados, the Bolivarian Republic of Venezuela, Brazil, Colombia, Costa Rica, the Dominican Republic, Ecuador, El Salvador, Guatemala, Haiti, Honduras, Mexico, Panama, Paraguay, Peru, the Plurinational State of Bolivia, Saint Vincent and the Grenadines, Trinidad and Tobago, and Uruguay.[15]

As the rapid spread of this initiative shows, the Internet governance debate has been gathering pace in the region. This underlines how initiatives by some countries can serve as an inspiration and encourage other countries in Latin America and the Caribbean to strengthen the national debate on Internet topics. Although this is not a necessary step for regional coordination, developments at the national level are also important because they increase human capital and policymakers' ability to work on the regional and global scales. ECLAC was cited by stakeholders as a pioneer and an important governance body with the infrastructure needed not only to promote capacity-building initiatives in countries where these issues have not yet been much worked on, but also to play an active role in catalysing the transformation more broadly.

Stakeholders mentioned regional entities that could address some of the issues covered in this report, such as the Inter-American Telecommunication Commission (CITEL) and the Latin American Telecommunications Regulators Forum (REGULATEL), but observed that genuine, meaningful regional cooperation and harmonization were still a long way off. There is a problem of continuity in the policies implemented, which suggests a need for medium- and long-term policies in the region.

2. A growing aspiration towards cooperation and coordination

Cooperation and coordination have become significant goals, and ones that are perhaps necessary if cross-border challenges are to be dealt with. The argument for coordinated action looks strong in the light of the potential gains for the economy (in terms of scale, access to markets and technology) and for security (cybersecurity and the protection of basic services and critical infrastructure). Cooperation and coordination also have a large role to play in tackling significant social challenges such as disinformation and cybercrime.

Uncoordinated action by a wide range of actors and initiatives risks hampering the digitalization of economies, governments and societies. Of the stakeholders interviewed, fully 73.17% agreed or strongly agreed that there was a need for coordination to address cross-border legal challenges.

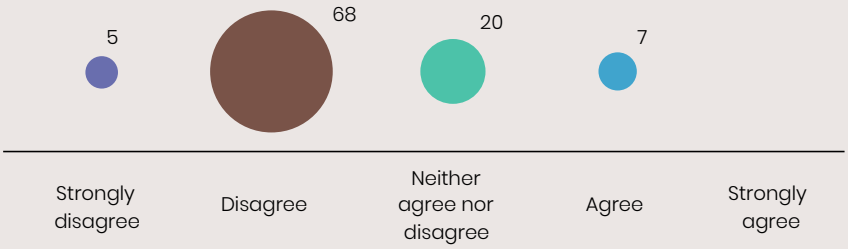
That number alone is enough to set the direction for this report, which is presented by the Internet &

[14] LACIGF, "Proposed first consultation for the review of LACIGF", 2020 [online] https://lacigf.org/en/proposed-first-consultation-for-the-review-of-lacigf/. For further information, see R. Echeberría, *Review of the Latin American and Caribbean Internet Governance Forum (LACIGF), Public Consultation Process, Report and Conclusions*, 2020 [online] https://lacigf.org/en/revision-del-lacigf/.

[15] IGF, Latin American and Caribbean Regional Group (GRULAC) [online] https://www.intgovforum.org/multilingual/content/latin-american-and-caribbean-regional-group-grulac; see also: C. Aguerre and others, *Mapping National Internet Governance Initiatives in Latin America*, University of Pennsylvania, 2018 [online] http://globalnetpolicy.org/wp-content/uploads/2018/06/Latin-American-Report_IPO_final.pdf.

Jurisdiction Policy Network (I&JPN) in coordination with the United Nations Economic Commission for Latin America and the Caribbean (ECLAC) to provide indispensable mapping and analysis of the regional ecosystem in Latin America and the Caribbean.

Is there sufficient international coordination and coherence to address cross-border legal challenges on the Internet?



Source: Internet & Jurisdiction Policy Network and Economic Commission for Latin America and the Caribbean (ECLAC).

With the Latin America and Caribbean region aiming to develop a digital single market, the stakeholders surveyed for this report sent a strong message, 78.04% agreeing that a significant effort to harmonize standards would be required for this goal to be achieved. As one of the stakeholders surveyed emphasized:

> "I believe that the MERCOSUR and Latin American countries should find a way to engage in broad cross-border regulation that can foster the digital economy in the region. The legal framework is very sparse at present, without common ground. This unevenness is compromising the region's development."

In a world that is transitioning towards a new decade, the countries of Latin America and the Caribbean have been presented with the opportunity to foster regional integration at a time when countries need to reinvent their roles on the global stage in the wake of the COVID-19 pandemic. The social and economic repercussions will be great, and understanding how different policy decisions about the Internet (and technology generally) might affect other countries will be crucial to the new frameworks that might arise from the crisis.

CHAPTER

OVERARCHING TRENDS

The combination of detailed desk research and stakeholder input (via the survey and interviews) brought out a number of overarching trends that are central to any discussion of the cross-border legal challenges associated with the Internet as a whole. Some of these trends are clearly reflective of those described in the *Internet & Jurisdiction Global Status Report 2019*,[16] and the present report highlights how they have been developing in the Latin America and Caribbean region specifically. These overarching trends are shaping topical trends (section IV) and, to a degree, are setting the parameters within which legal and technical approaches can be explored (section V).

A. Increased connectivity is necessary but can reinforce socioeconomic inequalities

Although various jurisdictional implications of the cross-border nature of the Internet have similar consequences around the globe, the number of cases, their impact and the feasibility of possible solutions will vary according to the degree of digital inclusion in a specific country. In Latin America and the Caribbean, 67% of the population are Internet users, with regional and national differences that vary by socioeconomic level and geographical location.[17]

Digital inclusion and technological development efforts should take account of certain inequalities, especially those related to income, gender, differences between urban and rural areas, the way indigenous communities access the Internet and how accessible and understandable online resources are for the elderly population.[18]

The degree to which national digital development strategies consider each of these factors varies. For instance, in a comparison between 14 national strategies in the region, only 4 were found to give priority to increasing access for those of a lower socioeconomic level, which means there is a need for a further political agenda focused on reducing inequalities in access to the Internet.[19] At the same time, at least 12 countries consider the digital divide from three important perspectives: (i) the development of a robust infrastructure for high-quality digital connectivity, (ii) promotion of the use of information and communications technologies (ICTs) in daily life and (iii) economic development with the use of digital platforms and services.[20]

When the Internet turned out to be the main way for citizens to work, study and access basic services during the COVID-19 crisis, different regional actors recognized that a developed digital ecosystem was intrinsically related to social and economic development and that the Internet was a necessary tool for various daily activities such as work, study, commerce and communication. Countries with a larger digital divide have suffered more negative consequences than those with a smaller one. Between 2004 and 2018, the digital ecosystem in Latin America and the Caribbean developed less than in any other developing region, excluding the Arab States.[21] Overall, Internet penetration has grown considerably in the Latin American and Caribbean countries, but differences remain between them. In Ecuador, 60.67% of the population had Internet access in

16 See [online] https://www.Internetjurisdiction.net/news/release-of-worlds-first-Internet-jurisdiction-global-status-report.
17 Development Bank of Latin America (CAF) and others, *Las oportunidades de la digitalización en América Latina frente al COVID-19*, Santiago, 2020, p. 9.
18 See R. Martínez, A. Palma and A. Velásquez, "Revolución tecnológica e inclusión social: reflexiones sobre desafíos y oportunidades para la política social en América Latina", *Social Policy series*, No. 233 (LC/TS.2020/88), Santiago, Economic Commission for Latin America and the Caribbean (ECLAC), 2020.
19 Ibid., p. 57.
20 Ibid., p. 55.
21 Asia and the Pacific: 9.39%; Africa: 8.27%; East Europe: 6.89%; Latin America and the Caribbean: 6.21% (Development Bank of Latin America (CAF) and others, *Las oportunidades de la digitalización en América Latina frente al COVID-19*, Santiago, 2020, p. 5 [online] https://repositorio.cepal.org/bitstream/handle/11362/45360/4/OportDigitalizaCovid-19_es.pdf).

2018, rising to 68.09% in 2020. In Honduras, the figure increased from 34.06% in 2018 to 39.33% in 2020.[22]

It is also important to note that digital inclusion is a concept that goes beyond access to the Internet per se. A Development Bank of Latin America (CAF) study has found that communication tools and social media account for the bulk of Internet use in the region.[23] This indicates a need for further development to unlock the full potential of digital inclusion in its social and economic aspects.

In any event, making the Internet available to all citizens is a major concern and also part of the 2030 Agenda for Sustainable Development. Target 9.c is to "significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020". According to a 2020 ECLAC study on scenarios and projections considering the COVID-19 pandemic, this target is "likely to be reached on the current trend" in the region.[24]

A digital and connected framework also has a role to play in the development of other technologies that are particularly important in the region, such as smart farming. The more disconnected a rural area is, the more distant the prospect of connected and efficient agriculture. Development can already be seen in digital inclusion initiatives focused on logistics and agro-industrial supply chains.[25]

Moreover, as countries develop their digital government strategies and increasingly offer public services partially or totally over the Internet (e.g., social benefit applications, tax filing and registration databases), being digitally included increasingly means enjoying basic citizen rights. The expansion of digital identity initiatives is also a good example of this trend.

Recent comparative studies on Latin American and Caribbean countries have recognized the importance of public policies for reducing the digital divide in the region.[26] Such policies usually include not only access to the network itself, but also provisions concerning infrastructure, device manufacturing and the development of digital skills. Developments differ in the region, but some highlights are mentioned below.

- In August 2020, Argentina issued Decree No. 690/2020 declaring information and communications technology (ICT) services to be public services subject to stricter administrative rules.[27] The decree also provided that there should be no increase in the prices of these services, including radio and telephony (mobile or home landline), until 31 December 2020.
- In Peru, Telefónica, Facebook, IDB Group and the Development Bank of Latin America (CAF) partnered to create the Internet para Todos (IpT) ("Internet for All") project. As of 2020, the project has connected more than 1.5 million Peruvians in rural areas with 4G technology. For 2021, the target is to provide Internet access to 30,000 rural communities.[28] Another aim is to expand the project to other Latin American and Caribbean countries.[29] It demonstrates the potential of public-private partnerships for Internet development in the region.

22 Telecom Advisory Services, *El estado de la digitalización de América Latina frente a la pandemia del COVID-19*, Development Bank of Latin America (CAF), April 2020, p. 18 [online] https://scioteca.caf.com/bitstream/handle/123456789/1540/El_estado_de_la_digitalizacion_de_America_Latina_frente_a_la_pandemia_del_COVID-19.pdf?sequence=1&isAllowed=y.

23 Ibid., pp. 4, 18-21.

24 Economic Commission for Latin America and the Caribbean (ECLAC), *The 2030 Agenda for Sustainable Development in the new global and regional context: scenarios and projections in the current crisis* (LC/PUB.2020/5), Santiago, 2020.

25 See, for instance, the example of Peru in Development Bank of Latin America (CAF), "Sector público y privado comprometido en hoja de ruta para la digitalización de la cadena agroexportadora en región Ica", 24 January 2020 [online] https://www.caf.com/es/actualidad/noticias/2020/01/sector-publico-y-privado-comprometido-en-hoja-de-ruta-para-la-digitalizacion-de-la-cadena-agroexportadora-en-region-ica/?parent=6429. See also G. Pérez, "Rural roads: key routes for production, connectivity and territorial development", *FAL Bulletin*, No. 377, Santiago, Economic Commission for Latin America and the Caribbean (ECLAC), July 2020.

26 L. Robinson and others, "Digital inclusion across the Americas and the Caribbean", *Social Inclusion*, vol. 8, No. 2, 2020.

27 Argentina, "Decreto 690/2020", *Boletín Oficial de la República Argentina*, 21 August 2020 [online] https://www.boletinoficial.gob.ar/detalleAviso/primera/233932/20200822.

28 Development Bank of Latin America (CAF), " 'Internet para todos' contribuye a cerrar la brecha digital y ya conecta a más de 1 millón y medio de peruanos en zonas rurales", 4 May 2020 [online] https://www.caf.com/es/actualidad/noticias/2020/05/Internet-para-todos-contribuye-a-cerrar-la-brecha-digital-y-ya-conecta-a-mas-de-1-millon-y-medio-de-peruanos-en-zonas-rurales/.

29 Inter-American Development Bank (IDB), "Internet para Todos: helping Latin America log on", 2020 [online] https://www.iadb.org/en/improvinglives/Internet-para-todos-helping-latin-america-log.

- The Plurinational State of Bolivia's digital inclusion programme includes the participation of citizen volunteers in support of ongoing activities in local communities.[30]
- In 2015, Brazil launched the Amazônia Conectada ("Connected Amazon") project, aimed at expanding broadband technology in the Amazon region. Although progress has been made with Internet infrastructure, the project has come in for considerable criticism and has been negatively assessed by the State Audit Court (TCU) because of technical and implementation failures.[31]
- In 2019, the United Nations Telecommunication Development Sector (ITU-D) involved 75 indigenous leaders across Argentina, the Bolivarian Republic of Venezuela, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, Mexico, Nicaragua, Panama, Paraguay, Peru and the Plurinational State of Bolivia in capacity-building with a focus on innovative tools.[32]

Digital inclusion is still a major challenge in Latin America and the Caribbean and a priority when discussing Internet regulation. Special attention should be given to the infrastructure layer of the Internet, where the transborder nature of the network comes up against basic local development needs. But could there be scope for further cooperation to develop solutions and innovative ways of tackling the digital divide? Further integration in the region has the potential to foster development and the sharing of best practices in closing the digital divide, as well as connecting more people to a single global Internet.

B. A changing technological landscape

Perceptions of how the Internet has affected almost everything, from trivial daily activities to the building blocks of international relations, have changed dramatically in the last decades. Latin America and the Caribbean has its own share of peculiarities that invite further analysis of how countries in the region have integrated the digital component into their national and international strategies. How much has access to the Internet changed the lives of citizens in the Latin American and Caribbean countries? Who are the actors shaping digital policies in the region, and how do they affect governments, companies and individuals across national boundaries?

1. Swings in perceptions: from tech euphoria to techlash

If the Internet is to connect us all, some have argued that no regulation whatsoever should be permitted in cyberspace. Back in 1996, the well-known document "A Declaration of the Independence of Cyberspace", by John Perry Barlow, drew a line between States as "weary giants of flesh and steel" and cyberspace as "the new home of Mind".[33] Proclaiming the virtues arising from the existence of a virtual space for the free flow of information, Barlow urged States not to interfere with the development of the network through regulations of any kind.

The debate over Internet regulation has changed since the late 1990s. In very general terms, the technological euphoria of Barlow's times has given way to a grimmer perception of how the Internet might be used to commit crimes and spread disinformation, hugely affecting the enjoyment of fundamental rights and eroding political discourse. What had started out as euphoria turned into a "techlash" involving significant regulatory efforts.

The beginning of the 2020s, however, has brought an important milestone. As the fight against COVID-19 has forced countries to close borders and impose lockdowns, it is the Internet that has served as a lifeline, allowing families, businesses and governments to continue to communicate

30 Plurinational State of Bolivia, "Bolivia: Decreto Supremo N° 3900, 8 de mayo de 2019", May 2019 [online] https://www.lexivox.org/norms/BO-DS-N3900.html. See also Electronic Government and Information and Communications Technologies Agency (AGETIC), "Decreto Supremo N° 3900", 10 June 2019 [online] https://digital.gob.bo/2019/06/contenido-libre/.

31 A. B. Gomes, F. Duarte and P. Rocillo, *Inclusão digital como política pública: Brasil e América do Sul em perspectiva*, Belo Horizonte, Institute for Research on Internet & Society (IRIS), 2020.

32 International Telecommunication Union (ITU), "Indicadores de nuestros programas de capacitación para el fortalecimiento de los pueblos indígenas" [online] https://www.itu.int/en/ITU-D/Digital-Inclusion/Indigenous-Peoples/Pages/Indicadores.aspx.

33 J. P. Barlow, "A Declaration of the Independence of Cyberspace", 8 February 1996 [online] https://www.eff.org/pt-br/cyberspace-independence.

during challenging times. We cannot return to the period of euphoria, but the pendulum seems to be swinging again, and the public perception of the role the Internet plays in people's lives might undergo another transformation.[34]

Paradoxical as it may seem, the closure of borders to contain the virus was matched by an increased level of activity by individuals, companies and authorities online. Thousands of public and private services were forced to go digital in order to carry on serving the general public.

Numerous countries have resorted to providing services online, from emergency benefits to basic day-to-day public actions. Even the legislatures and judiciaries of a great many countries have moved their activities to the Internet. In the private sector, many firms have been offering their services online in order to survive, moving all employees whose activities can be performed away from their physical premises to home office work. Quite suddenly, millions of people and thousands of companies have had to adapt to the digital age.

The Internet has gained in relevance and importance, showcasing its positive aspects and many of its complexities. On the one hand, people have been able to maintain some degree of interpersonal relations because of it. One the other, they have become more vulnerable to disinformation, fraud and cybercrime, likewise owing to the Internet having become the only option for accessing a number of services traditionally provided offline.

2. Transnationalism is an emerging new dynamic

Another aspect that the pandemic has made starkly clear is that borders are a construct. They are also porous. Globalization, which in many ways is dependent on how humanity deals with geography, has been presented in a different light, through a constant international flow of information and services.[35] Despite actual borders being closed, the Internet allows communications and data to enter and leave. Our shared experiences during this time have thus reaffirmed a conclusion that may seem self-evident: the Internet has turned transnationalism into an emerging new dynamic.

Latin America and the Caribbean has in many ways embraced the phenomenon. The borderless nature of the Internet has created a perfect environment for ideas to reach a wider audience. For business as well, countries in the region have been serving as a proving ground for numerous inventive solutions to the most diverse challenges. For large multinationals and promising start-ups, the region continues to offer many opportunities.

However, the feasibility of these opportunities is sometimes dependent on the national and regional regulatory framework. Deciding how to mix foreign inspiration with regional innovation is the first step towards understanding how to tackle Internet policy in Latin America and the Caribbean.

3. Foreign multinationals are influential in the region

Multinational companies from many countries are competing for the attention of Latin American and Caribbean citizens and are part of all market layers, from infrastructure to over-the-top media services. The rise in connectivity (further discussed in section III.A) has made Latin America and the Caribbean one of the biggest markets in the world. Mobile connectivity has been increasing the availability of Internet services for a growing majority of its citizens.[36]

Corporations with a global footprint have been involved both in developing the market itself and in exploring the opportunities Latin America and the Caribbean has to offer. This has brought problems of its own, however, with cross-border issues becoming more of a normal occurrence. Whereas in the physical market a company would need a robust presence on the ground to provide goods and services, online activities do not necessarily require this. Certain services can be made available

[34] The Internet & Jurisdiction Policy Network has prepared three framing briefs dealing, respectively, with user data access, content moderation challenges, and abuse at the domain name service (DNS) level in the context of COVID-19. See [online] https://www.Internetjurisdiction.net/publications.
[35] J. Sachs, *The Ages of Globalization: Geography, Technology, and Institutions*, New York, Columbia University Press, 2020.
[36] Internet Live Stats, "Internet users by country (2016)" [online] http://www.Internetlivestats.com/Internet-users-by-country/.

without the provider having any presence in the region. Foreign corporations may not even have legal representation, still less a headquarters or incorporation in any of the countries in the region. Yet these corporations may still have an effect on Latin American and Caribbean markets or consumers, and one that is more difficult to deal with.

Consumers, used to enforcing their rights in their own countries' courts, eventually notice how much more challenging it can be when there is an international component to their claims. The need for international judicial cooperation is increased because diplomatic services may be involved and different standards in legal procedures and protection may be highlighted.

At the other end of the spectrum, foreign companies may not necessarily know what countries their customers live in or may not have the tools to verify this (see section V.B.1 for more on geolocation technologies). As a consequence, non-compliance is a possibility with several practical consequences.

From the standpoint of public administration, if companies want to be able to participate in the region's market, they will have to comply with its laws and be available for adjudication locally. Neither the expectations of the company providing Internet services nor the convenience (or otherwise) of the place of jurisdiction are usually taken into consideration.

Additionally, multinational companies are often faced with the predicament of having to comply with contradictory legal obligations. The extraterritorial or global reach of certain national laws, judicial orders or administrative requests may lead to such conflicts. Corporations are then put in a position where they have to select which legal obligation they will comply with.[37]

In Latin America and the Caribbean, this phenomenon has manifested itself particularly in the matter of access to data stored overseas. Multinational companies, particularly those that provide or use cloud services, store data outside the territory where they are providing services, thus potentially subjecting the data to at least two jurisdictions. Whenever the country where the data are located has what is called a blocking statute that only allows access to data under particular conditions, the possibility of conflict with the laws of the jurisdiction where the services are provided (or the data collected) is increased.

Such clashes have led to instances where multinational corporations have refused to comply with valid orders issued under the domestic laws of Latin American and Caribbean countries. This has led to the application of legal remedies ranging from the levying of large fines on parent companies and against assets in the country to criminal charges against employees of multinational corporations.

The stakeholders interviewed pointed to harmonization of laws, coordination of efforts and cooperation between States as a way of dealing with these challenges. Harmonized standards lead to predictable results, making companies better prepared to comply with regulations. Similarly, by coordinating and cooperating, States can achieve better results and nurture an environment of general compliance.

4. The business environment for start-ups in the region is variable

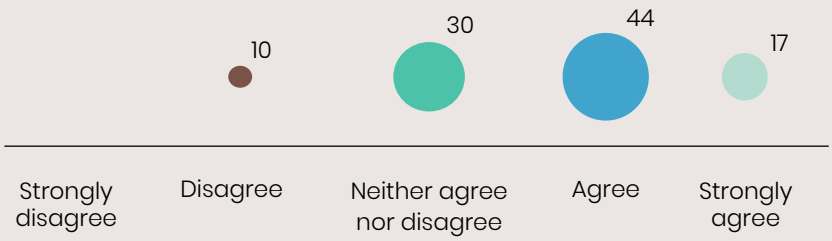
The other side of the coin is that a number of companies in Latin America and the Caribbean are taking the opportunity to expand into other markets both within the region and outside it. There is a growing mix of emerging opportunities for both established companies and start-ups to benefit from the transnational characteristics of the Internet. One expert interviewed also mentioned the existence of unexplored commonalities in the region that could allow markets to expand rapidly, such as common Iberian cultural traits and linguistic kinship.

There is thus a trend for regional producers of goods and services to partake in the platform economy, benefiting from international marketplaces (e-commerce platforms) that provide access to customers abroad. In this way, even small and medium-sized companies can become exporters and find new customers outside their usual markets.[38]

[37] D. J. Svantesson, *Solving the Internet Jurisdiction Puzzle,* Oxford University Press, 2017.
[38] See S. Lund and J. Manyika, *How Digital Trade is Transforming Globalisation*, E15 Initiative, Geneva, International Centre for Trade and Sustainable Development (ICTSD)/World Economic Forum, 2016. For particular data, see eBay "The State of Small Online Businesses: Worldwide Results from eBay's 5-Year Study" [online] https://www.ebaymainstreet.com/facts-and-figures/state-small-online-businesses-worldwide-results-ebays-5-year-study.

Not only is the domestic business environment expanding in many of the region's countries, particularly where technology start-ups are concerned, but a number of companies are expanding throughout the region and even internationally. One expert noted that several financial start-ups and blockchain-enabled projects were scaling up quickly and having to face the growing pains that come with this (see section IV.C.4 for more on financial technology (fintech)).

However, the majority of the experts surveyed (60.97%) were of the opinion that legal challenges were a barrier for cross-border Internet businesses, particularly small and medium-sized enterprises (SMEs). They mentioned that these regional companies were now facing several challenges as they sought to expand, including: (i) differing regulations and standards, (ii) being subjected to unexpected adjudication, (iii) regulatory hurdles, (iv) tax incoherence and (v) logistical and administrative burdens.



Cross-border legal challenges affecting the Internet are a barrier for small and medium-sized enterprises (SMEs) in the region

Source: Internet & Jurisdiction Policy Network and Economic Commission for Latin America and the Caribbean (ECLAC).

In discussing the new role companies in the region are playing and the opportunities they have online, it is important to note that cross-border legal challenges may or may not be a competitive hindrance. The region has a great opportunity to facilitate this expansionary trend through increased cooperation and integration, which may take the form of a digital single market (dealt with more fully in section IV.C.1).

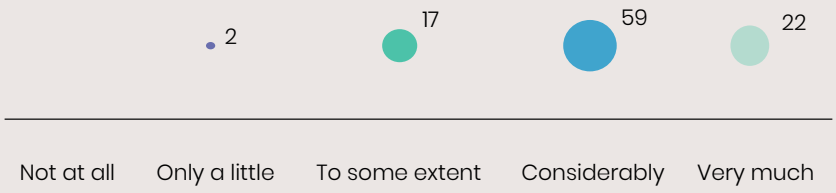
C. Foreign regulatory initiatives are inspiring regional and national proposals

While the Internet was not designed with countries' borders in mind, regulation of the network has an impact far beyond the frontiers of any single State. This transborder impact may arise because the scope of enforcement of domestic policies often encompasses activities taking place beyond territorial borders. Laws from one country can also serve as templates or sources of inspiration for others.[39]

The overwhelming majority of the stakeholders surveyed said that foreign regulatory approaches did impact domestic efforts in Latin America. In figures, 80.5% of stakeholders indicated that domestic regulatory initiatives were either "very greatly" or "greatly" inspired, 17% that they were inspired "to some extent" and just 2.5% that they were inspired "only slightly" by foreign ones. None of the stakeholders surveyed stated that foreign initiatives were not a source of inspiration. In their comments, stakeholders noted that initiatives originating in the United States and Europe had the most effect on the development and application of domestic legal frameworks in the Latin American and Caribbean countries.

[39] A. Bradford, *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, 2020.`

To what extent do regulatory approaches in foreign countries and regions such as the European Union or the United States inspire national initiatives on Internet governance and regulation in Latin America and the Caribbean?



Source: Internet & Jurisdiction Policy Network and Economic Commission for Latin America and the Caribbean (ECLAC).

Between them, the stakeholders identified five reasons for this influence: (i) the social and cultural affinity between the United States, Europe and Latin America and the Caribbean and the similarities between their legal systems, making decision-makers readier to seek inspiration from these sources; (ii) the global nature of the Internet, which creates pressure for harmonization and makes it important to look at approaches outside the region; (iii) international treaty obligations, which encourage consideration of global solutions; (iv) the belief that countries outside the region are more experienced with digital technologies and more closely acquainted with the problems they may bring; and (v) the fact that not all countries have the technical capacity to deploy and implement such regulations, which makes them receptive to international technical cooperation mechanisms through which international initiatives and approaches can operate, helping with implementation. Accordingly, the overarching trend is that Latin America and the Caribbean's domestic Internet governance and regulation initiatives are inspired by foreign approaches.

As one of the stakeholders surveyed mentioned: "There are always fashions and the need to follow trends. There is great awareness today of topics such as cybersecurity, personal data and privacy, for example. Yet not everything is always copied from legislation elsewhere. There have been bilateral efforts: Mexico-European Union, Argentina-European Union. The Chilean Net Neutrality Act was pioneering. The Brazilian Internet Bill of Rights was also pioneering. Either way, the debate is global."

1. Policy initiatives have been proliferating as the appetite for regulating cyberspace increases

There is now a general consensus that some regulation is needed for the Internet. However, there is less of a consensus when it comes to the kinds of complexities regulation can bring. As the *Internet & Jurisdiction Global Status Report 2019* points out, the question is not so much whether the Internet should be regulated, as how and by whom. Globally, there has been an increase in forms of regulation that may include international treaties, domestic laws, administrative regulations, judicial decisions, codes of conduct, domestic or international guidelines, declarations, technical standards, conventions, company and community policies and contractual obligations. These initiatives have created an intricate patchwork of normative frameworks, some of which lack legal standing but nonetheless impact the policy landscape.

Countries in the Latin America and Caribbean region are having to grapple with this multitude of initiatives, not all of their own making. Three major phenomena can be identified among stakeholder responses.

Firstly, there are the compliance challenges that enterprises face when striving to understand the applicable legal framework. Therefore, the first question that needs to be answered is: which national legislation is applicable to a specific case?

Secondly, regulations may create legal uncertainty just by being complex and multilayered. Even once the applicable national legislation has been identified, a plethora of legal instruments such as laws, decrees, ordinances, judicial decisions and other legal sources might make it harder to navigate the country's legal framework.

Thirdly, regulatory actions can have unintended consequences. Such consequences might arise because the balancing of different rules and rights does not necessarily have a predetermined outcome. This is the case with requests for electronic evidence from a cloud service provider, as the data may be covered by different laws depending on where they are stored. It may also happen that an application infringes some national rules and the effects of sanctioning the company responsible for the infringement are felt far beyond a country's borders. The blocking of the messenger application WhatsApp in Brazil, which affected users in Argentina and Chile, is an illustration of this (app blocking is further discussed in section V.B.4).

A profusion of regulations may solve some problems, yet it is itself a source of others. The majority of stakeholders seem to be of the opinion that there should be more coordination and cooperation around Internet policymaking in Latin America and the Caribbean and that certain topics are more regulated than others.

2. Legislative and judicial inspiration: cross-fertilization or imitation?

The profusion of national regulatory initiatives may hide the extent to which foreign legislation and judicial decisions spark national and regional debates in Latin America and the Caribbean. Domestic efforts may mimic, imitate or directly copy approaches and rationales originating overseas. The literature review and the input from the stakeholders surveyed suggest there is a fine line between cross-fertilization and imitation.

This overarching trend of imitation is exemplified by many cases in different areas of Internet regulation where an external effort has resulted in domestic or regional initiatives.

- This has been the case with the discussion about net neutrality in the United States, with the approach of the Federal Communications Commission (FCC) providing the basis for the debate on the matter all over Latin America and the Caribbean.[40]
- The European Court of Justice ruling in the Costeja case affirming a "right to be forgotten" has divided experts, countries and courts in Latin America and the Caribbean (see section IV.A.5 for more on this topic).
- The approval and subsequent entry into force of the European Union General Data Protection Regulation (GDPR) has prompted many countries either to adopt new legislation or to embark on a reform of their data protection regime. No fewer than four laws on data protection have been approved since 2016 (the year the GDPR came into force), and countries such as Argentina, Chile, Colombia and Uruguay have either initiated reviews or reformed their data protection legislation. Some countries have also decided to bring in new general data protection legislation, including Barbados, El Salvador and Jamaica, to name just a few.

The recent adoption of the new European Union Directive on Copyright stimulated discussion about platform regimes for third-party copyright violations (see section IV.C.2), with impacts already being felt in Latin America and the Caribbean.

This influence is having both positive and negative consequences in the region. On the one hand, stakeholders have pointed out that they serve as a harmonizing tool: by making initiatives in the countries similar to those elsewhere, they are having a coordinating effect. Interestingly, initiatives in Latin America and Caribbean countries might be influencing others within the region as well, increasing the consonance between different countries.

Stakeholders nonetheless expressed concern that, in some circumstances, foreign solutions were not appropriate to the social, economic and cultural context of the region. One mentioned that even if the solutions were sound, they might not be applied at the optimal level. The institutions in charge might lack the resources or authority to achieve the policy objectives for which they were intended.

A final consideration is that if the rationale underpinning the foreign initiative is contentious or invasive, its adoption in the region may have a similar effect, potentially leading to conflict.

[40] Intervozes - Coletivo Brasil de Comunicação Social/Derechos Digitales, *Neutralidad de red en América Latina: reglamentación, aplicación de la ley y perspectivas. Los casos de Chile, Colombia, Brasil y México*, São Paulo/Santiago, 2017.

D. Concerns over international influence and normative plurality

In many areas of law, domestic legislation is still the main form of regulation. For the Internet, however, it can hardly be said to be the only element regulating and guiding online conduct. Other factors such as international agreements, foreign regulatory initiatives (with and without extraterritorial effects), technical and industry-specific standards, national and international guidelines, enterprises' terms of use and service, community guidelines and architectural decisions (coding) weigh significantly on the online environment as well.

Cyberspace as a network is influenced and impacted by its multiple elements. Rapid circulation ("virality") is not only a feature associated with videos, images and pieces of information. A plurality of normative initiatives may cause a regulatory butterfly effect on the Internet, impacting online conduct far and wide.

As mentioned in the *Internet & Jurisdiction Global Status Report 2019*, a pyramidal regulatory model[41] with hard regulations issued by the State cannot account for the profusion of normative initiatives and their relative impact. In the Latin America and Caribbean region, countries are both attracted to and sceptical of foreign initiatives. What cannot be denied is that a plurality of efforts, not confined to States or the region itself, are influencing and governing online conduct.

1. Rules are set for (and by) large and well-established international actors

The stakeholders interviewed and surveyed pointed out that not all initiatives had an equal impact and not all actors the same standing in the decision-making process. They emphasized that, in many circumstances, bigger States and companies had more of a voice and greater influence in setting rules for the Internet than smaller ones.

Normative initiatives seem to suffer from a gravitational pull towards bigger actors. The bigger the actor, the more strongly the rules are moulded to its ambitions. Norms seem to be designed to meet the interests of larger nations and enterprises and are less adapted to the circumstances of SMEs or businesses in smaller or less developed countries.

The majority of stakeholders regard this trend as a barrier to SMEs and companies in smaller States competing internationally. Some interviewees mentioned that most smaller nations and enterprises did not have the resources or human capital necessary to comply with complex sets of regulations.[42]

As for cross-border transactions and international initiatives, despite some recent successes, companies from the region are still substantially affected by the lack of harmonization and coordination of efforts. Latin American and Caribbean companies that act transnationally tend to be financed by foreign venture capital or acquired by better-capitalized foreign companies.

This situation is reflected in the survey, with the majority of stakeholders taking the view that cross-border legal challenges affecting the Internet are a barrier for SMEs in the region.

2. The growing role of company norms: the "constitutional" status of terms of service

Companies, particularly platforms, set their own rules to regulate online behaviour. It is widely acknowledged that the choice of architecture (code) impacts and regulates the conduct of actors online and can affect what online activity is possible. Without a "like" button, users cannot express their satisfaction or lack thereof with some online comment, photo or video.[43] If a message can only

41 F. Ost and M. van de Kerchove, *De la pyramide au réseau ? : pour une théorie dialectique du droit*, Brussels, Université Saint-Louis - Bruxelles, 2002.
42 S. Hubbard, "Fake news is a real antitrust problem", *Antitrust Chronicle*, vol. 1, No. 3, December 2017.
43 See, for example, SPIEGEL International, " 'Like' button battle: Facebook agrees to voluntary privacy code", 8 September 2011 [online] https://www.spiegel.de/international/germany/like-button-battle-facebook-agrees-to-voluntary-privacy-code-a-785190.html.

be forwarded to one person rather than five or twenty, this is a disincentive to spread information (and disinformation).[44] These are just two examples of how code can impact online conduct.

Yet code is only one of the dimensions in which platforms influence behaviour. Terms of service and community guidelines provide a normative basis for Internet service providers to act as regulators and to police cyberspace. Depending on the platform, they may be sophisticated enough to create institutions that resemble those of a State.[45] Facebook very recently instituted a parallel quasi-judicial body called the Oversight Board that will function as an appellate body for its content moderation decisions.[46] E-commerce platforms have dispute settlement mechanisms, extending to copyright protection.[47] Reddit allows communities to draw up their own set of rules and advises them to have active moderators and appeals procedures.[48] The list of platforms and their actions resembling those of State institutions is growing.

The above-mentioned initiatives have given rise to terms of service that resemble constitutions. Despite being company norms, they appear to be the first line of recourse. If online conduct is considered offensive or harmful, actions by platforms are expected, and they are based chiefly on their terms of service. At the same time, platforms are increasingly affirming users' rights in an almost "constitutional" way.

These trends are having a number of overarching consequences. The first (discussed in section IV.A below) is that platforms are being called on to take more responsibility for what happens inside their domains. The second is that they are able to act across jurisdictions, since rules of conduct are not limited by States' frontiers and a company can change the terms for all its platforms across all countries or a selection of them. The third is that companies can agree amongst themselves on particular common standards and implement them in a coordinated fashion, without the need for State coordination.[49]

There is another set of implications: these company norms lack any public or democratic approval process and can potentially clash with national regulations. In Latin America and the Caribbean, there has been more than one such clash. The case that has caught international attention has been one regarding "stay-up orders", judicial decisions that require platforms to keep speech online, even if it allegedly violates terms of service.[50] On the positive side, these company norms may facilitate harmonized cross-border standards. Transnational application of them leads to international discussion and may prompt a coordinated or harmonized response. However, the stakeholders surveyed drew attention to the lack of transparency and clarity in the setting of these terms. In the comments, one stakeholder noted that the global DNA of such terms of service —set up by mainly multinational platforms— may not be well-prepared or flexible enough to encompass the diversity and idiosyncrasies present in local realities, particularly in smaller and developing nations such as those of Latin America and the Caribbean. There could be said to be a risk that the "constitutions" of global platforms may not be inclusive enough for the local realities of smaller countries.

44 This is a reference to the changes the messenger app WhatsApp has made to its architecture to limit the opportunities for resending messages that have already been forwarded many times. See *The Guardian*, "WhatsApp to impose new limit on forwarding to fight fake news", 7 April 2020 [online] https://www.theguardian.com/technology/2020/apr/07/whatsapp-to-impose-new-limit-on-forwarding-to-fight-fake-news.

45 A. Chander, "Facebookistan", *North California Law Review*, vol. 90, 2012. See also R. MacKinnon, "Facebookistan and Googledom", *Consent of the Networked: The Worldwide Struggle for Internet Freedom*, Basic Books, 2012.

46 See [online] https://about.fb.com/news/2020/05/welcoming-the-oversight-board/.

47 See [online] https://www.mercadolivre.com.br/brandprotection/enforcement.

48 See [online] https://www.redditinc.com/policies/moderator-guidelines-for-healthy-communities.

49 This has recently been done through a joint statement against the spread of misinformation in relation to the COVID-19 pandemic. See [online] https://techcrunch.com/2020/03/16/facebook-reddit-google-linkedin-microsoft-twitter-and-youtube-issue-joint-statement-on-misinformation/.

50 See Waqas, "Brazil will sue Facebook for blocking picture of indigenous woman", HackRead, 20 April 2015 [online] https://www.hackread.com/facebook-blocking-brazil-indigenous-picture/. For an analysis of stay-up decisions, see D. Keller, *Dolphins in the Net: Internet Content Filters and the Advocate General's Glawischnig-Piesczek v. Facebook Ireland Opinion*, Stanford Center for Internet and Society, 2019.

E. The role of territoriality and the exercise of sovereignty are different in a global network

The concept of territoriality has been difficult to reconcile with some of the features of cyberspace. Territoriality is supposed to fulfil the function of a guiding principle, both to provide grounds for a State to exercise power and to define the geographical extent of that power, placing a topographical limit on State sovereignty.

The Internet, on the other hand, was developed to be borderless or at least border-neutral, so that information can flow despite geographical barriers. Hence, a territorial jurisdiction loses its precise meaning in a cyberspace that was not supposed to mirror the underlying political State divisions of the physical world. Countries cannot, however, ignore the fact that certain online actions impact both property and people located in the physical world and within their own allotted territory. The increased interconnection of the physical and virtual worlds has blurred the line between the two, leading to more geographically extensive State regulations.

States have sought to use the location of persons, devices or servers as territorial anchor points to justify the exercise of online jurisdiction. To a certain extent, jurisdiction is attached in relation to acts that may be legally linked to more than one territory and potentially to more than one jurisdiction. The consequence is that in some cases States have either overreached, attaching jurisdiction where there is only a tenuous connection, or underreached, meaning that certain victims are left without recourse.

Latin America and the Caribbean has a unique relationship with the legal concept of territoriality, being considered the birthplace of the principle of non-intervention.[51] It is not an accident that the most famous definition of "State" comes from a convention drafted in the region, the Convention on Rights and Duties of States of 1933. The Convention defines territory as one of its constituent elements.[52] This context has implications for the understanding of certain types of subject-matter as being within the purview of the domestic jurisdiction of a State. It is against this background that States in the region conceptualize territorial jurisdiction, including online jurisdiction.

The fact that Latin America and the Caribbean is the birthplace of the non-intervention principle colours the understanding of jurisdiction there. The region's approach is illustrated by the treatment of foreign companies that appear not to follow domestic laws. The escalation to app blocking or arresting company executives seems to be a consequence of this notion: a State's law has to be respected within its territory. Similarly, with e-evidence, it appears that national law enforcement agencies are puzzled when they do not have access to data on crimes committed within their borders.

In some circumstances, the rationale for jurisdiction is territorially dependent and independent at the same time. There is an appetite for regulating what happens in or impacts Latin American and Caribbean territory, but jurisdiction may be extended beyond the region thereafter, examples being extraterritorial application of data protection regulations and conditions for cross-border personal data transfers. In defamation and content moderation cases, take-down orders often focus on removing speech or even closing down accounts, with a global and not only local reach.

There is an overarching trend for jurisdiction to focus more on the location of behaviour or conduct than on the location where data are stored. However, the location and movement of data are still sometimes relevant factors to be considered.

1. The increasing extraterritorial reach of national laws

States are increasingly irked by the way the fluidity of the online environment, in which there are no clear barriers to cross-border interaction, is exploited to circumvent domestic legislation. Understandably, they want regulation to discourage such behaviour. The rationale is that laws should be respected online as much as in the offline world. Each State considers itself entitled to govern

[51] For an overview of the development of the principle, see J. P. Scarfi and A. Tillman (eds.), *Cooperation and Hegemony in US-Latin American Relations*, New York, Palgrave Macmillan, 2016. For one of the first statements of it, see: A. Alvarez, "Latin America and international law", *American Journal of International Law*, vol. 3, No. 2, April 1909.
[52] See [online] https://treaties.un.org/doc/Publication/UNTS/LON/Volume%20165/v165.pdf.

what happens and what is available online. There is a perception that if behaviour impacts or has an effect on a State's territory, then it must fall within that State's jurisdiction.

In the absence of binding international or regional instruments, many States, including States in the region, end up claiming wide jurisdiction either through new laws or through the expansionary interpretation of existing ones. In Latin America and the Caribbean, this overarching trend is particularly visible in the areas of data protection (section IV.3) and access to electronic evidence by law enforcement agencies (section IV.2).

In the view of the stakeholders surveyed, this approach to regulation (increasing the geographical reach of national laws) can lead to either arbitrary enforcement or frustration. The latter arises because actual enforcement might be difficult or nearly impossible in certain cases. Regarding the former, people may be surprised to be prosecuted in a faraway country for violating a local law unawares. Another aspect is that the scope of regulation may be so broad that it can be challenging to determine which behaviours will be encompassed, in which case enforcement may seem discretionary.

A parallel global trend picked up by countries in Latin America and the Caribbean is to enact regulations with steep fines for non-compliance. Threats of sanctions are used to encourage compliance. The concern expressed by Latin American and Caribbean States is that, carrying less prohibitive sanctions, their laws will be an afterthought and may be ignored by international players. The difficulty with this rationale seems to be that it motivates other countries to do the same and compete to impose the highest fines and the harshest sanctions, impeding the flow of data and business.

2. Extraterritoriality brings enforceability challenges

Broad jurisdictional claims can be difficult to enforce, and the broader they are, the harder enforcement may be. Claiming jurisdiction is not the same as being able to enforce it. A State applying its laws on the basis of a tenuous link – that between conduct and the State itself – may find it difficult to have its actions accepted as legitimate. Similarly, affirming jurisdiction without being able to enforce it may be detrimental to perceptions of the efficacy of the regulation and run counter to the objective of encouraging compliance.

Asserting broad claims of jurisdiction may, however, be a strategy in itself. It makes it clear that a particular issue affects an important societal value, i.e., that the State cares about it. This strategy may be intended as a way of laying down jurisdictional lines and articulating a point of view on the extent of a State's interests.

A State may also see a need to rely on cooperation with another State. Real assets or data might be in another country and hence out of the enforcing country's reach or not realistically accessible to it. This creates the potential for regulatory clashes, constituting both a challenge to inter-State cooperation and an opportunity to find mutually acceptable solutions.

This is reinforced by the fact that once jurisdiction is asserted, the country has to be willing to see it reciprocated: other States may claim equally broad jurisdiction. Latin America and the Caribbean has a tradition of international reciprocity. Thus, foreign affirmations of jurisdiction are likely to be matched by the region's countries.

Several stakeholders pointed out that not all countries in Latin America and the Caribbean had the same capacity to extend their jurisdiction beyond their borders. They noted the differences in size, economic weight and power between the countries in the region and highlighted the potential obstacles to efforts to match outside action. Hence, an assertion of extraterritorial or broad jurisdiction by a Latin America or Caribbean country might be found wanting when it comes to enforcement.

This also works the other way. Some of the stakeholders surveyed mentioned that smaller nations might be powerless when bigger nations flexed their legal muscles. The online gambling case brought by Antigua and Barbuda before the World Trade Organization (WTO) is an illustrative example.[53] Although the dispute was ultimately decided by the Appellate Body in favour of the United

[53] See [online] https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm.

States, it would have been challenging for the Caribbean nation to assert its rights and safeguard its businesses against a North American law with cross-border effect.[54] In actuality, even if legal from the standpoint of WTO, the outcome ended up being a "market destroying measure"[55] and the service could no longer continue.

F. Intermediaries are being expected to play new roles

Intermediaries are very diverse: search engines, social media networks, e-commerce or streaming platforms, digital payment mechanisms and many other actors that facilitate the most well-known activities online. As the Internet became more mainstream, intermediaries gained in importance, becoming integrated into the routine of Internet users. They have become the conduits connecting different people and businesses and facilitating transactions. The result has been a change in the morphology of cyberspace: once a largely self-organized wilderness, it has now become a multiplicity of organized and more or less walled gardens.

The degree of dependence on Internet intermediaries is disputed. It is clear, though, that they account for a significant share of traffic, and from a user-centric point of view they simplify Internet use. With this newly achieved centrality, a discussion has emerged on the roles of these actors and their responsibility for what happens in cyberspace, the view being that intermediaries should share more of the burden of overseeing what happens online.

1. Increasing responsibility is being placed on private operators

Traditionally, countries have considered Internet intermediaries to be deserving of legal protection because of their important function as crossroads, gateways or meeting places for Internet users. However, a number of situations involving child pornography, explicit violence, terrorism, disclosure of private images ("revenge porn"), disinformation campaigns ("fake news") and large-scale copyright infringements, among others, have exposed the shortcomings of such an approach if followed without safeguards.[56]

Countries throughout Latin America and the Caribbean have been moving in the direction of assigning a larger role in Internet governance to private operators. The issue has become more important to countries in the region, particularly in the fields of hate speech and harmful speech, disinformation (chiefly in the context of elections), copyright infringements, the sale of counterfeit goods, and privacy and data protection.

Intermediaries end up performing quasi-State functions, e.g., in their quasi-judicial role of deciding when to take down content and suspend or close the accounts of repeat copyright offenders. It is they who are called upon to decide on the legality of content, whether it is political satire (allowed) or defamatory speech (not permitted), for example. They may take such actions voluntarily in accordance with their terms of service or under the compulsion of domestic regulation and court decisions.

Legal regimes that until recently shielded intermediaries from prosecution have given way to more nuanced approaches.[57] In Latin America and the Caribbean, strategies have varied between countries. The Bolivarian Republic of Venezuela and Cuba seem to be among the strictest, having enacted legislation that creates obligations for Internet service providers (ISPs) to monitor and "regulate" speech. They also provide extensive powers for public agencies, which may even shut down intermediaries that flout their authority.[58] Other countries have sought to regulate specific areas such as hate speech, making intermediaries liable if they fail to take down speech deemed illegal. Other approaches have been to issue codes of conduct or enter into administrative agreements with intermediaries.

54 A. Chander, "Freeing trade in cyberspace", *The Electronic Silk Road: How the Web Binds the World Together in Commerce*, Yale University Press, 2013.
55 See D. Svantesson, *Private International Law and the Internet*, third edition, Alphen aan den Rijn, Wolters Kluwer, 2016.
56 G. Frosio (ed.), *Oxford Handbook of Online Intermediary Liability*, Oxford University Press, 2020.
57 As an example, the Brazilian Internet Bill of Rights (Law No. 12965 of 2014) enshrines a safe harbour provision. Chilean Law No. 20430 of 2010 reformed the country's copyright legislation to provide a safe harbour from third party liability in respect of Internet copyright.
58 See [online] http://www.leyresorte.gob.ve/wp-content/uploads/2012/07/Ley-de-Responsabilidad-Social-en-Radio-Television-y-Medios-Electrónicos.pdf; and Office of the Special Rapporteur for Freedom of Expression, *Special Report on the Situation of Freedom of Expression in Cuba*, Organization of American States (OAS), 2018.

Some of the stakeholders surveyed emphasized that this trend could have cross-border implications. These are particularly acute in cases where companies are left with no choice but to comply with one State's regulation (including judicial orders) at the risk of violating the legal regime of another if there is a conflict of laws. The consequences might not be easy to foresee, especially for a Latin American or Caribbean country. Enterprises may implement a strictest common denominator approach, potentially limiting freedom of expression in the region, or, when pressed, may choose not to implement local laws, which could impact domestic legal legitimacy.

Stakeholders noted that requiring platforms to play this role as Internet gatekeepers could erode the legitimacy of and confidence in State institutions and the sense of justice, while in election situations it could impact the democratic process. It means that companies are put in charge of what information can circulate and how. Yet disinformation can also have a detrimental effect on democratic elections.

2. Intermediaries are increasingly being asked to provide data to support investigations

When telephones turned into a major means of communication, line tapping became an important investigative resource for law enforcement agents, giving them access to the actual communications of suspected criminals and providing a way to learn how crimes were planned, when they would happen or how they had been discussed. Even *mens rea* could be better determined by listening in on conversations that would have been private were it not for clues connecting them to crime investigations.

The Internet has changed the situation. A myriad of different services perform the same function, allowing information on illegal conduct to be shared whether it occurs online or offline. The techniques of the telephone age do not transfer well to the Internet. Support for investigative functions has moved from the intermediaries providing the infrastructure to those directly providing certain very popular Internet applications. These Internet intermediaries are the ones capable of providing access to information. This raises at least four major issues: access to stored data; access to bulk data (general data or data troves); the use of cryptography; and the categories of data services that companies might be obliged to collect and provide.

Since many intermediaries are extending their reach globally, all such issues tend to have a cross-border component. As for access to data, different domestic rules govern when and how law enforcement officers may be given this. If they are stored overseas, the challenges tend to be even greater. In order to bypass the complexities of international judicial cooperation, countries in the region are exploring the idea of placing obligations on Internet intermediaries. These include: (i) data localization; (ii) a physical presence in the country or appointment of a representative; and (iii) the obligation to provide access to data, remote or otherwise. The last two points are the subject matter of article 32 of the Fake News Bill approved by the Brazilian Senate, for instance.[59]

Intermediaries are also being required to provide access not only to specific data, but to large volumes of data. In many circumstances, they are being asked to make a whole haystack available in the search for an ill-defined needle. Such requests have been made, unsuccessfully, in relation to mobile phone tower location data in the United States, for example.[60] In Latin America and the Caribbean, however, there have been instances of high courts granting such broad requests, even if this is not the standard response.[61] The COVID-19 pandemic has extended the scope of such requests from the field of criminal investigations to the application of public policy (at least during the pandemic).[62]

---

59 The bill also contained a data localization obligation, but this was dropped before the vote in the Senate. See [online] https://www.bloomberg.com/news/articles/2020-07-01/brazil-s-senate-approves-draft-bill-to-rein-in-on-fake-news. For the original text of the bill (in Portuguese) and discussion of it, see [online] https://www25.senado.leg.br/web/atividade/materias/-/materia/141944. For a discussion on the impact of art. 32, see C. A. Souza and C. Perrone, " 'Fake news' e acesso a dados armazenados no exterior", JOTA, 2020 [online] https://www.jota.info/coberturas-especiais/liberdade-de-expressao/fake-news-e-acesso-a-dados-armazenados-no-exterior-30062020.

60 Supreme Court of the United States, *Carpenter v. United States* [online] https://www.scotusblog.com/case-files/cases/carpenter-v-united-states-2/.

61 See [online] https://www.telesurenglish.net/news/Google-Must-Share-Data-Related-To-Marielle-Franco-Murder-Case-20200827-0004.html.

62 M. P. Canales, *La herejía tecno-optimista florece en pandemia: un repaso crítico a las tecnologías disponibles*, Derechos Digitales, 2020 [online] https://www.derechosdigitales.org/wp-content/uploads/herejia-tecno-optimista.pdf.

The obligations imposed on intermediaries in support of investigations have created another difficult dilemma. Several intermediaries have used or intend to use more privacy-preserving techniques involving different types of cryptography, including end-to-end (E2E) cryptography. It could thus become harder (or sometimes even technically impossible) to comply with such a role, as information may not be accessible.

In these circumstances, Latin American and Caribbean countries, like many of their international counterparts, are seeking to oblige intermediaries either not to use cryptographic techniques or to provide a key. They are even finding other ways to gain access to information, such as using an unidentified interloper. This is similar to what would happen in a wiretapping situation, but with potentially much wider consequences, since all conversations could be listened in on, not only specific ones, and this could be done by anyone capable of accessing them, not only law enforcement agents.

Another strategy proposed in the region has been for messaging services to collect more information so that this is accessible for future investigations. Two formats have been mooted: either requesting the identification of individuals, thus restricting online anonymity, or requiring intermediaries to trace certain categories of message, particularly those with widely distributed content.[63]

All such new roles require substantial arrangements to balance rights and may have a significant impact on the actions of Internet intermediaries, particularly when they provide services globally. Experts who were interviewed pointed out the need to harmonize the legitimate needs of law enforcement with the organization of the Internet, user rights and the global reach of Internet service providers.

3. Transparency is essential to enhance trust, but implementation varies

The greater roles assigned to Internet intermediaries have also increased demands for more transparency regarding their procedures, decisions and actions. The need for greater moderation of content or behaviour by platforms also creates incentives for them to rely on automated decision-making algorithms in order to meet expectations that controversial content and behaviour will be analysed. This is a scenario in which discussion of transparency in procedures, criteria and the justifications for decisions becomes more important.

The issue has now been addressed to some extent in relation to data protection and discussion of the right to an explanation when automated moderation takes place. Many companies themselves issue transparency reports and set out some of their procedures in their terms of use or community standards.[64]

The question of whether this should be dealt with through binding regulations or through codes of conduct, co-regulation or self-regulation is still open for discussion. In Latin America and the Caribbean, several civil society organizations are of the view that more transparency is of the essence. Countries have addressed this by proposing binding rules,[65] but these have to be carefully crafted, as they may have a detrimental impact on the development of new solutions and impose a burden of high costs and bureaucracy on nascent companies and start-ups.

As a principle, then, transparency is important for the development of sound Internet governance in Latin America and the Caribbean. If it is to be imposed on Internet intermediaries, however, consideration has to be given to the different variables at work in the region, intermediaries' capacity to deal with it and the effects on the developing innovation and start-up environment.

63 See [online] https://www.eff.org/deeplinks/2020/06/5-serious-flaws-new-brazilian-fake-news-bill-will-undermine-human-rights. See also [online] https://blog.mozilla.org/netpolicy/2020/06/29/brazils-fake-news-law-harms-privacy-security-and-free-expression/.
64 See [online] https://rankingdigitalrights.org/.
65 The Fake News bill proposed in Brazil contains provisions on transparency for social networks and messaging services. For the text of the bill (in Portuguese), see [online] https://www25.senado.leg.br/web/atividade/materias/-/materia/141944.

4. Growing attention is being paid to due process in content moderation activities

Another significant aspect of the changing role of intermediaries is the importance of providing opportunities for content moderation decisions to be contested. The speed and pervasiveness of Internet services mean that subsequent review by the judiciary may either be inaccessible to users or cause significant hardship or damage. Making private actors, namely Internet intermediaries, answerable for their actions or providing a way for users to protest, appeal or defend themselves may prove crucial for the preservation of important societal values and fundamental rights (further dealt with in section V.A.5).

It is certainly the case that, as with transparency, legally mandating such challenge procedures may lead to difficult situations in which not all intermediaries will be able to cope with the demands placed on them. It is important, however, for a certain level of review to be available in principle, particularly from the standpoint of protecting citizens in Latin America and the Caribbean. One of the experts surveyed noted that the region tended to consume technologies developed outside it and that these were not adapted to the circumstances of Latin American and Caribbean citizens. Providing a space for results to be contested and reviewed is thus a way to make services sounder and more compatible with the needs of individuals and more consistent with their rights and the context they live in. It should be seen as an opportunity for adaptation.

The consequences of such new roles for intermediaries, be they changes in liability or further regulation and the imposition of new obligations on them, raise new cross-border issues in their turn, including questions about how to better preserve human rights and the global nature of the Internet, with the opportunities for innovation it provides. Latin American and Caribbean countries, like other States around the globe, have to balance the advantages and disadvantages of the new roles of Internet intermediaries with the methods used to mitigate risks.

CHAPTER II

MAJOR TOPICAL TRENDS IN LATIN AMERICA AND THE CARIBBEAN

A. Expression

1. Fake news and disinformation

1.1. Regulatory action is increasing

The Internet has lowered barriers for citizens wishing to inform and express themselves. At the same time, disinformation –mass dissemination of information that is either false, out of context or intended to cause harm– has also become more prevalent.

The speed, volume and "virality" of information flows make them hard to control. The use of personal data in microtargeting campaigns[66] and the effect some algorithms have of creating filter bubbles[67] or echo chambers, with people only seeing, hearing and listening to what they want or expect, increases the need for access to reliable information. At issue is people's ability to form their thoughts, ideas and opinions without being unduly influenced.

This situation is particularly acute during elections. The stakeholders surveyed repeated many of the concerns international actors have conveyed. Disinformation may lead to polarization,[68] information silos, voter suppression[69] and manipulation of the political agenda, among other negative impacts.[70] One stakeholder mentioned that attacks and manipulation were the work of both foreign and domestic actors using the network to intentionally sow division and polarization.

As one interviewed stakeholder put it:

> "Election interference is a major threat to the universal right of people to take part in the democratic process. This is an issue that both governments and technology companies are grappling with to meet the challenges of the latest election meddling tactics and technologies. It is worth noting that attacks and coordinated manipulation are no longer coming from malign foreign powers alone. Increasingly, interference in election processes is used by domestic actors as a way of sowing division and polarization in both authoritarian and democratic contexts."

Latin American and Caribbean countries have responded to these tendencies in a variety of ways. Most of them have followed the trend of producing regulations that either criminalize the spread of disinformation, usually under the heading of so-called fake news, or impose a duty for Internet platforms to be more proactive in their monitoring of speech, often shifting the burden of liability on to Internet intermediaries.

66 See [online] https://datasociety.net/wp-content/uploads/2018/10/DS_Digital_Influence_Machine.pdf.
67 E. Pariser, *The Filter Bubble: What the Internet Is Hiding from You*, New York, Penguin, 2011.
68 C. Sunstein, *Republic: Divided Democracy in the Age of Social Media*, Princeton University Press, Princeton, 2017.
69 A. Mcstay, "Fake news and the economy of emotions: problems, causes, solutions", *Digital Journalism*, vol. 6, No. 2, 2018 [online] https://www.tandfonline.com/doi/full/10.1080/21670811.2017.1345645.
70 Organization of American States (OAS), *Guide to Guarantee Freedom of Expression Regarding Deliberate Disinformation in Electoral Contexts*, 2019 [online] https://www.oas.org/en/iachr/expression/publications/Guia_Desinformacion_VF%20ENG.pdf.

The threat of criminalization has been the strategy used in Peru, for instance, where the Ministry of Justice and Human Rights stated that speech that manipulates citizens in order to obtain a benefit or disturb public order might be punished as a crime.[71] Other countries, including Argentina, Colombia, Costa Rica, Mexico and Uruguay, have initiated public discussions on the matter in order to steer platforms towards integrating fact-checking initiatives into their architecture.[72]

Brazil has widened the array of tactics deployed, with the Supreme Court[73] and Congress[74] having separately initiated investigations into individuals and coordinated networks allegedly spreading hate speech and disinformation. Additionally, a lengthy bill purporting to regulate "fake news" was approved by the Federal Senate on 30 June 2020.[75] In fact, it regulates a wide variety of matters, substantially revising the role played by social media platforms and messaging services. They are now required to track widely distributed ("viral") messages, to require proper identification under certain circumstances, to moderate content, establishing a very detailed defence and appeal procedure, and to provide access to data no matter where it originates or is stored. The bill also proposes the creation of an advisory body and creates stiff sanctions for non-compliance (see section V.A.4 for more on this trend).

There is little doubt that the fight against misinformation has cross-border impacts: companies offering goods and services across borders will have to adapt their policies to deal with these new responsibilities.

1.2 Bots have automated fake news and disinformation

Organic, authentic behaviour may lead to information spreading widely, but when it is coupled with automated tools or "bots", artificially created accounts that are partially or completely controlled by automation software, then the potential to reach a much wider audience increases.[76] These tools also drive traffic (and people's attention) to particular issues and types of information and may foster an artificial sense of popularity and relevance.[77] Hence, automation adds more "acceleration" to the mist of virally spreading information and, for that matter, disinformation.

On the one hand, the use of such automation tools may have a positive impact by pushing important but marginalized ideas and voices to the front of the public debate. On the other hand, though, this very function can be used to manipulate information, amplify its reach, create a sense of support or consensus where there may be none, and obscure important facts.[78] In other words, these tools may be amplifiers of disinformation.[79]

The use of bots and automation on global platforms raises a number of other cross-border issues. From the standpoint of origin, such tools may be foreign. Bots may be developed in foreign countries, or they may function from outside the targeted country, perhaps within a coordinated international network.

---

71 Peru, *Gestión*, "Personas que difundan noticias falsas podrían recibir hasta 6 años de prisión", April 8, 2020 [online] https://gestion.pe/peru/coronavirus-peru-personas-que-difundan-noticias-falsas-podrian-recibir-hasta-6-anos-de-prision-segun-minjus-ministerio-de-jusiticia-estado-de-emergencia-cuarentena-nndc-noticia/?ref=gesr.

72 The public fact-finding platform Confiar in Argentina is an example. See [online] www.argentina.gob.ar/noticias/confiar-la-plataforma-oficial-para-combatir-la-infodemia. Also, the fact checking organization Chequeado, created in Argentina, has coordinated the LatamChequea coalition with 35 organizations across Latin America. See [online] https://chequeado.com/latamcoronavirus/.

73 Federal Supreme Court of Brazil, "Inquiry 4781" [online] http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=444198&ori=1.

74 Federal Senate of Brazil, "Comissão Parlamentar Mista de Inquérito - Fake News" [online] https://legis.senado.leg.br/comissoes/comissao?0&codcol=2292.

75 See [online] https://www.bloomberg.com/news/articles/2020-07-01/brazil-s-senate-approves-draft-bill-to-rein-in-on-fake-news. For the original text of the bill (in Portuguese) and discussion of it, see [online] https://www25.senado.leg.br/web/atividade/materias/-/materia/141944.

76 C. Shao and others, "The spread of low-credibility content by social bots", *Nature Communications*, vol. 9, 2018 [online] https://www.nature.com/articles/s41467-018-06930-7.

77 J. Bayer and others, "Disinformation and propaganda – Impact on the functioning of the Rule of Law in the EU and its Member States", *HEC Paris Research Paper*, 2019 [online] http://dx.doi.org/10.2139/ssrn.3409279.

78 P. Howard, *How Political Campaigns Weaponize Social Media Bots*, 2018 [online] https://spectrum.ieee.org/computing/software/how-political-campaigns-weaponize-social-media-bots. See also P. Howard, *The Lie Machines: How to Save Democracy from Troll Armies, Deceitful Robots, Junk News Operations*, and Political Operatives, Yale University Press, 2020.

79 S. Bradshaw and P. Howard "Troops, trolls and troublemakers: a global inventory of organized social media manipulation", *Oxford Computational Propaganda Research Project*, 2017 [online] http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf.

In Latin America and the Caribbean,[80] for instance, there have been reports of bots using the Cyrillic script during Brazilian elections, which would appear to indicate a Russian origin.[81] In another instance, Brazilian bots have been found to have been used in a Mexican presidential election.[82]

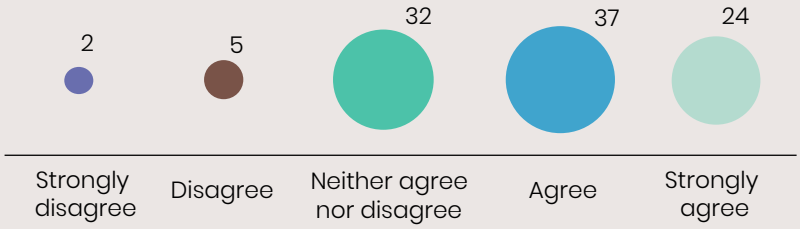
Global platforms have also uncovered networks of automated accounts engaging in what is called "coordinated inauthentic behaviour". In significant instances, the behaviour originated in one country but had its focus in another.[83]

A second issue concerns investigations into such foreign use of automated tools or bots. In many instances they may violate electoral and even criminal laws on the spreading of disinformation. Important information may be held by foreign platforms that may or may not have a legal representative in the country concerned. Data may also not be readily available or may be stored in servers overseas.

While attention has generally been on how to deal with these techniques at the national level, international aspects may have a large impact on future regulations to curb fake news and disinformation. They highlight the need for cooperation and coordination in order to find solutions to online disinformation campaigns.

In the 2016 Rio de Janeiro municipal elections, a mix of automated tools and coordinated authentic behaviour was used. A feature called "donate a like" ("*doe um like*") was implemented by a candidate's official campaign. It consisted in a request for people to support the candidate by donating the ability to "like" and share content for a three-month period. Once accepted, a tool would capture the user's profile and password and be used to spread the candidate's content. Thus, real accounts belonging to real people would follow and, under a coordinated automated regime, participate in a candidate's campaign.[84]

Does the cross-border nature of the Internet facilitate foreign interference with the democratic process?



Source: Internet & Jurisdiction Policy Network and Economic Commission for Latin America and the Caribbean (ECLAC).

2. Defamation

2.1. Cross-border challenges are increasing

Respect and protection for personal honour and reputation are found in the laws of a multitude of countries with diverse cultural backgrounds. As a core common value, defamation is illegal both offline and online. The implementation, interpretation and scope of the concept, however, vary considerably. The Internet has heightened the importance of these legal differences and created more potential for conflict between jurisdictions.

80 For a general report, see Atlantic Council, *Disinformation in Democracies: Strengthening Digital Resilience in Latin America*, 2019 [online] https://www.atlanticcouncil.org/wp-content/uploads/2019/09/Disinformation-in-Democracies.pdf.
81 See [online] http://dapp.fgv.br/en/fgv-survey-dapp-reveals-evidence-russian-robots-2014-presidential-election-campaigns/.
82 See [online] https://horizontal.mx/bots-su-deteccion-y-la-participacion-en-las-campanas-electorales-en-mexico/#_edn1.
83 See [online] https://about.fb.com/news/2020/07/removing-political-coordinated-inauthentic-behavior/. See also [online] https://www.theverge.com/2018/10/25/18021456/twitter-q3-2018-earnings-9-million-mau-decline.
84 D. Arnaudo, "Computational propaganda in Brazil: social bots during elections", *Oxford Computational Propaganda Research Project*, 2017 [online] https://blogs.oii.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2017/06/Comprop-Brazil-1.pdf.

Cross-border challenges arise particularly in three circumstances: (i) when speech published in one country has an impact in another; (ii) when the medium employed for publication is outside the country where the person offended normally lives or works, either because the company providing the service is established in another country or because the servers are; and (iii) when the damage to a person's honour or reputation occurs in more than one jurisdiction.

The *Internet & Jurisdiction Global Status Report 2019* pointed out that this is not a novel development. Because of the potentially global geographical reach of the Internet, cross-border defamation has been a common occurrence online. In the *Dow Jones v. Gutnick* case, for instance, the High Court of Australia had to decide whether publication had occurred where the article was posted online or where it was downloaded.[85] This court was one of the first to understand that an online publication may defame someone across borders.

The matter of damages was not up for determination since the plaintiff had limited his claim to damages experienced in the place where he sued, Australia, which was also where he was primarily concerned to protect his reputation. However, the door was left open for a much broader discussion on whether he could potentially sue in more than one jurisdiction, shopping around for the most favourable courts, and whether he could claim for damages that might have occurred globally in any or all of them. In a sense, the question is whether a reputation can be international and damages should also take account of a potential extraterritorial dimension. Decisions on the matter may potentially interfere with other countries' legal provisions and their citizens' rights. If a court decides to award damages globally, it can potentially take into consideration countries where that speech would not be considered defamatory, indirectly curtailing freedom of expression.

This issue may have further cross-border implications. For example, in Latin America and the Caribbean, requests for damages in defamation cases have often been accompanied by requests for removal or rectification of the content deemed defamatory. Plaintiffs frequently pursue Internet intermediaries, which are then put in the position of having to comply with judicial orders and decide the territorial scope of these.

This was the case with Google's blogger.com service. Colombian[86] and Mexican[87] courts instructed Google to remove blog posts considered defamatory. In Brazil, Facebook was ordered to remove content and take down a whole profile deemed to defame a political candidate.[88] Each of these cases contributes to an understanding that such content may be affected worldwide by domestic court rulings.

The discussion reached the Court of Justice of the European Union in the case of *Glawischnig-Piesczek v. Facebook Ireland*.[89] The question at issue was whether the European Union (EU) Directive on electronic commerce regulated the scope of jurisdiction, authorizing domestic courts to order Facebook to remove content arguably defamatory to an Austrian politician with global effect, or preventing this. The court's answer was not definitive. It stated that the EU directive did not regulate the scope of remedial jurisdiction and that this was for domestic courts to decide, taking into consideration their own domestic laws and international law (see section 5.A.2 for more on the geographical scope of remedial jurisdiction).

A number of other issues concerning defamation have surfaced as well. In the region, there have been cases dealing with the auto-complete techniques[90] used in different Internet services, particularly

85 See High Court of Australia, *Dow Jones and Company Inc v. Gutnick [2002] HCA 56* [online] http://eresources.hcourt.gov.au/showCase/2002/HCA/56.

86 Colombian Constitutional Court rules that Google must delete a blogger.com blog that contained defamatory statements. See I & J Retrospect Database [online] https://www.internetjurisdiction.net/publicationsretrospect#article-6369_2017-10.

87 Internet & Jurisdiction Policy Network, December 2017. Mexican Supreme Court rejects Google's argument that Mexican courts do not have jurisdiction over the platform. See I & J Retrospect Database [online] https://www.internetjurisdiction.net/publications/retrospect#eyJ0byI6IjIwMjAtMDMifQ==.

88 See [online] https://olhardigital.com.br/noticia/juiz-manda-bloquear-facebook-em-todo-o-brasil-por-24horas/62909.

89 Court of Justice of the European Union, "Case C-18/18 Glawischnig-Piesczek", 2019.

90 For an interesting analysis of the challenges of auto-complete techniques, see Paul Baker and Amanda Potts, "Why do white people have thin lips? Google and the perpetuation of stereotypes via auto-complete search forms", *Critical Discourse Studies*, vol. 10, No. 2, 2013, pp. 187-204.

search engines.[91] Another issue that has gained prominence is the potential liability of persons merely for supporting (e.g., by "liking") content deemed defamatory or harmful[92] or sharing that content.[93] Lastly, another issue is the extent to which administrators of social media groups or communities such as those of the WhatsApp messaging service should be responsible for moderating content within that group or community.[94]

2.2. Defamation is still a criminal offence in certain countries of the region

In many Latin American and Caribbean countries, defamation is not only a civil matter, but a criminal one.[95] The criminalization of speech that violates a person's reputation is still a widespread legal tradition in the region, even though the Inter-American Human Rights System has condemned it as an undue restriction on freedom of expression.[96] Online defamation can likewise have criminal repercussions, which may be even more concerning in the case of speech during elections, when the suggested remedy should preferably be rectification or the right to a response.[97]

The criminalization of speech harmful to a person's reputation also has a chilling effect on the activities of professional journalists, citizen journalists and bloggers alike, especially in small towns in Latin America and the Caribbean. It is easy for local authorities to severely curtail speech if anyone breaking news or producing reports that might displease them risks their freedom by doing so.

3. Online bullying

Different types of cyberbullying emerge as technology develops.[98] Bullying is traditionally recognized as occurring when there is an offender and a victim subjected to emotional or physical harassment. Bullying by means of electronic technologies, especially the Internet, includes private messages, the creation of websites focused on doing some kind of harm to someone else, online posting of unflattering or inappropriate pictures without permission, and hurtful or unpleasant treatment via mobile phones or online.[99]

Cyberbullying affects as many as 1 in 10 children.[100] According to the International Telecommunication Union (ITU) 2020 "Guidelines on Child Online Protection", most are able to distinguish cyberbullying from joking or teasing online, recognizing that cyberbullying is intended to harm.[101] The *Guidelines for policy-makers on Child Online Protection* recommend the development of appropriate national legislation and affirm that harmonization and coordination at the international level is a key step in

91 There have been rulings on the matter in Brazil. See [online] https://www.migalhas.com.br/arquivos/2014/9/art20140917-05.pdf. The Constitutional Court of Colombia has also decided that search engines are not liable when links to speech deemed defamatory appear among their results. Colombia, Constitutional Court, "Sentencia T-040/13", 28 January 2013 [online] http://bit.ly/1FyIMlk; Constitutional Court, "Sentencia T-453/13", 15 July 2013 [online] http://bit.ly/1R6lHaO; Constitutional Court, "Sentencia T-634/13", 13 September 2013 [online] http://bit.ly/1OyMApE.

92 Regarding the international situation, see [online] https://blog.oup.com/2017/09/traps-of-social-media/. See also [online] https://www.internationallawoffice.com/Newsletters/Litigation/Switzerland/Lenz-Staehelin/Liking-or-sharing-defamatory-Facebook-posts-can-be-unlawful.

93 It was ruled in a Brazilian case that the person could be liable. See [online] https://www.conjur.com.br/2017-nov-10/limite-penal-curtir-compartilhar-publicacoes-ofensivas-redes-sociais-crime.

94 See [online] https://www.uol.com.br/tilt/noticias/redacao/2018/07/17/justica-pode-mirar-administrador-de-grupo-no-whatsapp-em-que-houve-crime.htm.

95 As an example, see the general study conducted by the Committee to Protect Journalists on South American criminal defamation laws [online] https://cpj.org/reports/2016/03/south-america.php. See also the study by the International Press Institute on criminal defamation laws in the Caribbean [online] https://ipi.media/ipi-adds-caribbean-defamation-laws-to-online-database/.

96 Inter-American Court of Human Rights, "Case of Herrera Ulloa v. Costa Rica. Preliminary Objections, Merits, Reparations and Costs. Judgment of July 2, 2004", Series C, No. 107; "Case of Ricardo Canese v. Paraguay. Merits, Reparations and Costs, Judgment of August 31, 2004", Series C, No. 111; "Case of Kimel v. Argentina. Merits, Reparations and Costs. Judgment of May 2, 2008", Series C, No. 177; "Case of Tristán Donoso v. Panama. Preliminary Objections, Merits, Reparations and Costs. Judgment of January 27, 2009". Series C, No. 193; "Case of González Medina and Family v. Dominican Republic, Judgement of February 27, 2012"; "Case of Vélez Restrepo v. Colombia, Judgement of September 3, 2012"; and "Case of Fontevecchia and D'Amico v. Argentina, Judgement of November 29, 2011".

97 See [online] https://www.oas.org/en/iachr/expression/publications/Guia_Desinformacion_VF%20ENG.pdf.

98 Peter K. Smith, Georges Steffgen and Ruth Sittichai, "The nature of cyberbullying, and an international network": *Cyberbullying through the New Media: Findings from an International Network,* Peter K. Smith and Georges Steffgen (eds.), Psychology Press: Taylor & Francis, 2013, p. 5.

99 United Nations Educational, Scientific and Cultural Organization (UNESCO), *Behind the Numbers: Ending School Violence and Bullying,* 2019, p. 14 [online] https://unesdoc.unesco.org/ark:/48223/pf0000366483?posInSet=8&queryId=a84f5b5a-3828-462f-b63c-d45eae258884.

100 Ibid., p. 7.

101 International Telecommunication Union (ITU), "Guidelines on Child Online Protection", 2020 [online] https://www.itu-cop-guidelines.com/.

protecting children online. This is because harmonized cybercrime laws and procedural rules in the matter would most effectively provide for the criminal sanctions required to deal with online harm to children.[102]

When the cyberbullying perpetrator is anonymized or uses a fake account, enforcing rules against this kind of practice is challenging and can lead to stronger decisions by policymakers. For instance, the Secret application was made unavailable in the Brazilian App Store after a number of reports of cyberbullying alleged to have taken place in the form of anonymous "secrets" posted in the app.[103] The same app was strongly criticized in Mexico, likewise for allegedly permitting cyberbullying practices.[104]

Global Kids Online is an important initiative to provide a cross-national evidence base for children's use of the Internet and to connect stakeholders. The countries in the region with research results available are Argentina, Brazil, Chile and Uruguay.[105]

In April 2020, SaferNet Brazil and the United Nations Children's Fund (UNICEF) jointly launched a campaign to combat cyberbullying, #ÉDaMinhaConta ("It's my business"). It offers instructions on how to act in situations of bullying, such as how to identify whether someone is a target or is carrying out bullying.

Research conducted by Fundación Paniamor in Costa Rica, involving 1,008 children between 9 and 17 years old, has yielded important findings about children's use of the Internet and risks related to violence and discrimination. Of a sample of children aged between 9 and 12, 5.9% said they had been discriminated against or abused via the Internet, and 2.5% said they did not know.[106] Among those aged between 13 and 17, 3.2% said they had and 2.8% were not sure.[107]

In Brazil, cyberbullying and direct offences are the most common motives for contacting the SaferNet helpline, ranking ahead of problems to do with data protection, fraud or hate speech.[108] In total, cyberbullying accounts for the greatest number of notifications, accounting for 2,310 out of 25,184 cases since 2007.

4. Non-consensual distribution of sexually explicit media

The non-consensual distribution of sexually explicit media can take different forms. It may be carried out by strangers who intentionally publish sexually explicit media online or by someone who has had an intimate relationship with the person and posts what is commonly known as revenge pornography (or revenge porn).

Countries in Latin America and the Caribbean have been taking different approaches to the issue. In some cases, the distribution of non-consensual sexually explicit media may be treated as defamation, while in others a more targeted approach is taken, with criminal legislation amended to treat the practice as a new type of criminal conduct.

Between mid-2018 and 2020, 17 states in Mexico passed the Olimpia Act reforming the General Law on Women's Access to a Life Free of Violence and the Criminal Codes to recognize digital violence as a crime, imposing penalties that can range up to eight years in prison (in Michoacán) and fines.[109]

Brazil has specific rules in both criminal and civil law. The transmission, publication, distribution or making available of pornography, sexually explicit media or nude images, with or without the victim's

102 See International Telecommunication Union (ITU), *Guidelines for policy-makers on Child Online Protection*, 2020, pp. 28-29 [online] https://www.itu-cop-guidelines.com/policymakers.
103 UOL, "Aplicativo Secret cria polêmica ao permitir postagem anônima de 'segredos' ", 2014 [online] https://www.uol.com.br/tilt/noticias/redacao/2014/08/13/secret-cria-polemica-ao-prometer-anonimato-acao-visa-proibir-o-aplicativo.htm. See also GI, "Secret é retirado de loja de aplicativos da Apple no Brasil", 2014 [online] http://g1.globo.com/tecnologia/noticia/2014/08/secret-e-retirado-de-loja-de-aplicativos-da-apple-no-brasil.html.
104 Milenio, "Secret, la 'app' preferida de los jóvenes para 'cyberbullying' ", 2014 [online] https://www.milenio.com/cultura/secret-la-app-preferida-de-los-jovenes-para-ciberbullying.
105 See Global Kids Online [online] http://globalkidsonline.net/about/.
106 See report on the first Kids Online survey in Costa Rica, *Niñas, niños y adolescentes en la Internet*, April 2019, figure 32 [online] http://globalkidsonline.net/wp-content/uploads/2019/07/Kids-Online-Costa-Rica-1-Julio.pdf.
107 Ibid.
108 SaferNet, Helpline [online] https://helpline.org.br/indicadores/.
109 Mexico, "Ley Olimpia" [online] http://ordenjuridico.gob.mx/violenciagenero/LEY%20OLIMPIA.pdf.

consent, is a crime punishable by between one and five years in prison.[110] Article 21 of the Brazilian Internet Bill of Rights, meanwhile, provides for a specific take-down regime for images, videos or other materials depicting nudity or sexual acts of a private nature: the Internet applications provider must remove the content upon receiving an extrajudicial notification, i.e., a report from the user.[111]

In Uruguay, non-consensual distribution of sexually explicit media is a crime, and Internet platforms are subject to sanctions if they do not immediately take the content down.[112] Other countries, such as Chile[113] and Peru,[114] are discussing bills to specifically address the non-consensual distribution of sexually explicit media.

Although in some cases it can be difficult for automated technologies to recognize the purpose of a publication with sexually explicit content (an issue which exercises the #WeTheNipple campaign[115]), intermediary platforms have increasingly taken steps to respond to gender-based violence.[116] First, the non-consensual distribution of sexually explicit media violates the community guidelines of all major platforms, as described in the *Internet & Jurisdiction Global Status Report* 2019.[117] Additionally, platforms are deploying machine learning and artificial intelligence to detect images or videos that are being shared non-consensually, and have also launched victim support hubs.[118]

Even so, civil society organizations are increasingly calling for a more proactive response from platforms, in terms of providing a faster response to notifications and being more transparent about data on gender-based violence.[119]

Besides all the above, it is important to consider that the victims of non-consensual distribution of sexually explicit media tend to belong to groups that are vulnerable and often discriminated against. Women, for instance, are usually the victims, while men are the perpetrators.[120] This type of abuse, however, is not the only one faced by women online.

Mexican campaigners have described at least 13 possible manifestations of online gender-based violence: unauthorized access and control of access; control and manipulation of information; impersonation and identity theft; surveillance and stalking; discriminatory speech; harassment; threats; non-consensual sharing of private information; extortion; disparagement; technology-related sexual abuse and exploitation; attacks on communication channels; and oversights by regulatory actors.[121]

Targeted abuse of this kind is particularly prevalent in a region where at least 12 women die every day because of incidents related to the mere fact that they are women,[122] and where gender equality

110 Brazil, Criminal Code, article 218-C [online] http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm.
111 Chiara A. S. de Teffé, "What is revenge porn and how can I protect myself?" *Brazil's Internet Bill of Rights: A Closer Look*, Carlos Affonso Souza, Mario Viola and Ronaldo Lemos (eds), 2017, p. 137 [online] https://itsrio.org/wp-content/uploads/2018/02/v5_com-capa__pages_miolo_Brazil-Internet-Bill-of-Rights-A-closer-Look.pdf.
112 Uruguay, Law No. 19580 of 2018, article 92 [online] https://www.impo.com.uy/bases/leyes/19580-2017.
113 Chile, Boletínes, No. 11923-25 and 12164-07 [online] https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=12444&prmBoletin=11923-25.
114 Peru, Bills 01669/2016-CR and 2460/2019, both making perpetrators criminally liable. See [online] http://www.leyes.congreso.gob.pe/Documentos/2016_2021/Proyectos_de_Ley_y_de_Resoluciones_Legislativas/PL0166920170717.pdf and http://www.congreso.gob.pe/comisiones2016/Justicia/ProyectosLey/.
115 The campaign calls on Facebook and Instagram to make an exception to their nudity restrictions to allow for art in the medium of photography. It is supported by representatives in different countries around the globe, including Brazil, Chile, Colombia and the Dominican Republic.
116 Juliana Pacetta Ruiz, Mariana Girogetti Valente and Natália Neris, "Between the perpetrator and the victim: the role of Internet intermediaries on violations against women", *Sociología y Tecnociencia*, vol. 9, No. 1, 2019, pp. 14-17. See [online] https://revistas.uva.es/index.php/sociotecno/article/view/2240/1779.
117 Internet & Jurisdiction Policy Network, *Internet & Jurisdiction Global Status Report*, 2019, p. 86.
118 Facebook, "Detecting Non-Consensual Intimate Images and Supporting Victims", March 2019. See [online] https://about.fb.com/news/2019/03/detecting-non-consensual-intimate-images/.
119 Mexico, "Internet es nuestra MX. Llamado a las plataformas digitales a agilizar procesos de denuncia tras agresiones que mujeres reciben en el marco de protesta #NoMeCuidanMeViolan", 2019. See [online] https://internetesnuestra.mx/post/187169630893/llamado-a-las-plataformas-digitales-a-agilizar.
120 Clare McGlynn, Erika Rackley and Ruth Houghton, "Beyond 'revenge porn': the continuum of image-based sexual abuse", 2017 [online] https://link.springer.com/content/pdf/10.1007/s10691-017-9343-2.pdf; Abby Whitmarsh, "Analysis of 28 days of data scraped from a revenge pornography Website", 2015 [online] https://everlastingstudent.wordpress.com/2015/04/13/analysis-of-28-days-of-data-scraped-from-a-revenge-pornography-website/.
121 GenterIT.org, "13 manifestations of gender-based violence online" (2018) [online] https://www.genderit.org/resources/13-manifestations-gender-based-violence-using-technology.
122 Economic Commission for Latin America and the Caribbean (ECLAC), "Feminicidio", Infografías, 24 October 2016 [online] https://www.cepal.org/es/infografias/feminicidio. In 2018, the Latin American countries with the highest rates of femicide per 100,000 women were El Salvador (6.8), Honduras (5.1), the Plurinational State of Bolivia (2.3), Guatemala (2.0) and the Dominican Republic (1.9). In the Caribbean, Saint Lucia (4.4) and Trinidad and Tobago (3.4) had the highest rates. See ECLAC, "Femicide or feminicide" [online] https://oig.cepal.org/en/indicators/femicide-or-feminicide.

is still far from a reality.[123] This being so, offline and online violence should be seen as interconnected and should not be treated separately.[124] It is not that a certain type of abuse starts and finishes online. Instead, the violence may take place both offline and, repeatedly (and continuously), online.[125] Examples are when sexual abuse is filmed and spread on social media or when women rights activists receive online threats followed by attacks in the street.

Difficulties in enforcing such content removal, sometimes because of jurisdictional issues, can also have life-altering consequences for women. In Colombia, for instance, a person sending threats to a woman could not be identified because they were sent from a public place (an Internet café). In another case, the perpetrator could not be identified because the address was a location in the United States.[126]

Such cases have an effect that extends beyond the victim, targeting women more broadly. As noted by the United Nations Special Rapporteur on violence against women, "despite the benefits and empowering potential of the Internet and ICT, women and girls across the world have increasingly voiced their concern at harmful, sexist, misogynistic and violent content and behaviour online. It is therefore important to acknowledge that the Internet is being used in a broader environment of widespread and systemic structural discrimination and gender-based violence against women and girls."[127]

In short, different types of abuses that could harm everyone must also be viewed through the specific lens of the groups targeted, whether they are women, ethnic minorities, indigenous people, immigrants or LGBTQ. The other part of this perspective is the way the Internet has also given socially marginalized groups a voice and helped them to build networks to fight online threats, combat gender-based violence and provide support to victims, examples being Take Back the Tech[128] (worldwide) and Vita Activa[129] (Mexico).

5. The "right to be forgotten" comes up against the region's particular characteristics

As explored in greater depth in section IV.C.6, several countries in the region have adopted a general data protection law, more or less inspired by the European General Data Protection Regulation (GDPR). Also influential has been a 2014 ruling by the EU Court of Justice in the Google Spain[130] case that a Spanish citizen could exercise his "right to be forgotten" against online search engines, obliging the companies concerned to remove some search results alleged to be damaging.

This decision unleashed a region-wide discussion, centring on the statutory situation in the many countries that have now recognized the right to be forgotten and the question of whether it is prudent or even desirable to institute such a right. The debate is more appropriately understood as a right to request "de-listing" or "de-indexing". In Spain, because the judgement did not establish such a requirement, the content itself is not erased. Instead, search engines such as Google, Bing and others are only instructed to remove the results of searches based on the individual's name and other identifiable personal markers connected to information that is deemed irrelevant, out of date or lacking in current value.

123 See "Indicators" [online] https://oig.cepal.org/en/indicators and ECLAC, "Gender equality plans in Latin America and the Caribbean: road maps for development", *Gender Equality Observatory for Latin America and the Caribbean. Studies*, No. 1 (LC/PUB.2017/1-P/Rev.1), Santiago, 2019.

124 InternetLab, *Online Gender-based Violence: Diagnosis, Solutions and Challenges. Joint Contribution to Inform the Work of the UN Special Rapporteur on Violence Against Women*, 2017, p. 15 [online] https://www.internetlab.org.br/wp-content/uploads/2017/11/Relatorio_ViolenciaGenero_ONU.pdf.

125 Swedish International Development Cooperation Agency (Sida), "Gender-based violence online", 2019. See [online] https://www.sida.se/contentassets/97224704b4f643cba3b4fca3d931e576/brief_gender-based_violence_online_sep-2019_webb.pdf.

126 Case Study Number 1, Colombia, (Ramírez Cardona (2014), cited in Association for Progressive Communications (APC), *From Impunity to Justice: Domestic Legal Remedies for Cases of Technology-Related Violence against Women*, "End violence: Women's rights and safety online" project (p. 22) [online] https://www.genderit.org/sites/default/files/flow_domestic_legal_remedies_0.pdf)

127 United Nations, *Report of the United Nations Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective* (A/HCR/38/47), 2018 [online] https://undocs.org/en/A/HRC/38/47.

128 See [online] https://www.takebackthetech.net/.

129 See [online] https://vita-activa.org/.

130 Court of Justice of the European Union, Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 2014.

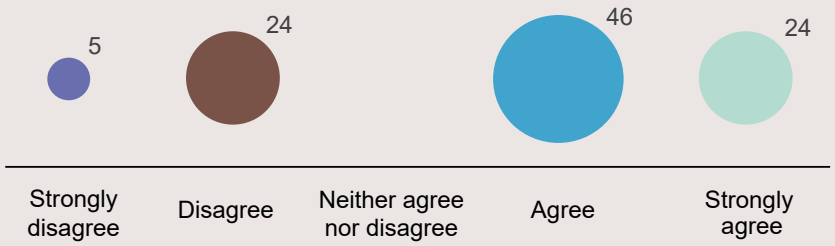
The Google Spain case has prompted a number of claims affirming this right in the context of the region. Differences in data protection regulations (or the lack thereof) have not prevented some domestic courts from recognizing the existence of "a right to be forgotten" and ordering search engines, and sometimes news outlets, to de-list information.[131] More often than not, the parameters of this right have been left unclear, so that its scope and even the question of who is responsible for de-listing and under what conditions are left open.[132]

Other courts have rejected or qualified the right.[133] The history of protecting freedom of expression in the region tends to act as a counterweight to de-listing, particularly without a court order.[134]

5.1. The "right to be forgotten" is broadly perceived as a global concept

The stakeholders surveyed were asked whether the right to be forgotten had attained global status or was applicable to Latin America and the Caribbean as a whole. One of the stakeholders said that the expression "right to be forgotten" had been used in Latin America and the Caribbean as an umbrella term, including every instance where users asked Internet service providers (ISPs) to remove, de-index, de-list or hide content. Others thought that the concept behind the right was gaining ground and that certain courts and countries were recognizing it. Overall, 70.73% of the stakeholders surveyed and interviewed agreed or strongly agreed that the right to be forgotten was indeed a global concept.

Do you consider that the "right to be forgotten" is becoming a global concept?



Source: Internet & Jurisdiction Policy Network and Economic Commission for Latin America and the Caribbean (ECLAC).

As one of the stakeholders surveyed remarked: "The right to be forgotten is a new right proposed in the context of the information society. Reactions to this right vary from country to country because the concept and rationale are not yet clearly defined. The absence of consensus on this point has the potential to create uncertainty in a society that is becoming increasingly borderless. Country-specific decisions are not enough for the smooth development of this concept, and there is an urgent need to reach a consensus around core points. Given the borderless character of today's world, the conflict between fundamental values –protection for the dignity of the individual versus the right to know and freedom of expression– is producing varying results."

5.2. Local amnesty laws and the countervailing notion of a "right to remember" impact the enforcement of a right to be forgotten

Certain elements of the legal order, history and culture of the region have diverged from their original European roots. For instance, many countries of Latin America and the Caribbean have passed through

131 See [online] https://law.stanford.edu/wp-content/uploads/2017/09/The-_Right-to-Be-Forgotten_-and-Blocking-Orders-under-the-American-Convention-Emerging-Issues-in-Intermediary-Liability-and-Human-Rights_Sep17-.pdf.

132 See [online] https://www.palermo.edu/cele/pdf/investigaciones/Towards_an_Internet_Free_of_Censorship_II_10-03_FINAL.pdf.

133 One of the most important cases involved the question of whether intermediaries could be held liable for content which impacted privacy or reputation. The court took the view that de-listing should only apply with a court order and/or where unlawful information was involved (Argentina, Supreme Court, *Rodríguez M. Belen c/ Google y Otro s/ daños y perjuicios*, Judgement R.522.XLIX, 28 October 2014). In Brazil, the right has been extensively debated and was the subject of a public hearing at the Brazilian Supreme Court. The Superior Court had granted the right with qualifications. For the minutes of the debate on the Aida Curi Case, see [online] http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/AUDINCIAPBLICASOBREODIREITOAOESQUECIMENTO_Transcries.pdf.

134 See[online]https://globalfreedomofexpression.columbia.eduwp-content/uploads/2016/04/GFOE-Presentation-Catalina-Botero-.pdf.

very recent authoritarian regimes, several of whose leaders have been accused of egregious human rights violations. In the transition to democracy, most of these States issued amnesty laws pardoning those responsible for the human rights violations and in many cases blocking both access to the truth about what happened and any prospect of reparation.

With substantial guidance from the Inter-American Human Rights System,[135] there has been an effort in the last few decades to develop the opposite right, a "right to remember", a right for victims to have access to the truth. On the basis of this right, amnesty laws have been repealed, truth commissions have been established and perpetrators have even been prosecuted.

Data protection experts, authorities and civil society organizations[136] now view a "right to be forgotten" as running counter to this cultural and human rights tradition.[137] Hence, regionally, de-listing as a concept has to exist alongside a "right to remember", particularly in situations concerning information on alleged or actual human rights violations.

Some countries have, however, included a right to the erasure of personal data in their data protection legislation with a wording similar to that of the so-called right to be forgotten at issue in the European case referred to.

The differences between Europe and Latin America and the Caribbean continue to be linked to the fact that countries in the region tend to treat data protection as concerning "back-end" stored data as opposed to content made public, which is more clearly understood as relating to free speech.[138] In some countries, too, the principle of net neutrality has prevailed, with de-listing or de-indexing regarded as undermining it.[139]

The precise form of any right to be forgotten, be it de-listing, de-indexing or even removal, appears not to have been spelled out in a consistent manner in the region, and the divide amongst the stakeholders surveyed seems to be a reflection of that.

B. Security

1. Increased cybersecurity coordination is needed to deal with widespread incidents in the region

Latin America and the Caribbean has a history of dealing with different levels of security issues, whether personal, institutional or national security-related. The emergence of the Internet did not radically change this. It did, however, change the security landscape. Cyberspace has become another territory where protection needs to be granted and where crimes may be committed.

The growing interconnectedness between the offline and online worlds, particularly with the so-called Internet of Things, is making security issues even more important. There have been an increasing number of cybersecurity incidents in Latin America and the Caribbean. At the same time, the region has become a major haven for perpetrators of such actions. Coupled with that is the fact that many of the most popular Internet services used in the region tend to be foreign, and significant

135 The views of the Inter-American Human Rights System can be found in the report *Standards for a Free, Open and Inclusive Internet*, 2016, paras. 134 ff. See [online] http://www.oas.org/en/iachr/expression/docs/publications/INTERNET_2016_ENG.pdf.

136 R3D, "El erróneamente llamado 'derecho al olvido' no es un derecho, es una forma de censura", 2015 [online] https://r3d.mx/2016/07/12/el-erroneamente-llamado-derecho-al-olvido-no-es-un-derecho-es-una-forma-de-censura/; Hiperderecho, "Protección de datos personales: la nueva puerta falsa de la censura", 2016 [online] http://www.hiperderecho.org/2016/07/proteccion-datos-personales-la-nueva-puerta-falsa-la-censura/.

137 There are those who have considered it "an insult" to the history of the region. Eduardo Bertoni, "The Right to Be Forgotten: An Insult to Latin American History", 2014 [online] https://www.huffpost.com/entry/the-right-to-be-forgotten_b_5870664. For a general analysis by the former Organization of American States (OAS) Special Rapporteur for Freedom of Expression, Catalina Botero, see [online] https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2016/04/GFOE-Presentation-Catalina-Botero-.pdf.

138 This can be understood from the way courts deal with such cases. An example is a Brazilian case involving a prosecutor accused of fraud in a public entrance exam for the post of judge and later cleared of wrongdoing. Superior Court of Justice, "Recurso especial No 1.660.168 - RJ (2014/0291777-1)", 2018 [online] https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1628798&num_registro=201402917771&data=20180605&formato=PDF. Another example can be found in Mexico; see [online] http://sise.cjf.gob.mx/SVP/word1.aspx?arch=1100/11000000188593240001001.docx_0&sec=_Mercedes__Santos_ Gonz%C3%A1lez&svp=1 [https://perma.cc/N8LW-9ZBZ].

139 Colombia, Constitutional Court, Ruling No. T-277 of 2015, "Acción de tutela instaurada por Gloria contra la Casa Editorial El Tiempo", 12 May 2015 [online] https://perma.cc/KF4Q-VW6S.

amounts of data pass through or are stored in countries outside Latin America and the Caribbean, chiefly more developed ones. This generates cross-border challenges that extend from difficulties in determining the location of cybercrime to access to evidence, control over data security standards and issues regarding surveillance.

One stakeholder surveyed remarked on how the need to expedite access to data and resolve cybersecurity incidents clashed with national legal identities and jurisdictional sovereignty. Large numbers of stakeholders noted that international cooperation on such cross-border issues was paramount in dealing with this challenge.

2. Cross-border investigations and electronic evidence

Corruption is a feature of life in Latin America and the Caribbean that the region is not proud to be known for. In the last two decades, scandals have escalated from isolated cases involving chiefly domestic matters to organized schemes, some encompassing more than one or even several jurisdictions. A significant example has been Operation Car Wash (*Operação Lava-Jato*), which started as an investigation in Brazil but uncovered sophisticated arrangements across dozens of countries. One company, Odebrecht, has been the focus of investigations in several States of the region, while former Presidents or Vice-Presidents of at least five countries are in prison or under investigation. Several high-level politicians from other countries are also being investigated.[140]

These multi-jurisdiction corruption schemes have led to investigations requiring cross-border cooperation by law enforcement agents and several other agents, with important jurisdictional debates. Perhaps the most salient of these concerns access to digital evidence in multiple jurisdictions and the need to reform the international cooperation instruments that provide mechanisms for both preservation of and access to electronic evidence across borders.

2.1. Accessing digital evidence in multiple jurisdictions

In the course of a multi-jurisdiction investigation, law enforcement agencies need to have access to information that may be located in another country, perhaps because the actions concerned have crossed jurisdictions. For example, a company might wire funds to an offshore account belonging to a corrupt official; or alleged criminals may use cloud Internet services that store data overseas. Evidence produced in one investigation can be relevant to another, and in some cases the investigation of a foreign corruption case can impact the security of an investigation in another country.[141]

The fact that relevant data may be connected to other countries gives rise to a number of jurisdictional issues. It is important to note, however, that there is a distinction between jurisdiction over a crime itself and jurisdiction over the evidence needed to investigate that crime.

Where jurisdiction over evidence is concerned, multiple issues are still being discussed. First, there may be a dispute about the connecting element needed to ascertain jurisdiction over digital evidence. The most common connecting element has traditionally been the location of the evidence. This brings at least two difficulties. Because of its digital nature and potential fluidity, digital evidence (data) can be split between different jurisdictions or transferred to another location without warning or effort. Cloud services perform both these actions, dividing up packages of information and moving them constantly between servers, which may be and usually are in different jurisdictions.

The location of the data is not the only possible connecting factor. There may be others, such as the nationality, domicile or usual place of residence of the data subject, or the place of establishment of the company in possession of the data.

Additionally, the success of any request to access data stored abroad may be dependent upon cooperation with the country where the data are located. Traditionally as well, foreign and domestic requests are subject to different criteria and procedures. Hence, the validity and enforceability of a foreign request to produce evidence may be disputed.

140 For an overview of the corruption scandal, see [online] https://www.bbc.com/news/world-latin-america-41109132.
141 For an analysis of the interconnectedness of corruption, foreign bribery and access to information and evidence, see [online] http://www.oecd.org/daf/anti-bribery/TypologyMLA2012.pdf.

Finally, countries may apply blocking statutes that do not allow data to be communicated internationally except under specific circumstances and subject to specific procedures. Some data protection legislation, for example, blocks transfers without a domestic warrant or consent.

These issues tend to pose a number of challenges for law enforcement agents. Access to evidence on a crime committed in country A by citizens of country A whose victims are also in country A may depend on an international procedure simply because the relevant evidentiary data are stored outside that country.

Some of the stakeholders surveyed highlighted the importance of access to evidence stored overseas for criminal investigations and the need for cooperation and information sharing. They noted as well that international processes could be cumbersome and not necessarily well adapted to the urgency and speed of today's investigations, suggesting the need for a paradigm shift in the region.

In the case of the Brazilian multinational company Odebrecht, the Department of Justice of the United States (DOJ) made an agreement with the company to monitor compliance with anti-corruption legislation. The agreement covered the sharing of information with a monitoring organization and the DOJ, including a requirement to transfer information –personal data among it– not in the context of an investigation but after its completion, to prevent future illegal actions.[142]

2.2. The mutual legal assistance system needs to be adapted to the digital age

The traditional way to request extraterritorial evidence is through international cooperation. There is a network of international agreements that provide for legal procedures to facilitate cross-border assistance and cooperation.

By far the most common are mutual legal assistance (MLA) treaties. States in the region are parties to a number of bilateral MLA agreements, as well as multilateral ones that are universal or regional in scope. The Inter-American Convention on Mutual Assistance in Criminal Matters (1992), for instance, has 26 Latin American and Caribbean countries as members.[143] Other specific conventions deal with mutual legal assistance and the need for international cooperation on such matters. All the countries in the region except Cuba are parties to Article XIV of the Inter-American Convention against Corruption (1996).[144]

The MLA treaty system is a step up from the traditional use of diplomatic cooperation and rogatory letters, yet it has its own set of difficulties. It depends on countries being parties to MLA treaties, and procedures are not uniform, as they may vary from agreement to agreement.[145] Additionally, the administrative system in place was structured to work with exceptional requests from abroad, not with large volumes of applications. The lack of automation and scalability means that procedures may not be timely. Meanwhile, investigations may stall, potential culprits may not be found and so may remain at large, there may be follow-on crimes, and evidence may be moved (to another jurisdiction) or destroyed.

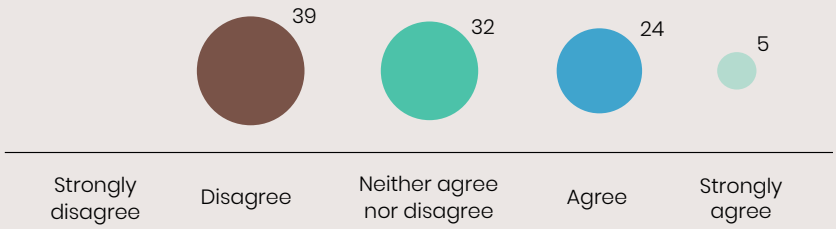
Several countries in the region believe that the MLA system requires reform.[146] The majority of the stakeholders surveyed also agree that there is a need to introduce more agile procedures into international cooperation arrangements. Some have cautioned, however, that the procedures should respect due process, data privacy and human rights in general. One stakeholder highlighted the need to guarantee the authenticity of documents and the credibility of the actors issuing the request.

142 See [online] https://globalinvestigationsreview.com/article/1139256/us-and-brazil-agree-local-odebrecht-monitors. See also [online] https://www.justice.gov/opa/press-release/file/919916/download.
143 See [online] https://www.oas.org/juridico/english/treaties/a-55.html. The convention has a protocol to which far fewer countries are parties [online] http://www.oas.org/juridico/english/treaties/a-59.html.
144 See [online] http://www.oas.org/en/sla/dil/inter_american_treaties_B-58_against_Corruption.asp.
145 See [online] https://www.justice.gov/archives/jm/criminal-resource-manual-276-treaty-requests.
146 Information submitted by Latin American and Caribbean States to the United Nations Office on Drugs and Crime (UNODC). See [online] https://undocs.org/A/74/130.

Generally, stakeholders do not advocate a complete overhaul of the MLA system, but instead call for it to be adapted to the digital age. Their view is that most issues derive from the fact that Internet companies are established overseas with a local presence. Their suggestions tend to revolve around a mechanism of direct requests to these companies (as data holders).

There is little consensus, however, about the instrument to be used for such reform. Because they are either bilateral or multilateral, MLA treaties tend to take time to negotiate and may not encompass all information access and preservation needs. Meanwhile, countries are seeking out solutions either unilaterally or as part of like-minded groups.

Do you agree with this statement: law enforcement cooperation regarding cross-border electronic evidence (through mutual legal assistance treaties or other procedures) needs significant improvement?



Source: Internet & Jurisdiction Policy Network and Economic Commission for Latin America and the Caribbean (ECLAC).

2.3. The contribution of the Budapest Convention on Cybercrime to cross-border investigations

Several States in Latin America and the Caribbean are parties or have acceded to the Council of Europe's Convention on Cybercrime of 2001 (Budapest Convention), which, amongst other stipulations, establishes mechanisms for international cooperation on cybercriminal matters.[147] Argentina, Chile, Colombia, Costa Rica, the Dominican Republic, Guatemala, Mexico, Panama, Paraguay and Peru are parties to the Convention, and Brazil was invited to accede to it in December.[148] The Convention provides for more expeditious arrangements for preserving and accessing evidence.

The stakeholders interviewed and surveyed were of the opinion that although the Budapest Convention did not solve all problems with the MLA system, it was a step in the right direction. One of the stakeholders noted that participation in the Budapest Convention provided an important forum for discussing the obstacles to accessing digital evidence.

The members of the Convention are discussing an additional protocol[149] that will provide more specific tools to create a more comprehensive and expeditious regime, especially for subscriber data stored in cloud services.[150] One significant difficulty, however, is to establish a common baseline of understanding with respect to privacy and other human rights. Some of the stakeholders surveyed expressed this concern.

2.4. Alternatives to the MLA treaty system are being explored outside the region

Since international processes have not yet reached full maturity, several countries have embarked on unilateral initiatives consisting of national legal reforms. One of the leading solutions has been the provision of legal authority to directly request access to data from those in possession of it, particularly ISPs.

147 See [online] https://www.coe.int/en/web/cybercrime/the-budapest-convention.
148 Council of Europe, "Budapest Convention: Brazil invited to accede", 2019 [online] https://www.coe.int/en/web/cybercrime/-/budapest-convention-brazil-invited-to-accede.
149 See [online] https://www.coe.int/en/web/cybercrime/t-cy-drafting-group.
150 In a UNODC survey, Latin American and Caribbean members mentioned updating the Budapest Convention on Cybercrime as one possible solution. See [online] https://undocs.org/A/74/130.

The United States has passed the Clarifying Lawful Overseas Use of Data (CLOUD) Act, which provides a mechanism allowing law enforcement agencies in countries that have a dedicated bilateral agreement with the United States to directly request companies to produce data. It clarifies that jurisdiction over digital evidence depends on the nationality or residency of the data subject (customer of the ISP). Department of Justice guidelines state that domestic ISPs can be requested to produce data they hold, regardless of where these data are located.[151]

Similarly, the EU has started a project called E-evidence. It consists of a draft regulation that would create enforceable orders for preservation of and access to digital evidence to be sent directly to Internet services operating in the EU, irrespective of the location of the data; foreign ISPs would in addition be required to establish a legal representative in the EU to receive such decisions and orders.[152]

Both projects recognize that there is still a need for international cooperation. ISPs may be subject to laws in third countries that prevent them from producing the evidence, meaning that special procedures are required to access it. The CLOUD Act authorizes the President to negotiate with countries that meet certain criteria of privacy and rights protection to arrive at executive agreements that can facilitate direct cooperation, allowing requests to be directed to the entities holding the data. On 5 February 2019, the European Commission was given a two-track mandate to initiate negotiations on cross-border access to digital evidence with the United States and within the context of the aforementioned additional protocol to the Budapest Convention.[153]

Interviewees have mentioned accession to the Budapest Convention (2001) as a way forward, while also noting that it cannot solve all issues. Law enforcement agents are still searching for ways to access data stored overseas. In the case of Brazil, for instance, this has grown into a discussion on the constitutionality of the MLA treaty with the United States. The Supreme Court was called upon to pronounce on the matter.[154] The discussion hinges on whether a local subsidiary of an ISP can be called upon to produce evidence held by the parent company outside the country, and whether article 11 of the Brazilian Internet Bill of Rights, stating that Brazilian law applies to data collected in Brazil or from a device in Brazil, provides a sufficient basis for bypassing the MLA treaty and directly requesting data stored overseas.

3. Surveillance

The Internet can be an instrument for liberation, facilitating access to information and allowing it to spread globally. It has often made it easier for people to communicate, find each other, exchange ideas, join forces and gain access to different types of goods and services. At the same time, though, the Internet allows all these actions to be tracked and traced. Troves of data on people's habits, tastes and movements have become more easily available. Behaviour online and to some extent offline can also be mapped out and rendered accessible. Thus, surveillance has turned out to be a reality to be contended with, and not only from the standpoint of very sophisticated monitoring or intelligence systems. Both the public and private sectors, companies perhaps even more now than State administrations, are capable of monitoring the population.

These two sides of the Internet tend to be hard to reconcile. Important initiatives may deliberately or inadvertently lead to surveillance. Many social security and social benefit systems are informed by data analysis and data-driven public policymaking. Making resource allocation more efficient,

151 See [online] https://www.justice.gov/opa/press-release/file/1153446/download.

152 See [online] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en. For more direct information, see European Commission, "Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters" (COM(2018) 225 final), 17 April 2018 [online] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0225&from=EN; "Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings" (COM(2018) 226 final), 17 April 2018 [online] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0226&from=EN.

153 See [online] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.

154 Brazil, Supreme Court (STF), "Ação direta de constitucionalidade", No. 51 [online] http://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379.

reducing fraud and finding and distributing goods and services for those who need or deserve them and fit the criteria are very important goals. All of them can be better achieved with more data and better oversight and analysis.

The other side of this enhanced efficiency is that the tools used to achieve it may also be used for surveillance. There is a high risk that the collection of such data may encroach on many fundamental rights and that this wealth of information may be misused or employed to discriminate, persecute or leave the most vulnerable even worse off than they were before.

In Latin America and the Caribbean, instances have been reported in which significant amounts of personal data have been collected within the framework of social programmes, public transportation arrangements and even popular events. The online impact of the pandemic has enhanced this tendency.[155] Such data tend to be compiled with an emphasis on the marginalized and more vulnerable portions of the population. This may lead to exclusion, unequal treatment and even discrimination, quite apart from the risk of data breaches.[156] In the region, too, certain groups tend to be at a particularly high risk of surveillance. These include journalists and human rights defenders, but also political activists and artists.[157]

Another issue concerns the use of technologies in public areas. Many countries in Latin America and the Caribbean are entertaining the possibility of implementing face recognition systems in streets and parks and at public events.[158] The aim is to curb crime and enhance public safety. The technology may, however, have an impact on other rights, such as freedom of expression and assembly, the right to protest and privacy.[159]

Surveillance tends to be analysed from a national perspective, but in Latin America and the Caribbean the cross-border implications are clearly visible. In several cases, the tools that are used to collect and analyse data or that are behind technologies such as face recognition tend to be implemented through public-private partnerships, chiefly with multinational corporations. Hence, the technology employed is frequently foreign, the servers where data are stored (usually cloud services) more often than not are outside the region, and neighbouring countries often receive similar offers or compete for the same services. Transnational jurisdictional clashes are then bound to occur with some frequency.

3.1. Encryption

The more services have moved online, the clearer the need for security has become. Encryption is one piece of the security puzzle. An enormous number of Internet services depend on encryption for their trustworthiness.[160] Banking and financial transactions are the first that come to mind, but others include opening a house, accessing cameras, sharing sensitive information and even booking a travel experience. The pandemic has made clear the need for encryption of dealings with doctors, hospitals and telemedicine.[161] Encryption is a cornerstone of and to some extent a prerequisite for all such online relationships.

The use of encryption, however, has had an impact in other areas. It can conceal important information from law enforcement and intelligence agents, thus creating tension between the use of encryption

155 See [online] https://ia801905.us.archive.org/23/items/data-justice-and-covid-19/Data_Justice_and_COVID-19.pdf.
156 See[online]https://www.derechosdigitales.org/13921/vigilancia-controle-social-e-desigualdade-a-tecnologia-reforca-vulnerabilidades-estruturais-na-america-latina/.
157 See [online] http://www.oas.org/en/iachr/expression/docs/reports/2014_04_22_Violence_WEB.pdf.
158 A number of countries have initiatives of this kind. To mention just a few, they include Argentina (see [online] https://documentosboletinoficial.buenosaires.gob.ar/publico/ck_PE-RES-MJYSGC-MJYSGC-398-19-5604.pdf); Brazil (see[online] https://www1.folha.uol.com.br/cotidiano/2019/11/151-pessoas-sao-presas-por-reconhecimento-facial-no-pais-90-sao-negras.shtml); Chile (see [online] https://www.infodefensa.com/latam/2020/04/08/noticia-ingesmart-implementara-chile-sistema-teleproteccion-camaras.html); Paraguay (see [online] https://www.tedic.org/quien-vigila-al-vigilante-reconocimiento-facial-en-asuncion/#sdfootnote1sym); and El Salvador, Honduras and Nicaragua (see [online] https://acceso.or.cr/assets/files/Art_Herramientas_Vigilancia_CA-mayo2020.pdf). For an overview of initiatives in the region, see [online] https://reconocimientofacial.info.
159 Al Sur, "New technologies and their impact on the promotion and protection of human rights in the context of assemblies and peaceful protests: The situation of Latin America", October 2019 [online] https://adc.org.ar/wp-content/uploads/2019/10/AL-SUR_Contribution_New-technologies-in-the-context-of-assemblies-and-peaceful-protests.pdf.
160 R. Polk and A. Froncek, "Your day with encryption", Internet Society, 2019 [online] https://www.internetsociety.org/blog/2019/10/your-day-with-encryption/.
161 For an overview, see D. Rozario, "Secure health care messaging in the era of COVID-19", IAPP, August 2020 [online] https://iapp.org/news/a/secure-health-care-messaging-in-the-era-of-covid-19/.

to protect privacy and other very important fundamental rights, on the one hand, and public safety and security, on the other. It is argued that the State should have access to information that is shared, even when encrypted, in order to safeguard the population against criminals, terrorists and other sources of danger. Otherwise, encryption acts as a barrier to this legitimate work and protects the guilty, those trying to subvert order and cause harm.

This tension has led to a technical, legal and ethical debate that has not yet been finally resolved. Both sides have valid points, and finding the right balance between sustaining encryption for many different purposes and permitting access to relevant data on national security and public safety grounds is not an easy task. In Latin America and the Caribbean, the discussion has surfaced in different forms: law enforcement agencies demanding access to data (particularly from messaging apps) despite encryption, mandating collection of more information (with potential impacts on encryption protocols) and requesting installation of back door access (akin to wiretapping).

3.2. Law enforcement access to encrypted information and messages

Access to encrypted information and messages for law enforcement purposes may be requested in different ways. Governments may order companies that create encryption mechanisms to provide a master key so that, under certain conditions, they will be able to access any necessary information as required.[162] The public administration may request companies with access to encrypted messages that it needs to divulge this information in an unencrypted form, without considering how decryption is to take place.

From a law enforcement point of view, the situation in Latin America and the Caribbean is that during an investigation, and with due cause, agents may be able to require companies and individuals to divulge information. The use or otherwise of encryption is not necessarily an issue that the legal system addresses. In the overwhelming majority of cases, the understanding is that if a company provides the service in a country, it has to comply with valid orders issued by its law enforcement agencies and particularly by judicial authorities.

Due to the way encryption protocols have been developed, intermediary companies are not always capable of providing such information, either because they no longer possess it (their architecture does not provide for storage of encrypted messages) or because they have no access to the decryption key (with end-to-end encryption, the private key is usually in the devices exchanging information and not available to the intermediary company).[163]

This can lead to difficult situations, as has happened in the region. The use of encryption has become contentious,[164] and ISPs have been caught in the crossfire. Apps have been blocked by court order, and company employees have even had to face jail time for disobeying orders to hand over messages (this is explored further in section V.B.4).

3.3. A difficult debate around anonymity

The region has traditionally struggled with the idea of anonymity. There is a view that it is very close to impunity, and instruments that permit anonymous speech tend to be frowned upon. The use of masks or similar devices during protests is one example.[165] Similarly, apps that permit anonymous messaging have been challenged in and out of court.[166]

---

162 H. Abelson and others, *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications*, Massachusetts Institute of Technology (MIT), 2015 [online] http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

163 K. Ermoshina, F. Musiani and H. Halpin, "End-to-end encrypted messaging protocols: an overview", *International Conference on Internet Science*, 2016 [online] https://link.springer.com/chapter/10.1007%2F978-3-319-45982-0_22.

164 See [online] http://www2.stf.jus.br/portalStfInternacional/cms/destaquesClipping.php?sigla=portalStfDestaque_en_us&idConteudo=330687.

165 See [online] https://www.derechosdigitales.org/wp-content/uploads/freedom-of-expression-encryption-and-anonymity1.pdf.

166 Tech Crunch, "Brazil Court Issues Injunction Against Secret and Calls for App to Be Remotely Wiped", 2014 [online] http://techcrunch.com/2014/08/20/brazil-court-issues-injunction-against-secret-and-calls-for-app-to-be-remotely-wiped/.

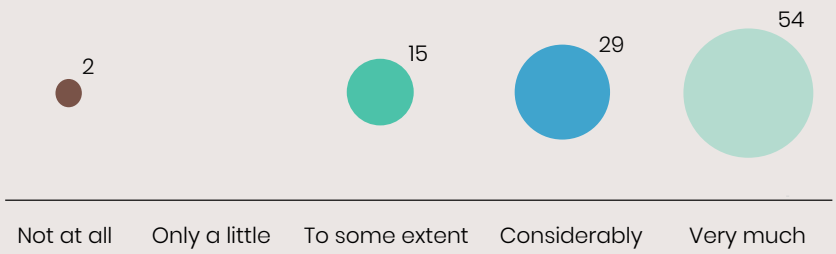
> The ability to exchange messages in a long chain, even if they are not anonymous speech per se, tends to create a situation in which finding the origin or source of a specific message may be challenging. This seems to be particularly acute in the context of misinformation campaigns, and potentially worse during elections.[167] Hence, in Brazil, for instance, a bill mandating the collection of information on all messages that go "viral" (forwarded more than 1,000 times) is currently before Congress.[168] Messaging services would be obliged to trace the source of such messages, so that if their content causes damage or is ruled to be criminal, the culprit will be more easily identifiable. Not only would the law require the retention of non-essential personal data, but experts claim that the encryption protocols used by services may be weakened if they are to comply with the requirements of the bill.[169]

The situation is unquestionably difficult and calls for careful analysis to determine whether this is a proportional response or whether there might not be other measures available that do not carry the same risks. The Inter-American System of Human Rights has underscored how important it is for responses to challenges involving access to information for law enforcement purposes and misinformation to safeguard and not undermine the "integrity of the computer systems on which the Internet works and the communications that are channeled through the network", including its encryption protocols.[170]

3.4. "Back doors" are perceived as undermining trust in encrypted systems

The stakeholders surveyed came out clearly against the inclusion of back doors in encrypted systems. When asked if that feature would undermine the legitimate security interests of users, 82.93% of the stakeholders agreed that it would.

How much would implementing "back doors" to encrypted systems undermine the legitimate security interests of users?



Source: Internet & Jurisdiction Policy Network and Economic Commission for Latin America and the Caribbean (ECLAC).

This finding is important because law enforcement agencies in Latin American and Caribbean countries are pushing for a way to decrypt the contents of messages sent via instant messaging apps. As applications such as WhatsApp have become increasingly popular in the region, there has been growing pressure to curb end-to-end encryption to provide some way of accessing message contents for criminal investigations.

It should be pointed out that encryption is essential to trust not only in messaging apps but also in e-commerce, Internet banking and all sorts of online activities. Breaking encryption for one user may mean breaking it for all others as well. At the same time, there are other ways of accessing the contents of a message in a duly authorized investigation that would not undermine the integrity of encrypted systems, even in the case of end-to-end encrypted instant messaging apps. They include

167 See [online] https://en.ejo.ch/specialist-journalism/mexicos-election-and-the-fight-against-disinformation.
168 The region is not alone; similar measures are reported to have been suggested in India. See [online] https://www.policyforum.net/encryption-and-attribution-indias-fake-news-problem/.
169 See [online] https://www1.folha.uol.com.br/poder/2020/08/veja-dez-razoes-para-rejeitar-artigo-10-do-projeto-sobre-fake-news-que-rastreia-mensagens.shtml. See also [online] https://www.eff.org/deeplinks/2020/06/current-brazils-fake-news-bill-would-dismantle-crucial-rights-online-and-fast.
170 See [online] https://www.oas.org/en/iachr/expression/publications/Guia_Desinformacion_VF%20ENG.pdf.

gaining access to the actual device used for communication (such as a mobile phone) and infiltration of law enforcement agents into messaging groups.

Law enforcement agencies in the region are exploring such alternatives as the legal debate over encryption matures.[171] The data that are available –metadata or data from other sources– can be leveraged to find the necessary answers. The use of modern investigative strategies is paramount to balance the debate and maintain national security and public safety while keeping privacy violations, cybersecurity threats and illegitimate surveillance, foreign or otherwise, at bay.

These situations may seem a domestic matter, but they have cross-border and even potentially international implications. Most encrypted services have a global reach, being used in multiple jurisdictions. If encryption is undermined for the benefit of one country's law enforcement, it may well have an effect on all the others. There may be a cascade effect not only for individuals living in democratic countries where human rights are respected, but also for defenders of human rights in more authoritarian regimes. Another aspect is that a significant number of companies offering services with embedded encryption may actually be using international protocols or application programming interfaces (APIs) from other corporations, domestic or foreign, so that the impact may extend beyond the direct supplier of the service.

Wherever the debate may go, it is important to bear in mind the complexity of the rights and interests being balanced and the fact that whatever bargains may be struck could have an impact beyond the country implementing them and could affect all groups, including vulnerable ones.

Quantum computing and encryption

Encryption is dependent on the difficulty and time involved in finding the combination to decrypt any message. In other words, encryption only works because it is hard and time-consuming to force the lock. Newer technologies such as quantum computing that increase the speed of computation may have a dual effect, creating encryptions that are even harder to break and rendering globally useless the systems available so far.[172] While a great deal of development is probably still needed to obtain working quantum computers, the mere concept helps to underscore the importance of encryption and the way a single key, or a single technological change, has the potential to cause havoc and put at risk any number of vital transactions.

4. Cybersecurity

The importance of securing cyberspace has grown exponentially in the last few years. The pandemic has recently highlighted the increasing dependence on technology of countries' infrastructure and basic services such as energy, water, sanitation, food transportation and supply chains, financial transactions, public services, and even the functioning of government procedures. All such services are prime targets for cyberattacks.

A number of major cyber incidents have originated in Latin American and Caribbean States or targeted victims there.[173] Such incidents have only increased with the expansion of connectivity and of the number of individuals accessing the Internet. Economically motivated cybercrime involving financial malware and credit card and online banking fraud tends to feature strongly among threats in Latin America and the Caribbean,[174] implying that public and national security is closely connected to cybersecurity. However, a number of countries in the region still have only a limited range of tools, capabilities and institutions to prepare for, identify and respond to attacks.[175]

171 See [online] https://carnegieendowment.org/2019/05/30/encryption-debate-in-brazil-pub-79219.

172 See [online] https://carnegieendowment.org/2019/04/25/implications-of-quantum-computing-for-encryption-policy-pub-78985.

173 Norton, "2017 Cyber Security Insights Report. Global Results", 2017 [online] https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf.

174 "ThreatMetrix Cybercrime Report: An Interview", November 2019 [online] https://resources.infosecinstitute.com/threatmetrix-cybercrime-report-an-interview/.

175 Organization of American States (OAS)/Inter-American Development Bank (IDB), *Cybersecurity Report, 2020* [online] https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf.

Lately, more and more cyber incidents have crossed borders, requiring international cooperation and coordination for their resolution. This international layer to cyber efforts shows the need for common approaches, standards and norms, not to mention resources and the ability to mount defences and increase resilience. There is a need to protect not only critical infrastructure but the whole information and communication infrastructure: not just one country or another's, but that of the region itself.

Levels of preparedness and resilience in the region are very uneven. Only just over a third of its countries have a cybersecurity strategy (Argentina, Brazil, Chile, Colombia, Costa Rica, the Dominican Republic, Guatemala, Jamaica, Mexico, Panama, Paraguay and Trinidad and Tobago). Somewhat fewer (10) have a government agency in charge of cybersecurity management and coordination. Twenty countries in the region have cybersecurity incident response teams (CSIRTs), also commonly referred to as computer emergency response teams (CERTs).[176]

It is clear that much remains to be done in terms of both national implementation and international and regional cooperation. At the CERT level, there is cooperation and coordination when risks and large-scale incidents are encountered. CSIRTAmericas.org, a platform for government-led CSIRTs in the Americas, serves as a network tool for early warning, distributed denial of service (DDoS) attack alerts and capacity-building.[177] The Latin American and Caribbean Internet Address Registry (LACNIC) has also created its own CERT.[178]

There is also much room for improvement in the cybersecurity governance structure. Inclusion of the different stakeholders (not only governments but also companies, civil society, academia and the technical community) is crucial for the overall system, both to overcome "silo thinking" and to ensure a systemic approach.[179] This is an ongoing process at both the national and regional levels. Participation by different actors is a feature of discussions at the level of the Organization of American States. Within the Inter-American Committee against Terrorism (CICTE), the cybersecurity programme is a major coordination effort and takes a multistakeholder approach.[180]

This is also the case at important intersections between the regional and international levels. For instance, at the regional consultations of the United Nations Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security, held with the Organization of American States, companies, civil society, academia and the technical community were invited to comment and take part in the discussions.[181]

> At the regional level, two instruments highlight the importance of cybersecurity and provide a framework for common commitments and cooperation: the 2012 Declaration on Strengthening Cyber Security in the Americas[182] and the 2015 Declaration on the Protection of Critical Infrastructure from Emerging Threats.[183]

Provisions for cyber-related offences in criminal legislation are usually another piece of the jigsaw. Countries in the region have yet to fully adapt their legislation to the demands of fighting cybercrime. As for the international layer, five countries are parties to the Budapest Convention on Cybercrime.[184] In this process of including cybersecurity in national agendas, some cybersecurity legislation has resulted in restrictions on digital rights. In Latin America and the Caribbean, the proposed Constitutional Law on Cyberspace of the Bolivarian Republic of Venezuela has been reported to assert wide powers in the interests of what is called the "comprehensive defence" of the country.[185]

176 Ibid.
177 See [online] https://the-gfce.instantmagazine.com/magazine/global-cyber-expertise-magazine-volume-5/csirtamericasorg/overlay/strengthening-incident-response-capabilities-in-the-americas/.
178 See [online] https://www.lacnic.net/4464/2/lacnic/.
179 Organization of American States (OAS)/Inter-American Development Bank (IDB), *Cybersecurity Report, 2020* [online] https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf.
180 See [online] http://www.oas.org/en/sms/cicte/default.asp.
181 See [online] https://www.un.org/disarmament/wp-content/uploads/2019/12/collated-summaries-regional-gge-consultations\-12-3-2019.pdf.
182 See [online] https://www.oas.org/en/sms/cicte/Documents/Declarations/DEC_1%20rev_1_DECLARATION_CICTE00749E04.pdf.
183 See [online] https://www.sites.oas.org/cyber/EN/Pages/contacts.aspx. See also [online] https://www.oas.org/es/sms/cicte/cipreport.pdf.
184 See [online] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=XXw51amG.
185 See [online] https://freedomhouse.org/country/venezuela/freedom-net/2019#footnoteref5_7rkdmen.

To achieve the right balance between promoting cybersecurity and at the same time avoiding violations of fundamental rights is a delicate matter and should be one of permanent concern for all States in the region. Thus, trust- and confidence-building measures are important to strengthen understanding of the different actors and the challenges that exist at the national and international levels.

5.1. Security breaches have exposed data processing vulnerabilities

Information security incidents and data breaches are commonly reported now. Data on enormous numbers of individuals have already been leaked. More often than not, this is the result of human error, either owing to a failure to configure security parameters properly, leaving space for intruders to explore, or because of basic mistakes such as using passwords that are easy to guess and hack or even accessing malware from an email or message on a computer or device without properly checking its source.

In 2019, for instance, data on almost the entire population of Ecuador were exposed: detailed information on adults and children alike, including addresses, family relationships and financial status, employment and school data, were found to be available on an unsecured and easily accessible server in Miami.[186] This highlights both the extent of the risk and its global nature.

Digitized services need not respect boundaries. Information need not be and often is not stored or processed in the country where it is collected. International offers of services become an important option for achieving scalability and cost-efficiency. However, such services are open to security incidents that affect more than one jurisdiction.

Cases of intentional intrusion and appropriation of personal information have also become more common. These range from simple procedures to more complex frauds and hacking. The origin and motivation of intrusions may vary widely, from corporate espionage to surveillance by a foreign power.[187] Some instances may involve more seemingly altruistic motives such as exposing crime and corruption. The Panama Papers scandal falls into this category.[188]

5.2. The development of biometric data and digital identities has been a source of controversy

Services are migrating to cyberspace and becoming fully digital. Banking is one example of a service where most functions can operate online without there necessarily being a need for a physical presence. Other services, including services provided by the public authorities, are being structured in the same way.[189] This brings gains in scale and efficiency. A senior citizen receiving a State pension, for instance, does not necessarily need to appear before a civil servant to provide proof of life: there are digital methods that involve less effort from the individual and less cost for the administration.

However, this shift brings the challenge of authenticating a person's identity: confirming that an individual is actually who they claim to be. A digital ID system seems to be a way of solving these difficulties and unambiguously authenticating a person. A digital ID can act as a key to unlock access to digital services, reducing transaction costs while increasing efficiency.[190]

Several States in Latin America and the Caribbean are exploring ways to institute forms of digital identity. Unlike other regions in the world, however, these countries usually have a national identity system already in place,[191] which both facilitates and complicates the process.[192] The protocols and

186 See [online] https://www.nytimes.com/2019/09/17/world/americas/ecuador-data-leak.html.
187 See [online] https://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillanc.
188 See [online] https://www.icij.org/investigations/panama-papers/pages/panama-papers-about-the-investigation/.
189 Information on Latin America from the *United Nations E-Government Survey, 2018* [online] https://www.un.org/development/desa/publications/2018-un-e-government-survey.html.
190 World Bank, *Principles on Identification for Sustainable Development: Toward the Digital Age* [online] http://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-identification-for-sustainable-development-toward-the-digital-age.pdf.
191 Inter-American Development Bank (IDB), "Registros civiles y oficinas de identificación: análisis y fichas de país", 2019 [online] http://dx.doi.org/10.18235/0001865.
192 It is important to note that countries in Latin America and the Caribbean have not achieved universal registration at birth, which means a potential problem with general inclusion as well. See United Nations Children's Fund (UNICEF), "Birth Registration in Latin America and the Caribbean: Closing the Gaps", 2016 [online] https://data.unicef.org/resources/birth-registration-latin-america-caribbean-closing-gaps/.

security arrangements available do not necessarily extend to or fit well with the requirements of digital IDs. Risks and concerns do not perfectly align. Chief amongst them are unauthorized access to and control of personal data and issues related to digital inclusion and cybersecurity.[193]

Many of the efforts being made to create digital IDs are throwing up a variety of potential cross-border issues relating to how they might be used online and their impact beyond the frontiers of the country concerned. Questions arise about the locations where data are stored, the origins of potential threats to cybersecurity, and how best to manage registration, authentication and authorization mechanisms.[194] Vendor lock-in, use of proprietary technology, non-interoperable systems and cloud services (international storage and data processing) are also important factors.[195] Depending on how these challenges are responded to, matters of efficiency, inclusion, transparency, security, resilience and privacy will come into play in different ways.[196]

With cloud-based arrangements, for instance, data may be stored abroad and in multiple locations. Dealing with access, data transfers and security incidents may have major cross-border jurisdictional repercussions that go beyond more common issues of e-government data storage. One example is the investigation of breaches or crimes connected to such services, which relies heavily on international cooperation.

The fact that these digital identities are usually accompanied by personal biometric attributes captured electronically (fingerprints, irises, facial images, etc.)[197] makes these decisions even more significant. A person cannot cancel and reissue their face or fingerprints if biometric data are leaked, as would happen with a stolen credit card, for example. This makes the structuring of such solutions a priority and means that high-level cybersecurity specifications are required by design.

A final issue is that mutual recognition of IDs may be a driver of regional and economic integration, including a digital single market. Southern Common Market (MERCOSUR) countries recognize each other's IDs for migration purposes, which is a first step. Several electronic signature initiatives have prospered both in MERCOSUR and in other regional arrangements.[198] However, it is recognition of digital IDs that can unlock the greatest potential for circulation of goods, services and businesses across the region and boost the digital economy.[199]

> Several countries in the region are moving towards digitizing their identification documents. Argentina, for instance, has integrated its process within the digital identity system (SID). Similarly, Uruguay has become a leader in e-government and has implemented a digital identity programme covering its whole population. Peru recently introduced an electronic national identity system (DNI-e), which provides access to a number of government services.[200] As regards applications, it is reported that, thanks to the widespread use of digital identities, the emergency relief benefits approved by the Chilean Government at the beginning of the pandemic were quickly made available to the population in greatest need even though a strong checking mechanism was applied.[201]

193 McKinsey, *Digital Identification: A Key to Inclusive Growth*, 2019 [online] https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth.
194 See [online] https://id4d.worldbank.org/guide/hosting-options.
195 This has happened in other regions. For comparison, see [online] http://documents1.worldbank.org/curated/en/156111493234231522/pdf/114628-WP-68p-TheStateofIdentificationSystemsinAfricaASynthesisofIDDAssessments-PUBLIC.pdf.
196 S. Bhadra, *Five Surprisingly Consequential Decisions Governments Make About Digital Identity*, 2019 [online] https://www.omidyar.com/blog/five-surprisingly-consequential-decisions-governments-make-about-digital-identity.
197 A. Gelb and J. Clark, "Identification for development: the biometrics revolution", *CGD Working Paper*, No. 315, Washington, D.C., Center for Global Development, 2013 [online] https://www.cgdev.org/publication/identification-development-biometrics-revolution-working-paper-315.
198 Economic Commission for Latin America and the Caribbean (ECLAC), "Regional digital market: strategic aspects", 2018 [online] https://repositorio.cepal.org/bitstream/handle/11362/43633/1/S1800569_en.pdf.
199 See [online] https://id4d.worldbank.org/guide/mutual-recognition-ids-across-borders-0.
200 Inter-American Development Bank (IDB), "Registros civiles y oficinas de identificación: análisis y fichas de país", 2019 [online] http://dx.doi.org/10.18235/0001865.
201 World Bank, "Harnessing the power of Digital ID", 20 August 2020 [online] https://blogs.worldbank.org/voices/harnessing-power-digital-id.

C. Economy

1. E-commerce: the aspiration of a digital single market

Unsurprisingly, the Internet has created a paradigm shift in international trade. The trade infrastructure developed over millennia for the exchange of goods through international business transactions faces major challenges in the effort to adjust to the speed and variety of transactions presented by online opportunities. Market access for goods and even services is qualitatively and quantitatively different online. New Internet-based technologies have reduced the costs of transboundary trade. Both services and goods cross borders regardless of volume or value. With lower costs, companies of all sizes can be integrated into the international value chain and take part in global trade.

The fact that the Internet is not based in one country or another means that a person in country A can supply services or goods to someone in country B through a platform –an intermediary service– that is in neither of the two countries. This clearly happens for music and video streaming, for goods (properly e-commerce), for news media and for finance, health and other services. This type of international trade may come in different shapes and forms: business-to-business (B2B), business-to-consumer (B2C), consumer-to-consumer (C2C) and business-to-government (B2G). The common denominator among such transactions is that the Internet has facilitated access to markets beyond national borders.[202] A different market is being forged, one that is completely digital.

Cross-border transactions, though, cannot necessarily be subjected to a single jurisdiction. In other words, markets may seem global, but the laws that apply to them tend to be local. The stakeholders surveyed noted that this was true of contractual transactions, dispute resolution mechanisms (access to courts), consumer protection, cross-border payments (further discussed in section IV.C.4 below), international data flows (section IV.C.6) and antitrust laws.

In order to find solutions to these problems, some regions have proposed strategies to harmonize rules and standards.[203] One of the best-known efforts is the European digital single market.[204]

In Latin America and the Caribbean too there are initiatives aimed at facilitating digital trade with a view to structuring a regional digital single market.[205] This section will discuss the cross-border opportunities and challenges of such initiatives and some of the peculiarities of the region.

1.1. Opportunities and challenges for a regional digital single market

Digitalization has taken the form of public services delivered online; of applications making the so-called Internet of Things a reality in houses and factories and on farms; of process automation; and of the large-scale use of big data and artificial intelligence to improve many different activities. The digital economy has had an impact on the goods and services that are most important for cross-border trade. Digital goods and services are now a familiar part of life, and online access to physical goods and services has become a daily routine. Thus, the economic and social importance of digital markets is being felt at all levels.

Fully benefiting from these advances requires market access and market integration or interoperability. The promotion of a digital single market is one important strategy. It is bound up with the borderless nature of the Internet notwithstanding geographical and jurisdictional divisions, spreading the benefits of a digital market among participants. Individuals and organizations residing anywhere in the region can offer services and goods to the whole of it, just as individuals and organizations are able to seek out services and goods they desire, regardless of their origin.

---

202 Estimates for the relative positions of each type can be found in the study by the United Nations Conference on Trade and Development (UNCTAD) [online] https://unctad.org/en/PublicationsLibrary/tn_unctad_ict4d06_en.pdf.

203 There are scholars who, instead of harmonization, use the concept of "glocalization", blending aspects of global distribution and access with customized conformity with local laws. See A. Chander, "Glocalization and harmonization", *The Electronic Silk Road*, Yale Press, 2013.

204 European Commission initiative, European Digital Single Market [online] https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market.

205 See [online] https://repositorio.cepal.org/bitstream/handle/11362/43633/1/S1800569_en.pdf.

This strategy has to include integration and harmonization of legal rules. Most of the States in Latin America and the Caribbean belong to one or more regional organizations and agreements connected with transnational digital trade, such as the Organization of American States (OAS), the Economic Commission for Latin America and the Caribbean (ECLAC), the Andean Community, the Caribbean Community (CARICOM), the Latin American Integration Association (LAIA), Asia-Pacific Economic Cooperation (APEC), the Central American Integration System (SICA), the Southern Common Market (MERCOSUR), the North American Free Trade Agreement (NAFTA), the Mesoamerica Project, the Pacific Alliance and the Trans-Pacific Partnership (TPP).[206] One noteworthy initiative is the CARICOM Single ICT Space, which aims to facilitate the creation of a unified digital area for goods, people, services and capital to circulate.[207]

There is still much to be developed in the region as regards common infrastructure and harmonized legal frameworks. There is no unifying central entity with the ability to bind countries into initiatives. Enforcement efforts are likewise left to each jurisdiction to manage separately. This is reflected in the views of the stakeholders interviewed, who indicated that the difficulty of establishing a digital single market in Latin America and the Caribbean lay in the fact that none of the integration efforts proposed had been successfully implemented. Thus, jurisdictional differences impact market access and growth opportunities in the region. One expert mentioned that legal and economic disparities and the lack of minimum common regulatory standards were the greatest barriers.

There are, however, some common trends among the countries in the region. E-commerce is expanding constantly. Additionally, the start-up environment is growing exponentially in areas such as logistics, transportation, digital payments and agricultural technology (agritech).[208] The road ahead is still a long one, however, particularly where intraregional arrangements are concerned.[209]

Several of the stakeholders surveyed mentioned the digitalization of the economy as an opportunity but underscored the need for regulatory harmonization. Harmonization was viewed as particularly crucial in areas such as consumer protection, personal data protection, digital IDs, digital payments, digital securities, transportation and logistics standards, and taxation regimes.

That perception seems to be in tune with the recommendations of international organizations.[210] Few legislative or regulatory initiatives in the region have taken into consideration the cross-border challenges of creating a more integrated digital market.[211] Such initiatives as there are still tend to be conceived from a domestic standpoint, resulting in a very fragmented situation with a multiplicity of standards.

1.2. The region has a strong consumer rights culture, but with different local standards

Virtually all countries in the region have consumer protection legislation in force, in most cases in the form of dedicated laws.[212] Some countries do have specific laws on online consumer transactions, but in most the State consumer protection regime is mainly geared towards offline relationships. This situation creates an opportunity to develop a digital single market for Internet platforms and e-commerce generally.

206 Economic Commission for Latin America and the Caribbean (ECLAC), "Regional digital market", 2018 [online] https://repositorio.cepal.org/bitstream/handle/11362/43633/1/S1800569_en.pdf.
207 See[online]https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC_Unleashing_Internet_in_Caribbean_20170221.pdf.
208 Economic Commission for Latin America and the Caribbean (ECLAC), "Regional digital market", 2018 [online] https://repositorio.cepal.org/bitstream/handle/11362/43633/1/S1800569_en.pdf.
209 World Bank data indicate that much needs to improve in the digital market of Latin America and the Caribbean. See [online] www.doingbusiness.org.
210 See, for instance, the study by the Organization for Economic Cooperation and Development (OECD) [online] https://www.oecd-ilibrary.org/docserver/9789264251823-16-en.pdf?expires=1588103565&id=id&accname=guest&checksum=233F2DB69A0B854F11BC076348793B73.
211 Andean Development Corporation (CAF), "Building a Digital Single Market Strategy for Latin America" [online] https://scioteca.caf.com/handle/123456789/980?show=full.
212 Economic Commission for Latin America and the Caribbean (ECLAC), "Regional digital market", 2018 [online] https://repositorio.cepal.org/bitstream/handle/11362/43633/1/S1800569_en.pdf. See also "World Consumer Protection Map" [online] https://unctadwcpm.org. For an overview of a number of national regimes and how they fare in comparison with other countries in the world, see Hans-W. Micklitz and Geneviève Saumier (eds.), *Enforcement and Effectiveness of Consumer Law*, Springer, 2018.

Market internationalization brings jurisdictional challenges for companies that operate across borders. These companies, in the areas of e-commerce, marketplaces or social media, have to be prepared to comply with consumer protection laws in all the jurisdictions where they conduct business. National consumer protection laws are applicable wherever an Internet company's physical headquarters may be. The mere fact of offering goods and services to local consumers triggers national protections.[213]

The presence of a common consumer protection culture in Latin America and the Caribbean has so far coexisted with the lack of a proper harmonized framework or a digital single market, exposing companies to a variety of different domestic standards of protection. Additionally, consumers may seek to resolve their disputes in their own country, with the result that companies are required to appear in court in several jurisdictions or to take part in different dispute settlement procedures outside the country where they are established.

In a further layer of complexity, many of the laws concerned are understood to be imperative norms (*lois de police*), which means that in most cases contractual stipulations ought not to contradict them. In other words, such laws are applicable irrespective of the terms and conditions and contractual stipulations present in Internet transactions.[214]

During the negotiations over the Inter-American Conference on Private International Law (CIDIP VII) concerning international protection for consumers, a number of countries contended that international consumer transactions should be subject to a "most favourable protection principle". The law applicable to the contract would be the one most favourable to the consumer, be it the law applying in the place of jurisdiction, of the consumer's habitual residence or of the contract.[215]

The lack of common consumer protection standards impacts the way ISPs can interact with consumers in the region. Different consumer protection laws may mean a variety of standards for advertising, unfair billing practices, contract termination, and switching of companies (portability and interoperability as well).[216] This situation could act as a barrier to trade.[217]

The other side of the equation is that, by contrast with the digital market in Europe, for instance, consumer protection laws in Latin America and the Caribbean tend to be enforced only within the boundaries of each national jurisdiction. Thus, it is a common practice for companies to use geolocation technologies to restrict access to goods and services in certain locations.[218]

In MERCOSUR, there have been initiatives to harmonize consumer protection standards. Recently, members proposed to structure and use a digital platform for the settlement of consumer disputes.[219] This could help to foster cross-border Internet services and e-commerce in the region by reducing the costs of consumer disputes and litigation.

1.3. Choice of law and choice of forum clauses tend to be frowned upon in e-commerce because of national consumer protections

The lack of harmonized rules and of a single digital market, coupled with the footloose nature of the Internet, makes ascertaining jurisdiction over cross-border transactions particularly challenging. To provide more predictability, most Internet companies elect to include in their contracts a choice of forum clause, or a method of dispute resolution (arbitration, mediation or conciliation), as well as a choice of law clause. By having these stipulations, they limit their exposure and reduce the potential for jurisdictional entanglement.

213 Andean Development Corporation (CAF), "Building a Digital Single Market Strategy for Latin America" [online] https://scioteca.caf.com/handle/123456789/980?show=full.

214 C. Marques, "A proteção da parte mais fraca em direito internacional privado e os esforços da CIDIP VII de proteção dos consumidores", OAS Course on International Law [online] http://www.oas.org/es/sla/ddi/docs/publicaciones_digital_XXXIV_curso_derecho_internacional_2007_Claudia_Lima_Marques.pdf.

215 The negotiations were not concluded, but the concept remained a significant one in international forums and provided a baseline for intraregional discussion [online] http://aebm.mo/en/2018Vol1Issue1/8.

216 See [online] https://www.oecd-ilibrary.org/docserver/9789264251823-16-en.pdf?expires=1588103565&id=id&accname=guest&checksum=233F2DB69A0B854F11BC076348793B73.

217 M. Durovic, "International consumer law: what is it all about?", *Journal of Consumer Policy*, vol. 43, 2020 [online] https://doi.org/10.1007/s10603-019-09438-9.

218 Andean Development Corporation (CAF), "Building a Digital Single Market Strategy for Latin America" [online] https://scioteca.caf.com/handle/123456789/980?show=full.

219 See [online] https://www.cancilleria.gob.ar/es/actualidad/noticias/comunicado-conjunto-de-los-presidentes-de-los-estados-partes-del-mercosur.

Legal regimes worldwide usually permit such choices under what is called party autonomy. Latin American and Caribbean countries struggled with the concept for most of the twentieth century,[220] culminating in the approval of the 1994 Inter-American Convention on the Law Applicable to International Contracts, although, partly because it enshrines the principle of party autonomy, this has not been widely accepted, with only the Bolivarian Republic of Venezuela and Mexico having ratified it.[221] In the last two decades, however, the principle has gained traction, and many countries have adopted a more flexible stance, accepting party autonomy for certain categories of contracts.[222]

Additionally, several States are parties to the United Nations Convention on Contracts for the International Sales of Goods (CISG) of 1980. Cross-border Internet sales of goods might thus be covered by its provisions, which provide for party autonomy. However, the convention does not necessarily supersede other considerations, particularly consumer protection.[223]

The issue of the place of forum and applicable law has thus become one of three parts: (i) whether a country allows choice of law and choice of forum; (ii) whether party autonomy is accepted for choices of non-judicial means to settle disputes (e.g., arbitration and mediation) and under what conditions; and (iii) whether certain categories of transactions, such as consumer transactions, receive a different level of protection.

The region's strong culture of consumer protection has left its mark on the way contracts are interpreted there. Many Latin American and Caribbean countries consider that contracts in which there is an inherent imbalance between the parties, with the stronger party imposing contractual obligations, ought to be subject to stronger scrutiny.[224] The consequence is that choice of law and choice of forum clauses tend to be frowned upon when they may be disadvantageous to the weaker party.[225] In some circumstances, they are seen as abusive, particularly if they limit the options for dispute settlement or access to the judiciary. This is particularly the case for transactions involving a consumer.[226]

Most Internet transactions (e-commerce and Internet services, for instance) are governed by so-called "click-wrap agreements" or "browse-wrap agreements", whose substantive clauses are found in the terms and conditions available online. These contracts leave little space for negotiation. Usually the weaker party (a consumer) has no option but to accept all clauses as they stand or forego access to that service or good. Such agreements are considered to be adhesion contracts and tend to be interpreted in favour of the weaker party. Not only may consumer protection laws apply, but the choice of forum and law clauses may be deemed non-enforceable, particularly if consumers challenge them in courts.[227]

Similarly, a dispute settlement mechanism clause may suffer the same fate. If the clause prevents a consumer from having access to the judiciary, this may be interpreted as abusive and courts may not enforce it. Internet companies that want to limit their exposure to different courts and laws may end up resorting to geolocation techniques in order to limit their geographic reach (see section V.B.1 below for more on these techniques).

220 See [online] http://www.oas.org/es/sla/ddi/docs/publicaciones_Contratos_Internacionales_OEA-ASADIP_2016_Publicacion_Completa.pdf.
221 See [online] https://www.oas.org/juridico/english/sigs/b-56.html.
222 In the region, only Uruguay explicitly rejects party autonomy, although there has been some acceptance in doctrine and case law. In Brazil, there is still discussion on whether it is fully applicable, and case law is not consistent. For an overview, see Inter-American Juridical Committee, "Guide on the Law Applicable to International Commercial Contracts", February, 2019 [online] https://www.oas.org/en/sla/iajc/docs/Guide_Law_Applicable_to_International_Commercial_Contracts_in_the_Americas.pdf.
223 For a list of country parties, see [online] https://uncitral.un.org/en/texts/salegoods/conventions/sale_of_goods/cisg.
224 See [online] http://www.oas.org/es/sla/ddi/docs/publicaciones_Contratos_Internacionales_OEA-ASADIP_2016_Publicacion_Completa.pdf.
225 The International Law Association has acknowledged that consumers tend to be the weaker parties in cross-border contracts. See International Law Association (ILA), "Resolution No.1/2016. Committee on the International Protection of Consumers", [online] https://www.ila-hq.org/images/ILA/docs/No.1_Resolution_2016_ProtectionOfConsumers_4Models.pdf. One clear example is article 2651 of the Argentine Civil Code, which permits party autonomy for all contracts except those involving consumers. Another are articles 89 and following of Panama's Code of Private International Law, which establish a special regime for contracts where the parties are not on an equal footing ("unequal or adhesion contracts").
226 There have been intraregional efforts to draft international conventions to deal with international cross-border jurisdictional issues involving consumers, of which CIDIP VII is one. It did not come to fruition, among other reasons, because there was no agreement on the role of party autonomy or the option to choose arbitration as a means to settle disputes. For an overview of this effort, see D. Fernández Arroyo and J. A. Moreno Rodríguez, *Protección de los consumidores en América: trabajos de la CIDIP VII (OEA)*, Asuncion, La Ley-CEDEP, 2007. See also [online] http://www.oas.org/es/sla/ddi/docs/publicaciones_digital_XXXIV_curso_derecho_internacional_2007_Claudia_Lima_Marques.pdf; and https://docplayer.es/80967826-The-inter-american-convention-on-the-law-applicable-to-international-contracts-and-the-furtherance-of-its-principles-in-the-americas.html.
227 See [online] http://www.oas.org/es/sla/ddi/docs/publicaciones_Contratos_Internacionales_OEA-ASADIP_2016_Publicacion_Completa.pdf.

1.4. Governments in the region are imposing stricter rules for content moderation and removal on online platforms

The *Internet & Jurisdiction Global Status Report* 2019 identified a global trend for States to take a tougher attitude towards Internet platforms. Countries in Latin America and the Caribbean have been part of this trend.

The peculiarities of Internet companies and the services they provide initially led to the widespread adoption of rules and guarantees that would shield them from major litigation over content created by third parties, mainly their own users. That tendency arose in the latter part of the 1990s, when section 230 of the Communications Decency Act (CDA) and the Digital Millennium Copyright Act (DMCA) created something of a safe harbour for Internet providers in the United States. The EU followed suit with the E-commerce Directive (2000/31/EC).

A lot has changed since the late 1990s, as e-commerce platforms have become ubiquitous and social media companies can have a majority of a country's population as their users without having any office there. At the same time, the astonishing speed with which content is produced online continues to reinforce the need to design a special regime for content moderation and liability. Numbers such as the 6,000 tweets sent per second and the 400 hours of YouTube video uploaded every minute are unquestionably challenging to deal with.

Some countries in the region have enshrined safe harbour protections for Internet intermediaries in their legislation, creating a specific exception to the enforcement of general liability rules or general consumer protection regimes for malfunctioning products or services.[228]

Even though the situation is rapidly changing and many local Internet companies are springing up, countries in Latin America and the Caribbean are still served mostly by Internet companies and platforms established outside the region. Thus, every interaction tends to be transnational, potentially raising jurisdictional issues.

The approach towards Internet platforms has changed in at least two areas: third party content (content moderation) and protection of intellectual property (piracy and counterfeiting). As mentioned in other sections, areas such as law enforcement (section IV.B.2), cyberbullying (section IV.A.3) and unauthorized exposure of intimate images (section IV.A.4) have also put pressure on Internet intermediaries to take on a more active role and cooperate with law enforcement agencies.

In Brazil, the Supreme Court has had to rule on whether the safe harbour provision (a clause that limits the liability of Internet intermediaries for hosting or transferring third party content) present in the Brazilian Internet Bill of Rights is consistent with the federal constitution.

A bill to regulate intermediary liability failed to receive the necessary support in Argentina.[229] Similarly, Mexico has struggled to find support for the establishment of a liability regime consistent with the Agreement between the United States of America, the United Mexican States, and Canada (USMCA), which provides for the creation of a safe harbour for cross-border digital trade amongst its parties.[230]

In Ecuador, a bill was proposed to regulate speech online, including provisions that would make Internet intermediaries directly responsible for taking down speech deemed illegal.[231] A similar bill was proposed in Honduras, providing very broad definitions of the kinds of illegal speech that Internet intermediaries should monitor.[232]

In the same vein, a law passed in the Bolivarian Republic of Venezuela emphasized the responsibility of intermediaries and provided for sanctions if they did not take down illegal speech. State entities can also directly request content to be taken down.[233] A bill in Paraguay sought to impose an obligation for ISPs to take down speech deemed "offensive".[234]

228 Only Brazil and Chile have "safe harbour" provisions, which limit the responsibility of Internet intermediaries for hosting or transferring third party content, enacted as part of their legislation. See Inter-American Development Bank (IDB), "Accelerating Digital Trade in Latin America and the Caribbean" [online] https://publications.iadb.org/publications/english/document/Accelerating-Digital-Trade-in-Latin-America-and-the-Caribbean.pdf.
229 See [online] https://www.lanacion.com.ar/tecnologia/los-intermediarios-internet-debate-seguira-pendiente-nid2192063.
230 See [online] Retrieved from: https://www.derechosdigitales.org/12564/usmca-y-el-futuro-de-internet/.
231 See [online] https://www.eluniverso.com/opinion/2017/06/13/nota/6229435/redes-sociales-censura.
232 See [online] https://www.accessnow.org/comunicado-ley-que-regula-los-actos-de-odio-y-discriminacion-en-internet-de-hons/. See also [online] https://www.hrw.org/news/2018/04/09/honduras-cybersecurity-bill-threatens-free-speech.
233 See [online] http://espaciopublico.ong/ley-odio-venezuela-amenaza-la-libre-expresion-america-latina/.
234 TEDIC, "Un proyecto de censura política", 11 October 2017 [online] https://www.tedic.org/un-proyecto-de-censura-politica/.

Civil society organizations have expressed concern about initiatives to increase the liability of intermediaries.[235] The Special Rapporteur for Freedom of Expression has echoed misgivings about the potential human rights risks of these legislative initiatives.[236]

Much of the focus has been on social media platforms, but e-commerce websites and marketplaces have not been ignored. Governments in the region have tightened measures against piracy and counterfeit goods, both restricting speech deemed illegal and strengthening protections for intellectual property rights.

Reform of intellectual property rights, including copyright, may also provide an opportunity for countries to harmonize their views and facilitate region-wide approaches, facilitating the circulation of copyrighted goods and services and of other classes of intellectual property.

2. Intellectual property

Various intersections between the Internet and intellectual property rights have already been highlighted in the *Internet & Jurisdiction Global Status Report* 2019. Intellectual property rights over patents, trademarks and designs in the digital environment do not have to be restricted to any particular territory. Their embodiment in a physical form may seem to be a limitation, as for instance when a movie in the past had to be in the format of a film, tape or digital videodisc (DVD) in order to circulate. But the more the flesh becomes word, to paraphrase Barlow, the less the physical barriers that hinder the circulation of intellectual property act as a restriction.[237] Copyrighted material can be downloaded or live streamed without regard to borders.

Intellectual property regulation, however, is still in many ways a domestic affair, particularly where exceptions are concerned. Thus, regulatory differences, ranging from interpretations of international treaties to actual enforcement mechanisms, tend to lead to cross-border difficulties. This is particularly challenging when individuals and companies use the borderless nature of the Internet to circumvent legislation or even judicial decisions aimed at effectively protecting intellectual property.

2.1. Intellectual property protection: impacts on the economy and human rights

Copyright enforcement mechanisms vary from State to State. The way they are structured is an important aspect of a very intricate balance between providing incentives to authors, protecting the economic interests of industry and safeguarding society's right to and interest in accessing the fruits of creation. In other words, copyright is a key institution that both fosters and safeguards culture. Enforce copyright too strictly, however, and it may actually restrict access to knowledge and the advancement of culture.

In an environment where memes are a major social trend, new works are often produced on the basis of earlier, usually copyrighted material. Restricting access to and use of copyrighted content limits both access to knowledge (ideas and material) and innovation.[238]

In Latin America and the Caribbean, it is paramount for the balance between protecting copyright and safeguarding access to be well reflected in regulations. The stakeholders surveyed noted the relationship between copyright and development, but also emphasized that in many circumstances copyright could be used to restrict societies' access to information. Copyright has even been used as a tool to restrict freedom of expression. This has been reported to be the case with material critical of President Correa during the Ecuadorian elections.[239]

---

235 See [online] https://www.derechosdigitales.org/internetesnuestra/desafios-gobernanza.pdf.

236 Organization for Security and Cooperation in Europe (OSCE), "Joint Declaration on Freedom of Expression and 'Fake News', Disinformation and Propaganda" [online] https://www.osce.org/fom/302796. The Inter-American Commission on Human Rights has also made its concern known with a similar initiative in the electoral context. See [online] https://www.oas.org/en/iachr/expression/publications/Guia_Desinformacion_VF%20ENG.pdf.

237 John Perry Barlow, "Selling wine without bottles: the economy of mind on the global net", *Duke Law and Technology Review*, vol. 18, 2019.

238 A. Chander and M. Sunder, "Dancing on the grave of copyright?", *Duke Law & Technology Review*, vol. 18, 2019 [online] https://ssrn.com/abstract=3436972.

239 See [online] https://www.hrw.org/world-report/2018. This is reported to have happened in other circumstances as well. See A. Ellerbeck, "How U.S. copyright law is being used to take down Correa's critics in Ecuador", Committee to Protect Journalists, 21 January 2016 [online] http://bit.ly/1Lu5Uoj.

Another aspect to be taken into consideration is that in many circumstances inaccurate information (including disinformation) is available free of charge and circulates without barriers, but actual knowledge and necessary information are restricted, "protected" by paywalls and databases that are hard to access.[240]

In this context, there has been a debate on how to better balance the protection of intellectual property, particularly copyright, against the rights to education, access to information and self-development and other human rights. The question, in some cases, has been whether strong enforcement procedures against piracy, and in some circumstances unauthorized reproduction, are the best way to achieve the policy goals of copyright.

One important example is the protection of traditional knowledge. Properly safeguarding the knowledge, traditions, procedures and cultural manifestations of traditional groups and indigenous populations in the region is paramount for the protection of their way of life and, by extension, their human rights. Many countries in the region have become more aware of the need to provide better and more specific rules recognizing traditional knowledge. The Bolivarian Republic of Venezuela, Brazil, Costa Rica and Peru are clear examples of this trend. There have been cases of countries lodging complaints with international corporations for their exploitation of traditional knowledge, with relationships being transferred in some cases to Internet intermediaries selling products with due protection.[241]

2.2. The cross-border effects of the filtering used to enforce intellectual property rights

The dynamics of protecting copyright online have many different facets. The private sector, and Internet intermediaries in particular, have been called on to play a more significant role lately. Voluntarily or through agreements with the public sector, a number of companies, chiefly marketplaces and social networks, have developed copyright protection mechanisms.

Amazon, for instance, has expanded its anti-counterfeiting "Project Zero" to 17 countries in total, including Brazil and Mexico in the Latin America and Caribbean region, as part of its intellectual property and brand protection initiative.[242] E-commerce platform Mercado Libre, with operations in 18 countries of Latin America, also has a copyright protection programme which operates in a similar fashion. These programmes include tools for rights holders and provide for sanctions for possible violations, extending to account suspension or cancellation for repeat offenders.[243]

These voluntary mechanisms are not necessarily sufficient, and certain jurisdictions have called for a review of current regulations on the matter. Recently, the EU issued Directive 2019/790, which has caused great controversy both in Europe and in the region.[244] The directive seeks to increase the liability of Internet intermediaries for third party content in their online environments (see section III.F for further information on the new role of Internet intermediaries).

Such regulations have impacted the region in two ways. First, they have spurred countries to review their own copyright legislation in order to include similar obligations. Second, as a direct cross-border effect, material owned by a number of artists or copyright holders may be taken down by such platforms and this will need to be contested in other countries (see section V.A.5 for more on online mechanisms for contesting such decisions).[245]

240 A. J. Robinson, "The truth is paywalled but the lies are free", *Current Affairs*, August 2020 [online] https://www.currentaffairs.org/2020/08/the-truth-is-paywalled-but-the-lies-are-free.

241 See [online] https://yourlatamflagship.com/2020/01/16/how-latin-america-countries-protect-their-traditional-knowledge-through-ip/. For more on this trend from a Latin American perspective, see L. Lixinski, *International Heritage Law for Communities: Exclusion and Re-Imagination*, Oxford University Press (OUP), 2019.

242 Press release, "Amazon Project Zero launches in seven new countries", August 2020 [online] https://press.aboutamazon.com/news-releases/news-release-details/amazon-project-zero-launches-seven-new-countries/.

243 Mercado Libre, "Brand Protection Program: qué es y cómo usarlo" [online] https://vendedores.mercadolibre.com.ar/blog/notas/brand-protection-program-que-es-y-como-usarlo/.

244 See [online] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0790.

245 See [online] https://br.creativecommons.org/a-diretiva-da-uniao-europeia-sobre-direito-de-autor-e-seu-impacto-sobre-os-usuarios-na-america-latina-e-no-caribe/.

Civil society organizations have expressed concern that the new EU copyright directive may become a template for copyright reform in the region and may have a chilling effect on speech and hinder online trade. In their view, the requirements of this legislation may lead to automatic filtering and provide very little space and time for contextual analysis.[246]

> In Brazil, the Fake News Bill (see section IV.A.1) has encouraged associations in the radio and television industry to propose compensation for publishers of press material as a form of copyright compensation when such material is used by ISPs. In their view, this measure would be effective in boosting professional journalism, potentially helping to combat disinformation and fake news.[247] A similar mechanism (the "link tax") provided for by article 15 of the EU Copyright Directive[248] has been widely criticized on the grounds that it could jeopardize access to information and because of the disadvantages it could bring to small and non-commercial services.[249]

Filters, which are automated tools for detecting and taking down copyrighted content, further exacerbate this phenomenon. The techniques they use often generate false positives, flagging and restricting content that is legal or fits one of the exceptions to copyright restrictions (parody, fair use, educational use, etc.). Hence, either companies must adapt their filters to different local laws and contexts, or they will have to opt for a general filter that may create more restrictions than necessary.

Latin America and the Caribbean is likely to be impacted by such filters and copyright controls. The circulation of copyrighted materials may suffer. The cultural and entertainment sectors are clear examples. Countries benefit from cultural cross-pollination among artists in the region. Online sharing tends to mean much bigger markets and audiences for local artists. Filters may protect copyright but may also limit exposure and make it harder to appeal against decisions reached by platforms (see section V.A.5 on the subject of appeals).

3. The Internet of Things (IoT)

A twofold phenomenon has been taking place worldwide: digitalization of the physical space and a merger of the physical world with the digital one. This superposition of the physical and the digital is reducing production, transaction and distribution costs. It is also creating new opportunities. The concept of the Internet of Things (IoT) covers a significant part of this. Connecting devices that were traditionally unconnected, from fridges to tractors and from water supply systems to power grids, makes more data and functions available. Thus, more specialized goods and services can be supplied, fact-based (data-based) decision-making can be streamlined, and overall experiences, including timeliness, can be improved.

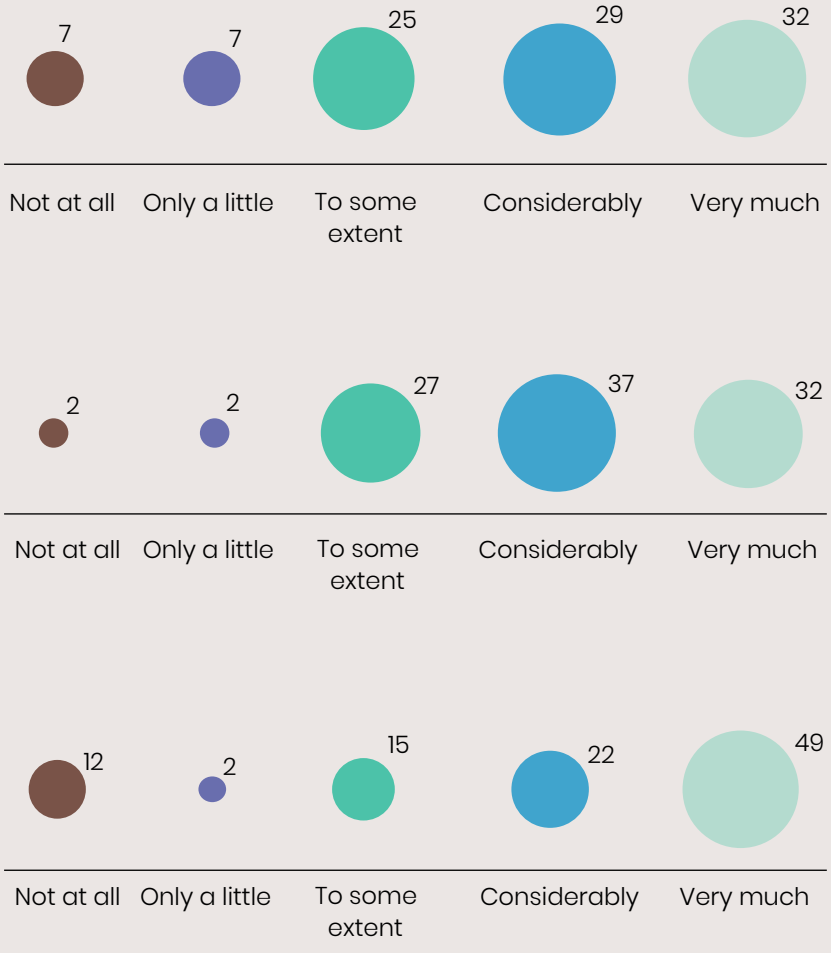
IoT is about more than providing an Internet connection: it creates technology-based ecosystems whose value is generated by capturing, recording and analysing data. The value of these functions is enhanced by combining them with cloud computing, blockchain, robotics and artificial intelligence.[250] Thus, a manufacturer of farm equipment can have access, for instance, to data on the weather, driving habits and crop yields. A smart watch developer can use the product's monitoring features to provide an array of goods and services that may help people better administer their exercise and their drinking and eating habits: in a word, their health. A city can make better decisions on how its transport system resources are allocated.

246 See [online] https://web.karisma.org.co/la-directiva-europea-de-derecho-de-autor-y-su-impacto-en-los-usuarios-de-america-latina-y-el-caribe-una-perspectiva-desde-las-organizaciones-de-la-sociedad-civil/.
247 O Globo, "Entidades pedem transparência e valorização do jornalismo profissional no projeto contra fake news", 18 August 2020 [online] https://oglobo.globo.com/brasil/entidades-pedem-transparencia-valorizacao-do-jornalismo-profissional-no-projeto-contra-fake-news-24593224.
248 European Union, "Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC" [online] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0790.
249 Cory Doctorow, "The European Copyright Directive: what is it, and why has it drawn more controversy than any other directive in EU history?", Electronic Frontier Foundation, 19 March 2019 [online] https://www.eff.org/pt-br/deeplinks/2019/03/european-copyright-directive-what-it-and-why-has-it-drawn-more-controversy-any.
250 Economic Commission for Latin America and the Caribbean (ECLAC), *Data, algorithms and policies: redefining the digital world* (LC/CMSI.6/4), Santiago, 2018.

Business models centred on IoT do not have to respect vertical economic structures or be constrained by national boundaries. They benefit from the borderless nature of the Internet to which they are connected and to some extent from the dematerialization that comes with digitalization. This means a "sensor society" where everything that can be linked to the Internet will be and any data that can be shared will be too. Cross-border trade and transborder data flows are a likely consequence of implementing IoT. To take full advantage of it, there is a need for scale, convergence, harmonization and an interoperable environment with an interconnected market.

The stakeholders surveyed pointed out that the key challenges related to the establishment of protocols, common standards, industry patterns and the harmonization of rules and regulations. Their concerns for the region mostly coincided with the ones recorded in the *Internet & Jurisdiction Global Status Report 2019*: security and privacy; common technical standards; product safety; availability of bandwidth and connectivity; rules on liability; and regional interoperability.

One stakeholder noted that full harmonization of regulations and standards within the region might be a hard goal to achieve, but that an agreement on rules or guidelines for how companies and States could navigate regulatory differences within Latin America and the Caribbean was manageable. Some of the stakeholders emphasized that structuring a system around incentives for private investment should be the priority, to allow the industry to operate across countries. All these concerns and suggestions highlight the need for intraregional and global coordination and cooperation.



Considering the potential of IoT for revolutionizing many areas of the economy such as agriculture, medicine and transportation, to what extent do you believe regulatory harmonization is needed globally, regionally or nationally (e.g., in federal States)?

Source: Internet & Jurisdiction Policy Network and Economic Commission for Latin America and the Caribbean (ECLAC).

3.1. From private to public: smart connected homes in smart connected cities

The opportunities offered by IoT extend to anything that can have a sensor fitted and be connected to the Internet, from the most intimate (the human body) to the most public (cities), taking in houses, industries and fields.[251] The cross-cutting nature of IoT means that opportunities and challenges can be found in a vast array of subject areas and sectors.

The application closest to human experience is in wearables: smart devices that people have on them, next to their bodies and assisting them with their daily activities. They range from the most widely used devices such as smart watches to more sophisticated ones that measure brain waves or heart rhythms. Their convenience and value derive from their capacity to easily provide information on a person's status, allowing for better decision-making.

The situation is similar with home IoT appliances. They undoubtedly offer many benefits, by increasing the ease and efficiency of use of goods and services that can reduce household consumption (electricity, water and gas), for example, or by providing safety and security, in the case of cameras that monitor the grounds of a dwelling or appliances that sense a fire or lock down the property when there is danger. They may serve to establish a better connection with the outside world, making it easier to buy groceries or to call for services.

They do, however, also bring potential risks. IoT works with data that yield the insights needed for innovative goods and services to be provided. The ubiquity[252] and intimacy of many such devices undermine the separation between the public and private spheres and could pervert the presumption of privacy that people associate with their homes and bodies.[253] It is hard for individuals to control and understand the classes of data collected and processed. Thus, issues of transparency, control, consent and liability need to be addressed.

Considering that providers may have a global reach,[254] cooperation and coordination seem to be paramount. Most initiatives have taken the form of national plans, strategies and policies. The majority have only marginally incorporated a global or regional dimension, failing to establish a link between these dimensions and the topic of IoT itself. The stakeholders surveyed agreed on the need for harmonization, yet they seemed to be divided on whether specific rules for IoT were necessary. For example, some questioned whether more underlying regulations dealing with matters such as consumer and personal data protection and cybersecurity should be interpreted broadly to encompass the challenges presented by this technology.

IoT plans, strategies and actions

Brazil has a National Internet of Things Plan focusing on four main sectors: smart cities, health, agribusiness and manufacturing. The plan also emphasizes four strategic areas for development: innovation and internationalization, human capital, regulatory safety and privacy, and infrastructure for connectivity and interoperability.[255]

Mexico has made it a policy priority to focus on the industrial IoT. Car manufacturing is one of the focal points.[256]

Both Argentina and Colombia have developed IoT policies in partnership with the private sector. Their focus is on incentivizing strategic partnerships, cooperation and commercial agreements to foster an environment conducive to IoT development.[257]

251 See [online] https://www.internetsociety.org/policybriefs/iot-privacy-for-policymakers/.
252 Some devices are always on, collecting personal data [online] https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf.
253 Internet Society, "Policy Brief: IoT Privacy for Policymakers", 19 September 2019 [online] www.internetsociety.org/policy briefs/iot-privacy-for-policymakers/.
254 A study by McKinsey has drawn attention to the global reach of certain service providers. See [online] https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/unlocking-value-from-iot-connectivity-six-considerations--for-choosing-a-provider.
255 In 2019, the plan was institutionalized by Presidential Decree No. 2984/2019 [online] http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9854.htm. The original plan was brought out in 2017 by way of a multistakeholder initiative in partnership with the Brazilian Development Bank (BNDES) [online] https://www.bndes.gov.br/wps/portal/site/home/conhecimento/pesquisaedados/estudos/estudo-internet-das-coisas-iot/estudo-internet-das-coisas-um-plano-de-acao-para-o-brasil.
256 See [online] https://www.gob.mx/promexico/acciones-y-programas/mapas-de-ruta-22850.
257 In Colombia, this was done through the Centre of Excellence for the Internet of Things (CEA-IoT). See [online] http://www.cea-iot.org. In Argentina, the Internet and IoT Chamber plays the same role. See [online] http://cabaseiot.com.ar.

Smart cities are another area where IoT plays a transformative role. This technology can be integrated into the city landscape, capturing and analysing data to allow the authorities to better solve their municipalities' problems, whether through traditional means or technological ones.[258] IoT helps organize the urban environment, creating the basis for faster, evidence-based responses. Implementation is on its way for areas such as traffic, parking, security, pollution and hygiene.[259]

Smart city projects tend to be implemented through public-private partnerships involving a multitude of actors, not all of them from the country concerned. Each layer involves a complex series of decisions on, for instance, which institutions and companies are to be involved, where the supplies should come from, what the set-up should be and how and by whom the project should be administered. The answers may require regional and international coordination.

Potential jurisdictional complexities are thus arising at many international touchpoints. Each layer, starting from the connectivity infrastructure (5G, for instance), is dependent on strategic alliances and cooperation between a number of suppliers and providers that may be situated anywhere on the planet. As the IoT ecosystem in the region becomes more complex and goods and services are increasingly supplied through a chain of providers that may not be established in the same country as the user, jurisdictional solutions may have to be reviewed.

The Latin America and Caribbean region is one of the world's most highly urbanized, and the challenges are correspondingly great. Thus, IoT for public services could have a substantial impact, altering the whole panorama of cities and the way public policies are designed for them. Cities themselves and the countries of the region alone cannot provide all the necessary solutions.[260] There is a tendency to seek partnerships and alliances with foreign providers, which makes the need for coordination even greater.

Two other aspects take on a particular character in Latin America and the Caribbean: open municipal data and citizen participation. By comparison with their peers elsewhere, cities in the region have been quick to embrace open data. This allows available data to be repurposed for innovative services. Starting with a Brazilian initiative in the 1990s, citizen participation in the allocation of municipal funds has become part of the administrative dynamics of many cities in the region.[261] In this context, the use of online platforms in combination with IoT can lead to discussions about accountability, control and the allocation of liability.

Notable smart city initiatives involving IoT in Latin America and the Caribbean

A number of cities in Argentina have been deploying IoT solutions.[262] Tigre, a city in greater Buenos Aires, was one of the first municipalities in Latin America and the Caribbean to implement an operations centre to protect the public and combat crime, employing face and number plate recognition cameras to track criminals and stolen cars, among other things. This initiative was achieved through a public-private partnership with multinational corporations and cloud data analysis.[263]

A "smart traffic lights" mechanism was developed for transport routes in Chacao and Maracay in the Bolivarian Republic of Venezuela. The system provides improved traffic management, reducing time spent on the road and road accidents.

Medellín in Colombia has developed an integrated operations centre that coordinates security and emergency actions, allowing agencies in the areas of security, transportation, emergency health care, disaster management, the environment and welfare to respond in a coordinated fashion to a single call. The programme relies on the extensive use of surveillance cameras and the georeferencing of calls.

258 Inter-American Development Bank (IDB), "Big urban data: a strategic guide for cities", 2019 [online] https://publications.iadb.org/en/big-urban-data-strategic-guide-cities.
259 Inter-American Development Bank (IDB), *IoT IN LAC 2019: Taking the Pulse of the Internet of Things in Latin America and the Caribbean* [online] https://publications.iadb.org/en/iot-lac-2019-taking-pulse-internet-things-latin-america-and-caribbean.
260 Inter-American Development Bank (IDB), *The Road toward Smart Cities: Migrating from Traditional City Management to the Smart City*, 2016 [online] https://publications.iadb.org/handle/11319/7743?locale-attribute=es&.
261 Inter-American Development Bank (IDB), "Big urban data: a strategic guide for cities", 2019 [online] https://publications.iadb.org/en/big-urban-data-strategic-guide-cities.
262 For an overview of the different smart city initiatives in Argentina, see [online] https://www.camarabilbao.com/ccb/contenidos.downloadatt.action?id=5334087.
263 See [online] https://www.nec.com/en/case/tigre/index.html.

In 2017, Chile launched a pilot programme in Temuco to pursue smart city solutions on an open platform. Four major areas were selected: air quality monitoring, virtual bus stops, refuse collection management and city incident management.[264]

Itu, in the state of São Paulo, Brazil, employs a public-private partnership to manage waste disposal. The municipality uses a vast number of containers and underground waste storage facilities connected to sensors that indicate whether there is a need for repairs or replacements, in addition to notifying the fill levels. This allows for better routing of collection trucks, reducing time, costs and environmental impacts.[265]

Digital inclusion and access to digital services is the aim of the Chihuahua Digital City programme in Mexico. The initiative is a public-private partnership that provides Wi-Fi coverage in a number of public areas of the municipality, including public offices and parks. It aims at democratizing access to the Internet and to digital public services.[266]

The city of Nassau in the Bahamas has developed a water management system that detects leaks, allows for advanced repair and replacement of pipes, monitors pressure and manages different levels of measurement. This has allowed the municipality to cut costs and reduce water loss from 58% to 29%.[267]

3.2. Smart farming could be a major regional opportunity

Some sectors of the Latin American and Caribbean economy seem more disposed than others to employ IoT in their activities, and none more so than agriculture. This accounts for a substantial share of the economy in most countries of the region and tends to be a bedrock of exports.[268] Raising productivity in this area can have an exponential impact on gross domestic product (GDP) and incidentally also have a positive effect on the environment by leading to more efficient use of land and other natural resources.[269]

Smart farming[270] and agricultural technology (AgTech) start-ups may present a major opportunity for the region. The deployment of IoT technology for the agriculture business can impact many areas, such as management of crops, precision crop cultivation, monitoring of livestock, intensive vertical farming both indoors and outdoors and better use of aquaculture. IoT for farms can have a positive impact on the whole value chain, improving both decision-making and the efficiency and precision of the actions taken. Planting, monitoring, harvesting, distribution, storage and marketing can be revolutionized.[271]

A significant part of the value added by IoT in agriculture comes from having access to data that otherwise would be very difficult to collect. Notable examples are soil humidity and microclimate indicators. These may vary sharply. Deploying IoT technologies may make it easier to map out and monitor these indicators. The greatest benefits come from advanced analytics that are dependent on the scale and volume of the data available and on processing capabilities.[272] These two aspects might lead to services being provided across jurisdictions and through partnerships with entities operating transnationally.[273]

264 See [online] https://www.ufro.cl/index.php/noticias/12-destacadas/1424-temuco-sera-la-primera-ciudad-inteligente-de-chile-y-piloto-para-otras-ciudades-de-latinoamerica.
265 See [online] https://exame.abril.com.br/revista-exame/o-que-aprender-com-a-excecao/.
266 See [online] https://www.researchgate.net/profile/Jose_Bordas-Beltran/publication/339389919_Chapter_11_Smart_territory_initiatives_in_an_emerging_economy/links/5e4ed07592851c7f7f48f66b/Chapter-11-Smart-territory-initiatives-in-an-emerging-economy.pdf.
267 Inter-American Development Bank (IDB), *The Road toward Smart Cities: Migrating from Traditional City Management to the Smart City*, 2016 [online] https://publications.iadb.org/handle/11319/7743?locale-attribute=es&.
268 Inter-American Development Bank (IDB), *The Next Global Breadbasket: How Latin America Can Feed the World: a Call to Action for Addressing Challenges and Developing Solutions*, 2018 [online] https://publications.iadb.org/en/publication/17428/next-global-breadbasket-how-latin-america-can-feed-world-call-action-addressing.
269 Inter-American Development Bank (IDB), *IoT IN LAC 2019: Taking the Pulse of the Internet of Things in Latin America and the Caribbean* [online] https://publications.iadb.org/en/iot-lac-2019-taking-pulse-internet-things-latin-america-and-caribbean.
270 Food and Agriculture Organization of the United Nations (FAO), "Smart farming is key for the future of agriculture", 2018 [online] http://www.fao.org/family-farming/detail/en/c/897026/.
271 See [online] https://www.researchandmarkets.com/research/lv69c3/global_iot_in?w=4.
272 See [online] https://www.researchandmarkets.com/reports/4600903/iot-in-agriculture-market-outlook-and-forecasts#rela1-4669235.
273 In a study by the World Bank, such partnerships are singled out as crucial for the development of the sector. See [online] http://documents.worldbank.org/curated/en/610081509689089303/pdf/120876-REVISED-WP-PUBLIC-Internet-of-Things-Report.pdf.

The cross-border aspects do not end there. Many of these IoT solutions do not come from traditional agriculture sector companies, such as those engaged in farming, or from conventional suppliers, such as farm equipment makers or suppliers or distributors of seeds, plant food or chemicals. Software developers and predictive data analytics companies are increasingly becoming part of agricultural operations. Many such non-traditional corporations are either themselves not based in the same country as the users (farms) or are assisted by or form part of a partnership or arrangement with entities in other countries. One clear example is the use of cloud services: most providers are not in the region, nor are data necessarily processed locally.

Notable developments and initiatives in smart farming

Rice farming in Colombia is benefiting from a project undertaken in partnership with a Japanese company. The IoT solution has sensors that collect environmental data such as air and soil temperature and humidity and solar irradiance. This project has led to both better decision-making and more efficient and timely responses.[274]

Livestock monitoring is also receiving attention, since constant checking of water and animal feed intake is required. In Brazil, a project undertaken in partnership with multinational corporations has made it easier to weigh livestock and analyse data on their development.[275] Additionally, start-ups and traditional companies provide technology that monitors the geolocation of herds and the health status of animals.[276] Others manage the whole chain "from farm to table", adding sensors and agricultural intelligence to all processes.[277] Similarly, in Argentina, start-ups are helping to monitor crops and livestock using a number of strategies from collar trackers to autonomous drones to capture and analyse information on agricultural activities.[278]

In Peru, some initiatives seek to use IoT for monitoring environmental and weather conditions. Antennas and drones are deployed to capture data from fields on a number of aspects ranging from topography to air quality.[279]

In Chile, naturally available resources in the form of genetically ancient vineyards are being leveraged by combining them with technology to produce in vitro a nursery for ancient varieties of vines.[280]

In Guanajuato, Mexico, an agricultural technology hub has sprung up and is incentivizing a number of projects for businesses, from crop monitoring to irrigation strategies.[281]

4. Digital payments

The Internet has changed the landscape of many different businesses worldwide. The financial sector has recently been experiencing the consequences of this.[282] New services and new business models are taking advantage of the connectivity of the online world to lower barriers to entry in the financial market so that more products and services can be provided to a broader base of clients. Their virtual nature means that they do not have to be based in any one country, but can foster and enable cross-border transactions.

274 See [online] https://www.e-kakashi.com/en/case/details01.
275 See [online] https://blog.bosch-si.com/agriculture/connected-agriculture-beefed-up-networking-in-brazil/. For a general study of its deployment in the south of Brazil, see [online] https://lume.ufrgs.br/handle/10183/178439?locale-attribute=en.
276 One example is Allflex (see [online] http://www.allflex.com.br/identificacao-eletronica/brincos-eletronicos-fdx/). Others are Intergado, Cowmed and Imeve (see [online] https://www.beefpoint.com.br/o-olho-do-dono-que-engorda-o-boi-agora-e-digital/).
277 An example is BovControl (see [online] https://www.bovcontrol.com; http://g1.globo.com/tecnologia/blog/startup/post/app-permite-a-fazendeiro-monitorar-bois-e-vacas-na-tela-do-pc.html).
278 For example, Tambero connects agricultural information data to a cloud service platform (see [online] https://www.tambero.com). At the other end of the spectrum, Skyagro uses autonomous drones to collect the necessary data (see [online] https://www.infocampo.com.ar/skyagro-drones-hechos-en-argentina-que-toman-y-analizan-imagenes-en-los-campos/).
279 Peruvian start-ups such as Spacedat and Qaira are significant examples. See [online] http://www.qairadrones.com/index.php?r=site/nosotros; and https://www.spacedat.com.
280 See [online] https://www.andeswines.com/business-acceleration-service/.
281 See [online] http://agrobioteg.org.
282 The World Bank and the International Monetary Fund (IMF) have sponsored the Bali Fintech Agenda, underscoring the opportunities and risks for innovative financial services providers. See [online] https://www.worldbank.org/en/topic/fintech.

There is still, however, a significant gap between people who are served by traditional financial institutions and those who are not. A substantial portion of the population is either underserved by or excluded from financial services. These gaps represent a significant impediment to a digital single market: people are either deterred from entering the market or simply are unable to access it. Thus, goods and services supplied via the Internet are also impacted, becoming inaccessible or hard to access for a large portion of the population.

In Latin America and the Caribbean, this is compounded by the relatively low penetration of banking services and international credit cards, an enduring cash culture and foreign exchange volatility. This presents an opportunity for new entrants to find fresh solutions, not only offering new products and services but increasing access to finance.[283]

Accordingly, start-ups and innovative projects are seeking to address the region's financial access asymmetries.[284] Latin America and the Caribbean is experiencing a boom in companies that are aligning new technologies with novel opportunities in the financial market.[285] There has been extraordinary growth in the so-called fintech market.[286] Initiatives have spread in different areas. Two have gained particular momentum in the region: digital payments, supported by growth in new banking enterprises (neobanks), and blockchain technologies in the form of both cryptocurrencies and other potential applications that will be explored below.

The stakeholders interviewed and surveyed highlighted this trend and the importance that fintech firms have been acquiring in the region. They have underscored their potential to lessen inequality of access to financial services and take advantage of the digital market. Stakeholders noted, however, that harmonization initiatives might be rendered more difficult by differences in financial regulation traditions in the region and the disparate size and nature of its economies.

4.1. Cross-border jurisdictional impacts on the activities of fintech firms

Payment mechanisms are crucial to the development of digital trade in goods and services. The ability to carry out payments digitally is not a given, particularly in cross-border transactions. It is necessary for payment arrangements to be efficient and affordable if they are to serve as conduits for funds to flow from one side all the way to the other in an online transaction.[287] The economic aspects of Internet transactions, then, are dependent on or may be resolved through a multi-layered series of intermediaries that maintain the digital payments infrastructure.

In the absence of accessible and affordable payment mechanisms, no digital market can properly work. In Latin America and the Caribbean, the financial environment is replete with opportunities to develop new approaches, be they new business models or new products and services. The growth in smartphone availability and mobile connectivity has also spurred the shift towards online and even mobile first approaches.

There are multiple digital payment and banking solutions in the region. The market has been moving towards novel approaches, leading to the creation of an ecosystem of companies that provide them.

283 Inter-American Development Bank (IDB), *FINTECH: Innovations You May Not Know were from Latin America and the Caribbean*, 2018 [online] https://publications.iadb.org/en/fintech-innovations-you-may-not-know-were-latin-america-and-caribbean.
284 Inter-American Development Bank (IDB), *Regulatory Sandboxes in Latin America and the Caribbean for the FinTech Ecosystem and the Financial System*, 2018 [online] https://publications.iadb.org/publications/english/document/Regulatory-Sandboxes-in-Latin-America-and-the-Caribbean-for-the-FinTech-Ecosystem-and-the-Financial-System.pdf.
285 Inter-American Development Bank (IDB)/Finnovista, *Fintech. Latin America 2018: Growth and Consolidation* [online] https://publications.iadb.org/publications/english/document/Fintech-Latin-America-2018-Growth-and-Consolidation-final.pdf.
286 Economic Commission for Latin America and the Caribbean (ECLAC), *Data, algorithms and policies: redefining the digital world* (LC/CMSI.6/4), Santiago, 2018.
287 See [online] https://www.fsb.org/wp-content/uploads/P090420-2.pdf.

The fintech environment in Latin America and the Caribbean is composed of hundreds of start-ups and new initiatives launched by more traditional actors.[288] By 2018, for instance, Brazil already had 380 fintech start-ups, Mexico 273, Colombia 148, Argentina 116 and Chile 84.[289] They encompass a number of different activities. Among the most important are solutions related to money transfers and management; international transfers and remittances; mobile points of sale; payment gateways and aggregators to accept, authorize and process payments on digital platforms; and neobanks, high-technology financial entities holding banking licences in their own right or on a third party basis.[290]

A number of these enterprises either offer transborder services, for instance international remittances, or are themselves transborder firms that have internationalized their operations. Government initiatives are important for providing an institutional framework to foster growth and create the conditions for new financial solutions. Attempts to foster regulatory convergence could help secure regional and international markets for these enterprises. However, cross-border jurisdictional aspects should be taken into consideration so that the process is supported rather than hindered.

There is already a tendency to regulate the fintech sector, and this has created an opportunity for coordination and cooperation among the countries in the region. In July 2018, for instance, the members of the Pacific Alliance agreed on a set of guiding principles for fintech regulation.[291]

At the national level, two paths are being explored by the countries of the region: (i) regulating the fintech sector as a whole, including digital payments and neobanking; and (ii) regulating it by adapting the existing legal framework.[292]

Mexico, for instance, has led the way with general legislation to regulate the fintech industry.[293] The legislation deals with four main areas: financial technology institutions, including crowdfunding enterprises and electronic payment institutions; virtual assets (cryptocurrencies); application programming interface (API); and regulatory sandboxes. Brazil, on the other hand, has followed the second approach, integrating fintech issues into existing regulation.[294] Honduras has issued a regulation to permit the use of e-wallets.[295] Peru has a similar regulation,[296] as does El Salvador.[297] In Colombia, the different actors are currently debating whether it is necessary to have a specific regulatory framework for fintech.[298]

4.2. Open banking and the fintech ecosystem

Open banking is one of the initiatives that are growing in the region from within the fintech ecosystem. It is an opportunity to generate the legal and technical infrastructure required for a more competitive financial environment. Open banking makes different financial services interoperable and opens up the market so that users can choose to share their financial data with different financial institutions and benefit from a broader set of products and services. It establishes a cross-industry data sharing environment, integrating different platforms and infrastructures. It usually involves the development of an application programming interface (API) that allows different financial service providers to interact.

288 Inter-American Development Bank (IDB)/Finnovista, *Fintech, Latin America 2018: Growth and Consolidation* [online] https://publications.iadb.org/publications/english/document/Fintech-Latin-America-2018-Growth-and-Consolidation-final.pdf.
289 According to Finnovista, the numbers are even higher in 2020. See [online] https://www.finnovista.com/tag/fintech-radar/.
290 Inter-American Development Bank (IDB)/Finnovista, *Fintech, Latin America 2018: Growth and Consolidation* [online] https://publications.iadb.org/publications/english/document/Fintech-Latin-America-2018-Growth-and-Consolidation-final.pdf.
291 See [online] https://alianzapacifico.net/wp-content/uploads/Principios-orientadores-para-la-regulación-Fintech.pdf.
292 International Monetary Fund (IMF), "Fintech: the experience so far", June 2019 [online] https://www.imf.org/en/Publications/Policy-Papers/Issues/2019/06/27/Fintech-The-Experience-So-Far-47056.
293 Ley para regular las instituciones de tecnología financiera, March 2018 [online] https://perma.cc/SB6N-RQY7.
294 International Monetary Fund (IMF), "Fintech: the experience so far", June 2019 [online] https://www.imf.org/en/Publications/Policy-Papers/Issues/2019/06/27/Fintech-The-Experience-So-Far-47056.
295 See [online] https://www.elheraldo.hn/pais/936203-466/uso-de-la-billetera-electrónica-será-legal-en-honduras.
296 See [online]: https://www.mef.gob.pe/es/por-instrumento/decreto-supremo/9970-decreto-supremo-n-090-2013-ef/file.
297 See [online] https://www.bcr.gob.sv/regulaciones/upload/NORMAS_PARA_LA_AUTORIZACION_DE_ADMINISTRADORES_DE_SISTEMAS_DE_PAGOS_MOVILES.pdf?v=1589709520.
298 Inter-American Development Bank (IDB)/Finnovista, "The Fintech ecosystem in Costa Rica", 2019 [online] https://www.finnovista.com/el-bid-y-finnovista-publican-un-diagnostico-del-ecosistema-fintech-en-costa-rica-2019/?lang=en.

The scope of most of these initiatives indicates little apparent awareness of the cross-border potential of open banking. Under a regional or wider legal framework, customers could benefit from financial products and services provided by a much larger network of providers. At the same time, the internationalization of the region's fintech will lead to the export of different open banking solutions that may either conflict or have to be reshaped.

Internationally, initiatives have taken one of two possible routes: a market-driven one, with the industry, government or a partnership of the two laying down guidelines and common standards and then leaving the market free to develop on that basis; and a regulatory one, with governmental authorities setting the overall framework for financial institutions to follow.

In the region, at least two countries seem to be following the second route. On 4 May 2020, Brazil issued a set of regulations through its financial oversight institutions. Implementation is divided into four phases, providing some leeway for the industry to set its own standards for sharing data and provide access to services.[299] Mexico's proposed legal framework for open banking forms part of its fintech regulations.[300] In other countries in the region, the industry itself has pushed for regulation so that the sector can advance.[301]

4.3. Innovative regulatory solutions: the appeal of regulatory sandboxes

New high-technology financial solutions depend on experimentation and innovation in financial products and services, and on business models. However, this may carry individual and/or systemic risks that should be explored beforehand. Traditional regulation is usually not capable of encompassing these innovative frameworks in a timely manner. Many countries, then, are testing non-traditional regulatory frameworks to address such risks in a secure and time-efficient fashion. Regulatory sandboxes have been proposed as an attractive strategy and are being implemented by some States, including a number in Latin America and the Caribbean.

Regulatory sandboxes provide an opportunity for innovative solutions to operate for a restricted number of users (clients) during a limited period. Initiatives are often subject to less stringent obligations on the condition that they will be continuously monitored and supervised by an authorized government body.

These sandboxes have the advantage of being testing grounds for new projects. They limit their impact and, consequently, their risks, allowing the supervisory authorities to monitor the reactions of agents and the market so that they can propose specific approaches, standards and rules.

The majority of the stakeholders surveyed stated that innovative approaches such as regulatory sandboxes helped foster economic growth in the region. They highlighted the differences in the economies of the region's countries, the possible lack of institutional capacity and the limited availability of human resources as potential hindrances to the applicability of these regulatory solutions.

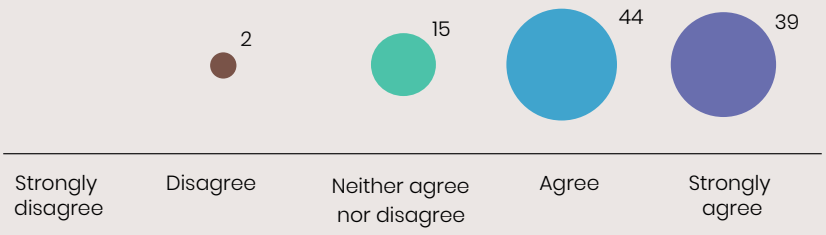
These reflections highlight the need and opportunity for cross-border cooperation and coordination. Countries in the region can benefit from their proximity and pool resources. Devising common standards and approaches can facilitate oversight work and reduce regulatory variation, thus making it possible to serve clients who are excluded or underserved by the traditional financial services sector.

299 See [online] https://www.bcb.gov.br/en/pressdetail/2284/nota. For Joint Resolution No. 4 of 2020 in Portuguese, see [online] http://www.in.gov.br/en/web/dou/-/resolucao-conjunta-n-1-de-4-de-maio-de-2020-255165055.

300 See[online]https://iupana.com/2020/02/28/mexicos-fintech-law-open-banking-rules-delayed/?lang=en#widget/?lang=en.

301 See, for instance, the study by FinteChile and EY on the future of open banking in Chile [online] https://www.ey.com/es_cl/financial-services/open-banking--oportunidades-y-desafios-para-chile. Colombia Fintech, in partnership with entities from the United Kingdom, has sought to develop open banking standards for the Colombian environment. See [online] https://www.ebankingnews.com/noticias/open-banking-desafios-y-oportunidades-en-colombia-0047125. For an analysis of the Colombian environment, see D. P. García Abella and J. C. Segura Cárdenas, "Open Banking: del concepto a la competencia" [online] https://repository.eafit.edu.co/bitstream/handle/10784/14228/DianaPatricia_GarciaAbella_2019_JuanCarlos_SeguraCardenas_2019.pdf?sequence=2&isAllowed=y.

Some of the countries in the region are already deploying such solutions and may lead the way. For example, Mexico's law regulating fintech companies[302] includes the possibility of temporary authorizations for "new financial models".[303] Similarly, in Colombia, the Financial Superintendence has put in place a legal framework that allows the use of regulatory sandboxes for innovative financial initiatives.[304] Brazil has regulatory sandbox initiatives overseen by the Central Bank of Brazil[305] and the Securities Commission (CVM).[306] Industry associations have put forward proposals as well, with an international federation of national associations aiming to create regulatory synergy in the region.[307]



Source: Internet & Jurisdiction Policy Network and Economic Commission for Latin America and the Caribbean (ECLAC).

Some countries in the Latin America and Caribbean region have used innovative frameworks (e.g., regulatory sandboxes) to allow experiments in fintech and digital payment technologies. Do you think that such an approach helps foster regional economic growth?

5. Blockchain and cryptocurrencies

Blockchain is another technology being developed to facilitate transactions. Blockchain may be understood as a distributed ledger where records of peer-to-peer transactions are kept without the necessity of a central authority to coordinate it. Satoshi Nakamoto conceptualized the technology in 2008 to eliminate the usual trusted middleman involved in most transactions.[308] It provides a way to cope with uncertainty. The distributed nature of the ledger and its immutable (tamper-proof) and self-executing nature make it unnecessary for the parties to know or trust each other. Trust becomes the result of the use of blockchain.[309]

The *Internet & Jurisdiction Global Status Report* 2019 has already highlighted the international interest in this technology from both the private and the public sectors. However, it also noted the considerable scepticism of some stakeholders, especially States, towards specific applications, most notably cryptocurrencies. Bitcoin has become widely known as one such currency. The legal difficulties with such currencies and with blockchain generally stem from the very features that in most cases make them appealing: the lack of a focal, central authority and the fact that people do not have to know or trust each other.

302 Ley para regular las instituciones de tecnología financiera, March 2018 [online] https://perma.cc/SB6N-RQY7.
303 See C. Kurc and A. Portilla, "Mexico: Fintech 2019. International Comparative Legal Guides" [online] https://iclg.com/practice-areas/fintech-laws-and-regulations/mexico.
304 See [online] https://forbes.co/2020/02/06/economia-y-finanzas/hacienda-cobijara-con-decreto-el-sandbox-de-la-superfinanciera/.
305 See [online] https://www.centralbanking.com/fintech/4397616/sandbox-initiative-central-bank-of-brazil. For a brief analysis suggesting that this may be an innovative sectoral regulatory sandbox approach, see [online] https://www.jota.info/coberturas-especiais/inova-e-acao/banco-central-ganha-premio-de-melhor-iniciativa-de-sandbox-do-mundo-04092019.
306 On 15 May 2020, CVM issued Instruction No. 626/2020 implementing regulatory sandboxes. See [online] http://www.cvm.gov.br/noticias/arquivos/2020/20200515-1.html.
307 See [online] http://fintechiberoamerica.com/wp-content/uploads/2018/06/protocolo_implementación_sandbox_iberoamerica.pdf.
308 S. Nakamoto "Bitcoin: A peer-to-peer electronic cash system", 2008 [online] https://bitcoin.org/bitcoin.pdf.
309 Economic Commission for Latin America and the Caribbean (ECLAC), *Data, algorithms and policies: redefining the digital world* (LC/CMSI.6/4), Santiago, 2018.

The distributed and dematerialized nature of the ledger makes borders and traditional jurisdictional elements significantly less relevant. Blockchain enables cross-border trade of all kinds to be carried out without the need for an intermediary to oversee and inspect it. This means that both legal and illegal transactions can flow without the knowledge of authorities or any need to establish jurisdiction.

Discussions on blockchain and cryptocurrencies tend to focus, then, on potentially illegal contexts where transactions may occur. For one thing, they can support criminal activities because they can change hands easily, remotely and without reference to any controlling authority. For another, they seem anonymous because no information on the identity of the people participating in the transaction is recorded. However, this does not necessarily mean that those involved cannot be identified. The blockchain protocol allows all transactions to be traced, making it possible to re-create their whole history. In this respect, it is much less anonymous than physical currency, whose movements are hard to trace once it has changed hands.

Blockchain, furthermore, can have many applications in different areas besides cryptocurrencies. It is used most notably for land and property registration and so-called "smart contracts", but it can be deployed in many areas, both private and public, where it serves to create a trusted online registry with automated functions.[310] With regard to "smart contracts", the term does not necessarily mean contracts made using blockchain. Blockchain-enabled contracts, however, are considered smart in three ways: they can be registered permanently in the blockchain; their clauses can be code-based; and there is a "guarantee of execution" because of automatic enforcement through the blockchain network.[311] The implications are enormous and may change the legal landscape for many sectors.

Scalability, data privacy and interoperability are seen as significant challenges. The first of these depends on the operations of the blockchain network and the technology underlying it. As regards privacy, the main issue is the exercise of the data subject's rights.[312]

Interoperability tends to be one of the most difficult problems. Without clear-cut common technical standards, the ecosystem may become fragmented and the benefits of the blockchain limited. Thus, standardization is essential to improve competitiveness and raise overall levels of compliance with other rules and values such as protection for human rights and the privacy already referred to.[313]

So far, the lead in developing global standards has been taken by the International Organization for Standardization (ISO)[314] and the International Telecommunication Union (ITU).[315] The Latin America and Caribbean region has yet to make a coordinated effort either to participate in global standard-setting forums or to establish its own regional standards.

There are some national initiatives that aim at regulating blockchain, though. The tendency is to focus on the financial aspects of the technology, particularly cryptocurrencies. Bermuda has issued a specific regulation embracing cryptocurrencies and aims to become an international hub for trading what are defined as "digital assets", including but not restricted to blockchain-based assets.[316] In Colombia, parliament is discussing a specific bill on crypto assets and virtual currencies.[317]

A slightly different approach is taken by Mexico's Fintech Act, for instance, which provides a set of rules for dealing with "virtual assets".[318] The government of Chile is following a similar path, proposing

310 For a broad array of potential applications, see Economic Commission for Latin America and the Caribbean (ECLAC), *Data, algorithms and policies: redefining the digital world* (LC/CMSI.6/4), Santiago, 2018.

311 D. Tapscott and A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*, 2016.

312 C. Kuner and others, "Blockchain versus data protection", *International Data Privacy Law*, vol. 8, No. 2, May 2018, pp. 103–104 [online] https://academic.oup.com/idpl/article/8/2/103/5047578.

313 Anna-Maria Osula, "The Global Rush for Standards in the Blockchain", April 2020 [online] https://directionsblog.eu/the-global-rush-for-standards-in-blockchain/.

314 ISO/TC 307 [online] https://isotc.iso.org/livelink/livelink/fetch/2000/2122/687806/ISO_TC_307__Blockchain_and_distributed_ledger_technologies_.pdf?nodeid=19772644&vernum=-2.

315 International Telecommunication Union (ITU), "Focus Group on Application of Distributed Ledger Technology" [online] https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx.

316 See [online] http://www.bermudalaws.bm/laws/Annual%20Laws/2018/Acts/Digital%20Asset%20Business%20Act%202018.pdf. For the regulations brought in by the Bermuda Monetary Authority, see [online] https://www.bma.bm/document-centre/policy-and-guidance-digital-asset-business.

317 See [online] http://leyes.senado.gov.co/proyectos/images/documentos/Textos%20Radicados/proyectos%20de%20ley/2018%20-%202019/PL%20028-18%20Criptomonedas.pdf.

318 Ley para regular las instituciones de tecnología financiera, March 2018 [online] https://perma.cc/SB6N-RQY7. For a positive view of the application of blockchain in Mexico, see Y. Martínez, "Compartimos los avances y retos de la estrategia digital en el Foro OCDE México 2018", Government of Mexico, 2018 [online] https://www.gob.mx/mexicodigital/articulos/compartimos-los-avances-y-retos-de-la-estrategia-digital-en-el-foro-ocde-mexico-2018.

to regulate the financial applications of blockchain under the aegis of fintech regulations.[319] Argentina, as one of the main regional hubs for cryptocurrency trading, is exploring a series of regulatory options, including specific fintech regulations.[320]

Some administrations have sought to use administrative regulations issued by central banks and other financial oversight agencies to provide guidelines on crypto assets.[321]

On taxation, different countries have sought to interpret their current legislation to include cryptocurrencies and curb the potential for financial fraud.[322] There are still vast areas where Latin America and the Caribbean can design a coordinated and cooperative initiative.

Future discussions should clearly distinguish between cryptocurrencies and blockchain as a generic technology with many diverse potential applications.

Noteworthy regional cases and initiatives

The Eastern Caribbean Central Bank (ECCB) has developed a pilot programme to facilitate compliance with international money laundering and terrorism finance reporting regulations and has developed a "blockchain-based currency" available to multiple States across the Caribbean.[323]

In 2018, the Bolivarian Republic of Venezuela announced a plan to launch an oil-backed cryptocurrency called the petro. The plan was to issue 100 million petro tokens worth US$ 6 billion with the intention that this would facilitate international transactions, reducing reliance on currencies such as the dollar and the euro.[324]

The Inter-American Development Bank (IDB) has launched LACChain, a global alliance to promote the use of blockchain in Latin America and the Caribbean, with the aim of coordinating efforts and developing blockchain technology in the region. It has already identified the lack of coordination and standardization as one of the main obstacles preventing the blockchain ecosystem from flourishing in Latin America and the Caribbean.

6. International and regional data flows: data protection regimes

Data privacy (or data protection) has gained momentum in Latin America and the Caribbean over the last half decade. Some factors have weighed heavily in this. The most notable one is the impact the EU General Data Protection Regulation (GDPR) has had on the transnational legal order. It has driven many countries to either review or develop their own data protection legislation. Potential access (or lack thereof) to the European data market is of significance for many countries, while the EU is regarded as a regulatory model for domestic efforts.

Another important development was the Cambridge Analytica scandal. The United Kingdom-based company profiled the electorate in order to provide electoral consultancy services, seeking to infer who would vote for each party and to influence the views of the undecided, allegedly bombarding them with one-sided views and/or disinformation in the process. Following this, countries around the globe decided it would be prudent to have in place data protection laws strong enough to discourage such behaviour and safeguard the democratic process.

Additionally, the digitalization of many different aspects of society, including public services, and the cyber breaches that have come with this, have created a greater awareness of the issue in the population. People know that their personal data are being collected and might become available for anyone to see if there is a breach.

319 See [online] https://www.criptonoticias.com/gobierno/regulacion/gobierno-chileno-adelanta-proyecto-regulacion-criptoactivos-2019/.
320 See [online] https://www.ambito.com/politica/criptomonedas/senado-analizo-regular-el-uso-las-laargentina-n5066872.
321 Brazil is one example and Costa Rica another. See Central Bank of Brazil, *Comunicado*, No. 31.379, 16 November 2017 [online] https://perma.cc/G4GM-8HV6; Central Bank of Costa Rica, *Posición del Banco Central de Costa Rica (BCCR) y sus Órganos de Desconcentración Máxima (ODM) con respecto a las criptomonedas*, October 2017 [online] https://perma.cc/KD4P-WXX8.
322 International Monetary Fund (IMF), "Fintech in Latin America and the Caribbean: Stocktaking", 2019 [online] https://www.imf.org/en/Publications/WP/Issues/2019/03/26/Fintech-in-Latin-America-and-the-Caribbean-Stocktaking-46677.
323 See [online] https://www.eccb-centralbank.org/news/view/eccb-to-issue-worldas-first-blockchain-based-digital-currency.
324 See [online] https://www.washingtonpost.com/news/worldviews/wp/2018/02/20/venezuela-launches-the-petro-its-cryptocurrency/.

6.1. Data protection regulations have been developing strongly in the Latin American and Caribbean countries

The region has seen a surge in regulatory initiatives dealing with data protection. As of 2012, according to a study conducted by the Organization of American States, 24 countries in the region either did not have data protection legislation or the domestic instruments they had only covered specific sectors, leaving many aspects of personal data unprotected by any particular legal instrument.[325]

Today, 16 countries have a specific data protection regulation (Antigua and Barbuda, Argentina, the Bahamas, Brazil, Chile, Colombia, Costa Rica, the Dominican Republic, Mexico, Nicaragua, Panama, Peru, Saint Kitts and Nevis, Saint Lucia, Trinidad and Tobago and Uruguay), 6 countries are discussing a bill (Barbados, Ecuador, Guatemala, Honduras, Jamaica and Paraguay) and 11 countries do not have specific data protection regulations (Belize, the Bolivarian Republic of Venezuela, Cuba, Dominica, El Salvador, Grenada, Guyana, Haiti, the Plurinational State of Bolivia, Saint Vincent and the Grenadines and Suriname).

Of the 10 countries that do not have a general data protection regulation, however, the majority have taken steps towards protecting personal data at some level. Dominica, Grenada and Saint Vincent and the Grenadines are parties to the Organisation of Eastern Caribbean States (OECS), which has approved the Data Protection draft bill as part of its E-Government for Regional Integration Project.[326] Belize, Guyana, Haiti and Suriname, as members of the Caribbean Community (CARICOM), have also taken part in initiatives that relate to data protection: the Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean (HIPCAR) project offers a number of model data protection policies that serve as regulatory guidelines.[327]

A few points should be noted. Countries that already have general data protection legislation are undergoing a process of reform and modernization which has led to the adoption of standards similar to the EU GDPR. Argentina[328] and Chile[329] are leading examples. Barbados is also discussing enacting data protection legislation inspired by European regulation.[330]

6.2. Towards a regional framework for data protection?

The stakeholders interviewed emphasized the institutional disparities in the region where the protection of personal data was concerned. One expert pointed to the need for regional coordination and the establishment of truly region-wide common standards of personal data protection.

Some countries in the region, such as Argentina[331] (2000), Uruguay[332] (2008) and Mexico (2010), have established data protection laws in the last decade. Others, such as Brazil (2018) and Panamá[333] (2019), have concluded the process in the last few years, clearly inspired by the EU GDPR.

Since regional initiatives have been addressing privacy and data protection as a major issue for efforts to promote economic integration and growth, it is expected that new efforts will be made to foster a regional dialogue on data protection, connecting the experiences of countries whose laws have already been recognized as adequate under EU standards (such as Argentina and Uruguay)[334] with

325 Organization of American States (OAS), "Comparative study: data protection In the Americas. Different existing legal regimes, polices and enforcement mechanisms for the protection of personal data, including domestic legislation, regulation, and self-regulation", 2012, p. 8 [online] http://www.oas.org/es/sla/ddi/docs/CP-CAJP-3063-12_en.pdf.
326 Organisation of Eastern Caribbean States (OECS), "Data Protection Act", 2016 [online] https://www.oecs.org/en/procurement/e-gov/data-protection-act.
327 See [online] https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Pages/default.aspx.
328 Argentina is bringing in several changes to its data protection regulations, including a major reform in its general data protection legislation to make it more akin to the EU GDPR. See [online] https://www.oecd-ilibrary.org/sites/5f8ec188-en/index.html?itemId=/content/component/5f8ec188-en.
329 Jaime Urzúa, "Avances en el Proyecto de ley sobre protección de datos personales: Consejo para la Transparencia será la nueva Agencia de protección de datos", September 2019 [online] https://www.alessandri.legal/avances-en-el-proyecto-de-ley-sobre-proteccion-de-datos-personales/.
330 Bartlett D. Morgan, "Barbados: a modern data protection regime", September 2019 [online] https://platform.dataguidance.com/opinion/barbados-modern-data-protection-regime.
331 See [online] https://www.oas.org/juridico/PDFs/arg_ley25326.pdf.
332 See [online] https://www.impo.com.uy/bases/leyes/18331-2008.
333 See [online] https://www.sucrelaw.com/blog/media/2019/04/Ley-81-de-2019_Sobre-Proteccion-de-Datos.pdf.
334 See [online] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

countries that are about to face the challenges of implementing a new data protection regulation. Chile is following the same path, with proposed legislation that is in tune with much of the logic of GDPR.[335] The same is true of Brazil's data protection legislation, with even its topography being inspired by the European standards.

Equally important is that data protection has become part of the digital trade agenda within regional trade forums such as the Pacific Alliance and MERCOSUR. The Additional Protocol to the Framework Agreement of the Pacific Alliance requires the country parties to maintain or adopt legislation on data protection.[336] On the Alliance's digital agenda, the approach taken is that countries should follow the best international standards, adopting a maximal view of personal data protection.[337] In the joint plan of action between MERCOSUR and the Pacific Alliance, the countries have stated their intention to work together to find common ground on personal data regulation. They view the matter as an important policy stepping-stone on the way to the establishment of a common digital market.[338] Proposals for MERCOSUR are being developed and seem to be a timely option.[339]

6.3. Data privacy restrictions on cross-border data transfers

Cross-border data transfers occur daily in a vast array of situations, from simple e-commerce contracts to complex international transactions. Such transfers are often conflated with regional markets or trade zones, yet personal data cross frontiers even without such international commercial arrangements.

The Latin America and Caribbean region, as a major consumer of digital services, is continuously having to deal with transnational services operating in the region and in many cases exporting data to their servers abroad. This has been a major subject of discussion in respect of many areas, particularly cloud services, and has motivated proposals for enforcing the localization of certain categories of data within the domestic territory of each country (see section V.B.4 for further discussion of data localization).

Transnational flows, however, are not restricted only by data localization strategies. Data protection legislation aimed at guaranteeing strong data protection standards for citizens may also create mechanisms that indirectly impact or hinder the flow of data outside countries' borders. Regulations on international personal data transfers modelled on European regulations (first EU Directive 95/46/EC and now the GDPR) have sprung up in many different countries of the region. Colombia, for instance, has established a list of countries that have met the standards for data transfers with which under certain circumstances data can flow freely; for all other countries, there is an elaborate procedure which usually includes strong contractual clauses.[340] Similarly, legislation in Argentina, the Bahamas, Brazil, Colombia, Costa Rica, the Dominican Republic, Mexico, Nicaragua, Panama, Peru, Saint Lucia, Trinidad and Tobago and Uruguay has provisions that constrain international transfers.

Of the countries mentioned, Argentina and Uruguay stand out because they have been recognized by the EU as approved countries for personal data transfer. Thus, the unilateral restrictions between these two countries and the EU have been lifted in both directions, ensuring that personal data can flow between each of the two and all countries in the EU.[341]

335 See [online] https://www.senado.cl/appsenado/index.php?mo=transparencia&ac=doctoInformeAsesoria&id=7045.
336 See [online] http://www.sice.oas.org/Trade/PAC_ALL/Pacific_Alliance_Text_s.asp#c13_a13_8.
337 See [online] https://alianzapacifico.net/wp-content/uploads/Hoja-de-Ruta-SGAD2016-2017.pdf.
338 See [online] http://www.cartillaciudadania.mercosur.int/oldAssets/uploads/Plan%20de%20Acción%20-%20Anexo%20declaración%20Puerto%20Vallarta.pdf.
339 Inter-American Development Bank (IDB), "Fueling Digital Trade in MERCOSUR: A Regulatory Roadmap", 2018 [online] https://publications.iadb.org/publications/english/document/Fueling-Digital-Trade-in-Mercosur-A-Regulatory-Roadmap.pdf.
340 Internet & Jurisdiction Policy Network, "Colombia establishes list of countries with adequate data protection for cross-border transfers", *I&J Retrospect Database*, July 2017 [online] https://www.internetjurisdiction.net/publications/retrospect#article-6188_2017-07.
341 For a full list of countries whose protections are considered adequate by the EU, see [online] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

7. Cross-border international and regional data flows

7.1. International and regional data flows are the keystone to digital trade

International flows of data have grown significantly in importance recently.[342] The growing international trade in services –not least in sectors where provision used to be solely domestic, such as education, health care and banking– and the data-intensive technologies of IoT and artificial intelligence, among others, have brought a new urgency to efforts to determine standards of data protection.[343] The potential cross-border economic implications are great. Thus, issues involving personal data are becoming increasingly important in the international trade agenda.

Since international organizations such as the World Trade Organization (WTO) and the Organization for Economic Cooperation and Development (OECD) have not yet found a settled basis for resolving issues of e-commerce, digital trade, data protection and cross-border data flows,[344] regional and bilateral trade agreements have begun to enshrine their own standards. In Latin America and the Caribbean, several countries are parties to trade agreements (bilateral or otherwise) containing specific clauses on such matters.

One of the very first agreements to contain a provision on e-commerce was the European Union-Caribbean Forum of African, Caribbean and Pacific States Economic Partnership Agreement (EPA), which entered into force in 2008 and involved Antigua and Barbuda, the Bahamas, Barbados, Belize, Dominica, the Dominican Republic, Grenada, Guyana, Jamaica, Saint Lucia, Saint Vincent and the Grenadines, Saint Kitts and Nevis, Suriname and Trinidad and Tobago.[345] Countries such as Belize, Colombia, Costa Rica, El Salvador, Guatemala, Honduras, Mexico, Nicaragua, Panama and Peru have also entered into agreements containing e-commerce clauses with States outside the region. Intraregionally, there are also cases such as the agreements concluded by Colombia with the Northern Triangle countries of Central America (El Salvador, Guatemala and Honduras), with Costa Rica and with Peru; those concluded by Mexico with Central America and Panama; and that between Chile and Uruguay. The scope and content of the agreements vary, but they tend to lay down policy on a wide range of issues, from online consumer protection to the protection of intellectual property rights in cyberspace.[346]

Not all agreements contain data protection clauses, though. The Trans-Pacific Partnership (TPP) agreement, which includes three countries of the region (Chile, Mexico and Peru), is one that does. Its e-commerce chapter deals with a number of important aspects such as privacy and data protection, cross-border data flows and data localization. It recognizes the benefits of data protection legislation and mandates member countries to maintain or adopt a "legal framework" to protect "personal information". The content of such a framework is open: each country can decide how exactly personal data are to be regulated. One important provision, however, recognizes the need to create mechanisms to "promote compatibility between these [potentially] different regimes".[347]

The United States, Mexico and Canada Agreement (USMCA) is another example. The Digital Trade chapter, the first of its kind, follows much the same strategy as the far broader Trans-Pacific

342 According to a study by McKinsey, cross-border data flows have a more significant impact on the global economy than trade in goods. McKinsey Global Institute, *Digital Globalization: The New Era of Global Flows*, 2016 [online] https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows.

343 See [online] https://www.theatlantic.com/international/archive/2019/06/g20-data/592606/.

344 See, for instance, the OECD discussion on Internet openness and data flows, the World Economic Forum debate on international data flow governance, the G20 Japan proposal for data free flow with trust, representing a potential international agreement on cross-border data flows, or the WTO controversy regarding e-commerce. See [online] https://www.oecd-ilibrary.org/trade/trade-and-cross-border-data-flows_b2023a47-en;jsessionid=dFRe-gxHPx7Res_noe9wGNEb.ip-10-240-5-180; http://www3.weforum.org/docs/WEF_Trade_Policy_Data_Flows_Report.pdf; https://pecc.org/resources/digital-economy/2616-data-free-flow-with-trust-and-data-governance/file; and https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm.

345 Haiti has signed the treaty but not yet ratified it. See [online] https://ec.europa.eu/trade/policy/countries-and-regions/regions/caribbean/.

346 Inter-American Development Bank (IDB)/International Centre for Trade and Sustainable Development (ICTSD), *Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System*, 2017 [online] https://www.ictsd.org/themes/global-economic-governance/research/digital-trade-related-provisions-in-regional-trade.

347 Trans-Pacific Partnership (TPP), art. 14(8)(5). See [online] https://www.mfat.govt.nz/assets/Trans-Pacific-Partnership/Text/14.-Electronic-Commerce-Chapter.pdf.

Partnership (TPP) negotiated previously.[348] There are provisions requiring each State to establish laws to protect personal data ("personal information" under the agreement). The treaty does not, however, establish a minimum common standard that should be followed, but only states that when regulating "personal information", "each Party should take into account principles and guidelines of relevant international bodies".[349]

The more connected goods and services (particularly goods with embedded information services) gain traction, the more important it will be to have common standards of data protection. This means not only standards applicable domestically but also ones that allow data to flow internationally. Different approaches may impact international trade by making it harder for companies to gain scale and operate across markets. Diverging data protection regulations make it necessary to adapt goods and services to meet each specific market's regulatory requirement. Equally, restrictions on cross-border flows have an impact on transborder offers of goods and services. Taking the example of IoT, in the first case, architecture and privacy settings have to be adapted before the device can be offered in a given country. In the second, the infrastructure used to provide the underlying service requiring the data might become much more complex, with either the flow of data being confined within the country's borders or procedures to allow international data transfer having to be settled beforehand. These may impact competition between domestic and foreign enterprises, potentially raising issues of arbitrary or unjustifiable discrimination. Thus, two types of initiatives are important: harmonization of data protection standards and facilitation of responsible and secure international data flows.

7.2. Regionalization: cross-border challenges and opportunities

Several of the recent trade initiatives that Latin America and the Caribbean is involved in have made provision for cross-border data flows. They acknowledge that different laws may provide different opportunities and conditions for international data flows. The initiatives seek to provide a framework that facilitates flows by settling the conditions that have to be fulfilled and/or the scope of the subject matter for which personal data flows are permitted.

Article 14(11)(2) of the Trans-Pacific Partnership (TPP) establishes that cross-border flows of data have to be allowed whenever the flow "is for the conduct of the business of a covered person". Article 19.11 of USMCA imposes the same obligation. Both add language akin to that of international treaties such as article XX of the General Agreement on Tariffs and Trade (GATT) and article XIV of the General Agreement on Trade in Services (GATS), allowing countries to regulate for "a legitimate public policy objective".

The clause dealing with financial services in the Economic Partnership Agreement between the CARIFORUM States and the EU (article 107) similarly states that countries should allow the flow of data for the conduct of that kind of business (financial services). The treaty adds a more specific clause stating that the parties will adopt adequate safeguards to protect the privacy, fundamental rights and personal freedom of data subjects, which should include data protection and privacy.

In the case of the EU-Mexico Trade Agreement currently being negotiated, the digital trade chapter does not specify any regime for cross-border data flows, but includes a "rendez-vous clause" providing for a three-year period to assess whether it is necessary to include "provisions on the free flow of data".[350]

Some bilateral trade agreements in the region have clauses dealing with bilateral data flows. Article 14(10) of the Mexico-Panama Free Trade Agreement establishes that data may cross borders, but with the caveat that this has to be in accordance with personal data protection requirements and international practices. Others only emphasize the need for cooperation to facilitate and maintain

348 See [online] https://www.cfr.org/blog/coming-north-american-digital-trade-zone.
349 United States-Mexico-Canada Agreement, art. 19(8), 30 November 2018. See [online] https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between.
350 Svetlana Yakovleva and Kristina Irion, "Pitching trade against privacy: reconciling EU governance of personal data flows with external trade", *International Data Privacy Law*, 30 March 2020 [online] https://doi.org/10.1093/idpl/ipaa003. For the text of the agreement negotiated, see [online] http://trade.ec.europa.eu/doclib/docs/2018/april/tradoc_156811.pdf.

data flows, examples being the Costa Rica-Colombia Free Trade Agreement, the Chile-Colombia Free Trade Agreement and the Colombia-Northern Triangle Free Trade Agreement.

These arrangements provide the basis for common understandings on how data can flow across borders. Potential tensions between regimes and restrictions on data flows are limited by the agreements, and international flows tend to be prioritized. There is still no general or regional agreement involving countries in Latin America and the Caribbean. Such an agreement would probably bring greater security to the flow of data and enhance trade, particularly in the digital economy.

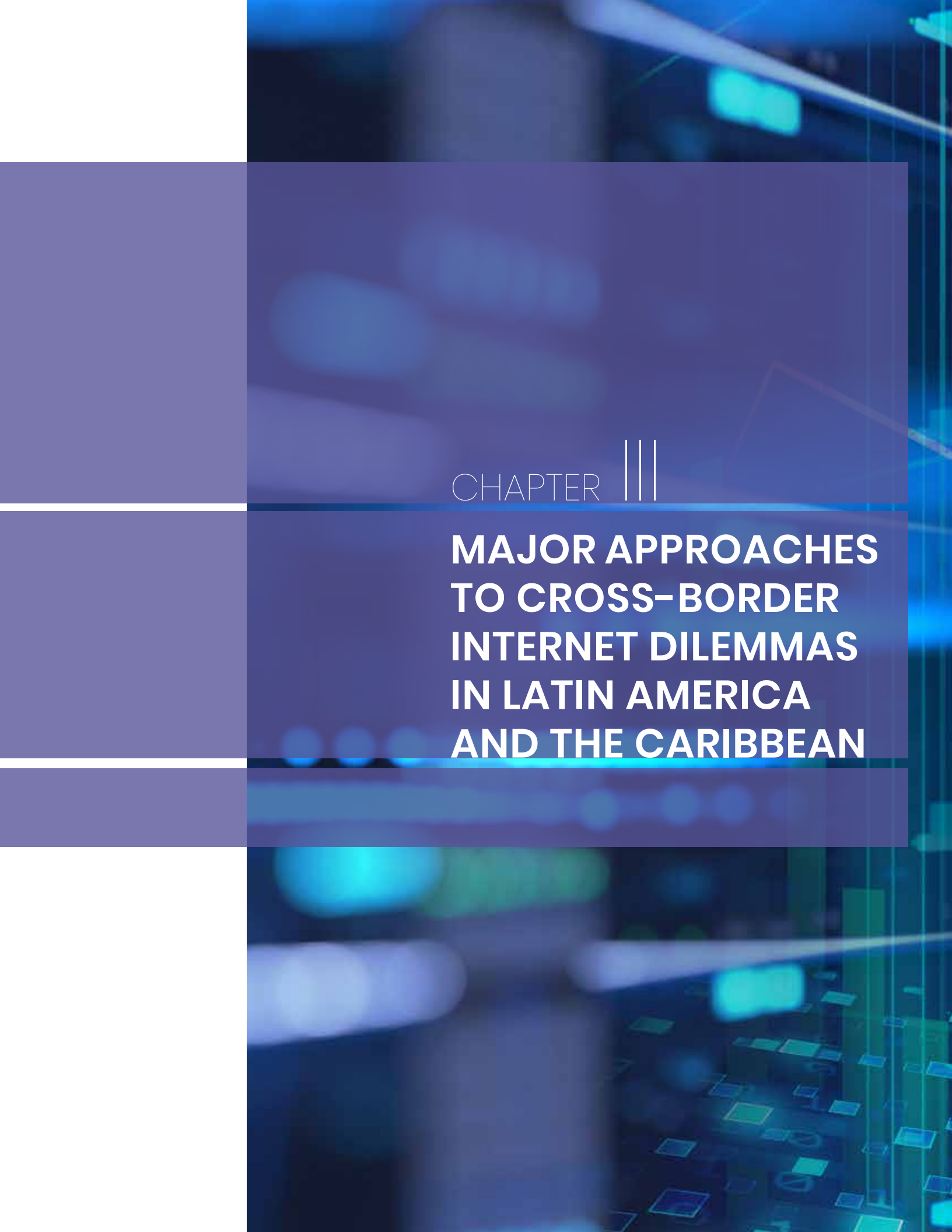
7.3. Regional initiatives are fostering standardization of cross-border data transfers

At the international and regional levels, there are no general agreements covering the protection of a person's reputation or permitting (or preventing) the free flow of data. However, some regional organizations have issued guiding principles aimed at harmonizing the different countries' standards.

The eleventh of the OAS Principles on Privacy and Personal Data Protection, "Trans-border Flow of Data and Accountability", acknowledges the need for harmonization of data protection standards in order not to hinder the flow of data across borders.[351]

The standards of protection approved by the Ibero-American Data Protection Network, to which several of the countries in the region are parties, also contain a recommendation that cross-border data transfers should be subject to a number of requirements which follow similar patterns to those of the European legislation, indicating that either countries should have protection deemed adequate or parties wishing to transfer data abroad should follow pre-arranged procedures.[352]

[351] See [online] http://scm.oas.org/pdfs/2016/CP35451EREPORTCJI.pdf.
[352] See [online] https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf.



CHAPTER III

MAJOR APPROACHES TO CROSS-BORDER INTERNET DILEMMAS IN LATIN AMERICA AND THE CARIBBEAN

The *Internet & Jurisdiction Global Status Report 2019* argued that it was no overstatement to say that a legal arms race was ongoing between many of the major international players, chiefly the United States, the European Union, China and, to some extent, Russia. As noted earlier, their measures directly impact the region. Many Latin American and Caribbean States are adopting and implementing technical and legal solutions within their domestic jurisdictions that resemble or are inspired by the normative and technical solutions adopted by other international actors.

Hence, initiatives in Latin America and the Caribbean largely mirror ones proposed elsewhere. They include national legislation with wide extraterritorial application, local court orders with global implications, fines and sanctions for companies with no physical presence in the country and mandatory content filtering, data localization and app blocking. In actual application, however, they tend to acquire a regional hue as solutions are transferred from one context to an entirely different one.

As mentioned in chapter II, social, economic, political and legal peculiarities have the effect of changing the way technical solutions are deployed in different countries. In a region as diverse as Latin America and the Caribbean, all such conditions play an important role in determining the success of legal and technical solutions to cross-border dilemmas.

However, these legal and technical solutions have for the most part been implemented without proper discussion of their cross-border effects. Accordingly, this part of the report sets out to analyse a selection of such initiatives and shed some light on their transborder impacts.

A. Major legal trends

Latin American and Caribbean States vary in the degree to which they employ legal solutions to perceived issues related to the regulation of the Internet. Overall, there is a growing trend towards extending the applicability of national laws to situations beyond countries' physical borders. It is becoming more and more standard to ascertain adjudicative jurisdiction on the basis of what is called the "effects doctrine" or a "targeting test". Courts have issued online content take-down (and/or stay-down) and stay-up orders. There is also an emphasis on coupling regulation applicable to the Internet with large fines and sanctions. Terms of service and community guidelines created by major international Internet platforms are playing an increasingly important and foundational role in guiding online behaviour.

1. States are increasingly resorting to an "effects doctrine" in asserting jurisdiction

There is a broad trend for States to assert jurisdiction over conduct and activities whose origin lies in another State or territory whenever they have a substantial connection to the country thus asserting jurisdiction. Activities usually understood to create such a connection include targeting consumers, doing business, causing harm, or affecting in a concrete way people or assets located within the borders of a country.

Under international law, this approach is usually understood to fall under the heading of an "effects doctrine". The logic is that States should be able to assert jurisdiction over conduct and activities that have an impact ("effect") on persons or assets in their territory. This is justified either by intent, because the active participant knew or at least should have known that the activity or conduct would have consequences in that country, or on the basis that States ought to be able to regulate activities that impact their markets, their citizens or assets on their territory.[353]

This approach was originally developed for the purposes of competition and antitrust law, but it gained momentum with the spread of the Internet. It is usually discussed with reference to a "targeting test". In early examples of this approach, the focus was on establishing adjudicative jurisdiction with particular reference to defamation (and harmful speech) and e-commerce. In *Young v. New Haven Advocate*, a United States court of appeals was asked to decide whether the courts of one state had jurisdiction to decide on a defamation case involving a newspaper (published online as well as offline) intended for distribution in another state. The court ruled that it was not enough that it was available in the second state, or that it discussed matters involving that state; the fact of its intended readership being in the other state was the key point.[354]

In the joined cases of *Peter* Pammer *v. Reederei Karl Schlüter GmbH & Co. KG* and Hotel Alpenhof *GesmbH v. Oliver Heller*, the Court of Justice of the European Union was called upon to decide on the features that would determine jurisdiction in cases concerning e-commerce, i.e., a consumer buying goods and services online. The European Court affirmed that a number of elements should be taken into consideration, such as the international nature of the service, itineraries from other member States (how the place the business traded from was reached), the language and currency options of the website or app, telephone numbers with international codes prefixed to them, top-level domain names other than that of the member State in which the trader was based, and mention of an international clientele composed of customers domiciled in various member States.

The decision also made it explicit that the mere fact of the service being available online in the consumer's country was not a sufficient connection (this has an impact on the use of geolocation technologies, as discussed below).[355] The rationale for such decisions is that traders should only be regulated at the European Union level if they first target the European Union market. This approach was replicated in recital 23 of the General Data Protection Regulation (GDPR)[356] and has informed other European Union regulatory processes.[357]

This view has had an impact in Latin America as well. Cases in different countries ranging from Colombia to Brazil have established that jurisdiction over Internet activities is to be determined by the intended or expected effects of actions taken online.[358] Cyberspace is seen as ubiquitous, but the actions and conduct of those participating in it are understood as having a focus, a target. When asserting jurisdiction, courts tend to rule in consideration of the place where the harm occurred, with the apparent intent of the actors involved being taken into consideration.

---

353 See B. Simma and A. Müller, "Exercise and limits of jurisdiction", *The Cambridge Companion to International Law*, J. Crawford and M. Koskenniemi (eds.), Cambridge, Cambridge University Press, 2012.

354 See United States Court of Appeals for the Fourth Circuit, *Young v. New Haven Advocate,* No. 315 F.3d 256, Richmond, 13 December 2002.

355 See Court of Justice of the European Union, *Judgment of the Court (Grand Chamber) of 7 December 2010 (references for a preliminary ruling from the Oberster Gerichtshof (Austria)) — Peter Pammer v. Reederei Karl Schlüter GmbH & Co KG (C-585/08) and Hotel Alpenhof GesmbH v. Oliver Heller (C-144/09),* No. 2011/C 55/06, Luxembourg, 19 February 2011.

356 General Data Protection Regulation (GDPR), recital 23: "it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union." See [online] https://www.privacy-regulation.eu/en/recital-23-GDPR.htm.

357 See European Commission, *Proposal for a directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings,* No. COM(2018) 226 final, Strasbourg, 17 April 2018 [online] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0226&from=EN; Proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, No. COM(2018) 225 final, Strasbourg, 17 April 2018 [online] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0225&from=EN.

358 For an overview concerning cases of defamation, see [online] https://www.palermo.edu/cele/cele/pdf/english/Internet-Free-of-Censorship/Jurisdiction_Eduardo%20Bertoni.pdf.

In the Jerónimo A. Uribe case, the Supreme Court of Justice of Colombia ruled that online speech, including death threats, was not to be understood as having occurred solely in the place where the speaker was located, i.e., his or her usual place of residence.[359] Similarly, in the Centro Comercial Campanario case, the same Supreme Court ruled that jurisdiction should be assigned to the place where the harm occurred, i.e., in an online fraud case, the place where the victim is.[360]

Following a similar reasoning, Brazil's Superior Court of Justice[361] has ruled in a number of cases that the location of servers is irrelevant when it came to ascertaining jurisdiction and that instead jurisdiction should be assigned to the place where the victim resides and works, since it is there that the harmful activity or speech will have the greatest impact and repercussions.[362]

In Argentina, likewise, a number of rulings have determined jurisdiction on the basis of where the harm occurred or where the victim is.[363] This takes on a different aspect when the alleged perpetrator of the offence is a news publication that has both an online and an offline presence. The reasoning is that the place where the "materials are printed" is the governing criterion. The underlying principle seems to be that, notwithstanding the online presence, the readership targeted is the one in the place where the print edition is distributed.[364]

In most cases in the region, the chief criterion for determining jurisdiction is simply the place where the harm is experienced, such as the victim's place of residence or business. This targeted approach is also seen in some pieces of legislation, including Argentine, Brazilian,[365] Colombian,[366] Mexican[367] and Peruvian[368] data protection laws. Another example is the Venezuelan Special Law against Computer Crime.

The main difficulty with this targeting approach is to understand the profile of the target. Does the fact that a website is available online, without geographical limitations, mean that it targets the whole world, or at least that its owners accept the risk of acting as though it did? Does a change in language matter? What are the precise criteria for determining the audience targeted? It might seem relatively easy to ascertain jurisdiction in the case of a peer-to-peer messaging app, but what would change if the same message were sent through a social network open to the public?

The controversial element here is the issue of whether the jurisdiction is fair for all the parties involved. On the one hand, confining jurisdiction to the domicile of the person providing the service, selling the product or publishing the message would leave the other party with very little recourse. One the other hand, if the potentially injured party is given too much protection, the service provider, seller or content publisher might have to defend itself in court anywhere in the world under a law whose application it may not have expected.

2. The expansion of jurisdictional reach

A significant number of the stakeholders surveyed noted that there was an imbalance of power and that while many countries were implementing legislation that was extraterritorial in scope, not all States were capable of enforcing such laws. A few pointed out that regulations of this type might be more effective if they were part of regional agreements, yet it is still very challenging to find common ground.

359 See Supreme Court of Justice of Colombia, *Caso Jerónimo A. Uribe*, No. 33.474/2010, Bogotá, 10 February 2010.
360 See Supreme Court of Justice of Colombia, *Caso Centro Comercial Campanario*, No. 34.564/2010, Bogotá, 25 August 2010.
361 See Superior Court of Justice, *Conflito de competência*, No. 66.981, Brasilia, 16 February 2009 [online] https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=200601611027&dt_publicacao=05/03/2009.
362 See Superior Court of Justice, *Conflito de competência*, No. 66.981, Brasilia, 16 February 2009; *Conflito de competência*, No. 107.938, Brasilia, 27 October 2010; *Agravo de instrumento*, No. 1.375.009, Brasilia, 15 March 2011.
363 See Federal Court of Appeal of Salta, *J. G. R. v. Google Inc.*, Salta, 4 July 2011; National Court of Appeal for Criminal and Correctional Matters of the City of Buenos Aires, *N.N. s/ injurias*, No. 1589/09, Buenos Aires, 21 October 2009.
364 See National Court of Criminal Appeals, *Alifano, Roberto Francisco s/ recurso de queja*, No. 9375, Buenos Aires, 3 March 2009; Supreme Court of Justice of Argentina, *Verazay, Santos Justo s/ querella por calumnias e injurias*, No. 1085, Buenos Aires.
365 See [online] https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf.
366 See Congress of Colombia, *Ley Estatutaria 1581 de 2012*, Bogotá, 2012 [online] https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf.
367 See National Institute for Social Development, *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, Mexico City, 2010; *Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, Mexico City, 2011; Secretariat of Economy, "Lineamientos del aviso de privacidad", *Diario Oficial de la Federación*, Mexico City, 17 January 2013.
368 Peru, Law No. 29.733 of 2011, Law on the Protection of Personal Data.

In the context of a border-neutral global Internet where conduct and actions initiated in one part of the world can have an impact –and may actually cause harm– in another, countries have sought to extend their powers beyond their own territory. They have unilaterally tried to close the international governance and regulation gap for online actions and conduct by claiming a jurisdiction that goes beyond what is traditionally acknowledged to be their territory, in some cases regardless of whether there is any prospect of actual or effective enforcement.

One example from the region can be found in article 11 of Brazil's Internet Bill of Rights. It states that "[i]n any operation involving collection, storage, retention and processing of personal data or communications data by connection providers and Internet application providers where at least one of these acts takes place on Brazilian territory, Brazilian law must be complied with".[369] Paragraph 2 goes on to encompass even "activities [...] carried out by a legal entity located abroad, when it provides services to the Brazilian public or at least one member of the same business group is established in Brazil".[370]

The trend towards claiming an expanded jurisdiction has been further strengthened by the example of article 3 of the European General Data Protection Regulation (GDPR). This regulation has had an impact on the design of new legislation in Latin American and Caribbean countries. Brazil, for instance, included in its General Data Protection Act an article 3 of its own inspired by its European counterpart, stating that "this Law applies to any processing operation carried out by a natural person or a legal entity incorporated under public or private law, irrespective of the means, the country in which the person or entity's headquarters are located or the country where the data are located, provided that: I – the processing operation is carried out on Brazilian territory; II – the purpose of the processing activity is to offer or provide goods or services or the processing of data on individuals situated on Brazilian territory; or III – the personal data being processed were collected on Brazilian territory." Article 3.1 of Brazil's General Data Protection Act also states that "data shall be deemed to have been collected on Brazilian territory when the person they concern is situated on Brazilian territory at the time of collection".[371]

This is also true of countries such as Colombia,[372] Mexico[373] and Peru,[374] which have likewise extended their data protection regulations to give them an extraterritorial dimension. From the standpoint of a developing nation, this approach may be seen as a show of strength against foreign companies with the potential to impact domestic markets from afar, especially when regulations are coupled with heavy fines and sanctions (discussed in section V.A.4 below). There seems to be international acceptance of this when what is being protected are the fundamental rights and values of the country passing the law.

Yet any jurisdictional claim, whether it concerns adjudicative or prescriptive jurisdiction, lives or dies by the possibility of it being enforced. When the ability to actually compel the parties to comply is lacking, the legitimacy of the regulation may be diminished. This approach has also been criticized for: (i) leading to arbitrary enforcement (too many potentially non-compliant actors, so that the authorities have to choose which to pursue); (ii) eroding legal certainty (too many perpetrators going unprosecuted, giving the impression that the law is a dead letter); and (iii) creating potential transborder compliance conflicts (the norms of two or more countries may require different actions to be taken in respect of the same conduct, leading to conflicts and obliging entities to choose which law to comply with).

One stakeholder surveyed mentioned that higher courts in Latin America had so far shown restraint and not issued orders with a global reach on issues concerning the Internet. Another was of the opinion that the potential global scope of individual online rights had not yet been determined in many countries of the region.

369 See Internet & Jurisdiction Policy Network, "Marco Civil puts Brazilian data stored abroad under Brazilian jurisdiction", Paris, 2014 [online] https://www.internetjurisdiction.net/publications/retrospect#article-5002_2014-04.
370 Ibid.
371 See [online] https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf.
372 Colombia, Law No. 1581 of 2012. See [online] https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf.
373 See National Institute for Social Development, *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, Mexico City, 2010; *Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, Mexico City, 2011; Secretariat of Economy, "Lineamientos del aviso de privacidad", *Diario Oficial de la Federación*, Mexico City, 17 January 2013.
374 Peru, Law No. 29.733 of 2011, Personal Data Protection Act.

The discussion goes beyond whether courts have jurisdiction over particular persons or types of subject matter or whether legislation applies to a situation that might be understood as lying outside what is traditionally understood to be the territory of a country. What is at issue is the scope of the effects of jurisdiction: the scope of remedial jurisdiction.[375]

> It has been reported that Justice Alexandre de Moraes of Brazil's Supreme Federal Court of Justice has ordered social networks Facebook and Twitter to block access to the accounts of 16 individuals being investigated for allegedly spreading disinformation and hate speech online.[376] The magistrate is reported to have requested a global reach (access to be blocked irrespective of the origin of the viewer's IP address) on the basis of a police report which stated that there had been incidents in which those under investigation had circumvented the restriction imposed by the previous order and continued to use their accounts to publish messages in contravention of the current court order, particularly hate speech.
>
> The event had a further repercussion, as one of the 16 who had their accounts globally blocked was able to use another account to make a very controversial statement against abortion. The comment not only involved the expression of views on the matter, but also included personal data on a 10-year-old girl who had been raped and was undergoing a legal procedure in hospital. Another judge instructed the same two social networks plus Google to remove the messages containing the minor's details.[377] It was reported that a member of parliament had asked for this incident to be added to the investigations that led to the global order being issued by Justice Moraes of the Supreme Federal Court of Justice.[378]

Cases concerning the so-called right to be forgotten have been dealing with the limits (scope) of delisting or de-indexing, i.e., whether it is enough for this to be done within the territory of the country (or of Europe) or it has to be global. Geo-blocking (discussed in section V.B.1 below) is being considered and dealt with in terms of the technique's efficiency and accuracy.[379]

The discussion on intellectual property rights has also advanced. The logic is that there is a high degree of international harmonization in this area (particularly of copyright law). Thus, an order by a court in one country may have a global impact, unless it is proved that regulations in another country oblige the platform to act differently.[380]

The Internet & Jurisdiction Policy Network has recently issued a publication providing guidance for governments and private entities on how to deal with the geographical scope of content restrictions. It identifies four categories of "international normative coherence" reflecting the degree of convergence among different bodies of legislation regarding content illegality. These categories should provide the basis for a scale with different levels of geographical scope for content removal, from the most proportionate and limited to the most global.[381]

In the region, the trend of imposing global delisting orders has not as yet gained much traction. This does not mean that there have not been some orders requesting platforms to carry out a global delisting or de-indexing.[382] The global scope provided for in some jurisdictions has also encouraged citizens in the Latin America and Caribbean region to request international relief. A Paraguayan citizen requested the Spanish Data Protection Authority (AEPD) to order Google to delist a number of

375 See D. Jerker, "Jurisdiction in 3D – 'scope of (remedial) jurisdiction' as a third dimension of jurisdiction", *Journal of Private International Law*, vol. 12, No. 1, Milton Park, Taylor & Francis, 2016.
376 See [online] https://www.reuters.com/article/us-facebook-brazil/facebook-puts-global-block-on-brazils-bolsonaro-supporters-idUSKCN24X3BN.
377 See [online] https://www.bbc.com/news/world-latin-america-53820497.
378 See [online] https://revistaforum.com.br/politica/alexandre-padilha-aciona-stf-contra-sara-winter-por-incitar-fundamentalistas-contra-menina-de-10-anos/.
379 See Court of Justice of the European Union, *Google LLC, successor in law to Google Inc. v. Commission nationale de l'informatique et des libertés (CNIL)*, No. C-507-17, Luxembourg, 24 September 2019 [online] http://curia.europa.eu/juris/liste.jsf?language=en&num=C-507/17; *Eva Glawischnig-Piesczek v. Facebook Ireland Limited*, No. C-18/18, Luxembourg, 3 October 2019 [online] http://curia.europa.eu/juris/liste.jsf?num=C-18/18.
380 See Supreme Court of Canada, *Google Inc. v. Equustek Solutions Inc.*, No. SCC 34, Ottawa, 2017.
381 See[online]https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-20-102-Geographic-Scope-Content-Restrictions.pdf.
382 See State Court of Justice of São Paulo, *Google Brasil Internet Ltda. v. Clóvis de Barros Filho*, São Paulo, 2019.

news articles in which he appeared. The AEPD denied his request, but it demonstrates the impact of such orders with global implications.[383]

Delisting cases provide some nuance to this issue. In the State Court of Justice of São Paulo in Brazil, for instance, there have been cases in which the court has ordered Google Brazil to delist search results from its website or to remove videos from YouTube on a global scale. In other cases, the very same court has questioned how its rulings could affect other jurisdictions. In the case of *Centro Espírita Beneficente União do Vegetal v. Google Brasil Internet Ltda.*, the judge stated that the court did not have jurisdiction to determine whether the video specified in the plaintiff's briefing was also available in other countries, such as Colombia and Germany, and that doing so would exceed the scope of its competence and be a violation of other countries' sovereignty.[384]

3. Take-down, stay-down and stay-up orders by courts

The Internet has made it possible for content to be seen and shared all over the world in both private and more public settings. Billions of messages are exchanged and millions of photos and hours of videos and music are uploaded every day, with a large proportion being on global platforms accessible to people in every part of the globe. This abundance of information is bound to have an impact, affecting people and even causing harm. Notwithstanding the high value set on freedom of expression, it is clear that some limits are bound to be imposed by normative requirements, which may vary from one country to another.

Another global trend reflected in Latin America and the Caribbean is that of courts issuing platforms with take-down, stay-down and stay-up orders for content posted online. The disparity in views regarding standards for the protection of different rights, particularly free speech, is a major source of cross-border disputes.

It is quite common for such orders to have transboundary elements. The platform may be foreign in origin, the technology used may come from abroad, data may be held in offshore servers; in short, a vast array of situations mean that many such orders have effects outside the territory of the country where they originate.

In addition, not all countries issue such orders for legitimate reasons. They may be used to restrict speech, persecute political opponents or discriminate, among other potential human rights violations. Any analysis of them is inextricably linked to the underlying subject matter they are intended to regulate and to the substantive national and international law covering this. Chapter IV of this report focused on some of the most important issues leading courts to issue take-down (and stay-down or stay-up) orders or require providers to delist, de-index and de-reference or even delete, block or remove content.

Take-down orders are the most common and are usually issued in connection with tort proceedings seeking monetary compensation. The relief consists in prohibiting continued display of the content. However, there may be other specific aims, such as the removal of information that is misleading or may damage someone's reputation.

In 2012, during an election campaign, a local judge in Brazil issued an order for Google to take down from its YouTube platform a video critical of a political candidate. While the appeal was pending, the same judge issued a warrant for the arrest of the Director of Google Brazil for flouting his judicial take-down request.[385]

In January, 2016, the Supreme Court of Justice of Chile ordered the removal of a news outlet that had damaged the reputation of an individual and granted the company three days to comply with the order.[386]

383 See [online] https://blog.cuatrecasas.com/propiedad-intelectual/derecho-al-olvido-audiencia-rechaza-aplicacion-extraterritorial/.
384 See State Court of Justice of São Paulo, *Centro Espírita Beneficente União do Vegetal v. Google Brasil Internet Ltda.*, São Paulo, 11 August 2016 [online] https://www.conjur.com.br/dl/justica-local-nao-obrigar-google2.pdf.
385 See [online] https://www.bbc.com/news/world-latin-america-19753158.
386 Supreme Court of Justice of Chile, decision of 21 January 2016. See [online] https://bit.ly/2MbDW6m.

Stay-down orders are issued in large numbers in the region as well. They address a particular weakness of take-down orders: the fact that it is virtually cost-free to republish content that has been taken down. Stay-down, then, imposes an obligation for content not to reappear. This creates two potentially challenging issues: (i) platforms are obliged to monitor future uploads in order to assess whether they are of the same illegal content and (ii) to expedite this monitoring and make it less resource-intensive, they are led to use automated techniques, i.e., filters driven by artificial intelligence.

This may create a privatized regime of censorship, with platforms perceived as policing it. Moreover, automated filters could conceivably result in a general ban on certain types of speech, which as a result will never see the light of day.

Arrangements of this kind are easier to justify on issues where there is little discussion about whether content should be considered illegal and the risk of "over-blocking" or "over-filtering" by platforms is likely to have less of an impact on protected speech or speech that may be deemed legal. An example is child abuse material, since there is a strong consensus that it is illegal.

There is also a discussion regarding whether an individual has to identify the specific URL address that is to be taken down, or whether identifying the content is enough. In the latter case, it is left up to the platforms to identify where the material was published and then take it down.

In 2007, a Brazilian judge instructed the YouTube platform to take down a sexually charged video of a famous model that had been posted without her consent. In view of the fact that it was constantly re-uploaded, the magistrate ordered access to the website to be blocked.[387] The order was amended the following day so as not to restrict access to YouTube in the country.

In 2012, an Argentine court ordered the "permanent" removal of sexual images of a certain model from a search engine. The court stated that the platform had the means to do this.[388]

In 2017, the Constitutional Court of Colombia instructed Google to delete an anonymous blog on its Blogger platform because it was violating the right to personal development and privacy.[389]

Stay-up decisions are not so common as yet, with very few countries having issued them. The understanding concerning online freedom of expression is that platforms have to respect freedom of speech. However, they have some leeway to enforce certain restrictions, mainly based on their terms of service and community guidelines.

However, some countries such as Germany and, in the region, Brazil have judged that there are circumstances where speech is protected and should not be restricted by platforms. Accordingly, courts have ordered speech that has been taken down to be put up again.[390]

In one recent example, in December 2019 the Court of Justice of the Federal District and Territories of Brazil granted an injunction against Facebook requiring it to keep online a post by a member of parliament, Eduardo Bolsonaro, in which he criticized journalists for a news article about his wife. Facebook stated that the journalists had reported unauthorized usage of their images, which constituted a violation of the terms of service of the platform.[391] A decision of February 2020 adjudicated in favour of Facebook on the case's merits, deeming that the member of parliament's freedom of expression had not been unduly interfered with.[392]

387 See [online] https://www.nytimes.com/2007/01/05/business/worldbusiness/05fobriefs-JUDGEBLOCKSY_BRF.html.
388 See [online] https://www.internetjurisdiction.net/uploads/pdfs/Papers/Internet-Jurisdition-Synthesis-2-Dec-2012.pdf.
389 See Constitutional Court of Colombia, *Acción de tutela interpuesta por John William Fierro Caicedo, contra Google Inc. y otros*, No. T-063A/17, Bogotá, 9 May 2018 [online] http://www.corteconstitucional.gov.co/relatoria/2017/t-063a-17.htm; Internet & Jurisdiction Policy Network, "Colombian Constitutional Court rules that Google must delete a blogger.com blog that contained defamatory statements", Paris, 2017 [online] https://www.internetjurisdiction.net/publications/retrospect#eyJ0byI6IjIwMjAtMDgifQ==.
390 See D. Keller, "Why DC Pundits' must-carry claims are relevant to global censorship", Stanford, Center for Internet and Society (CIS), 13 September 2018 [online] http://cyberlaw.stanford.edu/blog/2018/09/why-dc-pundits-must-carry-claims-are-relevant-global-censorship.
391 See [online] https://www.uol.com.br/tilt/noticias/redacao/2019/12/03/posts-de-novo-no-ar-facebook-perde-para-eduardo-bolsonaro-na-justica.htm.
392 See [online] https://www.migalhas.com.br/quentes/323429/facebook-nao-indenizara-eduardo-bolsonaro-por-remover-posts-que-violaram-regras-da-rede-social.

Taken together, such orders may have important consequences for platform content moderation across different countries. Minimum common denominators amongst different countries' standards are hard to find when some courts can order certain content to be taken down while others may order the same content to be kept up. There is thus real potential for jurisdictional conflict. Platforms are called upon to be the guardians of balance and may not over-remove or under-remove content.

The Internet & Jurisdiction Policy Network, through its Content & Jurisdiction thematic programme, has proposed a number of frameworks and solutions to enable both governments and platforms to strike a balance and manage content, taking into consideration the diversity of laws, customs and cultures around the globe, and specifically in Latin America and the Caribbean.[393]

4. Fines and sanctions

Administrative sanctions imposed by local authorities are an important tool for enforcing Internet-related regulation. The authorities concerned might vary depending on the specific issue at hand, such as consumer, antitrust, environmental or data protection. The sanctions usually range from warnings and fines to suspension or termination of a particular activity.

As described in previous sections, many of the data protection regulations in the region were inspired by the European legal framework, which provides for severe administrative sanctions. One notable difference, however, is that European regulations provide for international cooperation between countries, while in Latin America and the Caribbean most rules concerning administrative liability are national in scope.

Administrative sanctions for breaches of personal data privacy in the region include fines of up to 100,000 pesos (approximately US$ 1,500) in Argentina[394] and up to 10,000 balboas (approximately US$ 10,000) in Panama. In Trinidad and Tobago, legal penalties are based on an enterprise's annual turnover, and a fine of up to 10% of this can be applied.[395] In Brazil, there are specific provisions requiring the authorities to consider the total revenue of the company concerned,[396] which could mean smaller fines for smaller businesses.

Even though national laws provide for cooperation between data protection authorities,[397] it is fair to say that sanctions and/or orders are being imposed in a domestic context. The competent regulatory agencies are usually faced with jurisdiction shopping by companies storing data in a country other than the one where the persons to whom the data relate are located or reside (and where the law is being enforced). On 1 April 2020, the Colombian Superintendence of Industry and Commerce reaffirmed its authority to impose administrative orders not only on Facebook Colombia, but also on Facebook Inc., located in the United States, and on Facebook Ireland, based in Ireland.[398]

One expert interviewed stated that recent data protection regulations were increasingly turning into a kind of extraterritorial law, as they produced effects in other countries while at the same time fostering a kind of "reconceptualization of sovereignty". This extraterritorial effect becomes evident when regulatory agencies impose sanctions that explicitly require actions of a company based elsewhere. In order to guarantee a regulatory ecosystem that preserves the transnational aspect of the Internet, authorities should exercise their international cooperation competences and consider bi- or multilateral agreements. International cooperation is one of the main courses of action for enforcing privacy[399] and should be treated as such.

Another situation present in a few countries of the region is uncertainty about which bodies are competent to enforce administrative sanctions. In Brazil, where the National Data Protection Authority is not yet fully operational, administrative procedures and orders relating to data protection

393 See [online] https://www.internetjurisdiction.net/news/content-jurisdiction-program-outcomes.
394 Law No. 25326, article 31. See [online] https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/actualizacion.
395 Data Protection Act, 2011, section 96. See [online] http://www.ttparliament.org/legislations/a2011-13.pdf.
396 Brazil, Law No. 13.709, article 52.4. See [online] http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.
397 See, for instance, Nicaragua, Law No. 787 of 2012, article 29.i.
398 Superintendence of Industry and Commerce, resolution No. 12.192 of 2020. See [online] https://www.sic.gov.co/sites/default/files/files/2020/Res%2012192%2001IV2020%20SIC%20Facebook%20Inc.pdf.
399 See A. Brian, "Data protection and enforcement in Latin America and in Uruguay", *Enforcing Privacy: Regulatory, Legal and Technological Approaches*, D. Wright and P. de Hert (eds.), Berlin, Springer, 2016.

have already been executed by the National Consumer Secretariat (SENACON), including fines for both Facebook Inc. and Facebook Serviços Online do Brasil Ltda.[400] It is true that data, consumer and competition regulations create scope to impose sanctions, but the extent to which they are required in each case might not be clear as yet. Thus, in some cases further cooperation and cohesion are needed not only in the international context, but also domestically.

Many countries in the region have adopted legislation imposing severe sanctions for non-compliance with sectoral norms that might apply to Internet activities, mostly inspired by European regulations. This is particularly prevalent in the field of data protection.

5. Terms of service are interlocking with national laws

Terms of service created by multinational companies have interlocked with national legislation in some ways, serving as a major source of guidance on what is allowed and what is not on such platforms. On the one hand, companies face the challenge of balancing freedom of expression against potentially harmful speech. On the other, they are having to cope with significant changes to the legal landscape in areas such as intellectual property, data privacy, liability limitations and consumer protection.

Terms of service and community guidelines implement legislative obligations (particularly as regards procedure), but supplement these with companies' own views of what the platform environment should be like. Several of the issues presented in this report stem from clashes between domestic regulations and providers' terms of service and community guidelines.

A major cross-border aspect is that such platforms tend to be built on a worldwide or at least regional architecture. Thus, many elements of the terms of service supporting this architecture have a common core. Standards developed by platforms cover vast areas of the globe and are commensurately influential. National regulatory and customary standards may clash with such terms and guidelines, leading to a need for accommodation.

The problem is more acute in cases where the entities behind the platforms have fewer resources or are start-ups. Fast growth can be particularly disruptive and lead to regulatory and cultural clashes. These can arise from an excess of self-regulation, when terms are more intrusive than the country's laws or provide different solutions (or, more often than not, are more liberal or less developed), or have lacunae or gaps, failing to deal with types of behaviour that should be covered, whether because of regulatory requirements or cultural needs.

A closely related issue concerns content moderation. Terms of service and community guidelines play a very important role. The platform environment is impacted by what types of speech are allowed and encouraged. Internet services that cater for children should restrict certain kinds of speech that might be legal but are not child-appropriate. At the other end of the spectrum, services that target a more adult clientele may be more liberal as regards the kinds of content permitted, yet should take into consideration standards regarding sexual content online; situations such as child pornography and revenge porn (as discussed in section IV.A.4) usually require a fast response.

Terms and guidelines serve to determine what content stays up and is taken down. Governments tend to rely on these tools for the purpose of pressuring companies to uphold certain moral standards or achieving certain objectives (such as law enforcement). To balance these needs, certain platforms have suggested having oversight bodies that may be able to suggest courses of actions in particularly thorny cases.[401]

This also holds true for intellectual property. The European Union has updated its Directive on Copyright in the Digital Single Market, creating incentives for platforms to provide mechanisms for moderating content even before it is published. The Directive has had an impact on countries in the region. A few have launched procedures to reform their IP legislation. Brazil, for instance,

[400] See Ministry of Justice and Public Security, "MJSP multa Facebook em R$ 6,6 milhões", Brasilia, 30 December 2019 [online] https://www.gov.br/mj/pt-br/assuntos/noticias/mjsp-multa-facebook-em-r-6-6-milhoes.
[401] See *The Economist*, "Facebook unveils details of its content-oversight board", London, 30 January 2020 [online] https://www.economist.com/business/2020/01/30/facebook-unveils-details-of-its-content-oversight-board.

has embarked on a consultation and initiated an extensive study on a new national strategy for intellectual property. One topic, mechanisms of protection against online piracy, draws heavily on the latest developments in European law.[402]

Certain governments in Latin America and the Caribbean have been pressuring or even entering into agreements with e-commerce platforms to improve the measures they take against piracy and the selling of counterfeit goods. These actions have led many e-commerce platforms to self-regulate and add non-judicial means of dispute resolution to their terms and conditions. They use in-house methods (automatic more often than not) to find and take down perceived violations (counterfeiting or piracy). These alternative dispute resolution mechanisms usually provide an opportunity for both the owner and the alleged violator to express their views.

In addition to dispute resolution systems set up by the private sector, governments in the region have been fostering co-regulation initiatives. These initiatives are inspired by the Memorandum of understanding on the sale of counterfeit goods on the Internet, facilitated by the European Commission and agreed by several platforms, rights owners and associations.[403]

In many instances, terms of service identify the jurisdiction to be used to settle disputes and the applicable law. They are considered contracts (albeit adhesion contracts) regulating the relationship with users and such matters as party autonomy. In the region, however, the tradition of consumer protection is robust, and there is a perception that party autonomy should be limited, particularly in circumstances where a consumer is involved and cannot negotiate the clauses of the contract. This reflects an emerging trend identified in the *Internet & Jurisdiction Global Status Report 2019* for courts not to uphold choice of forum and choice of law clauses in international Internet platforms' terms of service.

B. Major technical approaches

Latin America and the Caribbean is no exception to the rule that a number of the most important legal issues related to the Internet and jurisdiction tend to be viewed through the lens of technical solutions. A number of them have followed similar lines to the solutions arrived at in other countries of the world, but others have ended up with a very particular regional flavour. This section sets out to present and analyse the most significant such technical approaches as they have presented themselves in the region and to highlight the peculiarities that have developed among the Latin America and Caribbean countries. The analysis has been carried out from the perspective of the transborder impacts they may have and their practical and legal implications.

Most of the technical approaches presented here aim to address the issue of how to control and limit access to content. They have been the source of major disputes on the Internet for the last decade. To some extent, countries began by embracing a more liberal *laissez-faire* approach to content production and distribution. Intermediaries were required to self-regulate, and content producers were liable for the content they made available. By the middle of the decade, some countries in the region had started to challenge this view and had developed and deployed the techniques discussed in this report.

Geolocation technologies, which were seldom part of the architecture of Internet services in the past, are now seen as more relevant. The *Internet & Jurisdiction Global Status Report 2019* pointed out, and the survey for this report confirmed, that there are contrasting views on the advisability of introducing such techniques on a larger scale. Perhaps the most important divergence relates to content filtering. A number of national initiatives have considered the appropriateness of mandating filtering technologies for specific parts of the Internet, particularly large social media networks.

The blocking of Internet services and applications (apps) is an important issue. In several instances, governments, courts and companies themselves have prevented access to specific services and apps,

[402] See [online] http://cultura.gov.br/ministerio-da-cidadania-abre-consulta-publica-sobre-reforma-da-lei-de-direitos-autorais/; http://www.mdic.gov.br/index.php/ultimas-noticias/3948-grupo-interministerial-de-propriedade-intelectual-inicia-atividades.

[403] See [online] https://ec.europa.eu/growth/industry/policy/intellectual-property/enforcement/memorandum-understanding-sale-counterfeit-goods-internet_en.

with varying degrees of transparency and due process. In many cases, this has been done to comply with either a local law or a judicial order of another nature. Shutdowns of the whole Internet have also occurred, but have usually been temporary and restricted to specific areas.

Other technical approaches that have been deployed include constraints on the Domain Name System (DNS) imposed under court orders requiring either suspension, deletion, non-resolution, seizure and transfer, or IP address blocking/re-routing and URL blocking. Lastly, some countries have discussed and to an extent implemented compulsory data localization. All such techniques constrain the functioning of the Internet as originally envisioned and are quickly changing the regulatory landscape. Technical approaches may be useful to deal with cross-border legal challenges, yet there is a need to understand their consequences and seek consensus on the appropriateness of their deployment.

1. Geolocation technologies

If a map of the Internet were to be drawn, the original version would have no borders. The protocols controlling the Internet were designed to disregard countries' frontiers, thus giving it a borderless character. However, geolocation technologies have served to bring back a degree of geography to the Internet. Broadly speaking, these technologies are capable of ascertaining users' geographical position, thus allowing service providers to adapt some attributes to the peculiarities of that place, changing features like the default language, providing more accurate results (e.g., showing where the nearest restaurant is) and even limiting access to certain components or content on the basis of cultural, social or legal customs and norms.

The technology behind geolocation is not uniform but relies on a number of aspects such as IP addresses, GPS, the default language of the device or the activities it is being used for (running, walking, driving), mobile phone tower triangulation and even Wi-Fi and Bluetooth signals. The degree of certainty and accuracy with which the device is located varies accordingly. Another aspect that may affect its accuracy is the use of a masking technology such as a virtual private network (VPN) employing techniques that either block or misreport the location of the person or device.

In many places around the world, the debate on the use of geolocation technologies has matured in the last two decades. In Europe especially, the debate started with a discussion on whether such techniques might be deployed, given their level of accuracy, and has evolved to focus on their appropriateness and the extent of their use. Alongside policies to constitute a European Digital Single Market, the European Union has even issued a regulation (No. 2018/302) concerning geo-blocking, one of the potential functions of geolocation technologies.

This regulation restricts the use of such technologies in cases of "unjustified geo-blocking", which is understood to occur in three circumstances: (i) the sale of goods without physical delivery (customers are entitled to buy products sold by stores in countries other than the one they are in); (ii) the sale of electronically supplied services (a customer may choose to use a service supplied by a provider from another country and should not be required to pay additional fees); (iii) the sale of services provided in a specific physical location (e.g., discounted prices for people in a specific location).

In Latin America and the Caribbean, the discussion on geo-blocking does not yet have the regulatory specificity that it does in other countries and regions. Yet there is a burgeoning political and legal debate on the implications of geolocation technologies in relation to consumer and data protection, especially geo-blocking and geo-pricing.

In Brazil, for instance, the online travel company Despegar has been fined for subjecting its customers to both geo-blocking and geo-pricing. The case concerned discrimination between customers from Brazil and Argentina, as some hotels listed higher average prices for Brazilian customers than for Argentine ones. Additionally, the company would block access to certain hotels and services (the rental of certain cars) for customers in one country and not the other.[404]

[404] See National Consumer Secretariat, *Nota Técnica*, No. 92/2018, Brasilia, 16 June 2018.

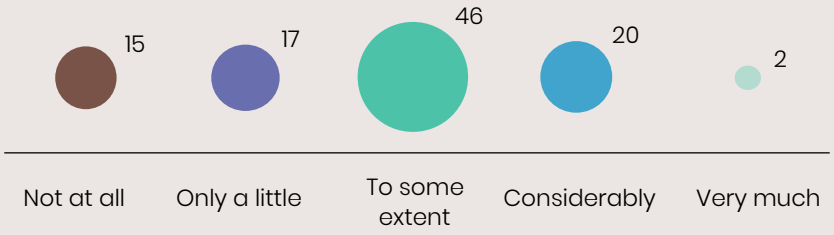
Data privacy laws make provision for the targeting of data processing activities on a specific country or place. This implies some degree of georeferencing and the use of geolocation technologies. The General Data Protection Regulation (GDPR), for instance, comes into play whenever companies target their activities on the common market. The same can be seen in the Brazilian General Data Protection Law.

As in the *Internet & Jurisdiction Global Status Report 2019*, the points raised by the stakeholders surveyed centred on three themes: (i) these technologies can be easily bypassed and might not be particularly effective, (ii) they may impact freedom of expression and access to information and (iii) they may be deployed in certain commercial circumstances. The similarity between the points made by global and regional respondents is striking, although experts from the region seem to be of the view that these technologies might be more useful in a commercial setting than in a more public environment. One expert mentioned that geolocation technologies might not be appropriate for democratic processes. The concern in the region appears to be about access to information. Thus, there is a view that geolocation technologies may prevent access to information stored outside the country.

As the fight against the COVID-19 pandemic continues, countries in the region are trying to make greater use of data to better deal with the spread of the virus. Geolocation technologies are increasingly playing a role in determining the degree of social distancing adopted by larger groups or mapping the routes and contacts of infected individuals.

Concerns over privacy and data protection are growing as the transborder nature of the Internet makes it easier for sensitive data to be stored in a foreign country. Additionally, countries with a recent history of authoritarian regimes are facing public demonstrations by people claiming that the use of geolocation data to fight the pandemic is an excuse for introducing unprecedented oversight of citizens.

The expectation must be that a more informed debate over the use of geolocation technologies, mingled with political, legal, and technical concerns, will develop in the region as a legacy of the fight against COVID-19.



How appropriate a tool do you believe geo-IP content filtering is for addressing the geographical scope of domestic rights?

Source: Internet & Jurisdiction Policy Network and Economic Commission for Latin America and the Caribbean (ECLAC).

2. Content filtering is on the rise as countries fight hate speech and disinformation

Hardly any countries in Latin America and the Caribbean organized their networks a priori to block (or filter) incoming content or police locally produced content. Such restrictions were not installed as part and parcel of the network in the infrastructure of the region's countries (also known as the Internet backbone). Nonetheless, many governments have sought to impose an obligation on access providers or Internet service providers to monitor, filter or take down certain categories of content in a short period of time. In certain circumstances, such regulations may have legitimate aims and be applied with reasonable limits and controls. In others, they may have an impact akin to censorship and may even shape political and cultural speech, inadvertently impacting freedom of expression or even extending copyright protections without justification.

As for filtering embedded in the backbone of the Internet, there have been reports that the Government of Cuba has in place technical measures capable of filtering Internet content.[405] The reports state that messages containing specific words such as "democracy" or "dictatorship" never reach their destination, and that certain Internet services deemed inconsistent with the values of the Cuban State are not available online.

> The Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights (IACHR) has analysed the institutional architecture that restricts and filters content available online in Cuba.[406] It has noted a few particularly salient pieces of regulation. Worth mentioning are resolutions No. 127/2007, which deals with information technology security, and No. 179/2008, a regulation for Internet service providers dealing with public access to the Internet. The former forbids the circulation of data or information contrary to "the social interest or public morals and mores". The latter creates an obligation for Internet service providers (ISPs) to monitor and "regulate" online content and establishes a regime of direct liability for intermediaries.[407] These pieces of regulation are deemed to impact freedom of expression and freedom of access to information.[408]
>
> In the Bolivarian Republic of Venezuela, the Law on Social Responsibility on Radio, Television and Electronic Media establishes that ISPs may be held liable for information they make available that creates anxiety among the citizenry, withholds recognition from the legitimately constituted authorities, disturbs public order or incites or encourages non-compliance with the laws.[409]

In early 2019, the Constituent National Assembly of the Bolivarian Republic of Venezuela brought in a bill called the Constitutional Law on Cyberspace of the Bolivarian Republic of Venezuela. It is reported to have provided for wide powers for the government to regulate the Internet within the country, including mandatory content filtering.[410] This is one type of regulatory landscape in which providers and ISPs in general have incentives to filter content.

Additionally, in November 2017 the Bolivarian Republic of Venezuela passed a Law against Hatred that authorizes the authorities to revoke licences and block Internet services if ISPs display content (including third party content) deemed by the government to promote hatred or intolerance.[411] It does not of itself require the application of content filters, but the severity of the sanctions creates an environment that incentivizes the deployment of these technologies.

Other countries in the region have been concerned by the spread of disinformation, particularly during elections. The scandal involving Cambridge Analytica, a company accused of using personal data to create personally tailored misinformation campaigns, has driven many countries in Latin America and the Caribbean to revise their laws concerning the role of Internet intermediaries.

Some countries have pushed for legislation that would require service providers to deploy mechanisms for identifying and, in certain cases, taking down speech containing disinformation, particularly during elections. The Special Rapporteur for Freedom of Expression has declared that under the standards of the Inter-American System for the protection of human rights, any regulation requiring ISPs to deploy content blocking or filtering should be restricted to exceptional cases such as child pornography, war propaganda and hate speech constituting incitement to violence or incitement to genocide, with the additional protection that an independent judge should determine the illegality of the content.

405 See A. Shahbaz and A. Funk, *Freedom on the Net 2019: The Crisis of Social Media,* Washington, D.C., Freedom House, 2019 [online] https://www.freedomonthenet.org/country/cuba/freedom-on-the-net/2019#B1.
406 See Special Rapporteur for Freedom of Expression, *Special Report on the Situation of Freedom of Expression in Cuba,* Washington, D.C., 2019.
407 Ibid.
408 Ibid.
409 See [online] http://www.leyresorte.gob.ve/wp-content/uploads/2012/07/Ley-de-Responsabilidad-Social-en-Radio-Television-y-Medios-Electrónicos.pdf.
410 See [online] https://www.accessnow.org/a-bill-in-venezuela-seeks-to-give-the-government-absolute-control-over-the-internet/.
411 See [online] https://www.bloomberg.com/news/articles/2017-11-08/venezuela-passes-anti-hate-law-threatening-media-censorship.

3. The Domain Name System: suspensions and blockings resulting from notifications and judicial and administrative orders

The Domain Name System (DNS) is at the very root of the Internet, operating as an addressing system that helps users find their way around the network. Every single device connected to the network has a unique address, a string of numbers called an IP address. The DNS allows these strings of numbers to be turned into sets of letters, thus making it easier for users to memorize them.

As mentioned in the *Internet & Jurisdiction Global Status Report 2019*, cross-border requests for domain name suspension are increasingly being sent to technical operators in relation to allegedly abusive content or activities on underlying websites.[412] This approach is attractive to requestors because the suspension of a domain name has a direct and immediate global effect.

The far-reaching effects of tampering with the Domain Name System mean there is a need for very cautious analysis of alleged infringements and reflection about the proportionality of the measure. Suspending or blocking an entire domain name means that all content on a particular website becomes unavailable. Operators ought therefore to regard tampering with the DNS as a measure of last resort to be used only if there is no other way of tackling the allegedly infringing conduct or content.

Because they have the practical effect of quickly taking content offline worldwide, suspensions and blockings at the DNS level have been used to tackle very different issues, from intellectual property infringements to harmful speech. The decision to take down a specific domain name can be triggered simply by a notification from the victim of an alleged infringement, but may also be compelled by administrative and judicial orders.

Notices to suspend or block domain names can naturally have a cross-border impact. The domain name "1dmx.org" was registered in order to host a website protesting against excessive use of force by the police in Mexico. The domain name was a reference to the day Enrique Peña Nieto took the oath as President in December 2012. A number of protests erupted that day and were repressed by the police. Dozens of students and protesters were detained, and one demonstrator died. A year later, the website was shut down following a request to suspend the domain name received by GoDaddy, the domain name registrar, from the United States Department of Homeland Security. The reason for the take-down was that the website was "part of an ongoing law enforcement investigation"[413] and that its content violated the company's terms of service.[414]

Some governments in the region are known for their practice of DNS blocking, although this measure is not widespread in the region as a whole. Recently, the Venezuelan Government blocked the Tor network, a tool that allows users to browse the Internet anonymously. The blocking was executed by the government-owned Internet service provider CANTV, the largest ISP in the country.[415] In order to access the blocked tool, Venezuelan users had to rely on virtual private networks (VPNs) to circumvent government regulations.

In Cuban "parknets" (the name given to public places from which the Internet can be accessed), a number of websites have reportedly been blocked, including media outlets.[416]

Following a global trend, judicial orders for the blocking or suspension of domain names are on the rise in Latin America and the Caribbean. In Argentina, for instance, the Argentine Chamber of Phonogram and Videogram Producers and other copyright management companies filed a lawsuit and were granted an injunction[417] to block Pirate Bay, a very popular file-sharing website.[418]

412 See D. Jerker, *Internet & Jurisdiction Global Status Report 2019*, Paris, Internet & Jurisdiction Policy Network, 2019.
413 See [online] https://www.civicus.org/documents/reports-and-publications/SOCS/2017/essays/freedom-of-expression-in-latin-america-the-struggle-continues-in-the-digital-environment.pdf.
414 See L. García, "Political Internet censorship: a reality in Mexico (with a little help from the United States and GoDaddy.com)", *Digital Rights: Latin America and the Caribbean*, E. Magrani (ed.), Río de Janeiro, GV Direito Rio, 2018 [online] https://itsrio.org/wp-content/uploads/2018/01/digital-rights.pdf.
415 See [online] https://www.accessnow.org/venezuela-blocks-tor/.
416 See [online] https://blog.torproject.org/measuring-internet-censorship-cubas-parknets.
417 See [online] https://www.scribd.com/fullscreen/232015119?access_key=key-2j7jKUaMaBADeV4XpAOw&allow_share=true&escape=false&view_mode=scrollar/.
418 See [online] https://www.derechosdigitales.org/7608/internet-bajo-censura-bloquean-pirate-bay-en-argentina/.

The injunction ordered ISPs to block several domain names associated with the file-sharing website, such as thepiratebay.org and thepiratebay.se.[419]

As noted by the non-governmental organization (NGO) Derechos Digitales, rather than blocking links to works for which an infringement is suspected, to the work of a particular artist or group of artists or to musical or phonographic works in general, the decision was taken to prohibit access to the entire website.[420]

Several rapporteurs for freedom of expression recently recalled that the "blocking of entire websites, IP addresses, ports, or network protocols provided by the State is an extreme measure that can only be justified when stipulated by law and is necessary to protect a human right or other legitimate public interest, which includes that it is proportionate, there are no less invasive alternative measures that could preserve that interest and respect minimum guarantees of due process".[421] [422]

4. Site and app blocking

Shutting down Internet access or services or blocking apps is a measure applied in many countries worldwide. The *Internet & Jurisdiction Global Status Report 2019* mentioned this trend and highlighted its cross-border implications. More often than not, service providers are foreign companies, and shutdowns are hardly localized.

Because of the architecture of the Internet and its interconnected nature, a shutdown in one place may impair access or usability in another. If the shutdown is implemented on the infrastructure layer of the Internet, it is even more likely to have repercussions beyond the territory originally intended. Users may not be confined to one country, and services may be provided through a transnational system.

Countries in Latin America and the Caribbean are no different. One stakeholder interviewed noted that the region's Internet infrastructure was shared by many countries and companies. An action in one part may have repercussions on others even across different States. Governments, courts and companies have often blocked certain Internet services and apps, with consequences that have been felt beyond the intended target area or service. Another stakeholder mentioned that what was once a tactic of last resort has now become common practice.

> In December 2015, a Brazilian judge ordered the instant messaging service application WhatsApp to be blocked for 48 hours because of a refusal to hand over communication data sought for ongoing criminal investigations. This was not an isolated case, as two other court orders blocking the same application followed in different states of the country. All the court orders were quickly reversed, but the matter is still pending a decision in two constitutional cases before Brazil's Supreme Federal Court. These cases concern the extent of judges' powers to order services to be blocked in this way and the argument that the data are technically impossible to access because of the end-to-end encryption used by the messaging service.
>
> The blocking order applied to telecommunication carriers, which complied by shutting down access at the infrastructure level. It was reported that users of the app in Argentina and Chile were also impacted and could not access the service either.[423]

One expert interviewed mentioned an injunction by an electoral judge in Santa Catarina (Brazil) requiring the blocking of Facebook for disobeying a judicial order regarding an allegedly fake profile mocking a mayor. Facebook argued that it had complied with the original order and so the injunction was not executed.[424]

419 See [online] https://www.lanacion.com.ar/tecnologia/la-comision-nacional-de-comunicaciones-ordena-el-bloqueo-de-the-pirate-bay-en-la-argentina-nid1705910/.
420 See [online] https://www.derechosdigitales.org/7608/internet-bajo-censura-bloquean-pirate-bay-en-argentina/.
421 See Organization for Security and Cooperation in Europe (OSCE) and others, *Twentieth Anniversary Joint Declaration: Challenges to Freedom of Expression in the Next Decade*, Vienna, 2019 [online] https://www.osce.org/representative-on-freedom-of-media/425282?download=true.
422 See [online] http://www.oas.org/en/iachr/expression/publications/Guia_Desinformacion_VF%20ENG.pdf.
423 See [online] https://www.nytimes.com/2015/12/18/world/americas/brazil-whatsapp-facebook.html.
424 See [online] https://olhardigital.com.br/noticia/juiz-manda-bloquear-facebook-em-todo-o-brasil-por-24-horas/62909.

In other instances, Brazilian judges have ordered the removal of apps from the Google and Apple app stores. In the case of the Secret app, the rationale was that it was a "sanctuary for cyberbullying".[425] In a similar case, a judge ordered Microsoft to remove the Cryptic app, which offered a similar anonymous messaging service, from Windows phones.[426]

In October 2019, coinciding with protests in Quito over President Lenin Moreno's publication of decree No. 883 introducing austerity measures, it was reported that certain messaging and multimedia sharing services such as Facebook and WhatsApp were not available in Ecuador.[427]

On 13 April 2016, a court order in the city of Buenos Aires in Argentina required the car-sharing platform Uber to halt its activities there. Internet service providers (ISPs) were instructed to shut down Uber's mobile application and online platform.[428] Not only was the multinational corporation's service interrupted in the city of Buenos Aires as intended, but areas beyond the capital were affected as well.

On 20 December 2019, the Colombian Superintendence of Industry and Commerce ruled against the car-sharing app Uber, stating that the company had violated competition and antitrust laws in the country.[429] The ruling instructed ISPs to block access to the application. Stakeholders argued that this order violated the principle of net neutrality.[430]

In 2019, it was reported that the Bolivarian Republic of Venezuela had suffered some kind of service restriction lasting for 171 hours and affecting most particularly Twitter, WhatsApp, YouTube, and Periscope.[431] It was widely broadcast as well that the online encyclopedia Wikipedia had been blocked following what was said to be an "editing war" over whether Juan Guaidó or Nicolás Maduro was the legitimate President of the country.[432]

On 14 November 2019, the Ministry of Transport and Communications of Peru issued decree No. 035/2019[433] empowering it to block transportation apps deemed to be offering illegal services (including bicycles, taxis and e-scooters) unilaterally and without a court order. It is reported that the Ministry has instructed ISPs to block certain transportation apps and Apple and Google app stores to stop displaying them.[434]

5. Service shutdowns

Internet shutdowns are a deliberate disruption of Internet access mandated by local authorities for short periods, usually in situations where there is a threat, real or alleged, to public order. They may have destabilizing consequences, as they prevent not only communication but also access to information. Without access to the Internet, a population's ability to realize many daily activities is obstructed. People find themselves unable to communicate online, carry out research and even access basic services, some of them public.

With financial transactions migrating more and more to the Internet, access to money and different resources may also be disrupted. More lasting consequences concern consumer confidence and the need for businesses to migrate to more costly alternatives in view of the instability of the network.

425 See Internet & Jurisdiction Policy Network, "Blocking apps: Brazil orders Apple, Google to remove Secret from stores and devices", Paris, 2014 [online] https://www.internetjurisdiction.net/publications/retrospect#eyJ0byI6IjIwMTktMTIifQ==.
426 See [online] https://www.sfgate.com/business/article/Brazil-wants-no-Secret-on-app-stores-5701537.php.
427 See [online] https://www.accessnow.org/disrupciones-de-internet-en-ecuador-como-ocurrieron-y-como-eludirlas/; https://twitter.com/cidh/status/1183475097727832066; C. Botero, "Ecuador restringe redes sociales durante las protestas de esta semana", *El Espectador*, Bogotá, 11 October 2019 [online] https://www.elespectador.com/opinion/ecuador-restringe-redes-sociales-durante-las-protestas-de-esta-semana-columna-885505.
428 See Internet & Jurisdiction Policy Network, "Argentina: Uber faces blocking order and investigation by the DPA", Paris, 2016 [online] https://www.internetjurisdiction.net/publications/retrospect#eyJ0byI6IjIwMTktMTIifQ==.
429 See [online] https://www.sic.gov.co/slider/superindustria-ordena-cese-de-la-prestación-del-servicio-de-transporte-uber.
430 See [online] https://www.elespectador.com/tecnologia/que-tiene-que-ver-la-neutralidad-de-red-y-la-orden-de-suspender-uber-en-colombia-articulo-898079.
431 See S. Woodhams and S. Migliano, *The Global Cost of Internet Shutdowns in 2019*, London, Top10VPN, 2020 [online] https://www.top10vpn.com/cost-of-internet-shutdowns/.
432 See [online] https://netblocks.org/reports/wikipedia-blocked-in-venezuela-as-internet-controls-tighten-XaAwR08M; A. Azpúrua and others, "From the blocking of Wikipedia to social media: Venezuela's political crisis", *VeSinFiltro*, Caracas, 29 January 2019 [online] https://vesinfiltro.com/noticias/report-jan-2019/.
433 See [online] https://busquedas.elperuano.pe/normaslegales/decreto-supremo-que-precisa-disposiciones-sobre-el-servicio-decreto-supremo-n-035-2019-mtc-1826768-5/.
434 See [online] https://www.accessnow.org/blocking-apps-by-ministerial-decree-enables-illegal-content-takedowns-in-peru/.

The effects of Internet shutdowns are not limited to the domestic dimension. A range of international services are prevented from working, and this may hamper plans to invest in the country and even leave services completely unprovided, as companies may decide to leave. Communications with the outside world are curtailed as well. Family members may be unable to contact one another. This may be particularly worrying given that Internet shutdowns tend to happen in situations of civil or political unrest. In view of a past in which forced disappearances were a not uncommon practice in many countries of the region, the inability to contact a loved one may have a disturbing social impact and lasting consequences.

In the Bolivarian Republic of Venezuela, for instance, not only have apps and Internet services been blocked, but there have been Internet shutdowns or connectivity disruption over whole areas for short periods of time. These events tend to be associated with significant political events. In 2019, Internet shutdowns or major disruptions to connectivity were reported to have occurred multiple times, particularly with the State Internet provider. They usually coincided with political activities by Juan Guaidó (President of the Venezuelan National Assembly and self-proclaimed President of the country). One notable instance of an Internet shutdown reportedly occurred during a meeting of Juan Guaidó and the President of Colombia at the border between their two countries.

Similarly, in 2018, amidst protests in different parts of Nicaragua, the Internet was reported to have been shut down or disrupted in different areas of the capital, Managua.[435] The government did not acknowledge the Internet disruption, but it was reported that there was a correlation between actions taken by government forces and the regions where the Internet went down.[436]

Regional human rights institutions such as the Inter-American System of Human Rights, acting through its Special Rapporteurship for Freedom of Expression, have condemned Internet shutdowns and disruptions. Such actions, when taken by governments or on government orders, are seen as "extreme measure[s] analogous to the prohibition of a newspaper or a radio or television station. Such blockades or restrictions cannot be justified, not even for reasons of public order or national security, and cannot be used as censorship measures or as mechanisms to prevent access to information of the population."[437]

The same Rapporteurship has joined other international organizations in deploring "arbitrary disruptions and shutdowns to restrict access to telecommunications networks and the Internet".[438] According to some civil society organizations monitoring the issue, the number of these increased from 1 to 14 in the region between 2018 and 2019 in countries that included Nicaragua, the Bolivarian Republic of Venezuela and Ecuador, in spite of such condemnations.[439]

6. Mandatory data localization

It is of the nature of data to be easily transmissible and accessible worldwide. Yet the fact that they are accessible anywhere but must be stored somewhere makes it hard to oversee the security arrangements for storing and ensuring continuous access to them.

Several countries in the region have debated and some mandated the storage of data locally. The most important arguments for such forced localization of data tend to relate to national security, national safety and law enforcement access to relevant data. The logic is that data stored in servers within the territory under the State's jurisdiction are more readily available, thus providing more security and control.

435 See [online] https://netblocks.org/reports/nicaragua-regional-internet-disruptions-amid-protests-gdAmMvA9.
436 See [online] https://www.accessnow.org/cms/assets/uploads/2019/07/KeepItOn-2018-Report.pdf.
437 See Special Rapporteurship for Freedom of Expression, "The Office of the Special Rapporteur condemns closure of Radio Caracas Radio 750 AM, the censorship of television channels, restrictions on the Internet, and the arrest of journalists in Venezuela", *Press Release*, No. R116/19, Washington, D.C., 15 May 2019 [online] http://www.oas.org/en/iachr/expression/showarticle.asp?artID=1140&lID=1.
438 See Organization for Security and Cooperation in Europe (OSCE) and others, *Twentieth Anniversary Joint Declaration: Challenges to Freedom of Expression in the Next Decade*, Vienna, 2019 [online] https://www.osce.org/representative-on-freedom-of-media/425282?download=true.
439 See [online] https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf.

Such possible benefits have to be weighed against potential limitations on e-commerce transactions that depend on foreign financial service providers, for instance, or on firms that operate via the cloud or indeed small and medium-sized enterprises (SMEs) that cannot readily comply with localization requirements in order to enter new markets. It may also hinder the creation of unified digital markets and restrict cross-border service provision, with particular disadvantages for companies deploying a centralized strategy.[440]

Data location does not need to be explicitly mandated, but can be a de facto result of a policy. There may be requirements that encumber cross-border data transfers: this has been called conditional or soft localization, as opposed to mandatory localization.[441] Requirements under privacy laws that make transfers conditional on a procedure guaranteeing the rights of those the data are held on may be put into this category. Most data protection legislation in Latin America and the Caribbean tends to follow the European model and require either a ruling on appropriateness or a procedure or mechanisms guaranteeing the other party's intent to comply with the same standards of protection as are granted within the country. This does not directly restrict the flow of data, but may create hurdles.

Since the scandal of the Snowden revelations in 2013, when data relating to senior officials in many countries were accessed, leaked or handed over to the United States National Security Agency,[442] several administrations in the region have considered requiring at least some particularly sensitive data to be stored in servers within their territory.

One very significant example is a proposed amendment to Brazil's so-called Internet Bill of Rights, intended to mandate data localization in a very general way.[443] The amendment is worded as follows: "The Executive Branch, by decree, may require connection providers and Internet application providers as regulated by art. 11 that exercise their activities in an organized, professional and commercial way to install or use data storage, management and dissemination facilities within the country, depending on the size of the provider, its sales in Brazil and the scope of the service supplied to the Brazilian public."[444]

The proposal was rejected, but the law as approved specifies that Brazilian law is applicable when companies, even foreign ones, offer services to the Brazilian public.[445]

Sometimes there is no clear legislation mandating data localization, yet questions are still raised about availability or the desirability of allowing certain data to be stored on servers in a different territory. One example concerns judicial data. On 21 February 2019, the Brazilian National Justice Council (CNJ) suspended procurement proceedings to source cloud computing services from Microsoft out of concern that the databanks of Brazilian courts held "information about the life, economy and society of Brazil [...] that may endanger the security and national interests of Brazil".[446] Although there was no order requiring judicial data to be stored on Brazilian territory, the suspension had the indirect consequence of blocking the service because of the cross-border location of the servers.

Similarly, the Ministry of Information and Communications Technologies of Colombia expressed concern about the risks of relying on cloud storage for deploying basic services. As a mitigation measure, the authority requested the Office of the Counsel-General to impose data localization requirements for cloud service procurement by government agencies.[447]

As regards indirect data localization mandates, Argentina's National Directorate for Personal Data Protection issued provision No. 18/2015, which treats cloud storage as an international transfer of data,

440 See Economic Commission for Latin America and the Caribbean (ECLAC), "Regional digital market: strategic aspects", *Project Documents* (LC/TS.2018/30), Santiago, 2018.
441 See [online] https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf.
442 See G. Greenwald, "NSA collecting phone records of millions of Verizon customers daily", *The Guardian*, London, 6 June 2013 [online] http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; G. Greenwald, R. Kaz and J. Casado, "EUA espionaram milhões de e-mails e ligações de brasileiros", *O Globo*, Brasilia, 7 December 2013 [online] http://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934#ixzz2lEHZqYwh.
443 See [online] https://itsrio.org/wp-content/uploads/2018/02/v5_com-capa__pages_miolo_Brazil-Internet-Bill-of-Rights-A-closer-Look.pdf; https://igarape.org.br/marcocivil/en/; Internet & Jurisdiction Policy Network, "Marco Civil puts Brazilian data stored abroad under Brazilian jurisdiction", Paris, 2014.
444 See National Congress, "Substitutive Bill Proposal to Bill No. 2126 from 2011", 2013 [online] http://infojustice.org/wp-content/uploads/2013/11/Marco-Civil-English-Translation-November-2013.pdf.
445 See [online] https://www.camara.leg.br/noticias/429574-camara-aprova-projeto-do-marco-civil-da-internet/.
446 See [online] https://www.conjur.com.br/dl/cnj-proibe-tj-sp-contratar-microsoft.pdf. This decision was appealed and upheld on 25 June 2019. See [online] https://www.conjur.com.br/dl/voto-schiefler-contrato-tj-sp-microsoft.pdf.
447 Colombia, Basic Digital Services project. See [online] https://estrategia.gobiernoenlinea.gov.co/623/w3-article-18756.html.

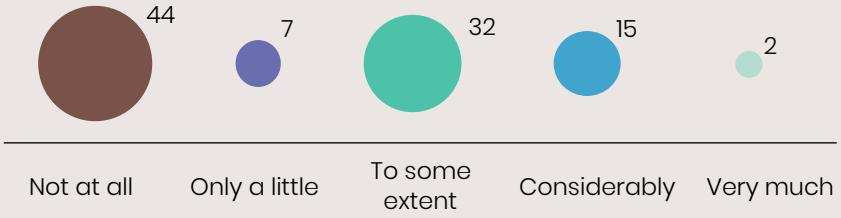
meaning that applications running on a cloud computing service must comply with the Personal Data Protection Act.[448] This may constitute a barrier to the flow of data and restrict this kind of application. It is also a hindrance to be obliged to obtain an additional express authorization from the user. Applications using servers inside the country have an advantage over those that use cloud computing.

The Bolivarian Republic of Venezuela is also reported to have data localization requirements. These seem to be particularly important as regards e-payment and payment processing infrastructure, as payment data must be processed locally.[449]

At the other end of the spectrum, Mexico has signed an agreement with the United States and Canada (Agreement between the United States, Mexico, and Canada (USMCA)) whose digital trade clauses include one banning any legislation that would require servers to be located within a member country's own jurisdiction.[450]

Of the stakeholders surveyed, more than 70% agreed or strongly agreed that compulsory data localization restricted the free flow of information and international trade.

Do you agree with the statement that compulsory data localization restricts the free flow of information and international trade?



Source: Internet & Jurisdiction Policy Network and Economic Commission for Latin America and the Caribbean (ECLAC).

A number of stakeholders mentioned in their comments that it was only natural for a networked global economy to have data flowing across borders unimpeded and that obligatory data localization restricted and clustered the Internet. As a technical matter, one of the stakeholders drew attention to how compulsory data localization could impact network speed and service quality. There might be costs not only in terms of higher prices but also in the potential for innovation. One stakeholder interviewed voiced concern that such obligations restricted the scale that smaller players could aspire to, as only the biggest firms would be able to afford the infrastructure costs of maintaining servers in different countries.

Some of the stakeholders pointed out that domestic data storage might be justified in certain cases, with the idea having some merit for confidential information, data pertaining to the public administration and national security data. There were some concerns about cloud computing and suggestions that it should be the object of regulation. One stakeholder observed, however, that it was a matter of abiding by local laws. Another noted that not all countries had the resources and tools to enforce domestic laws, particularly when enforcement had an extraterritorial component.

It should be noted that, the globalizing trend notwithstanding, voluntary domestic localization of data occurs more often than not in Latin America and the Caribbean. There are many possible factors behind this, but the perception of control and the desire to better satisfy local requirements might be the most common. National choices and public policy may indirectly favour local storage of data.

The policy coherence needed to build a thriving and integrated regional digital ecosystem demands the same coherence in the definitions that shape the debate. The Internet was created more than 50 years ago, and the World Wide Web has passed its thirtieth anniversary.

448 See [online] https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.
449 See [online] https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.
450 Agreement between the United States, Mexico, and Canada (USMCA) (30 November 2018), article 19.12, location of computing facilities: "No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory." See [online] https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between.

GLOSSARY

Some concepts have become established over the years, serving as recognized entry points for policy discussion, but others that seek to capture the essential aspects of new technological trends are still very contentious. This short glossary aims to familiarize readers new to the field with key concepts mentioned in the report, thus helping to clarify the trends and the legal and technological solutions mentioned.

1. The **Internet** is the global system of interconnected computer networks relying on the Internet protocol suite (Transmission Control Protocol (TCP)/Internet Protocol (IP)) for communications between networks and devices.
2. **IP** (Internet Protocol) is "the communications protocol underlying the Internet, allowing networks of devices to communicate over a variety of physical links. Each device or service on the Internet has at least one IP address that uniquely identifies it from other devices or services on the Internet."[451]
3. The **World Wide Web** (WWW) is an information system in which documents and other resources are interlinked by hypertext and are accessible over the Internet, making it "easy for anyone to roam, browse, and contribute to."[452]
4. The **DNS** (Domain Name System) is the naming system that "helps users to find their way around the Internet". Every computer on the Internet has a unique address, consisting of a string of numbers (the IP address), and the DNS makes using the Internet easier by allowing a familiar string of letters (the domain name, such as www.internetjurisdiction.net) to be used instead of the IP address.[453]
5. **Jurisdiction** has different meanings in international law. In this report it is used to signify an authority or a formally constituted legal body's power to hear and/or to take decisions regarding a specific matter. It is usually related to the idea of territory, but the two concepts are not always associated. That is particularly true when it comes to Internet-related topics, owing to the cross-border nature of the Internet.[454]

As already pointed out in the *Internet & Jurisdiction Global Status Report 2019*:

> "A distinction is often drawn between personal jurisdiction and subject matter jurisdiction. Personal jurisdiction relates to a court having jurisdiction over a particular legal or natural person. Subject matter jurisdiction relates to whether a court has jurisdiction over the type of dispute in question. Recent litigation, however, has brought attention to a third type of jurisdictional issue: 'scope of jurisdiction'. Scope of jurisdiction relates to the geographical scope of orders rendered by a court that has personal jurisdiction and subject matter jurisdiction.
>
> This issue —which overlaps with the law of remedies— has lately arisen with courts making global blocking, de-referencing or content removal orders. Considerations as to the appropriate scope of jurisdiction are intrinsically linked to the strength of the relevant claim of personal jurisdiction, as well as to the choice of law. For example, where a court has a relatively weak claim of personal jurisdiction, it may not be in a position to opt for an expansive scope of jurisdiction. A court opting for an expansive scope of jurisdiction may also not be able to apply only its own law, given the impact its judgment will have abroad."[455]

451 See [online] https://www.icann.org/resources/en/glossary.
452 See [online] https://www.w3.org/WWW/.
453 See [online] https://www.icann.org/resources/en/glossary.
454 See D. Svantesson, *Solving the Internet Jurisdiction Puzzle*, Oxford, Oxford University Press, 2017.
455 See [online] https://www.internetjurisdiction.net/news/release-of-worlds-first-internet-jurisdiction-global-status-report.

6. **Choice of law** is the ability of contractual parties to choose which law will govern any disputes between the parties and the interpretation of the contract. The report addressed this concept when referring to the choice of law clause usually included in the terms of service and community guidelines of international Internet platforms. In online agreements of this type, "party autonomy" in choosing this law is usually questionable, as the user is presented with unilaterally predetermined contractual terms.

7. **Encryption** is "the process of encoding data so that it can be interpreted only by intended recipients".[456] It is used as a key security and privacy feature by several popular applications, from e-commerce to Internet banking and from instant messaging to video communications apps.

8. **Blockchain** is "a shared ledger of transactions between parties in a network, not controlled by a single central authority". The blockchain works like a ledger, since it "records and stores all transactions between users in chronological order. Instead of one authority controlling this ledger (like a bank), an identical copy of the ledger is held by all users on the network, called nodes."[457]

9. **Financial technology** (abbreviated as fintech) refers to the technology used by entities that specialize in providing financial services chiefly through technologically enabled online platforms.[458]

10. **Regulatory sandboxes** are spaces provided for companies to experiment with the operation of innovative products or services in a limited fashion with less stringent rules, under the supervision of a government regulatory authority.[459]

11. **Fake news** is a term used in the last decade as a politically charged label to refer to any "false and misleading information, disguised and disseminated as news".[460] The academic debate over a more appropriate term is still ongoing, with authors suggesting the use of definitions such as "disinformation" or "misinformation". Disinformation can be defined as false information that is deliberately created or disseminated with the express purpose of causing harm. Producers of disinformation typically have political, financial, psychological or social motivations. Misinformation, on the other hand, is information that is false, but not intended to cause harm. For example, individuals who are unaware that a piece of information is false may spread it on social media in an attempt to be helpful.[461]

12. **Deepfake** is a term currently used to describe fabricated media produced using artificial intelligence. By processing elements from existing video or audio files, it can be used to create new content in which individuals speak words and perform actions with no basis in reality.[462] As the technology evolves, it is likely that deepfake will be increasingly used in disinformation campaigns.[463]

13. The **Internet of Things** is a system of interrelated devices with the ability to collect and transfer data over a network without requiring continuous human interaction. In a more complex scenario, the Internet of Things can be defined as "a self-configuring, adaptive, complex network that interconnects 'things' to the Internet through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/actuation capability, a programmability feature and are uniquely identifiable. The representation contains information including the 'thing's' identity, status, location or any other business, social or privately relevant information. The 'things' offer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability. The service is exploited through the use of intelligent interfaces and is made available anywhere, anytime, and for anything taking security into consideration."[464]

---

456 See [online] https://firstdraftnews.org/wp-content/uploads/2018/07/infoDisorder_glossary.pdf?x25702.
457 See [online] https://www.oecd.org/finance/OECD-Blockchain-Primer.pdf.
458 For further information, See W. Magnuson, "Regulating fintech", College Station, Texas A&M University, 2018 [online] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3027525.
459 See [online] https://publications.iadb.org/publications/english/document/Regulatory-Sandboxes-in-Latin-America-and-the-Caribbean-for-the-FinTech-Ecosystem-and-the-Financial-System.pdf.
460 See [online] https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0.pdf.
461 See C. Wardle and H. Derakshan, *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*, Strasbourg, Council of Europe, 2017 [online] https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c.
462 See [online] https://firstdraftnews.org/wp-content/uploads/2018/07/infoDisorder_glossary.pdf?x25702. For further information, see Y. Li, M. Chang and S. Lyu, "In ictu oculi: exposing AI generated fake videos by detecting eye blinking", 2018 [online] https://arxiv.org/pdf/1806.02877.pdf.
463 For further information, see [online] https://www.lawfareblog.com/deepfakes-looming-crisis-national-security-democracy-and-privacy.
464 See [online] https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf.

The *Internet & Jurisdiction and ECLAC Regional Status Report 2020* is Latin America and the Caribbean's first comprehensive exercise in mapping the different policy trends relating to the cross-border nature of the Internet and the way this affects different stakeholders such as governments, companies and civil society.

How might differing regional and national regulations create barriers to cross-border e-commerce and investment in digital markets? What economic and social benefits could be realized by harmonizing frameworks throughout the region? A better understanding of this situation is vital to efforts to foster investor confidence, promote innovation and economic diversification, create greater trust in e-commerce and boost a market of more than 600 million people, while opening up opportunities for businesses, most particularly small and medium-sized enterprises.

Conversely, uncoordinated action by a wide range of actors and initiatives risks hampering the digitalization of economies, governments and societies. It is to help policymakers navigate the challenges ahead and to mutualize knowledge that the Internet & Jurisdiction Policy Network, in coordination with the Economic Commission for Latin America and the Caribbean (ECLAC), is presenting the *Internet & Jurisdiction and ECLAC Regional Status Report 2020*.

ECLAC

Economic Commission for Latin America and the Caribbean (ECLAC)
Comisión Económica para América Latina y el Caribe (CEPAL)
www.eclac.org

LC/TS.2020/141