

UNIVERSIDADE DE COIMBRA

FACULDADE DE DIREITO



**FACULDADE DE DIREITO
UNIVERSIDADE D
COIMBRA**

**RGPD, RAI E A RELAÇÃO LABORAL – A INFLUÊNCIA ALGORÍTMICA
NA SELEÇÃO DE CANDIDATOS A EMPREGO, AVALIAÇÃO DE
DESEMPENHO E DESPEDIMENTO DE TRABALHADORES**

Inês Sofia Costa Queirós

*Dissertação apresentada à Faculdade de Direito da Universidade de Coimbra no âmbito do
2.º Ciclo de Estudos em Direito (conducente ao grau de mestre), na Área de Especialização
em Ciências Jurídico-Empresariais, com Menção em Direito Laboral, sob orientação do
Senhor Professor Doutor João Leal Amado*

Coimbra

2024

es conveniente no dejarse llevar por el brillo provocado por la Inteligencia Artificial y todos los instrumentos vinculados a las nuevas tecnologías, pues no de sus atractivo es su apariencia de neutralidad, en lo que se ha denominado la "fachada de la tecnología objetiva", causante de "sesgos de automatización" o "complacencia inducida", de manera que "muchas personas quieren creer que una máquina que imita las funciones del cerebro humano puede estar libre de limitaciones humanas, incluyendo sesgos económicos, sociales, culturales y políticos particulares [;sin embargo], la ética y los valores de los seres humanos que construyen sistemas de Inteligencia Artificial y de los sistemas

ROBERTO FERNÁNDEZ FERNÁNDEZ¹

¹ ROBERTO FERNÁNDEZ FERNÁNDEZ, *Selección de trabajadores y algoritmos: desafíos ante las nuevas formas de reclutamiento*, Thomson Reuters, 2022, p. 57 e 58.

Agradecimentos

À minha irmã,

que me acompanhou ao longo deste percurso, apoiando-me incondicionalmente.

Ao Vaz,

o irmão que nunca tive e que fez do longe perto.

Ao Roberto,

o melhor amigo que me motivou e ajudou, incansavelmente, ao longo desta jornada.

À Marta e Vânia,

as minhas amigas de todas as horas.

Resumo

A presente dissertação foca-se no estudo do atual quadro legal (nacional e internacional) laboral tendo em consideração o forte desenvolvimento tecnológico vivenciado desde a pandemia COVID-19.

Se é verdade que o Direito Laboral é uma área desenvolvida a partir das tradicionais formas de trabalho – sobretudo físico –, também o é que este ramo do direito, como qualquer outro ramo, necessita de se adaptar às novas realidades que vão surgindo com o desenvolvimento – e, em concreto, o desenvolvimento tecnológico.

Neste estudo iremos analisar a legislação laboral vigente e correlacioná-la com a evolução tecnológica, em particular com a utilização de algoritmos no âmbito das relações de trabalho. As novas metodologias utilizadas para processos de seleção de candidatos a emprego, avaliação de desempenho de trabalhadores e determinação de trabalhadores a despedir são os principais temas em análise.

Iremos explorar como é que as novas tecnologias, ao facilitarem o acesso a dados pessoais, impactam as práticas de gestão empresariais e a conformidade com as disposições em matéria de proteção de dados.

Palavras-chave: Direito Laboral, RGPD, RIA, candidatos a emprego, despedimento, despedimento coletivo, avaliação de desempenho, inteligência artificial, algoritmo.

Abstract

This dissertation focuses on the study of the current (national and international) labor law framework, considering the strong technological development experienced since the COVID-19 pandemic.

While it is true that labor law is a field developed from traditional forms of work – mainly physical – it is also true that this branch of law, like any other branch, needs to adapt to the new realities that arise with development – and, specifically, technological development.

In this study we will analyze current labor legislation and correlate it with technological developments, in particular with the use of algorithms in the workplace. The new methodologies used for selecting job candidates, evaluating employees' performance and determining which employee should be made redundant are the main topics being explored.

We will study how new technologies, by facilitating access to personal data, impact business management practices and compliance with data protection provisions.

Keywords: Labor Law, GDPR, AI Act, job candidates, dismissal, collective redundancies, performance evaluation, artificial intelligence, algorithm.

Siglas e abreviaturas

BDSG – Bundesdatenschutzgesetz

CC – Código Civil

CDFUE – Carta dos Direitos Fundamentais da União Europeia

CEDH – Convenção Europeia dos Direitos do Homem

CNPD – Comissão Nacional de Proteção de Dados

CRC – Código dos Regimes Contributivos do Sistema Previdencial de Segurança Social

CRP – Constituição da República Portuguesa

CT – Código do Trabalho

DUDH – Declaração Universal dos Direitos do Homem

EPD – Encarregado de Proteção de Dados

HDSG – Hessisches Datenschutzgesetz

LPDP – Lei da Proteção de Dados Pessoais

NPL – Processamento de Linguagem Natural

OIT – Organização Internacional do Trabalho

RGPD – Regulamento Geral de Proteção de Dados

RIA – Regulamento da Inteligência Artificial

TFUE – Tratado sobre o Funcionamento da União Europeia

TJUE – Tribunal de Justiça da União Europeia

Índice

<u>Agradecimentos</u>	3
<u>Resumo</u>	4
<u>Abstract</u>	5
<u>Siglas e abreviaturas</u>	6
<u>Introdução</u>	11
<u>1.O contrato de trabalho: A relação laboral</u>	14
<u>1.1.Noção legal</u>	14
<u>1.1.1.O contrato de trabalho</u>	15
<u>1.1.2.A prestação de atividade</u>	16
<u>1.1.3.A subordinação jurídica</u>	16
<u>1.1.4.A retribuição</u>	18
<u>2.O direito à proteção de dados</u>	19
<u>2.1.Contexto histórico</u>	19
<u>2.1.1.Estados Unidos da América: o <i>Special Subcommittee on Invasion of Privacy</i></u>	20
<u>2.1.2.Europa</u>	23
<u>2.2.A proteção constitucional</u>	24
<u>2.3.Regulamento Geral de Proteção de Dados</u>	27
<u>2.3.1.Âmbito de aplicação</u>	28
<u>2.3.2.Noção de “dados pessoais”</u>	30
<u>2.3.2.1.Qualquer informação</u>	30
<u>2.3.2.2.Relativa a</u>	31
<u>2.3.2.3.Pessoa singular</u>	33
<u>2.3.2.4.Identificada ou identificável</u>	33
<u>2.3.3.O Encarregado de Proteção de Dados</u>	34
<u>2.3.4.Comissão Nacional de Proteção de Dados</u>	36
<u>2.4.Princípios gerais no âmbito da proteção de dados</u>	38
<u>2.4.1.Princípio da livre circulação</u>	38
<u>2.4.2.Princípio da licitude</u>	39
<u>2.4.3.Princípio da lealdade</u>	40
<u>2.4.4.Princípio da transparência</u>	41
<u>2.4.5.Princípio do propósito limitado ou da limitação das finalidades</u>	41

2.4.6.Princípio da minimização dos dados	42
2.4.7.Princípio da precisão e exatidão	43
2.4.8.Princípio do limite à retenção/conservação dos dados	44
2.4.9.Princípio da integridade e confidencialidade	45
2.4.10.Princípio da responsabilidade	45
2.4.11.Princípio da proporcionalidade	46
2.5.Direitos dos titulares dos dados	47
2.5.1.Direito à informação	48
2.5.2.Direito de acesso	48
2.5.3.Direito de retificação	49
2.5.4.Direito ao apagamento (direito a ser esquecido)	50
2.5.5.Direito à limitação do tratamento dos dados pessoais	51
2.5.6.Direito de portabilidade	52
2.5.7.Direito de oposição	52
2.5.8.Direito à não avaliação com base num tratamento automático	53
2.6.A proteção de dados no contexto laboral	54
2.6.1.A licitude para o tratamento de dados pessoais	57
2.6.1.1.O consentimento do trabalhador	58
2.6.1.2.O tratamento de dados pessoais do trabalhador para o cumprimento de obrigações adstritas à entidade empregadora	62
2.6.2.Dados sensíveis no contexto laboral	63
3.A utilização algorítmica no contexto laboral	64
3.1.O Regulamento da Inteligência Artificial no contexto laboral	65
3.1.1.Âmbito de aplicação	66
3.1.2.A hierarquização dos riscos	67
3.1.2.1.Risco inaceitável	68
3.1.2.2.Risco elevado	68
3.2.O conceito de algoritmo: notas características	70
3.3.O processo de recrutamento	72
3.3.1.Considerações preliminares	72
3.3.2.A legitimidade da entidade empregadora para o tratamento dos dados pessoais do candidato a emprego	73
3.3.3.A limitação ao prazo de conservação dos dados pessoais dos candidatos a emprego	75
3.3.4.As fases de recrutamento e a influência algorítmica	76

3.3.4.1.Fase 1: procura dos candidatos	76
3.3.4.2.Fase 2: avaliação dos candidatos	77
3.3.4.3.Fase 3: seleção e contratação	79
3.4.Avaliação de desempenho do trabalhador.....	79
3.4.1.Sistemas biométricos para controlo de assiduidade	80
3.4.2.Controlo de alcoolémia e substâncias psicoativas	83
3.4.3.Sistemas de geolocalização	84
3.4.4.Sistemas de videovigilância	86
3.4.5.Sistemas de controlo da utilização de telefones, do correio eletrónico, do acesso à Internet ou do computador.....	89
3.4.5.1.Controlo do e-mail do trabalhador.....	90
3.4.5.2.Monitorização do uso da Internet	92
3.4.5.3.Acesso remoto ao computador do trabalhador	93
3.4.5.4.Controlo de dados de comunicações telefónicas e de tráfego	93
3.4.5.5.O caso paradigmático do Acórdão do TEDH: BĂRBULESCU V. ROMANIA	95
3.4.6.A utilização algorítmica nos processos de avaliação de desempenho do trabalhador	98
3.5.O poder disciplinar e sancionatório da entidade empregadora com base numa análise algorítmica.....	102
3.5.1.A conservação dos dados pessoais do trabalhador após a cessação do vínculo contratual	106
3.6.Algoritmo como novo desafio legal.....	107
3.6.1.As vantagens da utilização algorítmica na relação laboral	108
3.6.2.A discriminação algorítmica.....	111
3.6.3.As decisões automatizadas	114
3.6.3.1.1.Fase de recrutamento	115
3.6.3.1.2.Fase de avaliação de desempenho	117
3.6.3.1.3.Fase de despedimento	119
3.6.4.A importância dos sindicatos na “negociação algorítmica”	123
3.6.5.Decisões algorítmicas: a quem responsabilizar?	126
3.6.6.Diretiva (UE) 2024/2831 do Parlamento Europeu e do Conselho, de 23 de outubro.....	130
3.6.7.Soluções.....	133
Conclusão.....	139
Bibliografia	141

Introdução

A última década ficou marcada por trazer consigo um conjunto de mudanças. Observamos uma forte evolução tecnológica acompanhada por um aumento da globalização, numa quase tentativa de derrube de quaisquer barreiras que ainda pudessem existir.

O funcionamento do mercado interno exigiu uma maior integração económica e social, provocando um aumento significativo de fluxos transfronteiriços de dados pessoais. O intercâmbio desses dados entre entidades públicas e privadas intensificou-se na União Europeia, aumentando, simultaneamente, a recolha e partilha dos mesmos numa escala nunca antes vista.

Uma evolução como esta exige do legislador um quadro de proteção de dados assentes em boas bases, impondo regras rigorosas.

Se, por um lado, o que se pretende é eliminar os obstáculos à circulação de dados pessoais na União Europeia, também é imperativo que exista uma base legislativa comum em todos os países permitindo, desta forma, uma partilha consciente e harmónica dos mesmos.

No que ao Direito do Trabalho diz respeito, a problemática da proteção de dados tem vindo a ganhar cada vez mais importância. A pandemia COVID-19 criou um conjunto de novos desafios, exigindo das entidades empregadoras, mas também dos trabalhadores, uma grande adaptação à realidade que estava a ser criada. É neste cenário de contínuas mudanças, em que o objetivo primordial era atingir alguma estabilidade nas relações de trabalho, que o regime de teletrabalho (que existia apenas no plano teórico²) começou a entrar em prática.³ E com o teletrabalho vieram os desenvolvimentos tecnológicos que lhe estavam associados.

² Segundo estudos da Eurostat, o número de pessoas a trabalhar a partir de casa em Portugal no final de 2019 correspondia a 6,5% (em comparação com a percentagem de 5,4% da UE-27). DGERT, *Teletrabalho no contexto da negociação coletiva*, Coleção: Negociação coletiva em foco, n.º 1 de 2020, 25 de novembro de 2020, Direção-Geral do Emprego e das Relações de Trabalho, Divisão de Promoção do Diálogo Social, p. 9.

³ O Decreto-Lei n.º 79-A/2020, de 30 de setembro, que estabeleceu “*um regime excecional e transitório de organização do trabalho*”, com o principal foco de minimizar os riscos da propagação da doença COVID-19, foi, posteriormente alterado pelo Decreto-Lei 94-A/2020, de 3 de novembro, que veio determinar a obrigatoriedade do recurso ao teletrabalho para todos os trabalhadores cujo local de trabalho se situasse em áreas territoriais em que a situação epidemiológica o justifique, definidas pelo Governo mediante resolução de Conselho de Ministros.

Ora, é de fácil compreensão que o aumento da captação de dados tenha explodido nos últimos anos.

No que diz respeito à questão algorítmica, e não descurando as conclusões anteriores, parece-nos que a implementação de algoritmos no mercado laboral é inevitável e veio para ficar.

O algoritmo tem sido utilizado para várias funções: ao nível da seleção de trabalhadores para determinar os perfis dos candidatos a emprego com base em determinados critérios, em matéria de execução dos contratos de trabalho através da distribuição de tarefas e no processo de avaliação de desempenho e no que diz respeito à cessação das relações laborais para seleccionar os trabalhadores a despedir⁴.

Não obstante, a legalidade do uso de algoritmos no contexto laboral tem sido bastante questionada. Terão as “máquinas” autonomia para despedir? Poderá o empregador “ser um algoritmo”? A passagem de decisões humanas para a inteligência artificial, com o objetivo de se atribuir uma determinada objetividade ao processo decisório, não tem sido isenta de críticas. Citando GUILHERME DRAY,⁵

Podem ser benéficos, em matéria de gestão laboral, por garantirem maior eficiência e objetividade nas decisões, mas podem também ser perniciosos, discriminatórios e profundamente injustos na abordagem dos temas

O desenvolvimento tecnológico é fulcral para uma própria evolução e aperfeiçoamento civilizacional, contudo, para que seja possível construirmos uma nova história, é necessário que a sua estrutura encontre assento legal.⁶

Se é verdade que estamos a caminhar para o progresso, também o é que o quadro normativo vigente se tem revelado, frequentemente, insuficiente para fazer face a todas as mudanças que estão a acontecer.

⁴ GUILHERME DRAY, *Algorithm Management e a Necessidade de “Humanização” da Gestão*, p. 1.

⁵ GUILHERME DRAY, *Algorithm... Ob. cit.*, p. 1.

⁶ Considerando (7) do RGPD: “Esta evolução exige um quadro de proteção de dados sólido e mais coerente na União, apoiado por uma aplicação rigorosa das regras, pois é importante gerar a confiança necessária ao desenvolvimento da economia digital no conjunto do mercado interno. As pessoas singulares deverão poder controlar a utilização que é feita dos seus dados pessoais. Deverá ser reforçada a segurança jurídica e a segurança prática para as pessoas singulares, os operadores económicos e as autoridades públicas”.

1. O contrato de trabalho: A relação laboral

1.1. Noção legal

A relação jurídica vigente entre trabalhador e empregador é regulada pelo contrato de trabalho.

A noção de contrato de trabalho é conseguida através da análise conjunta dos artigos 1152.º do CC⁷ e 11.º do CT – que não se opõem, mas complementam-se entre si.

O artigo 1152.º do CC dispõe o seguinte:

Contrato de trabalho é aquele pelo qual uma pessoa se obriga, mediante retribuição, a prestar a sua atividade intelectual ou manual a outra pessoa, sob a autoridade e direção desta.

A definição dada pelo Código Civil é compreendida como “a noção geral”, tendo o Código de Trabalho de 2009 introduzido algumas particularidades a esta noção.⁸ Vejamos:

Contrato de trabalho é aquele pelo qual uma pessoa singular se obriga, mediante retribuição, a prestar a sua atividade a outra ou outras pessoas, no âmbito de organização e sob a autoridade destas.

Da análise do artigo 11.º do CT é possível observar, quase de forma imediata, as seguintes alterações: (1) cingiu-se o prestador da atividade (o trabalhador) a uma “pessoa singular”; (2) supriu-se a referência ao poder de direção por parte da entidade empregadora; (3) incluiu-se, de forma expressa, a referência ao desenvolvimento da atividade laboral dentro de uma determinada organização desenvolvida pelo empregador; (4) excluiu-se a referência à natureza “intelectual ou manual” da atividade e (5) admitiu-se situações de pluralidade de empregadores.^{9/10}

⁷ Refira-se, ainda, o artigo 1153.º do CC que refere que “[o] contrato de trabalho está sujeito a legislação especial”. A este propósito veja-se JOÃO LEAL AMADO, *Contrato de Trabalho: noções básicas*, 4.ª Edição, 2023, Almedina, p. 11 a 30.

⁸ ANTÓNIO MENEZES CORDEIRO, *Direito do Trabalho II – Direito Individual*, Almedina, 2019, p. 31 a 35.

⁹ ANTÓNIO MENEZES CORDEIRO, *Direito... Ob. cit.*, p. 32 e 33.

¹⁰ Como refere João Leal Amado por referência a Jorge Leite, “o *Direito do Trabalho é o conjunto das normas jurídicas, de origem estadual e convencional, que visam regular, com vista à sua normalização, as relações individuais e coletivas que têm como seu elemento unificante e desencadeante o trabalho assalariado*”. Confirmar JOÃO LEAL AMADO, *Contrato de Trabalho: noções básicas... Ob. cit.*, p. 34.

Para chegarmos a um melhor entendimento sobre o que é e em que é que se baseia o contrato de trabalho iremos analisar, em particular, quatro aspetos: (i) o contrato; (ii) a prestação de atividade; (iii) a subordinação jurídica e (iv) a retribuição.¹¹

1.1.1. O contrato de trabalho

O contrato de trabalho é um negócio jurídico bilateral, isto é, um acordo onde vigoram duas manifestações de vontade¹² opostas, mas convergentes entre si. Cada um dos contraentes persegue um interesse individual e, através de uma regulamentação comum, chegam a um resultado idêntico e unitário.¹³

O empregador expressa a sua vontade de empregar o trabalhador com o objetivo que esse trabalhe para si tendo por base as funções que lhe estão adstritas pelo contrato de trabalho, pagando-lhe, como contrapartida da prestação dessa atividade, uma retribuição. O trabalhador obriga-se a executar determinadas tarefas, sob a organização e autoridade daquele, recebendo a retribuição correspondente a essa atividade.¹⁴

Como referido anteriormente, os interesses das partes são diferentes, e, citando BERNARDO LOBO XAVIER,¹⁵

ao empregador interessa conseguir a maior quantidade e a melhor qualidade de trabalho possível contra a menor retribuição, enquanto o trabalhador procura conseguir a maior retribuição em troca do seu trabalho

No fundo, é através do contrato de trabalho que as partes harmonizam e organizam os seus interesses.

¹¹ BERNARDO DA GAMA LOBO XAVIER, *Manual de Direito do Trabalho*, com colaboração de P. Furtado Martins, A. Nunes de Carvalho e Joana Vasconcelos, 4.^a Edição, Revista e Atualizada, Rei dos Livros, 2020, p. 306.

¹² O facto do negócio jurídico englobar duas manifestações de vontade não significa que envolva apenas duas pessoas, uma vez que uma das partes pode ser representada por um conjunto de pessoas.

¹³ BERNARDO DA GAMA LOBO XAVIER, *Manual de Direito do Trabalho...* Ob. cit., p. 306.

¹⁴ BERNARDO DA GAMA LOBO XAVIER, *Manual de Direito do Trabalho...* Ob. cit., p. 306.

¹⁵ BERNARDO DA GAMA LOBO XAVIER, *Manual de Direito do Trabalho...* Ob. cit., p. 306.

1.1.2. A prestação de atividade

O disposto no artigo 11.º do CT pretende, desde logo, indicar as duas principais obrigações das partes: a prestação de trabalho, por parte do trabalhador, e a retribuição, na esfera da entidade empregadora.¹⁶

A prestação de atividade traduz-se na “*exteriorização da força de trabalho*”¹⁷ e é um elemento fundamental para a distinção entre trabalho subordinado e trabalho autónomo.¹⁸ Neste último, o prestador de serviços apenas se obrigada a apresentar um resultado do seu trabalho, podendo utilizar os meios que achar conveniente para atingir o resultado que foi estipulado no contrato. Em contrapartida, no contrato de trabalho o que está em causa é a atividade em si pelo que, citando ANTÓNIO MONTEIRO FERNANDES,^{19/20}

o trabalhador que tenha cumprido diligentemente a sua prestação não pode ser responsabilizado pela frustração do resultado pretendido.

1.1.3. A subordinação jurídica

A subordinação jurídica é o terceiro elemento que aqui analisamos e, talvez, o mais relevante para delimitar a pessoa do trabalhador.²¹

A atividade prestada pelo trabalhador terá de ser feita “*no âmbito da organização e sob autoridade*” da entidade empregadora, pelo que a diferenciação entre trabalhadores autónomos ou independentes e trabalhadores subordinados passa pela existência deste elemento. Contudo, nem sempre é fácil distinguir estas duas categorias de trabalhadores.²²

¹⁶ BERNARDO DA GAMA LOBO XAVIER, *Manual de Direito do Trabalho...* Ob. cit., p. 307.

¹⁷ ANTÓNIO MONTEIRO FERNANDES, *Direito do Trabalho*, 20.ª Edição, Almedina, 2020, p. 139.

¹⁸ JOÃO LEAL AMADO, *Contrato de Trabalho: noções básicas...* Ob. cit., p. 57.

¹⁹ ANTÓNIO MONTEIRO FERNANDES, *Direito...* Ob. cit., p. 139.

²⁰ Veja-se, a título de exemplo, as decisões jurisprudenciais do Supremo Tribunal de Justiça: Acs. STJ 02.05.2007 – Proc. n.º 06S4368; 22.09.2010 – Proc. n.º 4401/04.7TTLSB.S1; 11.07.2012 – Proc. n.º 3360/04.0TTLSb.L1.S1 e 05.03.2013 – Proc. n.º 3247/06.2TTLSB.L1.S1.

²¹ MARIA DO ROSÁRIO PALMA RAMALHO, *Tratado de Direito do Trabalho, Parte I – Dogmática Geral*, 5.ª Edição, Almedina, 2020, p. 365.

²² MARIA DO ROSÁRIO PALMA RAMALHO, *Tratado de Direito do Trabalho, Parte I – Dogmática Geral...* Ob. cit., p. 364 e MARIA DO ROSÁRIO PALMA RAMALHO, *Tratado de Direito do Trabalho, Parte II – Situações Laborais Individuais*, 8.ª Edição, Almedina, 2021, pontos 1.4.2., 1.6. e 3.

A determinação pela existência de subordinação jurídica implica, necessariamente, duas considerações: primeiro, que o Direito reconhece esse poder ao empregador, atribuindo-lhe, assim, o chamado poder disciplinar; segundo, que outras formas de dependência podem surgir na relação laboral.^{23/24}

Como explica BERNARDO LOBO XAVIER²⁵

o empregador dirige, define, especifica, encaminha a prestação de trabalho, tanto em abstrato (regulamentando) como em concreto (dando ordens e contra-ordens, em ajustamento contínuo).

Estas orientações dadas pela entidade empregadora são importantes uma vez que o contrato de trabalho não especifica, detalhada e taxativamente, cada atividade que o trabalhador terá de realizar ou como o deverá fazer. Como afirma o autor,²⁶

se não fosse a possibilidade de ajustamentos contínuos, o contrato de trabalho não poderia ser um contrato duradouro e o regime de segurança no emprego não permitira que o contrato de trabalho desempenhasse a sua função económica.

No entanto, as instruções dadas pela entidade empregadora podem não se expressar em todos os momentos da relação de trabalho. A verdade é que existem períodos – que, porventura, são bastante frequentes – em que o trabalhador não está a receber ordens, aparentando ter autonomia na prestação de trabalho. Esta é uma ideia falaciosa pelo facto de ser suficiente, para que se verifique a existência de subordinação jurídica, o *potencial* estado de dependência do trabalhador à entidade empregadora.²⁷

No fundo, o empregador pode não ter interesse em dar ordens ao trabalhador com o objetivo de beneficiar plenamente das capacidades e conhecimentos deste. Esta é uma realidade cada vez mais presente, uma vez que o desenvolvimento individual e profissional dos atuais

²³ ANTÓNIO MONTEIRO FERNANDES, *Direito...* Ob. cit., p. 147.

²⁴ MARIA DO ROSÁRIO PALMA RAMALHO, *Tratado de Direito do Trabalho, Parte II...* Ob. cit., p. 35.

²⁵ BERNARDO DA GAMA LOBO XAVIER, *Manual de Direito do Trabalho...* Ob. cit., p. 308.

²⁶ BERNARDO DA GAMA LOBO XAVIER, *Manual de Direito do Trabalho...* Ob. cit., p. 311.

²⁷ ANTÓNIO MONTEIRO FERNANDES, *Direito do Trabalho...* Ob. cit., p. 147 e 148.

trabalhadores – face à grande competitividade do mercado de trabalho – tem demonstrado que estes conhecem melhor o trabalho que têm a realizar do que o próprio empregador.^{28/29}

Em suma, importa, contudo, referir que este critério tem vindo a sofrer alguma flexibilização interpretativa face às alterações civilizacionais que vêm surgindo, nomeadamente:

- (i) A subordinação jurídica não implica uma subordinação económica. O facto de um determinado trabalhador não depender da remuneração do seu trabalho por ter, desde logo, outras fontes de rendimentos, não exclui a existência de subordinação jurídica.
- (ii) A subordinação jurídica, como suprarreferido, não tem de se expressar em todos os momentos, seja por motivos de confiança depositada no próprio trabalhador, seja porque o empregador pretende beneficiar do máximo de conhecimentos do seu trabalhador na execução do trabalho.
- (iii) A subordinação jurídica é compatível com a autonomia técnica e deontológica do trabalho, nos termos do artigo 116.º do CT.
- (iv) A subordinação jurídica está limitada funcionalmente, estando o empregador cingido pelo próprio contrato de trabalho.

1.1.4. A retribuição

A retribuição é o último elemento deste elenco e traduz-se na contrapartida pela prestação de trabalho.³⁰ Além disso, representa um elemento fundamental para a determinação pela existência de contrato de trabalho, uma vez que qualquer forma de trabalho gratuito é automaticamente excluída da relação laboral.³¹

Acresce que, como explica MARIA DO ROSÁRIO PALMA RAMALHO,³²

²⁸ ANTÓNIO MONTEIRO FERNANDES, *Direito do Trabalho...* Ob. cit., p. 148.

²⁹ JOÃO LEAL AMADO, *Contrato de Trabalho: noções básicas...* Ob. cit., p. 61.

³⁰ JOÃO LEAL AMADO, *Contrato de Trabalho: noções básicas...* Ob. cit., p. 60.

³¹ MARIA DO ROSÁRIO PALMA RAMALHO, *Tratado de Direito do Trabalho, Parte II...* Ob. cit., p. 30 e 31.

³² MARIA DO ROSÁRIO PALMA RAMALHO, *Tratado de Direito do Trabalho, Parte I...* Ob. cit., p. 26.

a exigência de retribuição no trabalho subordinado é um corolário do requisito da liberdade do prestador, já que o pagamento da actividade faz sentido para o trabalho livre e não para o trabalho servil.

A retribuição é, normalmente, paga em dinheiro, podendo, contudo, ser paga parcialmente em géneros, nos termos do artigo 259.º, n.º 1 do CT.

No que concerne ao modo de cálculo da retribuição, este também será diferente conforme estejamos perante um contrato de trabalho ou um contrato de prestação de serviços. Via regra, e quando oneroso, ao contrato de prestação de serviços corresponde uma remuneração em função do resultado atingido. No caso do contrato de trabalho, a retribuição é normalmente calculada em função do tempo de trabalho.³³

Não obstante, este critério mostra-se, no cômputo geral, um quanto falível, seja porque existem contratos que, apesar do preço ser um elemento essencial, o elemento remuneração não é operativo (e.g. contrato de empreitada, nos termos do artigo 1207.º do CC), seja por, no que diz respeito ao modo de cálculo, existirem contratos de prestação de serviços cuja remuneração é estabelecida em função do tempo (e.g. contrato de avença). A mais, também nas situações em que vigora o contrato de trabalho existe a possibilidade do cálculo da remuneração ser feito em função do resultado atingido (e.g. trabalhador subordinado com pagamentos à comissão).³⁴

2. O direito à proteção de dados

2.1. Contexto histórico

O direito à proteção de dados enquanto direito fundamental foi sendo moldado pela evolução das relações sociais e económicas.

Apesar de não ser um fenómeno recente, a necessidade de regulamentação da matéria referente à proteção de dados ganhou maior visibilidade com os avanços tecnológicos e em particular com a substituição do tratamento dos dados manualmente pelo tratamento informatizado.

³³ MARIA DO ROSÁRIO PALMA RAMALHO, *Tratado de Direito do Trabalho, Parte II... Ob. cit.*, p. 32.

³⁴ MARIA DO ROSÁRIO PALMA RAMALHO, *Tratado de Direito do Trabalho, Parte II... Ob. cit.*, p. 31 e 32.

Ainda assim, podemos hoje dizer, tendo por base uma perspectiva histórica, que o Direito da Proteção de Dados teve as suas origens no Direito Público, uma vez que o primeiro grande diploma a regular esta matéria (o HDSG) apenas versava entidades públicas como destinatárias. Esta tendência foi, contudo, rapidamente quebrada: o primeiro diploma estado-unidense (o *Fair Credit Reporting Act*) apenas englobava entidades privadas e o primeiro diploma europeu (o sueco *Datalag*) e alemão (o BGSF) abrangiam entidades públicas e privadas.³⁵

Façamos uma breve análise histórica dos acontecimentos que criaram uma consciencialização em matéria de proteção de dados.

2.1.1. Estados Unidos da América: o *Special Subcommittee on Invasion of Privacy*

Como é frequente na história, os primeiros passos no sentido de uma regulamentação de dados aconteceram nos Estados Unidos da América, em 1965, com a constituição do *Special Subcommittee on Invasion of Privacy*.³⁶

Como o próprio nome indica, este *Special Subcommittee* tratava de questões relacionadas com invasão de privacidade e, conseqüentemente, com proteção de dados. Ali foram debatidas três questões fundamentais: (i) a violação, pelas agências federais, da privacidade dos cidadãos, (ii) a constituição de uma base de dados centralizada pelo Estado e (iii) a proteção dos dados pessoais dos investidores no âmbito das agências de crédito.³⁷

A violação do direito de privacidade por parte das agências federais conduziu à tomada de medidas fundamentadas na necessidade de limitar e fiscalizar a intervenção do Estado em matérias do domínio da vida privada dos cidadãos.

Em 1966 foram desenvolvidas novas reuniões no sentido de se criar um *National Data Center* ou *National Data Bank* cujo principal objetivo focava-se na centralização da informação recolhida pelas várias agências federais dos Estados Unidos.

³⁵ A. BARRETO MENEZES CORDEIRO, *Direito da Proteção de Dados à Luz do RGPD e da Lei n.º 58/2019*, Almedina, 2022, p. 39.

³⁶ Para uma análise mais profunda, confirmar VERN COUNTRYMAN, *The Diminishing Right of Privacy: The personal Dossier and the Computer*, In *Law in Contemporary Society, The Orgain Lectures*, The University of Texas Press, Austin and London, p. 61 a 95.

³⁷ A. BARRETO MENEZES CORDEIRO, *Direito da Proteção de Dados... Ob. cit.*, p. 54.

Posteriormente, em 1968, o foco do *Special Subcommittee* direcionou-se para as agências de crédito (*Commercial Credit Bureaus*). À data, estas entidades recolhiam grandes quantidades de dados sobre clientes e potenciais clientes através de informação pública (e.g. notícias de jornais e jurisprudência), acedendo a contratos de mútuo celebrados e, em casos extremos, contratando investigadores privados para recolherem todas as informações relevantes de cada cliente e potencial cliente.³⁸

Este escrutínio era desenvolvido sobretudo por entidades empregadoras, agência de crédito e senhorios que pretendiam obter mais informação sobre os seus potenciais candidatos (a emprego, a contratos de seguro e a contratos de arrendamento, respetivamente).³⁹

Recolhida a informação, eram elaborados relatórios individuais (os chamados *Credit Reporting Bureaus*) que continham, frequentemente, informação “*incorreta, irrelevante, viciada, pessoal e secreta, [que] fugiam totalmente ao controlo do visado*”⁴⁰ e que tinham um enorme pendor no sucesso ou insucesso da contratação.⁴¹

É nesta sequência de acontecimento que, em 1968, é desenvolvido o primeiro projeto-lei denominado *Fair Credit Reporting Bill*, que seria promulgado em 1970 com a designação de *Fair Credit Reporting Act*.

Deste modo, e como referido no § 602 (4) do *Fair Credit Reporting Act*, o seu objetivo primordial assentava em assegurar que as “*agências de informação ao consumidor exerc[essem] as suas grandes responsabilidades com justiça, imparcialidade e respeito pelos direitos e pela privacidade do consumidor*”.⁴²

Mais tarde, em 1974, foi aprovado o *Privacy Act 1974* que viria a regular a matéria referente à recolha, conservação, utilização e disseminação de informação pelas agências federais e teria um papel fundamental no Direito da Proteção de Dados.⁴³

³⁸ A este propósito, confirmar RICHARD H. GOLDSTEIN/ MARK S BRODIE, *Commercial Credit Bureaus: The Rights to Privacy and State Actions*, 24 AM. U. L. REV. 421, 1975.

³⁹ LENORE COOPER GARON, *Protecting Privacy in Credit Reporting*, Journal Article, Stanford Law Review, Vol. 24, no. 3 (Feb. 1972), p. 553.

⁴⁰ A. BARRETO MENEZES CORDEIRO, *Direito da Proteção de Dados... Ob. cit.*, p. 56.

⁴¹ Para melhor exposição sobre os procedimentos de investigação, confirmar. LENORE COOPER GARON, *Protecting... Ob. cit.*, p. 553.

⁴² “*Consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and respect for the consumer’s rights and privacy*”, Fair Credit Reporting Act, 1970.

⁴³ A. BARRETO MENEZES CORDEIRO, *Direito da Proteção de Dados... Ob. cit.*, p. 59.

Este diploma tinha duas finalidades: (i) preservar o interesse individual dos cidadãos e (ii) reconhecer a importância do acesso à informação pelos governantes.⁴⁴

A partir deste momento a prossecução da salvaguarda dos direitos dos titulares dos dados começa a assumir um papel primordial no âmbito legislativo. Prova disso foi o primeiro relatório sobre essa matéria, publicado pelo *Secretary's Advisory Committee on Automated Personal Data Systems*, em 1993, cujo título era *Records, Computers and Rights of Citizens*⁴⁵ e que defendia que:

Não dev[iam] haver sistemas de manutenção de registos de dados pessoais cuja própria existência seja secreta.

Dev[ia] haver forma de o indivíduo saber que informação sobre ele consta de um registo e como é utilizada.

Dev[ia] haver forma de o indivíduo impedir que a informação sobre ele obtida para um determinado fim seja utilizada ou disponibilizada para outros fins sem o seu consentimento.

Dev[ia] haver forma de o indivíduo corrigir ou alterar um registo de informação identificáveis sobre ele.

Qualquer organização que crie, administre, utilize ou divulgue registos de dados pessoais identificáveis deve assegurar a fiabilidade dos dados para a utilização pretendida e deve tomar precauções para evitar o uso indevido dos dados.

(tradução nossa)

⁴⁴ JAMES BEVERAGE, *The Privacy Act of 1974: An Overview*, Duke Law Journal, Vol. 1976, No. 2 Seventh Annual Administrative Law Issue (May 1976), p. 301 a 329.

⁴⁵ *Records, Computers and the Rights of Citizens*, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Department of Health, Education & Welfare, July 1973, DHEW Publication NO. (OS) 73-94, p. 10 e 11: "There must be no personal data record-keeping systems whose very existence is secret. There must be a way for an individual to find out what information about him is in a record and how it is used. There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent. There must be a way for an individual to correct or amend a record of identifiable information about him. Summary and Recommendations Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data".

2.1.2. Europa

Apesar da grande – e constante – influência americana, a primeira lei referente a matérias de proteção de dados foi desenvolvida na Alemanha, em 1970, pelo Parlamento do Estado de Hesse: o *Hessisches Datenschutzgesetz* (HDSG).⁴⁶

Este diploma estava cingido aos dados recolhidos e tratados por entidades pública e não continha qualquer limitação ou contextualização sobre o tratamento, ainda que lícito, dos dados pessoais, bastando-se pelo reconhecimento aos titulares dos dados direitos secundários (e.g., direito a corrigir os dados).⁴⁷

O HDSG ficou, ainda, marcado pela referência à figura do “Supervisor de Dados Pessoais”, correspondente ao atual Encarregado de Proteção de Dados.

Se é verdade que o HDSG se cingia ao Estado de Hesse, a sua influência foi de tal modo que nas décadas posteriores começaram a ser elaborados diplomas similares nos restantes Estados alemães.

Foi então que, em novembro de 1973, foi apresentado o primeiro projeto de lei de proteção de dados a nível nacional, que se viria a consolidar três anos depois, em 1977 – o BDSG, a Lei Federal de Proteção de Dados Alemã.

Ainda que a predominância alemã no campo jurídico seja bastante forte, o primeiro diploma nacional aplicável a entidades públicas e privadas surgiu na Suécia, em 1973 – o *Datalag*. Isto deveu-se a dois fatores: (i) desde a década de 60 que a administração pública suíça vinha a promover a digitalização no processamento de informações dos cidadãos e (ii) entre 1968 e 1970 iniciou-se um debate público sobre informática e política e os seus benefícios.⁴⁸

Assim, e citando MENEZES CORDEIRO,⁴⁹

⁴⁶ Para melhor entendimento desta temática, confirmar COLIN J. BENNETT, *Regulating Privacy: Data Protection and Public Policy in the Europe and the United States*, Cornell University Press, Ithaca, 1992, p. 74 e seguintes.

⁴⁷ A. BARRETO MENEZES CORDEIRO, *Direito da Proteção de Dados... Ob. cit.*, p. 64.

⁴⁸ PER LUNDIN, *Computers and Welfare: The Swedish Debate on the Politics of Computerization in the 1970s and the 1980s. 4th History of Nordic Computing (HiNC4)*, Aug 2014, Copenhagen, Denmark, 10.1007/978-3-319-17145-6_1. hal-01301200, p. 3 a 11.

⁴⁹ A. BARRETO MENEZES CORDEIRO, *Direito da Proteção de Dados... Ob. cit.*, p. 66.

A prática de legislar sobre a proteção de dados de forma integrada, i.e., com um diploma nuclear complementado por legislação sectorial, iniciada pela Suécia e pela Alemanha, mantém-se, várias décadas volvidas, como um elemento central da conceção europeia. Esta visão, hoje claramente maioritária, contrasta com o modelo tradicional estado-unidense, historicamente avesso a este enquadramento geral.

2.2. A proteção constitucional

Apesar das novidades chegarem mais tarde a Portugal – como já é tradição –, a verdade é que, no que à proteção de dados diz respeito, Portugal foi o primeiro país a consagrar constitucionalmente alguma proteção aos titulares dos dados pessoais.

Na versão originária do artigo 35.º da CRP era possível ler:⁵⁰

- 1. Todos os cidadãos têm o direito de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a retificação dos dados e a sua atualização.*
- 2. A informática não pode ser usada para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se trate do processamento de dados não identificáveis para fins estatísticos.*
- 3. É proibida a atribuição de um número nacional único aos cidadãos.*

Posteriormente, com a revisão constitucional de 1982 o texto legal ficou nos seguintes termos:⁵¹

- 1. Todos os cidadãos têm o direito de tomar conhecimento do que constar de registos informáticos a seu respeito e do fim a que se destinam as informações, podendo exigir a retificação dos dados e a sua atualização.*
- 2. São proibidos o acesso de terceiros a ficheiros com dados pessoais e a respetiva interconexão, bem como os fluxos de dados transfronteiras, salvo em casos excecionais, salvo em casos excecionais previstos na lei.*

⁵⁰ JORGE MIRANDA, RUI MEDEIROS, *Constituição Portuguesa Anotada*, Tomo I, Introdução Geral, Preâmbulo, Artigos 1.º a 79.º, Coimbra Editora, 2005, p. 372 e seguintes.

⁵¹ LC n.º 1/82 (que aditou o n.º 2 e 4 e alterou os n.ºs 1 e 3).

3. *A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa ou vida privada, salvo quando se trate do processamento de dados estatísticos não individualmente identificáveis.*
4. *A lei define o conceito de dados pessoais para efeitos de registo informático.*
5. *É proibida a atribuição de um número nacional único aos cidadãos.*

Mais tarde, em 1989, o artigo sofre novas alterações:⁵²

1. *Todos os cidadãos têm o direito de tomar conhecimento dos dados constantes de ficheiros ou registos informáticos a seu respeito e do fim a que se destinam, podendo exigir a sua retificação e atualização, sem prejuízo do disposto na lei sobre segredo de Estado e segredo de justiça.*
2. *É proibido o acesso a ficheiros e registos informáticos para conhecimento de dados pessoais relativos a terceiros e respetiva interconexão, salvo em casos excecionais previstos na lei.*
3. *A informática não pode ser utilizada para o tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa ou vida privada, salvo quando se trate do processamento de dados estatísticos não individualmente identificáveis.*
4. *A lei define o conceito de dados pessoais para efeitos de registo informático, bem como de bases e bancos de dados e respetivas condições de acesso, constituição e utilização por entidades públicas e privadas.*
5. *É proibida a atribuição de um número nacional único aos cidadãos.*
6. *A lei define o regime aplicável aos fluxos de dados transfronteiras, estabelecendo formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.*

A última alteração ao artigo 35.º ocorreu em 1997, fortemente influenciada pelo conteúdo da Diretriz n.º 95/46, transposta pela Lei n.º 67/98, de 26 de outubro, e criou a atual versão deste preceito legal:⁵³

⁵² LC n.º 1/89 (que alterou a redação dos n.ºs 1, 2 e 4 e aditou o n.º 6).

⁵³ LC n.º 1/97 (que alterou os n.ºs 1, 2, 3, 4 e 6 e aditou o n.º 7).

1. *Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.*
2. *A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente.*
3. *A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.*
4. *É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei.*
5. *É proibida a atribuição de um número nacional único aos cidadãos*⁵⁴.
6. *A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.*
7. *Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei.*

É através deste artigo que ficam salvaguardados um conjunto de direitos fundamentais contra um qualquer tratamento informático de dados pessoais, nomeadamente: (i) o direito de acesso e informação do cidadão aos registos informáticos para conhecimento dos seus dados pessoais, com a possibilidade de atualização e retificação dos mesmos (n.º 1 e 6); (ii) o direito ao sigilo em relação aos responsáveis de ficheiros automatizados e a terceiros dos dados

⁵⁴ “Não podíamos terminar esta anotação ao artigo 35.º, sem referir a proibição da concessão aos cidadãos de um número nacional único capaz de concentrar toda a informação relativa a uma só pessoa, e que chegou a estar previsto na Lei n.º 2/73, regulada pelo Decreto-Lei n.º 555/73, de 26 de Outubro (...). Não parece, todavia, injustificado o receio de que, através da junção de toda a informação disponível em bancos de dados, designadamente os que pertencem aos vários serviços do Estado (...) se chegue exatactamente ao mesmo efeito que se pretendeu evitar, tornando-se possível compor, através de dados e elementos diversificados, uma imagem completa da pessoa.”. JORGE MIRANDA, RUI MEDEIROS, *Constituição Portuguesa Anotada... Ob. cit.*, p. 389.

personais informatizados e direito à sua não interconexão (n.º 4); e (iii) o direito ao não tratamento informático de certos tipos de dados pessoais (n.º 3).

Em suma, e apesar da epígrafe deste artigo ter permanecido intocável, as fortes alterações implementadas pelas várias revisões tiveram grandes impactos: por um lado, promoveram uma maior proteção aos titulares dos dados, por outro forneceram uma grande ajuda na sedimentação das bases fundamentais do Direito da Proteção de Dados, mais tarde consagrado pelo RGPD.⁵⁵

2.3. Regulamento Geral de Proteção de Dados

Como temos vindo a expor, o foco na proteção de dados remota à década de 90. Não obstante, os primeiros passos em direção à criação do RGPD aconteceram por intermédio do Programa de Estocolmo no qual o Conselho reforçou a importância de se criarem mecanismos eficazes para a proteção da privacidade dos cidadãos europeus, apoiado num investimento na regulação do tratamento e transferência de dados pessoais.⁵⁶

Dois anos volvidos, em 25 de janeiro de 2012, foi apresentado pela Comissão uma Proposta de Regulamento sobre a Proteção de Dados.

Até à versão final do Regulamento, que ocorreu em 2016, foram realizadas inúmeras alterações, de forma a criar um diploma coeso e unânime para todos os visados.

As duas principais diferenças entre as duas versões do Regulamento foram: (i) a (quase) extinção das competências atribuídas à Comissão aquando da Proposta e (ii) a criação de várias cláusulas de abertura em benefício de Estados-Membros e da própria União – o que não estava previsto na versão da Proposta de Regulamento.⁵⁷

Finalmente, em 25 de maio de 2018 a aplicação do Regulamento Geral de Proteção de Dados tornou-se efetiva.

⁵⁵ A. BARRETO MENEZES CORDEIRO, *Direito da Proteção de Dados... Ob. cit.*, p. 76.

⁵⁶ *Programa de Estocolmo – Uma Europa aberta e segura que sirva e proteja os cidadãos*, Conselho Europeu, (2010/C 115/01).

⁵⁷ A. BARRETO MENEZES CORDEIRO, *Direito da Proteção de Dados... Ob. cit.*, p. 83.

2.3.1. Âmbito de aplicação

No que ao âmbito de aplicação do RGPD diz respeito podemos fazer um desdobramento em duas fações: (i) o âmbito material e (ii) o âmbito territorial.

Iniciando esta abordagem pelo âmbito material, nos termos do artigo 2.º, n.º 1 do diploma, o Regulamento aplica-se ao tratamento de dados (i) por meios totalmente automatizados; (ii) por meios parcialmente automatizados e (iii) por meios não automatizados desde que contidos em ficheiros ou a eles destinados.

Ao contrário do que se poderia esperar, o legislador não densificou o conceito de “meios automatizados”, deixando esta denominação em aberto. Segundo MENEZES CORDEIRO^{58/59}

Não se trata de uma lacuna, mas de uma posição premeditada: pretendeu evitar-se que o RGPD fosse, com fundamento no eventual conteúdo positivado, contornado ou que se tornasse, a breve trecho, obsoleto.

Em termos práticos, o tratamento por meios automatizados traduz-se no tratamento de quaisquer dados pessoais por meios como computadores, dispositivos móveis, etc., ou seja, uma acessão ampla de equipamentos de processamento de dados.^{60/61}

Nesta senda, o tratamento de dados por meios não automatizados traduzir-se-á no tratamento de dados manuais – armazenamento físico, em papel, etc. Não obstante, o RGPD não se aplica a todos os tratamentos não automatizados, mas só aos ficheiros⁶², conjunto de ficheiros ou capas que estejam devidamente estruturados, de acordo com critérios específicos.⁶³

⁵⁸ A. BARRETO MENEZES CORDEIRO, *Direito da Proteção de Dados... Ob. cit.*, p. 85.

⁵⁹ Sobre esta questão, veja-se o Considerando 15 do RGPD referente o princípio da neutralidade tecnológica): “A fim de evitar o sério risco sério de ser contornada a proteção das pessoas singulares, esta deverá ser neutra em termos tecnológicos e deverá ser independente das técnicas utilizadas”.

⁶⁰ A. BARRETO MENEZES CORDEIRO, *Direito da Proteção de Dados... Ob. cit.*, p. 85.

⁶¹ *Manual da Legislação Europeia sobre Proteção de Dados*, Edição de 2018, Agência dos Direitos Fundamentais da União Europeia e Conselho da Europa, 2022, p. 115.

⁶² Por ficheiros entende-se, nos termos do artigo 4.º, 6) do RGPD “qualquer conjunto estruturado de dados pessoais, acessíveis segundo critérios específicos, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico”.

⁶³ Considerando 15 do RGPD: “A proteção das pessoas singulares deverá aplicar-se ao tratamento de dados pessoais por meios automatizados, bem como ao tratamento manual, se os dados pessoais estiverem contidos ou se forem destinados a um sistema de ficheiros. Os ficheiros ou os conjuntos de ficheiros bem como as suas capas, que não estejam estruturados de acordo com critérios específicos, não deverão ser abrangidos no âmbito do presente regulamento”.

Apesar de preenchidos os requisitos supra indicados, o RGPD não se aplica, nos termos do artigo 2.º, n.º 2 do RGPD, a tratamentos: (i) efetuados no exercício de atividades não sujeitas à aplicação do direito da União; (ii) efetuados pelos Estados-Membros no exercício de atividades abrangidas pelo âmbito de aplicação do título V, capítulo 2, do TUE; (iii) efetuados por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas e (iv) efetuados pelas autoridades competentes para efeitos de prevenção, investigação, detenção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e prevenção de ameaças à segurança pública.

No que concerne ao âmbito territorial, o RGPD “*aplica-se ao tratamento de dados pessoais efetuados no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União*” – artigo 3.º, n.º 1 do RGPD.

Nestes termos, o titular dos dados objeto de tratamento não tem de ser cidadão europeu, nem tem de se encontrar no território europeu quando o tratamento ocorre.⁶⁴

2.3.2. Noção de “dados pessoais”

A definição de dados pessoais encontra-se no artigo 4.º, 1) do RGPD, traduzindo-se na “*informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»)*”.

No sentido de facilitar a análise deste conceito façamos uma subdivisão dos diferentes elementos aí previstos: (i) qualquer informação; (ii) relativa a; (iii) pessoa singular; (iv) identificada ou identificável.

⁶⁴ Neste seguimento, confirmar Considerando 2: “*Os princípios e regras em matéria de proteção das pessoas singulares relativamente ao tratamento de dados pessoais deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente o direito à proteção dos dados pessoais(...)*” e Considerando 14: “*A proteção conferida pelo presente regulamento deverá aplicar-se às pessoas singulares, independentemente da sua nacionalidade ou do seu local de residência, relativamente ao tratamento dos seus dados(...)*”.

2.3.2.1. Qualquer informação

O primeiro elemento da noção de dado pessoal é a existência de uma informação.

Da análise do preceito legal não é possível determinar quais as informações que se encontram aqui englobadas, pelo que se deve entender que a intenção do legislador mais não foi do que englobar toda e qualquer informação, permitindo, desta forma, interpretações amplas.

Assim, devemos entender que informação pessoal engloba toda e qualquer informação, desde dados sobre a vida pessoal ou profissional⁶⁵, objetivos ou subjetivos, independentemente da sua veracidade.^{66/67}

De referir, ainda, que o Regulamento aplica-se a qualquer informação, independentemente do formato segundo a qual foi recolhida ou armazenada (e.g., fotográfico, numérico, alfabético, vídeo⁶⁸, registos de tempos de trabalho⁶⁹, etc.).⁷⁰

2.3.2.2. Relativa a

O Regulamento aplica-se aos dados pessoais referentes a uma pessoa. Este elemento é fundamental na delimitação do campo de aplicação do RGPD que vem, desta forma, excluir da sua abrangência todas as realidades jurídicas não subjetiváveis.

Não obstante, nem sempre é fácil assinalar quais as informações relevantes para a aplicação do Regulamento. Se é verdade que em determinadas situações é fácil identificar se estamos

⁶⁵ Veja-se, a título de exemplo, o Acórdão do TJUE, no processo C-615/13 P, de 16 de julho de 2015, no qual se afirmar que *“o facto de essa informação se inscrever no contexto de uma atividade profissional não lhe pode retirar a qualificação de conjunto de dados pessoais”*.

⁶⁶ GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2007 sobre o conceito de dados pessoais*, WP 136, Adotado em 20 de junho, p. 6 e 7.

⁶⁷ Confirmar ponto 2.5.3. sobre retificação de dados pessoais.

⁶⁸ Confirmar Acórdão TJUE, Processo C-212/13, de 11 de dezembro de 2014: *“(…) da Diretiva 95/46 deve ser interpretado no sentido de que a exploração de um sistema de câmara que dá lugar a uma gravação de vídeo de pessoas, guardada num dispositivo de gravação contínua, como um disco rígido, sistema esse instalado por uma pessoa singular na sua casa de família, para proteger os bens, a saúde e a vida dos proprietários dessa casa, e que vigia igualmente o espaço público, não constitui tratamento de dados efetuados no exercício de atividades exclusivamente pessoais ou domésticas, na ascensão desta disposição”*.

⁶⁹ Confirmar Acórdão TJUE, Processo C-342/12, de 30 de maio de 2013: *“A recolha, o registo, a organização, a conservação, a consulta e a utilização desses dados por um empregador assim como a sua transmissão por este às autoridades nacionais com competência para a fiscalização das condições de trabalho são, portanto, características de um «tratamento de dados pessoais», na aceção do artigo 2.º, alínea b), da Diretiva 95/46(…)”*.

⁷⁰ GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2007... Ob. cit.*, p. 8.

perante dados pessoais ao abrigo deste diploma (e.g., imagens de vídeo, resultados médicos, etc.), existem outras que se mostram ambíguas (e.g., registo de oficina de um carro, onde a oficina estabelece uma ligação entre o veículo e o proprietário para fins de faturação – é um dado relativo ao proprietário ou ao veículo?). No sentido de facilitar esta seleção, veja-se o referido por MENEZES CORDEIRO⁷¹

A informação relativa a objetos, quando conjugada com informação respeitante a pessoas, passa a ser tratada como um dado pessoal, independentemente de essa informação ser presente ou passada – p.ex: (i) foi feita uma chamada do telemóvel; e (ii) o telemóvel X pertence a A. A ligação de (i) a (ii) converte (i) num dado pessoal.

No que concerne aos dados factuais, também estes podem ser considerados dados pessoais sempre que a informação recolhida permita identificar um determinado sujeito.⁷²

Esta expressão – “relativa a” – pode ainda ser subdividida em três elementos: (i) conteúdo; (ii) finalidade e (iii) resultado.⁷³

O primeiro elemento corresponde a toda a informação *sobre* a própria pessoa que é objeto de análise (e.g., análises clínicas dizem respeito ao doente, a avaliação de desempenho diz respeito ao trabalhador, etc.).

No que diz respeito ao elemento finalidade, este existe sempre que os dados utilizados permitam “*avaliar, tratar de determinada forma ou influenciar o estatuto ou o comportamento de uma pessoa*”⁷⁴ (e.g., registo de chamadas telefónicas, avaliação de tempos de trabalho, etc.).

O terceiro e último elemento – o resultado – “*estende-se a toda a informação que não incida sobre uma pessoa (conteúdo) e que não vise avaliá-la ou influenciá-la (finalidade), mas que, em abstrato, o permita fazer*”⁷⁵ (e.g., controlo do posicionamento dos táxis para otimizar o serviço, com impacto nos motoristas⁷⁶).

⁷¹ A. BARRETO MENEZES CORDEIRO, *Direito da Proteção de Dados... Ob. cit.*, p. 110.

⁷² GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2007... Ob. cit.*, p. 8.

⁷³ GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2007... Ob. cit.*, p. 10 e ss.

⁷⁴ GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2007... Ob. cit.*, p. 11.

⁷⁵ A. BARRETO MENEZES CORDEIRO, *Direito da Proteção de Dados... Ob. cit.*, p. 112.

⁷⁶ Exemplo apresentado no *Parecer 4/2007...*, p. 11 e 12.

Estes três elementos, ao contrário do que pode parecer, devem ser considerados como condições alternativas e não cumulativas, pelo que estando preenchido um dos elementos não existe a necessidade da verificação dos restantes. Consequência de tal é o facto de a mesma informação poder ser, simultaneamente, relativa a várias pessoas, tendo em consideração qual dos elementos é que está presente para cada uma delas.⁷⁷

2.3.2.3. Pessoa singular

Nos termos do artigo 1.º, n.º 1 do RGPD o diploma é aplicável às pessoas singulares, pelo que as pessoas coletivas, coisas⁷⁸ ou animais se encontram, necessariamente, excluídos da aplicação do mesmo.

No que às pessoas coletivas diz respeito, o Considerando 14 afirma que *“o presente regulamento não abrange o tratamento de dados pessoais relativos a pessoas coletivas, em especial a empresas estabelecidas enquanto pessoas coletivas, incluindo a denominação, a forma jurídica e os contactos da pessoa coletiva”*. Assim, os dados das pessoas coletivas relevantes para o Regulamento são apenas aqueles que digam respeito – direta ou indiretamente – a pessoas singulares.⁷⁹

Não obstante, o TJUE já se demarcou no sentido de deixar claro que nada impede que os Estados-Membros alarguem o âmbito de aplicação da legislação nacional às pessoas coletivas, desde que em conformidade com o direito comunitário.⁸⁰

⁷⁷ GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2007...*, *Ob. cit.*, p. 12.

⁷⁸ Como referido no ponto 2.3.2.2., nem sempre é fácil proceder à identificação do que são dados pessoais ou sobre objetos. A esse título, confirmar *What is personal data? Key definitions*, The General Data Protection Regulation, Information Commissioner's Office, 17 October 2022 – 1.0.11, p. 23 e 24.

⁷⁹ Confirmar acórdão TJUE, Processo C-92/09 e C-93/09, de 9 novembro de 2010: *“as pessoas colectivas só podem invocar a protecção dos artigos 7.º e 8.º da Carta a respeito de tal identificação desde que a denominação legal da pessoa colectiva identifique uma ou mais pessoas singulares. É o que se passa com a recorrente na causa principal no processo C-92/09. Com efeito, a denominação legal da sociedade identifica directamente pessoas singulares, que são sócios dessa sociedade”*.

⁸⁰ Neste sentido, confirmar acórdão TJUE, Processo C-101/01, de 6 de novembro de 2003: *“Em contrapartida, nada se opõe a que um Estado-Membro alargue o alcance da legislação nacional que procede à transposição da Diretiva 95/46 a domínios não incluídos no seu campo de aplicação, desde que nenhuma outra disposição do direito comunitário a tal obste”*.

2.3.2.4. Identificada ou identificável

Por fim, no que diz respeito ao último fator, e como referido no Parecer 4/2007 sobre o conceito de dados pessoais,

*uma pessoa singular pode ser considerada “identificada” quando, de entre um grupo de pessoas, ele ou ela é “distinguido” de todos os outros membros do grupo. Da mesma forma, uma pessoa singular é “identificável” quando, apesar da pessoa ainda não ter sido identificada, é possível fazê-lo...*⁸¹

Além disso, uma pessoa pode ser identificada direta (e.g., nome) ou indiretamente (e.g., número de cartão de cidadão, contacto telefónico, etc.), pelo que os termos da sua identificação vão sempre depender de cada situação em concreto.⁸² Assim, e como estabelecido no Considerando 26 do Regulamento,

para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular.^{83/84}

2.3.3. O Encarregado de Proteção de Dados

O Encarregado de Proteção de Dados (EPD) é a pessoa que presta “aconselhamento sobre o cumprimento das regras sobre proteção de dados em organizações que efetuam tratamento de dados”.⁸⁵

Segundo o n.º 5 do artigo 37.º do RGPD,

O encarregado da proteção de dados é designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do

⁸¹ GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2007... Ob. cit.*, p. 12.

⁸² Para uma análise mais profunda sobre esta questão, confirmar GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2007... Ob. cit.*, p. 13.

⁸³ Confirmar, ainda, o Considerando 30.

⁸⁴ Para uma análise mais profunda sobre esta questão, confirmar A. BARRETO MENEZES CORDEIRO, *Direito da Proteção de Dados... Ob. cit.*, p. 120 a 129.

⁸⁵ *Manual da Legislação Europeia sobre Proteção de Dados*, Edição de 2018, Agência dos Direitos Fundamentais da União Europeia e Conselho da Europa, 2022, p. 197.

direito e das práticas de proteção de dados, bem como na sua capacidade para desempenhar as funções referidas no artigo 39.º.

Este preceito é completado com o Considerando 97 que refere que o EPD é

(...) um especialista em legislação e prática de proteção de dados no controlo do cumprimento do presente regulamento a nível interno (...) [sendo que] O nível necessário de conhecimentos especializados deve ser determinado, em particular, em função do tratamento de dados realizado e da proteção exigida para os dados pessoais tratados pelo responsável pelo seu tratamento ou pelo subcontratante. Estes encarregados da proteção de dados, sejam ou não empregados do responsável pelo tratamento, deverão estar em condições de desempenhar as suas funções e atribuições com independência.

Ora, além de ter amplos conhecimentos jurídicos e informáticos, o EPD também deve ter conhecimento relativo ao setor em que irá atuar, desenvolvendo a sua atividade de forma independente.^{86/87}

A designação de um EPD é obrigatória, nos termos do artigo 37.º, n.º 1 do RGPD, quando:

- a. O tratamento for efetuado por uma autoridade ou um organismo público, excetuando os tribunais no exercício da sua função jurisdicional;*
- b. As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou*
- c. As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados nos termos do n.º 9 ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.º.*

⁸⁶ A. BARRETO MENEZES CORDEIRO, *Direito da Proteção de Dados... Ob. cit.*, p. 367 a 370.

⁸⁷ Nos termos do n.º 3 do artigo 38.º do RGPD, o EPD não pode ser destituído ou penalizado pelo facto de exercer as suas funções. Esta norma é uma clara transposição da intenção do legislador em salvaguardar a independência do EPD.

Além das situações elencadas no n.º 1, o responsável pelo tratamento ou o subcontratante devem, sempre que o direito da União ou os Estados-Membros assim o exigirem, designar um EPD – n.º 4 do artigo 37.º do RGPD.

Apesar da obrigatoriedade imposta pelo n.º 1 do artigo 37.º do RGPD nada impede que uma determinada entidade designe livremente um EPD, aplicando-se, nessas situações o estipulado entre os artigos 37.º a 39.º do RGPD.⁸⁸

Por fim, e no que às funções diz respeito, o artigo 39.º, n.º 5 do RGPD vem elencar as cinco principais tarefas do EPD:

- i. Informar e aconselhar o responsável pelo tratamento ou subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações segundo o RGPD e da demais legislação em matéria de proteção de dados;
- ii. Controlar o cumprimento do RGPD, da demais legislação em matéria de proteção de dados e das políticas das entidades designadoras relativas à proteção de dados pessoais, incluir a repartição de responsabilidades, a sensibilização e a formação do pessoal implicado nas operações de tratamentos de dados, e as auditorias independentes;⁸⁹
- iii. Prestar aconselhamento, quando lhe seja solicitado, relativo à avaliação do impacto sobre a proteção de dados e controlar a sua realização, nos termos do artigo 35.º do RGPD;
- iv. Cooperar com a autoridade de controlo;
- v. Atuar como ponto de contacto com a autoridade de controlo sobre questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo

⁸⁸ A este propósito, confirmar GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Orientações sobre os encarregados da proteção de dados (EPD)*, WP 243 rev.01, Adotadas em 13 de dezembro de 2016, Com a última redação revista e adotada em 5 de abril de 2017, p. 7: “Nada impede uma organização, que não seja obrigada por lei a designar um EPD e não pretenda designar um EPD a título voluntário, de recorrer, apesar disso, a pessoal ou consultores externos com funções ligadas à proteção dos dados pessoais. Neste caso, é importante assegurar que não há confusão quanto ao seu cargo, estatuto, posição e atribuições. Por conseguinte, deve ficar claro, em todas as comunicações no seio da empresa e com as autoridades de proteção de dados, os titulares de dados e o público em geral, que o cargo deste funcionário ou consultor não corresponde à função de encarregado de proteção de dados (EPD)”.

⁸⁹ A propósito da realização de auditorias veja-se GEMMA GALDON CLAVELL, *AI Auditing: Checklist for AI Auditing*, Support Pool of Experts Programme, European Data Protection Board, 2023; GEMMA GALDON CLAVELL, *AI Auditing: Proposal for Algo-scores*, Support Pool of Experts Programme, European Data Protection Board, 2023 e GEMMA GALDON CLAVELL, *AI Auditing: Proposal for AI leaflets*, Support Pool of Experts Programme, European Data Protection Board, 2023.

36.º do RGPD, e consulta, sempre que necessário, a autoridade de controlo sempre que necessário.

2.3.4. Comissão Nacional de Proteção de Dados

Ao abrigo do artigo 2.º da Lei 43/2004, de 18 de agosto, sobre a organização e funcionamento da Comissão Nacional de Proteção de Dados (CNPd),

A CNPD⁹⁰ é uma entidade administrativa independente⁹¹, com personalidade jurídica de direito público e poderes de autoridade, dotada de autonomia administrativa e financeira, que funciona junto da Assembleia da República.^{92/93}

Composta por sete membros (artigo 3.º da Lei Orgânica da CNPD) a Comissão funciona nos termos dos artigos 13.º e seguintes do mesmo diploma.

A reunião e deliberação por parte da Comissão está dependente da presença de, pelo menos, quatro dos seus membros, sendo as deliberações tomadas por maioria dos membros presentes, tendo o presidente voto de qualidade – artigo 15.º da Lei Orgânica da CNPD.

São da competência da CNPD: (i) representar a Comissão; (ii) superintender os serviços de apoio; (iii) convocar sessões e fixar a ordem de trabalhos; (iv) ouvida a Comissão, nomear o pessoal do mapa e autorizar transferências, requisições e destacamentos, bem como (v) autorizar a contratação do pessoal referido no artigo 30.º, n.º 5; (vi) outorgar contratos em nome da Comissão e obrigá-la nos demais negócios jurídicos; (vii) autorizar a realização de despesas dentro dos limites legalmente compreendidos nas competências dos ministros; (viii) aplicar coimas e homologar deliberações; (ix) fixar as regras de distribuição dos processos, ouvida a Comissão; (x) submeter à aprovação da Comissão o plano de atividades e (xi) assegurar o cumprimento das leis e a regularidade das deliberações – artigo 19.º, n.º 1 da Lei Orgânica da CNPD.

⁹⁰ Confirmar artigos 3.º e seguintes da LE.

⁹¹ Apesar de a CNPD ser uma entidade administrativa independente, não lhe é aplicável a Lei-Quadro das entidades administrativas independentes com funções de regulação da atividade económica dos setores privado, público e cooperativo – Lei n.º 67/2013, de 28 de agosto.

⁹² Confirmar artigo 20.º, n.º 2 da Lei 43/2004, de 18 de agosto e artigo 219.º, n.º 1 da CRP.

⁹³ Confirmar artigo 4.º, n.º 1 da LE.

Tal como o EPD, a CNPD tem de agir sempre com total independência⁹⁴ e imparcialidade⁹⁵, nos termos do artigo 52.º, n.º 1 e 3 do RGPD⁹⁶, respetivamente.

2.4. Princípios gerais no âmbito da proteção de dados

No sentido de orientar e facilitar a interpretação da legislação de proteção de dados, foram criados um conjunto de cânones fundamentais: os princípios gerais da proteção de dados. É através de uma leitura conjunta dos preceitos legais com os princípios gerais que conseguimos uma aplicação equilibrada do Direito a cada caso. Vejamos:

2.4.1. Princípio da livre circulação

O objetivo primordial da criação de um diploma que regulasse a proteção dos dados pessoais dos cidadãos europeus assentou, por um lado, na salvaguarda dos interesses individuais dos proprietários dos dados e, por outro, na agilização da circulação dos mesmos dentro da União Europeia.

Neste sentido, parece-nos, desde logo, lógica a abertura do respetivo diploma assente num princípio de livre circulação de dados – artigo 1.º do RGPD.

⁹⁴ Neste sentido, confirmar Acórdão TJUE, Processo C-518/07, de 9 de março de 2010: *“Além disso, importa saliente que o mero risco de as autoridades de tutela poderem exercer uma influência política nas decisões das autoridades de controlo é suficiente para impedir o exercício independente das suas funções. Por um lado, como afirmou a Comissão, podia haver uma «obediência antecipada» dessas autoridades, atendendo à prática decisória da autoridade de tutela. Por outro, o papel de guardiãs do direito à vida privada que as referidas autoridades desempenham exige que as suas decisões e, consequentemente, elas próprias, estejam acima de qualquer suspeita de parcialidade”*; e, ainda, Acórdão TJUE, Processo C-288-12, de 8 de abril de 2014: *“(…) as autoridades de fiscalização competentes para a supervisão do tratamento de dados pessoais devem gozar de uma independência que lhes permita exercer as suas funções sem influência externa. Esta independência exclui, designadamente, qualquer instrução e qualquer outra influência externa, sob qualquer forma, seja direta ou indireta, suscetíveis de orientar as suas decisões e que podem assim pôr em causa o cumprimento, pelas referidas autoridades, da sua função de estabelecer um justo equilíbrio entre a proteção do direito à vida privada e a livre circulação dos dados de natureza pessoal (…)”*.

⁹⁵ Confirmar Considerando 129: *“(…) Os poderes das autoridades de controlo deverão ser exercidos em conformidade com as garantias processuais adequadas previstas no direito da União e do Estado-Membro, com imparcialidade, com equidade e num prazo razoável (…)”*.

⁹⁶ Confirmar Considerando 117, artigo 4.º, n.º 1 da LE e artigo 2.º, n.º 4 da Lei Orgânica da CNPD.

2.4.2. Princípio da licitude

Nos termos do artigo 6.º do RGPD, o tratamento dos dados pessoais só será considerado lícito se estivermos perante uma das seguintes situações: (i) consentimento do titular dos dados; (ii) execução de um contrato ou diligências pré-contratuais onde o titular é parte; (iii) cumprimento de uma obrigação jurídica; (iv) defesa de interesses vitais do titular ou de outra pessoa singular; (v) exercício de funções de interesse público ou exercício da autoridade pública ou (vi) interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiro.

De notar, ainda, o Considerando 40 do RGPD que refere que

Para que o tratamento seja lícito, os dados pessoais deverão ser tratados com base no consentimento da titular dos dados em causa ou noutro fundamento legítimo, previsto por lei, quer no presente regulamento quer noutro ato de direito da União ou de um Estado-Membro referido no presente regulamento, incluindo a necessidade de serem cumpridas as obrigações legais a que o responsável pelo tratamento se encontre sujeito ou a necessidade de serem executados contratos em que o titular dos dados seja parte ou a fim de serem efetuadas as diligências pré-contratuais que o titular dos dados solicitar.

Assim, concluímos que o princípio da licitude pode ser interpretado de duas formas: em sentido restrito, segundo o qual o tratamento dos dados pessoais deve estar subsumido a alguma das causas de licitude elencadas no artigo 6.º do RGPD; e em sentido amplo, o qual impõe o cumprimento do RGPD e da legislação aplicável a cada momento.⁹⁷

Não obstante, e como refere MENEZES CORDEIRO,⁹⁸

Apesar de ambas as aceções serem corretas e relevantes, os termos licitude e ilicitude são, em princípio, utilizados no RGPD num sentido estrito, ou seja, a licitude do tratamento. Esta interpretação é também suportada pelo artigo 8.º/2 da Carta: “... com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei”.

⁹⁷ A. BARRETO MENEZES CORDEIRO, *Direito da Proteção de Dados... Ob. cit.*, p. 152.

⁹⁸ A. BARRETO MENEZES CORDEIRO, *Direito da Proteção de Dados... Ob. cit.*, p. 152.

Deste modo, os titulares dos dados pessoais devem ser alertados dos riscos, regras, direitos associados ao tratamento e meios que estão à sua disposição para exercer esses direitos.

2.4.3. Princípio da lealdade

A lealdade⁹⁹ no tratamento dos dados pessoais implica, desde logo, que o tratamento se desenvolva tendo por base os interesses e as expectativas legítimas dos titulares dos dados. Por outras palavras, o tratamento dever-se-á desenvolver após a concordância do seu titular, ou seja, o seu consentimento.¹⁰⁰

Nos termos do Considerando 32,

O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito (...).

O RGPD define consentimento do titular dos dados como

*Uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento.*¹⁰¹

Ora, o consentimento só será, por isso, leal se o seu titular não estiver sujeito a qualquer pressão no momento que o presta.

Além disso, o titular dos dados deve ser devidamente informado sobre o objeto e as consequências do seu consentimento, bem como do âmbito de incidência do mesmo, que deverá ser, desde logo, razoavelmente concreto.¹⁰²

⁹⁹ Sobre a falta de harmonização na tradução deste princípio, confirmar A. BARRETO MENEZES CORDEIRO, *Direito da Proteção de Dados... Ob. cit.*, p. 153.

¹⁰⁰ Artigo 7.º do RGPD.

¹⁰¹ Artigo 4.º, 11) do RGPD.

¹⁰² De notar o referido no Considerando 32 do RGPD: “*Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins*”.

Impõe-se um tratamento dos dados que cumpra uma dupla finalidade: por um lado, salvguarde os interesses dos titulares dos dados e, por outro, proteja os interesses dos responsáveis pelo tratamento e subcontratantes.

O incumprimento do princípio da lealdade implica a prática de contraordenação muito grave, sancionada nos termos dos artigos 83.º, n.º 5, al. a) do RGPD e 37.º, n.º 1, al. a) da LPDP.

2.4.4. Princípio da transparência

Expressamente consagrado no artigo 5.º, n.º 1, al. a) do RGPD, o princípio da transparência encontra-se, ainda, difuso por vários artigos do Regulamento, entre os quais os artigos 12.º, 13.º, 14.º, 34.º e 37.º, bem como os Considerandos 39 e 59.

Um tratamento transparente dos dados pessoais implica que as informações e/ou comunicações relacionadas com o tratamento sejam de fácil acesso e compreensão, formuladas numa linguagem acessível – simples e clara.¹⁰³

A violação deste princípio faz o responsável pelo tratamento de dados incorrer em contraordenação muito grave, prevista e sancionada nos termos dos artigos 83.º, n.º 5, al. a) do RGPD e 37.º, n.º 1, al. a) e n.º 2 da LPDP.

2.4.5. Princípio do propósito limitado ou da limitação das finalidades

O princípio do propósito limitado determina que os dados pessoais só podem ser recolhidos para finalidades (i) determinadas, (ii) explícitas e (iii) legítimas, pelo que só depois de apurada a finalidade do tratamento é que será possível concluir se a informação recolhida é necessária ou excessiva – artigo 5.º, n.º 1, al. b) do RGPD

Apesar de autonomizado dos princípios da licitude, legalidade e transparência, consagrados no artigo 5.º, n.º 1, al. a) do RGPD, o princípio da limitação das finalidades encontra-se intrinsecamente ligado a estes na medida em que é obrigatório informar o titular dos dados

¹⁰³ Estas exigências são mais evidentes quando dirigidas a crianças.

sobre as finalidades do seu tratamento, sendo, desde logo, ilícito o tratamento para finalidades incompatíveis com as autorizadas/consentidas pelo titular.¹⁰⁴

De referir, ainda, a parte final do artigo 5.º, n.º 1, al. b), do RGPD, que cria uma importante exceção à prossecução de finalidades não determinadas inicialmente:

*O tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.º, n.º 1.*¹⁰⁵

A violação deste princípio faz o responsável pelo tratamento de dados incorrer em contraordenação muito grave, prevista e sancionada nos termos dos artigos 83.º, n.º 5, al. a) do RGPD e 37.º, n.º 1, al. a) e n.º 2 da LPDP.

2.4.6. Princípio da minimização dos dados

O princípio da minimização dos dados, previsto no artigo 5.º, n.º 1, al. c) do RPDG, delimita o tratamento aos dados que se mostrem estritamente relevantes, necessários, adequados, pertinentes e limitados para o cumprimento da finalidade a que se propõe, pelo que uma solicitação excessiva determina, consequentemente, a ilicitude do tratamento.^{106/107}

¹⁰⁴ Neste sentido veja-se o Considerando 50, o qual refere que “[o] tratamento de dados pessoais para outros fins que não aqueles para os quais os dados pessoais tenham sido inicialmente recolhidos apenas deverá ser autorizado se for compatível com as finalidades para as quais os dados pessoais tenham sido inicialmente recolhidos”.

¹⁰⁵ Confirmar Considerando 50 do RGPD.

¹⁰⁶ A este respeito veja-se o Parecer 37/2018 da CNPD, Processo n.º 8439/2018: “No que respeita à morada, sendo esta informação relevante perante a entidade na qual o trabalhador desempenha funções, não o é para uma base de dados centralizada cujo fim é a definição das políticas de organização do Estado e da gestão dos respetivos recursos humanos. Com efeito, parece ser suficiente para este fim conhecer a freguesia onde residem os trabalhadores. Nesse sentido, a recolha e conservação destas informações não cumpre o princípio da minimização dos dados pessoais, consagrado na alínea c) do n.º 1 do artigo 5.º do RGPD, que apenas permite o tratamento dos dados necessários à prossecução das finalidades deste. Se o que se pretende é apenas informação para fins estatísticos, então estes dados poderão ser recolhidos e conservados em termos que não permitam a sua consulta e relacionamento com a identidade do seu titular.

No que se refere à data de nascimento, não se vê qualquer utilidade no registo da exata data de nascimento dos trabalhadores, sendo suficiente para a finalidade visada com o tratamento dessa informação, o registo do mês e ano de nascimento.

Assim, recomenda-se a não recolha da morada nem do dia de nascimento, pela sua desnecessidade para as finalidades visadas com o SIOE, e, pela mesma razão e pelo potencial discriminatório, a desassociação da nacionalidade da identificação dos trabalhadores”.

¹⁰⁷ Veja-se, ainda, GRUPO DE TRABALHO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, Parecer 02/2016 sobre a publicação de dados pessoais para efeitos de transparência no setor público, WP 239, Adotado em 8 de junho

A violação deste princípio constitui contraordenação muito grave, sancionada nos termos dos artigos 83.º, n.º 5, al. a) do RGPD e 37.º, n.º 1 e 2 da LPDP.

2.4.7. Princípio da precisão e exatidão

O princípio da precisão e exatidão exige, em termos gerais, que os dados estejam atualizados e exatos devendo, para isso, ser adotadas medidas adequadas para que os dados inexatos sejam apagados ou retificados com a maior brevidade possível – artigo 5.º, n.º 1, al. d) do RGPD.

Este princípio é fundamental uma vez que a existência de dados errados pode ter uma influência enorme na vida dos seus titulares.¹⁰⁸ Ainda assim, importa salientar que existem dados que, apesar de desatualizados, não devem sofrer alterações. É o que acontece com dados que digam respeito a realidades passadas, como é o caso das fichas médicas sobre o anterior estado de saúde do paciente.

O incumprimento deste princípio gera contraordenação muito grave, prevista e sancionada nos termos dos artigos 83.º, n.º 5, al. a) do RGPD e 37.º, n.º 1, al. a) da LPDP.

De notar que este princípio se relaciona diretamente com o princípio da retificação dos dados, previsto no artigo 16.º do RGPD. Situação diferente é aquela do artigo 17.º do RGPD, referente ao direito ao apagamento dos dados. Este princípio não se confunde com aquele direito, desde logo porque este último pode acontecer independentemente da veracidade dos dados recolhidos.

de 2016: “Algumas regras nacionais em matéria de transparência preveem a publicação em linha de informações relativas ao montante do rendimento individual e das remunerações recebidas pelas pessoas que exercem funções administrativas de alto nível (por exemplo, titulares de altos cargos administrativos). Geralmente, para cumprir tais obrigações, em conformidade com o princípio de minimização, a publicação do montante total das verbas recebidas pelas pessoas em causa poderá ser suficiente. Já a publicação de dados como o número de contribuinte, relatórios financeiros integrais, dados pormenorizados extraídos das declarações fiscais ou dos recibos de pagamento de pessoas singulares, bem como os seus dados bancários, endereços privados, números de telefone ou endereços de correio eletrónico pessoais, dificilmente poderá ser considerada proporcionada”.

¹⁰⁸ Imagine o seguinte cenário: um trabalhador que, aquando da sua contratação, vivia numa determinada residência que, entretanto, foi mudada. As comunicações com a sua entidade empregadora ficam comprometidas (e.g., em caso de processo disciplinar).

2.4.8. Princípio do limite à retenção/conservação dos dados

Como o nome indica, o princípio do limite à retenção dos dados pessoais impõe uma fronteira temporal para a conservação desses dados, nomeadamente durante o período estritamente necessário para atingir as finalidades previstas para o tratamento – artigo 5.º, n.º 1, al. e) do RGPD.¹⁰⁹

Assim, deverá o responsável pelo tratamento dos dados estipular um prazo para os dados serem ou apagados, ou revistos. Não obstante, os dados podem ser conservados por períodos maiores desde que sejam tratados *exclusivamente* para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou ainda para fins estatísticos, nos termos do artigo 89.º, n.º 1 do RGPD. Nestas situações o responsável pelo tratamento dos dados deverá aplicar as medidas que se mostrem necessárias para que os direitos do titular dos dados sejam salvaguardados e devidamente tratados.

Citando FILOMENA VIEIRA,¹¹⁰

A conservação de dados pessoais por uma entidade que procede ao seu tratamento comporta riscos e, deste modo, quanto maior o tempo de conservação, maior a exposição dos dados a riscos de acesso indevido, transferência ou até perda.

A violação deste princípio constitui contraordenação muito grave, prevista e sancionada nos termos dos artigos 83.º, n.º 5, al. a) do RGPD e 37.º, n.º 1, al. a) da LPDP.

2.4.9. Princípio da integridade e confidencialidade

O princípio da integridade e confidencialidade traduz-se, de forma sucinta, no princípio da segurança dos dados. Este preceito impõe que os dados sejam tratados garantindo a sua segurança, isto é, a proteção contra o tratamento não autorizado ou ilícito, contra a sua perda, destruição ou danificação (ainda que accidental).

¹⁰⁹ De igual modo veja-se o Considerando 39 do RGPD que determina que o prazo de conservação deve ser limitado ao mínimo, pelo período estritamente necessário para a finalidade em causa.

¹¹⁰ FILOMENA VIEIRA, *RGPD para cidadãos atentos: manual de curso online*, Direção-Geral da Qualificação dos Trabalhadores em Funções Públicas (INA), Lisboa, novembro de 2018, p. 12.

Para tal deve o responsável pelo tratamento dos dados adotar medidas técnicas e organizativas que se mostrem adequadas a cumprir ambas as disposições e, assim, evitar o acesso indevido e a utilização desses dados por pessoas não autorizadas.

A violação deste princípio faz o responsável pelo tratamento de dados incorrer em contraordenação muito grave, prevista e sancionada nos termos dos artigos 83.º, n.º 5, al. a) do RGPD e 37.º, n.º 1, al. a) e n.º 2 da LPDP.

2.4.10. Princípio da responsabilidade

O princípio da responsabilidade¹¹¹ encontra-se consagrado nos artigos 5.º, n.º 2 e 24.º do RGPD.

Este princípio determina que o responsável pelo tratamento dos dados, além de ter de assegurar o cumprimento dos princípios salvaguardados no RGPD – e, desde logo, no artigo 5.º –, deve comprovar que as medidas técnicas e organizativas adotadas para o tratamento e conservação dos dados pessoais foram adequadas e devidamente aplicadas.

No sentido de aplicar as medidas apropriadas o responsável pelo tratamento de dados deve, como referido no Considerando 90,

(...) proceder, antes do tratamento, a uma avaliação do impacto sobre a proteção de dados, a fim de avaliar a probabilidade ou gravidade particulares do elevado risco, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento e as fontes do risco. Essa avaliação do impacto deverá incluir, nomeadamente, as medidas, garantias e procedimentos previstos para atenuar esse risco, assegurar a proteção dos dados pessoais e comprovar a observância do presente regulamento.

A violação deste princípio gera contraordenação muito grave, prevista e sancionada nos termos dos artigos 83.º, n.º 5, al. a) do RGPD e 37.º, n.º 1, al. a) e n.º 2 da LPDP.

¹¹¹ Para uma análise mais profunda confirmar GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Opinion 2/2010 on the principle of accountability*, WP 173, Adotado a 13 de julho de 2010, DANIEL ALVES DA CUNHA, ANA HIERRO E DIOGO RODRIGUES DA SILVA, *Guia do Processo da Adequação ao Regulamento Geral de Proteção de Dados – Implementação e Auditoria*, Almedina, 2021, p. 12 a 14, e A. BARRETO MENEZES CORDEIRO, *Direito da Proteção de Dados... Ob. cit.*, p. 161 a 163.

2.4.11. Princípio da proporcionalidade

Por fim, mas não menos importante, o princípio da proporcionalidade. Segundo princípio, as medidas adotadas para o tratamento dos dados devem ser aquelas que se mostrem menos suscetíveis de afetar a privacidade do seu titular.

Apesar de não se encontrar expressamente consagrado num artigo, o princípio da proporcionalidade encontra-se subentendido em todo o diploma, sendo a sua maior referência nos Considerandos do RGPD.¹¹²

A este propósito, é importante mencionar que a atuação do TJUE tem sido conduzida tendo por base este princípio. A título de exemplo, veja-se o Acórdão de 20 de maio de 2003:¹¹³

Coloca-se, porém, a questão de saber se a indicação do nome das pessoas em causa em relação com os rendimentos auferidos é proporcional ao objectivo legítimo prosseguido e se os motivos invocados no Tribunal de Justiça para justificar tal divulgação se afiguram pertinentes e suficientes.

(...)

Incumbe aos órgãos jurisdicionais de reenvio verificar se tal publicidade é, simultaneamente, necessária e proporcionada ao objectivo de manutenção dos salários dentro de limites razoáveis e, em especial, apreciar se tal objectivo não poderia ter sido alcançado de forma igualmente eficaz através da transmissão das informações nominativas apenas às instâncias de controlo. Do mesmo modo, coloca-se a questão de saber se não teria sido suficiente informar o grande público apenas das retribuições e outras vantagens pecuniárias de que as pessoas empregadas pelas entidades públicas em causa podem contratual ou estatutariamente beneficiar, mas não das importâncias que cada uma dessas pessoas efectivamente recebeu, no decurso do ano em causa, e de que uma fracção, variável, pode depender da respectiva situação familiar e pessoal.

¹¹² Veja-se, a título de exemplo, o Considerando 4, 156 e 170.

¹¹³ Acórdão TJUE, Processos apensos C-465/00, C-138/01 e C-139/01, de 20 de maio de 2003.

2.5. Direitos dos titulares dos dados

Como referimos anteriormente no ponto 2.3.2., o titular dos dados será, necessariamente, uma pessoa singular, identificada ou identificável, independentemente da sua nacionalidade ou do local de residência¹¹⁴.

Assim, a aplicação do Regulamento ocorrerá sempre que exista um tratamento de dados pessoais efetuado no contexto de atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União (independentemente desse tratamento ocorrer dentro ou fora da União).¹¹⁵

Analisemos, agora, cada um dos princípios em causa.

2.5.1. Direito à informação

Comecemos a nossa análise pelo direito à informação. Esta escolha não é em vão, uma vez que este direito pode ser considerado o mais importante de todos, visto que sem ele o titular dos dados dificilmente conseguirá utilizar os restantes direitos.

No momento da sua recolha, e em qualquer momento depois desta sempre que solicitado, o titular dos dados tem o direito a ser informado sobre (i) a finalidade do tratamento, (ii) o prazo de conservação dos dados, (iii) quem é o responsável pelo tratamento dos dados e (iv) a quem o responsável transmite informações sobre os mesmos.

O direito à informação encontra-se intrinsecamente ligado aos princípios da lealdade e da transparência, exigindo-se, desta forma, que a informação a ser prestada ao titular dos dados seja transparente, concisa e de fácil acesso (nomeadamente através de linguagem clara e simples) – artigo 12.º, n.º 1 e Considerando 39, ambos do RGPD.¹¹⁶

¹¹⁴ Confirmar Considerando 2 e artigo 3.º, n.º 2 do RGPD.

¹¹⁵ Confirmar artigo 3.º, n.º 1 do RGPD.

¹¹⁶ De notar que, nos termos dos artigos 13.º e 14.º do RGPD, os critérios variam conforme os dados tenham sido recolhidos diretamente junto dos seus titulares ou indiretamente. Veja-se, a título meramente exemplificado, o estabelecido nos artigos 13.º, n.º 4 e 14.º, n.º 5 do RGPD, segundo os quais a obrigação de informar os titulares dos dados não se aplica se o seu titular já tiver conhecimento de todas as informações.

2.5.2. Direito de acesso

Nos termos do artigo 15.º do RGPD, o titular dos dados tem direito a saber se os seus dados pessoais estão a ser tratados e, em caso afirmativo, a ter acesso aos mesmos. Assim, sempre que o titular dos dados solicite tais informações devem as mesmas ser fornecidas pelo responsável pelo tratamento dos dados através de uma cópia, sem restrições, demoras ou custos excessivos.

Em particular, todos os titulares de dados têm direito a obter do responsável pelo tratamento as seguintes informações: (i) as finalidades do tratamento; (ii) as categorias de dados em causa; (iii) os destinatários ou as categorias de destinatários a quem são comunicados os dados; (iv) o prazo previsto de conservação ou, se não for possível, os critérios usados para fixar esse prazo; (v) se os dados estão sujeitos a decisões automatizadas e se há definição de perfis e (vi) se os dados são transferidos para países ou organizações internacionais fora do Espaço Económico Europeu, bem como quais as garantias que existem para que os dados pessoais continuem a usufruir de um nível de proteção adequado após transferência internacional.

Ainda assim, a proteção conferida por este direito revela-se, na prática, bastante menos eficaz quando o subsumimos às inferências algorítmicas. Como refere MARIANA ALVES TEIXEIRA,¹¹⁷

seguindo uma interpretação teleológica do Direito da Proteção de Dados, considerar-se-á que o direito de acesso não abrange informações sobre o raciocínio subjacente às decisões – mas tão só o resultado final, porquanto não foi este direito pensado para garantir tal transparência do processo de tomada de decisão e, por conseguinte, não está em causa um direito de acesso total aos dados pessoais.

¹¹⁷ MARIANA ALVES TEIXEIRA, *Da (des)proteção do Candidato a Emprego em Face da Inteligência Artificial*, Almedina, 2023, p. 85 e 86.

2.5.3. Direito de retificação

Os titulares dos dados têm o direito de obter a correção dos mesmos, como consagrado no artigo 16.º e no Considerando 60 do RGPD.

Este direito é um verdadeiro espelho do princípio da exatidão, na medida em que o próprio titular dos dados, por se encontrar numa posição de maior conhecimento, poderá pretender fornecer informações mais exatas sobre os seus dados.

Note-se que a aplicabilidade deste princípio às inferências algorítmicas não é líquida, uma vez que o que este direito visa é a proteção da confidencialidade e integridade dos dados pessoais utilizados e não a garantia da precisão do processo de tomada de decisão (dados inferidos).¹¹⁸ Se adotarmos este entendimento, então podemos concluir que o que o RGPD permite é um controlo procedimental do titular sobre os seus dados, mas já não um controlo substantivo, i.e., como é que os seus dados deverão ser utilizados no momento da decisão.¹¹⁹

2.5.4. Direito ao apagamento (direito a ser esquecido)

O titular dos dados tem o direito de requerer o apagamento dos seus dados pessoais nas situações previstas no n.º 1 do artigo 17.º do RGPD.¹²⁰ Assim, sempre que o titular dos dados deixe de permitir o tratamento dos mesmos e não existam razões legítimas para a sua conservação, os dados deverão ser obrigatoriamente apagados.

¹¹⁸ MARIANA ALVES TEIXEIRA, *Da (des)proteção...* Ob. cit., p. 88.

¹¹⁹ SANDRA WACHTER, BRENT MITTELSTADT E CHRIS RUSSEL, *Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI*, Computer Law & Security Review, n.º 41, 2021, p. 57.

¹²⁰ Nos termos do artigo 17.º, n.º 1 do RGPD, “O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos: a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento; b) O titular retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6.º, n.º 1, alínea a), ou do artigo 9.º, n.º 2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento; c) O titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 2; d) Os dados pessoais foram tratados ilicitamente; e) Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito; f) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8.º, n.º 1”.

No mesmo sentido veja-se o Considerando 65 do RGPD.

Caso o responsável pelo tratamento tenha tornado públicos os dados pessoais e for obrigado a apagá-los deve tomar as medidas que se mostrem razoáveis para informar os responsáveis pelo tratamento efetivo de que o titular dos dados lhe solicitou o seu apagamento – artigo 17.º, n.º 2 do RGPD.

Contudo, este direito não poderá ser exercido sempre que se revelar necessário (i) ao exercício da liberdade de expressão e de informação; (ii) ao cumprimento de uma obrigação legal que exija o tratamento, prevista pelo direito da União ou de um Estado-Membro a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento; (iii) por motivos de interesse público no domínio da saúde pública, nos termos do artigo 9.º, n.º 2, alíneas h) e i), bem como do artigo 9.º, n.º 3; (iv) para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 89.º, n.º 1, na medida em que o direito referido no n.º 1 seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento e/ou (v) para efeitos de declaração, exercício ou defesa de um direito num processo judicial – n.º 3 do artigo 17.º do RGPD.

2.5.5. Direito à limitação do tratamento dos dados pessoais

O artigo 18.º do RGPD concede ao titular dos dados um direito provisório: através da limitação do tratamento de dados, o titular dos dados pessoais pode “congelar” a utilização dos mesmos pelo responsável pelo tratamento por um período limitado.

Este direito temporário apenas pode ser utilizado nas situações elencadas no n.º 1 do artigo 18.º do RGPD, nomeadamente: (i) para contestar a exatidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão; (ii) quando o tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização; (iii) quando o responsável pelo tratamento já não precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial e (iv) se o titular dos dados se tiver oposto ao tratamento nos termos do artigo 21.º, n.º 1, até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados.

Quando o titular dos dados obtiver o deferimento do seu pedido de limitação de tratamento, o tratamento dos dados apenas pode ocorrer mediante prévio consentimento do titular ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial, de defesa dos direitos de outra pessoa (singular ou coletiva) ou por motivos ponderosos de interesse público da União ou de um Estado-Membro – n.º 2 do artigo 18.º do RGPD.

Antes de ser anulada esta limitação, o responsável pelo tratamento deverá informar o titular dos dados pessoais – n.º 3 do artigo 18.º do RGPD.

2.5.6. Direito de portabilidade

Sempre que o tratamento dos dados pessoais se realize por meios automatizados e se baseie no consentimento dos seus titulares ou na necessidade de cumprimento de uma obrigação contratual, o titular dos dados tem direito à portabilidade dos mesmos – artigo 20.º e Considerando 68 do RGPD.

Quando exista a possibilidade de o titular dos dados requerer a sua portabilidade, na sua esfera jurídica nasce o direito: (i) a receber de um responsável pelo tratamento os seus dados pessoais, num formato estruturado, de uso corrente e de leitura automática; (ii) de transmitir os dados a outro responsável; (iii) a que os seus dados sejam transmitidos diretamente entre os responsáveis pelo tratamento, sempre que tal for tecnicamente possível e (iv) à portabilidade dos dados abrangendo apenas os dados fornecidos por si.

No entendimento do GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, o direito à portabilidade dos dados procura oferecer ao titular dos dados o controlo sobre os mesmos, *“apoia[ndo] a liberdade de escolha do utilizador, o controlo do utilizador e a capacitação do utilizador”*.¹²¹

¹²¹ GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Orientações sobre o direito à portabilidade dos dados*, WP 242 rev.01, adotadas em 13 de dezembro de 2016 e revistas em 5 de abril de 2017, p. 4.

2.5.7. Direito de oposição

“O titular dos dados tem direito a opor-se a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito” quando essa oposição tenha por base: (i) os interesses legítimos do responsável pelo seu tratamento ou de terceiro; (ii) interesse público ou (iii) quando haja uma reutilização dos dados para uma finalidade diferente, mas compatível, com aquela que motivou a sua recolha inicial, incluindo a definição de perfis – artigo 21.º do RGPD.

Nestes casos recai sobre o responsável pelo tratamento a obrigação de pôr fim ao mesmo, salvo se apresentar razões imperiosas e legítimas que prevaleçam sobre os interesses, direitos e liberdades do titular, ou para efeitos de exercício de um direito num processo judicial.

O direito de oposição ao tratamento dos dados pessoais pode ser exercido por meios automatizados.¹²²

2.5.8. Direito à não avaliação com base num tratamento automático

Como estipulado no Considerando 71 do RGPD

O titular dos dados deverá ter o direito de não ficar sujeito a uma decisão, que poderá incluir uma medida, que avalie aspetos pessoais que lhe digam respeito, que se baseie exclusivamente no tratamento automatizado e que produza efeitos jurídicos que lhe digam respeito ou o afetem significativamente de modo similar, como a recusa automática de um pedido de crédito por via eletrónica ou práticas de recrutamento eletrónico sem qualquer intervenção humana.

Assim, nos termos do artigo 22.º do RGPD, o titular dos dados tem o direito¹²³ de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado,

¹²² Para uma análise mais profunda sobre o direito de oposição confirmar *Manual da Legislação Europeia sobre Proteção de Dados*, Edição de 2018, Agência dos Direitos Fundamentais da União Europeia e Conselho da Europa, 2022, p. 259 a 264.

¹²³ O “direito” referente nesta disposição legal não se limita a um direito que tem de ser ativamente invocado pelo titular dos dados, atuando como uma verdadeira proibição geral. Confirmar GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (EU) 2016/679*, adotadas em 3 de outubro de 2017, com a última redação revista e adotada em 6 de fevereiro de 2018, p. 21.

incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.

Apesar de o legislador não ter densificado os conceitos “esfera jurídica” e “significativamente de forma similar”, entendemos que o artigo 22.º apenas irá abranger situações com implicações particularmente graves para o titular dos dados.

No que diz respeito às decisões que produzam efeitos jurídicos, e como bem referido pelo GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, falamos de decisões que afetem direitos legais (e.g., rescisão de um contrato, a contratação, etc.).¹²⁴ Note-se, contudo, que nem sempre é necessária uma alteração dos direitos dos titulares dos dados, bastando que os mesmos “*sofr[am] um impacto suficiente para solicitar as proteções garantidas*” (“de forma similar”).¹²⁵

Não obstante, as decisões automatizadas que produzam efeitos jurídicos ou afetem significativamente as pessoas podem ser admitidas se forem (i) necessárias para a celebração ou execução de um contrato entre o titular dos dados e um responsável pelo tratamento; (ii) autorizadas pelo direito da União ou pelo Estado-Membro a que o tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou (iii) baseadas no consentimento explícito do titular dos dados.¹²⁶

Ademais, sempre que as decisões tomadas digam respeito a dados sensíveis, o responsável pelo tratamento deve assegurar o cumprimento do disposto no n.º 4 do artigo 22.º do RGPD, i.e., que sejam aplicadas as medidas adequadas para a salvaguarda dos direitos e liberdades e os legítimos interesses dos titulares dos dados.

¹²⁴ GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Orientações sobre as decisões individuais automatizadas...* Ob. cit., p. 23.

¹²⁵ GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Orientações sobre as decisões individuais automatizadas...* Ob. cit., p. 23.

¹²⁶ Sobre a questão do consentimento, veja-se o ponto 2.6.1.1.

2.6. A proteção de dados no contexto laboral

Como vimos a referir ao longo desta dissertação, os dados pessoais são utilizados em diversos contextos, pelo que a atuação do legislador no sentido de impor limites ao seu emprego mostra-se fulcral. Esta limitação é tão-mais importante no contexto laboral.

Com o desenvolvimento tecnológico o tratamento dos dados pessoais em contexto laboral vem-se intensificando, impondo ao legislador uma maior intervenção neste domínio¹²⁷, uma vez que este progresso aporta avanços que permitem ao empregador aceder a ferramentas cada vez mais sofisticadas para controlar o cumprimento das obrigações contratuais estabelecidas com o trabalhador.¹²⁸

Como é de fácil compreensão, toda e qualquer empresa, independentemente da sua dimensão, trata dos dados pessoais dos seus colaboradores, ficando, conseqüentemente, vinculada a um tratamento de dados em conformidade com o RGPD.

Atualmente as empresas deparam-se com inúmeros desafios referentes ao tratamento de dados em diversas matérias: (i) nos processos de seleção de trabalhadores; (ii) no controlo dos tempos de trabalho; (iii) na utilização de sistemas de monitorização de vídeo; (iv) na monitorização da atividade dos trabalhadores nas redes sociais; etc.

O progresso tecnológico sujeitou os trabalhadores a vários controlos que vão desde a assiduidade aos níveis de alcoolémia e substância psicoativas. Ora, como referido no Considerando 11 do RGPD,

[a] proteção eficaz dos dados pessoais na União exige um reforço e a especificação dos direitos dos titulares dos dados e as obrigações dos responsáveis pelo tratamento e pela definição do tratamento dos dados pessoais, bem como poderes equivalentes para controlar e assegurar a conformidade das regras de proteção dos dados pessoais e sanções equivalentes para as infrações dos Estados-Membros.

Uma das problemáticas da utilização de dados pessoais no contexto laboral – também ela elementar e um quanto complexa – assenta na legitimidade da entidade empregadora no

¹²⁷ TERESA COELHO MOREIRA, *Algumas Implicações Laborais do Regulamento Geral de Proteção de Dados Pessoais no Trabalho 4.0*, Revista Questões Laborais, n.º 51, dezembro, 2017, p. 10 e 11.

¹²⁸ ANA DE LA PUEBLA PINILLA, *Geolocalización y control biométrico*, III Encuentro Internacional sobre Transformaciones del Derecho del Trabajo Ibérico, ISBN 978-84-697-0418-9, p. 44.

tratamento de dados. Em matéria laboral tem-se debatido se o consentimento do trabalhador se mostra fundamento legítimo e suficiente para o tratamento de determinados dados pessoais, como iremos analisar adiante.

Como observamos previamente, o tratamento dos dados pessoais surge numa época em que as tecnologias atuam no sentido de ajudar as pessoas. Assim, e seguindo este mote, o direito à proteção de dados “*deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade*”.¹²⁹

Sufragando este entendimento, o legislador procurou criar um conjunto de disposições legais que permitissem limitar os diferentes sujeitos jurídicos de invadirem áreas da vida privada dos restantes. Assim, através do artigo 16.º do CT o legislador determinou que:

1. *O empregador e o trabalhador devem respeitar os direitos de personalidade da contraparte, cabendo-lhes, designadamente, guardar reserva quanto à intimidade da vida privada.*
2. *O direito à vida à reserva da intimidade da vida privada abrange quer o acesso, quer a divulgação de aspetos atinentes à esfera íntima e pessoal das partes, nomeadamente relacionados com a vida familiar, afetiva e sexual, com o estado de saúde e com as convicções políticas e religiosas.*

Em matéria de proteção de dados o legislador procurou limitar o poder da entidade empregadora, balizando as informações que podem ser exigidas aos candidatos a emprego e trabalhadores, nomeadamente em matéria da vida privada e saúde destes – artigo 17.º do CT.

Ainda assim, as limitações legais impostas podem ser flexibilizadas em conformidade com as características do candidato a emprego/trabalhador. Como refere LURDES DIAS ALVES¹³⁰

o direito à reserva da intimidade da vida privada é variável de acordo com a pessoa em causa, abrangendo as informações que, embora de natureza privada, o titular partilha apenas com um número restrito de pessoas e que tem o interesse de

¹²⁹ Confirmar Considerando 4 do RGPD.

¹³⁰ LURDES DIAS ALVES, *Proteção de Dados Pessoais no Contexto Laboral: o direito à privacidade do trabalhador*, Almedina, 2020, p. 12.

preservar. Encontram-se incluídos nesta esfera privada, nomeadamente, factos relativos ao domicílio ou hábitos de vida.

(sublinhado nosso)

Este ligeiro desvio às limitações aplicáveis à intervenção na vida privada de cada sujeito tem-se mostrado fundamental para espoletar uma discussão que, como vimos a observar ao longo dos últimos anos, em sede laboral tem tomado proporções enormes.

Com o desenvolvimento tecnológico e a proliferação das redes sociais aquilo que até há umas décadas seria considerado privado mostra-se, hoje, de difícil categorização. As partilhas dos momentos em família, das fotografias em férias e de todos aqueles que seriam, noutros tempos, considerados momentos privados, começam a ser divulgados publicamente, esvanecendo a, agora, ténue linha que separa a vida pessoal da vida pública.

Esta alteração no paradigma social aporta consigo enormes questões práticas, não ficando o Direito Laboral imune a estas consequências.

2.6.1. A licitude para o tratamento de dados pessoais

Durante a relação contratual o empregador tem legitimidade para tratar dos dados pessoais dos seus trabalhadores para as finalidades e com os limites definidos no Código do Trabalho e na legislação complementar – artigo 28.º da LPDP. É, contudo, importante frisar que muitas dessas finalidades não se encontram expressas na lei, pelo que será necessário fazer uma análise casuística sobre a possibilidade desse tratamento.¹³¹

Note-se que o tratamento de dados pessoais no contexto laboral desenvolve-se ao abrigo do artigo 6.º do RGPD – salvo as situações de tratamento de dados sensíveis, como veremos infra. Ao analisar esses dados as entidades empregadoras devem salvaguardar o respeito

¹³¹ A título de exemplo veja-se o artigo 217.º, n.º 1, al. b) do CT, no qual o legislador impôs ao empregador o pagamento pontual do salário. Ainda que indiretamente, através desta obrigação foi criada uma finalidade legítima para o tratamento dos dados do trabalhador (o processamento salarial). SIMÃO DE SANT'ANA E VITORINO GOUVEIA, *O RGPD e os recursos humanos: guia prático para a conformidade*, Almedina, junho 2022, p. 155.

pelos direitos fundamentais dos seus titulares consagrados no Código do Trabalho (artigos 14.º a 22.º do CT) e no RGPD.¹³²

Passemos à análise das situações que legitimam o tratamento de dados pelas entidades empregadoras.

2.6.1.1.O consentimento do trabalhador

O primeiro fundamento para a licitude do tratamento dos dados pessoais é o consentimento do titular desses dados – artigo 6.º, n.º 1, al. a) do RGPD.¹³³

Nos termos do artigo 4.º, n.º 11 do RGPD, o consentimento do titular dos dados traduz-se

[n]uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento.

Não obstante, consciente da existência de relações contratuais nas quais existe um forte desequilíbrio entre as partes, como é o caso da relação laboral, o legislador comunitário determinou, no Considerando 43 do RGPD, que o consentimento

*não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, (...) [uma vez] que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa.*¹³⁴

¹³² TERESA COELHO MOREIRA, *Dados pessoais: breve análise do art. 28.º da lei n.º 58/2019, de 8 de agosto*, Revista Questões Laborais (Ano XXVI, n.º 55, julho/dezembro 2019), 2020, p. 54.

¹³³ JOANA MAGINA, *Fundamentos de licitude do tratamento de dados pessoais em contexto laboral*, In MARIA DO ROSÁRIO PALMA RAMALHO E TERESA COELHO MOREIRA, *O regulamento geral de proteção de dados e as relações de trabalho – Estudos APODIT 6*, Lisboa, AAFDL Editora, 2020, p. 58.

¹³⁴ É de notar que, antes da entrada em vigor do RGPD, o Parecer 15/2011 já referia que “[o] consentimento apenas será válido se a pessoa em causa puder exercer uma verdadeira escolha e não existir nenhum risco de fraude, intimidação, coação ou consequências negativas importantes se o consentimento for recusado. Se as consequências do consentimento comprometerem a liberdade de escolha da pessoa, o consentimento não será livre”. Neste sentido, confirmar GRUPO DE TRABALHO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição de consentimento*, WP187, adaptado em 13 de julho de 2011, p. 14.

Face ao exposto, a prestação do consentimento no âmbito laboral tem estado no centro dos debates juslaboralistas, no sentido de se criar um consenso sobre a legitimidade do mesmo nas relações entre empregadores e trabalhadores. Ainda assim, a tendência vai no sentido de que o consentimento prestado pelo trabalhador não é fundamento válido para o tratamento dos seus dados pessoais.¹³⁵ Entendem os autores que, face à sua relação de subordinação para com a entidade empregadora, o consentimento prestado pelo trabalhador não se traduz numa manifestação livre da sua vontade.¹³⁶ Como explicado por TERESA COELHO MOREIRA,¹³⁷

As relações de trabalho são um exemplo paradigmático da existência de relações privadas desiguais não só no plano factual, mas também no plano jurídico. Na verdade, no plano factual, os sujeitos contraentes – trabalhador e empregador – não dispõem da mesma liberdade no que concerne à celebração do contrato nem à estipulação de cláusulas contratuais, o que origina o aparecimento de um desequilíbrio contratual que se acentua em alturas de desemprego generalizado. No plano jurídico, a conclusão do contrato de trabalho coloca o trabalhador numa situação de subordinação face ao empregador. Assim, figurando-se o domínio económico e social de uma parte, não se pode invocar, sem mais, o princípio da liberdade contratual para se poder escolher arbitrariamente a contraparte, ou seja, o trabalhador.

Ainda assim, temos alguma dificuldade em concordar com tal posição.

Como referimos, o consentimento deverá ser simultaneamente esclarecido e livre. Relativamente ao primeiro pressuposto, como comprovam os diferentes estudos estatísticos,

¹³⁵ Refira-se, contudo, que existem autores que entendem que o único fundamento legítimo para o tratamento de dados pessoais na relação laboral é a prossecução de interesses legítimos da empresa, nos termos da al. b) do n.º 1 do artigo 6.º. Neste sentido, confirmar TERESA COELHO MOREIRA, *Dados pessoais: breve análise do art. 28.º da lei n.º 58/2019, de 8 de agosto*, Revista *Questões Laborais* (Ano XXVI, n.º 55, julho/dezembro 2019), 2020.

¹³⁶ No entendimento do Grupo de Trabalho do Artigo 29.º PARA A PROTEÇÃO DE DADOS “*pode haver situações em que seja possível ao empregador demonstrar que o consentimento foi dado livremente. Atendendo ao desequilíbrio de poder entre empregadores e empregados, estes só podem dar o seu consentimento livremente em circunstâncias excecionais quando o ato de dar ou recusar o consentimento não produza quaisquer consequências negativas*”. Não obstante, temos sérias dúvidas da capacidade de prova da liberdade do consentimento por parte da entidade empregadora. GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679*, adotadas em 28 de novembro de 2017, última redação revista e adotada em 10 de abril de 2018, WP259 rev. 01, p. 8.

¹³⁷ TERESA COELHO MOREIRA, *Dados pessoais: breve análise do art. 28.º da lei n.º 58/2019, de 8 de agosto*, Revista *Questões Laborais* (Ano XXVI, n.º 55, julho/dezembro 2019), 2020, p. 54.

a taxa de analfabetismo tem vindo a diminuir consideravelmente desde a década de 1960¹³⁸, sendo esta a geração mais bem formada dos últimos anos. É, pois, de concluir que uma comunidade devidamente formada tem as condições necessárias para compreender, quando devidamente informada, os pressupostos e o alcance da prestação do seu consentimento. A este propósito, refira-se que em matéria de tratamento de dados, a entidade empregadora encontra-se obrigada, independentemente da (i) legitimidade da prestação de consentimento, de informar, de forma completa e precisa, os seus trabalhadores sobre o tratamento de dados pessoais.^{139/140}

Se o primeiro requisito não gera grande contestação é no segundo, referente à liberdade de prestação do consentimento, que a águas se dividem.

Como sabemos, as relações contratuais são compostas por declarações de vontades que, ainda que opostas, convergem entre si para atingirem um objetivo. No direito laboral encontramos-nos perante uma relação em que, pela prestação de trabalho pelo trabalhador, existe uma contrapartida pecuniária paga pela entidade empregadora. No sentido de atingirem um entendimento e finalizarem o negócio, as partes mostram-se, frequentemente, dispostas a fazerem cedências mútuas.

Ora, o trabalhador devidamente informado (esclarecido) terá sempre o direito a aceitar ou recusar o tratamento dos seus dados sem que, para tal, tenha de ser prejudicado. Não obstante, é importante notar que os interesses das partes têm de convergir para que o contrato se forme. Note-se que não falamos dos interesses da entidade empregadora, mas sim de ambas as partes. Isto significa dizer que, recebendo uma oferta de trabalho cuja remuneração fique aquém das suas expectativas, terá o trabalhador toda a legitimidade para a recusar. Do mesmo modo, entendendo a entidade empregadora que o consentimento do trabalhador para o tratamento de determinados dados é fundamental para finalizar a contratação, tal não deve, nem pode, ser visto como um mecanismo de coação.¹⁴¹ Se assim não fosse rumaríamos para

¹³⁸ PRODATA, *Taxa de analfabetismo segundo os Censos: total e por sexo*, disponível para consulta [aqui](#).

¹³⁹ ALEXANDRE SOUSA PINHEIRO, CRISTINA PIMENTA COELHO, TATIANA DUARTE, CARLOS JORGE GONÇALVES E CATARINA PINA GONÇALVES, *Comentário ao Regulamento Geral de Proteção de Dados*, Coimbra, Edições Almedina, dezembro 2018, p. 323.

¹⁴⁰ Veja-se, a título meramente exemplificativo, a Deliberação/2019/494 da CNPD.

¹⁴¹ Assumindo a licitude do tratamento desses dados nos termos do RGPD.

um entendimento segundo o qual todo e qualquer consentimento prestado pelo trabalhador se encontra viciado por falta de liberdade o que, na prática, não acontece.¹⁴²

De referir que esta abordagem incide sobretudo na prestação de consentimento pelo trabalhador numa fase pré-contratual. Ainda assim, é fundamental ter em consideração que o consentimento é prestado, com frequência, durante o desenrolar da relação laboral. Nessas situações adotamos um entendimento similar ao do EUROPEAN DATA PROTECTION BOARD¹⁴³ segundo o qual

Atendendo ao desequilíbrio de poder entre empregadores e empregados, estes só podem dar o seu consentimento livremente em circunstâncias excecionais, quando o ato de dar ou recusar o consentimento não produza quaisquer consequências negativas. (...) o consentimento só pode ser válido se o titular dos dados puder exercer uma verdadeira escolha e não existir qualquer risco de fraude, intimidação, coação ou consequências negativas importantes (p. ex. custos adicionais substanciais) se o consentimento for recusado. O consentimento não será dado livremente nos casos em que exista qualquer elemento de obrigatoriedade¹⁴⁴, pressão, incapacidade de exercício da livre vontade

Contudo, reforçamos a ideia de que trabalhador não pode ser taxado como um mero submisso da entidade empregadora e que, portanto, é livre de prestar o seu consentimento sempre que assim o entender e se encontre devidamente esclarecido.

¹⁴² A este propósito veja-se o artigo 28.º, n.º 3 do CT segundo o qual o consentimento do trabalhador só constitui requisito de legitimidade (i) se resultar uma vantagem jurídica ou económica para o trabalhador ou (ii) se for necessário para a execução do contrato. Ora, parece-nos que seria mais coerente uma disposição legal segundo a qual seria proibido o consentimento em situações que acarretem uma desvantagem jurídica ou económica. Caso contrário, o trabalhador não teria legitimidade de prestar o seu consentimento para utilização da sua imagem em publicações do empregador (veja-se, a título exemplificativo, o Acórdão da Relação de Coimbra, de 29.06.2021, proferido no âmbito do processo n.º 302/19.2T8MGL.C1, disponível para consulta em www.dgsi.pt), uma vez que não lhe traria qualquer vantagem jurídica ou económica, nem seria necessário para a execução do contrato (salvo se se tratasse de uma profissão cuja imagem é fundamental, e.g., modelo).

¹⁴³ Diretrizes EDPB 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679, adotadas em 4 de maio de 2020, p. 10 e 11.

¹⁴⁴ Não obstante partilharmos do mesmo entendimento que o European Data Protection Board, cremos que a subsunção do consentimento prestado pelo trabalhador na fase pré-contratual a um consentimento não livre pela existência de um elemento de obrigatoriedade é excessiva. Isto porque, como referimos previamente, a relação de trabalho assenta numa combinação de interesses opostos, mas convergentes entre si. Se assumirmos que a exigência da prestação de consentimento para o tratamento de dados nessa fase é opressora vamos perpetuar condutas discriminatórias camufladas, segundo as quais o trabalhador será taxado de “pouco apto” para aquele posto quando, na verdade, os interesses das partes apenas não se mostram em harmonia.

Todavia, a entidade empregadora deve salvaguardar-se, adotando mecanismos próprios para a prestação de consentimento pelo trabalhador (e.g., resposta a um questionário que comprove a compreensão do alcance do consentimento prestado, nos termos dos artigos 13.º e 14.º do RGPD). Isto porque, como explica RODRIGO SERRA LOURENÇO¹⁴⁵

no âmbito do RGPD, é o empregador, enquanto responsável pelo tratamento, que deve demonstrar ter legitimidade e causa de licitude válida para cada operação de tratamento de dados pessoais do trabalhador ao seu serviço.

Ainda assim, e como veremos de seguida, no âmbito laboral podemos legitimar o tratamento ausente de consentimento sempre que tal seja necessário para a execução de um contrato no qual o titular dos dados é parte – artigo 28.º, n.º 3, al. b) do LPDP.

2.6.1.2.O tratamento de dados pessoais do trabalhador para o cumprimento de obrigações adstritas à entidade empregadora

Ao contrário do que acontece em outros ramos do direito, no direito laboral o tratamento de dados pessoais é frequentemente exigência para o cumprimento contratual.

Nos termos do artigo 6.º, n.º 2, al. b) do RGPD, é lícito o tratamento de dados pessoais quando se mostre necessário à execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados.

Ainda na fase de recrutamento já existe um forte tratamento de dados do candidato a emprego que se inicia com a apresentação e posterior análise de todos os documentos associados à candidatura apresentada (e.g., currículo, fotografia, etc.).

Apesar do interesse da entidade empregadora em analisar determinados dados dos seus trabalhadores, como veremos mais à frente, existem verdadeiras obrigações legais na recolha (e.g., registo dos tempos de trabalho – artigo 202.º do CT – e declaração de remunerações – artigo 40.º do CRC) e conservação dos mesmos (e.g., manter os registos dos processos de recrutamento efetuados nos últimos cinco anos – artigo 32.º do CT).

¹⁴⁵ RODRIGO SERRA LOURENÇO, *Consentimento e acordo do trabalhador para tratamento dos seus dados pessoais – Comentário ao Acórdão da RC de 19/06/2021*, In REVISTA DO CENTRO DE ESTUDOS JUDICIÁRIOS, *Privacidade e Dados Pessoais*, 2023 - II, p. 163.

Face ao exposto, e como referido no ponto anterior, ainda que não se entenda que o consentimento não é fundamento legítimo para o tratamento de dados pessoais dos trabalhadores – o que não se concede –, a verdade é que esses dados, de uma forma ou de outra, frequentemente seriam tratados para o cumprimento de imposições criadas pelo próprio legislador.

2.6.2. Dados sensíveis no contexto laboral

Como veremos de seguida, as empresas detêm acesso a inúmeras informações pessoais dos candidatos a emprego, trabalhadores e ex-colaboradores. Essas informações podem ser categorizadas em conformidade com o nível de pessoalidade – e foi exatamente isso que o legislador fez aquando da elaboração do RGPD.

Nos termos do artigo 9.º do RGPD

É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

Por outras palavras, estes são dados que incidem sobre aspetos da vida privada do seu titular e que merecem um tratamento mais cauteloso em comparação com os restantes dados.¹⁴⁶ Enquanto os dados pessoais dizem respeito a aspetos da vida privada, os dados sensíveis exprimem aspetos mais íntimos do indivíduo e cuja incorreta divulgação pode comportar fortes consequências para este.¹⁴⁷

No âmbito laboral a proteção destes dados mostra-se tão-mais importante, uma vez que o seu conhecimento pode ser um condicionador à contratação e progressão na carreira, mas também um impulsionador de despedimentos arbitrários.¹⁴⁸

¹⁴⁶ A. BARRETO MENEZES CORDEIRO, *Direito da Proteção de dados... Ob. cit.*, p. 238 e 239.

¹⁴⁷ MARIA DEL MAR CRESPI FERRIOL, *El tratamiento de los datos personales relativos a salud de los trabajadores*, Revista General de Derecho del Trabajo y de la Seguridad Social 52, 2019, p. 257-298.

¹⁴⁸ ELISA SIERRA HERNÁIZ, *Las categorías especiales de datos del trabajador: Estudio de los límites y garantías legales para su tratamiento em la relación laboral*, Pamplona: Aranzadi-Thomson Reuters, 2021, p. 57.

Consciente do referido, o legislador comunitário limitou o tratamento destes dados apenas às situações referidas no n.º 2 do artigo 9.º do RGPD, pelo que será sempre necessário (i) ou o consentimento expresso do titular dos dados para o seu tratamento; ou (ii) uma disposição legal que autorize esse tratamento (e.g., matéria laboral, segurança social, proteção social, medicina do trabalho, etc.) ou (iii) a existência de motivos de interesse público.¹⁴⁹

3. A utilização algorítmica no contexto laboral

A utilização de mecanismos de inteligência artificial por empresas tem-se mostrado cada vez mais aliciante e o número de utilizadores tem vindo a aumentar. Segundo estudos do Eurostat, 8% das empresas da União Europeia com 10 ou mais trabalhadores utilizou inteligência artificial no ano de 2023 no sentido de prevenir, recomendar ou decidir a melhor opção para atingir os seus objetivos.^{150/ 151}

Com efeito, de modo a criar a proteção necessária face ao forte desenvolvimento tecnológico atual, o legislador comunitário procedeu à criação do Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024 (RIA), o qual marcou um avanço significativo na regulação da inteligência artificial, representando um verdadeiro reconhecimento a nível europeu desta nova realidade no quotidiano.¹⁵²

Como iremos analisar infra, os temas abordados na presente dissertação, i.e., a utilização algorítmica na contratação, avaliação de desempenho e despedimento de trabalhadores, encontram-se classificados, nos termos do RIA, como sistemas de risco inaceitável e elevado, que merecerão, em seguida, uma análise cuidada da nossa parte.

¹⁴⁹ ANTÓNIO BARRETO MENEZES CORDEIRO, *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*, Coimbra, Almedina, 2021, p. 136.

¹⁵⁰ Confirmar EUROSTAT, *8% of EU enterprises used AI technologies in 2023*, 29 May 2024.

¹⁵¹ A este propósito veja-se JOSÉ JOÃO ABRANTES E ISABEL VALENTE DIAS, *Regulação do uso do algoritmo nas relações laborais*, In *Questões Laborais* N.º 63: Agenda do Trabalho Digno, Ano XXX – n.º 63 – Jul/Dez 2023 – Periodicidade Semestral, p. 42: “*Podem ser diversas as utilizações de algoritmos e sistemas de inteligência artificial no contexto laboral. Na verdade, os algoritmos e inteligência artificial são ferramentas tecnológicas que podem ser usadas pelos empregadores para tomar decisões que incidem sobre as diferentes etapas da relação de trabalho, i.e., desde o momento da formação do contrato, passando pela sua execução e até à sua cessação*”.

¹⁵² Confirmar Considerando 4 do RIA.

Consciente do avanço tecnológico atual, o legislador português adiantou-se e, anteriormente à elaboração do RIA, legislou sobre a possibilidade de as entidades empregadoras utilizarem algoritmos e sistemas de IA no desenvolvimento da sua atividade. Para tal, devem informar devidamente os seus trabalhadores sobre *“os parâmetros, os critérios, as regras e as instruções em que se baseiam os algoritmos ou outros sistemas de inteligência artificial que afetam a tomada de decisões sobre o acesso e a manutenção do emprego, assim como as condições de trabalho, incluindo a elaboração de perfis e o controlo da atividade profissional”* – artigo 106.º, n.º 3, al. s) do CT.¹⁵³

3.1. O Regulamento da Inteligência Artificial no contexto laboral

O RIA é o primeiro documento normativo a nível mundial a regulamentar o desenvolvimento, implementação e utilização da inteligência artificial. O Regulamento entrou em vigor no dia 1 de agosto de 2024, passando a aplicar-se na generalidade a partir de 2 de agosto de 2026.¹⁵⁴

Além de unificar o mercado interno, este regulamento cria um elevado nível de proteção dos direitos fundamentais de forma a permitir um consciente avanço tecnológico.¹⁵⁵

No ponto 2.6.2. analisamos os dados que, face às suas características, mereciam especial proteção (os dados sensíveis). Tendo em consideração a frágil posição que se encontra o trabalhador e o candidato a emprego face às entidades empregadoras, o legislador comunitário criou um elevado nível de proteção destes sujeitos quando submetidos a mecanismos de inteligência artificial.

Conforme estipulado no Considerando 57 do RIA

Os sistemas de IA utilizados nos domínios do emprego, da gestão de trabalhadores e do acesso ao emprego por conta própria, nomeadamente para efeitos de

¹⁵³ JOSÉ JOÃO ABRANTES E ISABEL VALENTE DIAS, *Regulação do uso do algoritmo nas relações laborais... Ob. cit.*, p. 43 a 47.

¹⁵⁴ Note-se que foram estabelecidos prazos de aplicabilidade diferentes consoante as matérias em questão. As práticas de risco inaceitável e certas disposições que incidam sobre governação devem ser aplicadas até 2 de fevereiro de 2025, já as normas referentes a sistemas de risco elevado relacionado com a legislação de harmonização da União Europeia em matéria de segurança dos produtos devem ser aplicadas até 2 de agosto de 2027.

¹⁵⁵ Confirmar Considerandos 1 e 3 do RIA.

recrutamento e seleção de pessoal, de tomada de decisões que afetem os termos da relação de trabalho, de promoção e cessação das relações contratuais de trabalho, de atribuição de tarefas com base em comportamentos individuais, traços ou características pessoais, e de controlo ou avaliação de pessoas no âmbito de relações contratuais de trabalho também deverão ser classificados como sendo de risco elevado, uma vez que podem ter um impacto significativo nas perspetivas de carreira, na subsistência dessas pessoas e nos direitos dos trabalhadores.

(...)

Ao longo do processo de recrutamento e na avaliação, promoção ou retenção de pessoal em relações contratuais de trabalho, esses sistemas podem perpetuar padrões históricos de discriminação, por exemplo, contra as mulheres, contra certos grupos etários, contra as pessoas com deficiência ou contra pessoas de uma determinada origem racial ou étnica ou orientação sexual. Os sistemas de IA utilizados para controlar o desempenho e o comportamento dessas pessoas podem ainda comprometer os seus direitos fundamentais à proteção de dados pessoais e à privacidade.

Nesta senda, o RIA veio prever um conjunto de normas com importantes reflexos no contexto laboral.

3.1.1. Âmbito de aplicação

Conforme estipulado no artigo 2.º, n.º 1, o RIA aplica-se aos:

- (i) prestadores que coloquem no mercado ou coloquem em serviço sistemas de IA ou que coloquem no mercado modelos de IA de finalidade geral no território da UE, independentemente de estarem estabelecidos ou localizados na UE ou num país terceiro;
- (ii) responsáveis pela implantação de sistemas de IA que tenham o seu local de estabelecimento ou que estejam localizados na UE;

- (iii) prestadores e responsáveis pela implantação de sistemas de IA que tenham o seu local de estabelecimento ou estejam localizados num país terceiro, se o resultado produzido pelo sistema de IA for utilizado na UE;
- (iv) importadores e distribuidores de sistemas de IA;
- (v) fabricantes de produtos que coloquem no mercado ou coloquem em serviço um sistema de IA juntamente com o seu produto e sob o seu próprio nome ou a sua própria marca;
- (vi) mandatários dos prestadores que não estejam estabelecidos na União;
- (vii) pessoas afetadas localizadas na União.

Em termos laborais, importa-nos frisar a aplicabilidade do RIA aos responsáveis pela implantação dos sistemas de IA¹⁵⁶ e às pessoas afetadas pela inteligência artificial localizadas na União Europeia. Deste modo, o regulamento será aplicável às entidades empregadoras localizadas na União Europeia ou, ainda que aí não se encontrem, utilizem dados gerados por inteligência artificial no território europeu. Além disso, é necessário que sejam utilizadores de um sistema de IA que faça uso de dados de trabalhadores e/ou participe ou tome decisões referentes ao trabalho (e.g., analise o desempenho do trabalhador, trace perfis de candidatos a emprego, etc.).

3.1.2. A hierarquização dos riscos

O Regulamento adotou uma intervenção legislativa em conformidade com o risco de atuação da inteligência artificial, ou seja, quanto maior o risco, mais exigentes são as obrigações. Deste modo, foram criados quatro níveis de risco:

- (i) risco inaceitável, impondo a exclusão de determinadas práticas desenvolvidas pela IA;
- (ii) risco elevado, sempre que as atividades desenvolvidas pela IA acarretam riscos significativos para a saúde, segurança e direitos fundamentais;
- (iii) risco limitado, em que são impostos requisitos de transparência específicos;

¹⁵⁶ Nos termos do artigo 3.º, n.º 4 do RIA entende-se por responsável pela implementação “*uma pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que utilize um sistema de IA sob a sua própria autoridade, salvo se o sistema de IA for utilizado no âmbito de uma atividade pessoal de carácter não profissional*”.

(iv) risco mínimo, segundo o qual não são impostas obrigações adicionais.

Tendo por base esta hierarquização de riscos vejamos os impactos que os mesmos podem ter na relação laboral.

3.1.2.1. Risco inaceitável

Os sistemas de risco inaceitável estão expressamente proibidos no artigo 5.º do RIA.

No que às relações laborais diz respeito, o legislador comunitário previu duas limitações: (i) os sistemas de IA utilizados para inferir emoções, salvo quando a sua utilização se justifique por razões médicas ou de segurança (al. f) e (ii) os sistemas de identificação biométrica remota em tempo real para deduzir ou inferir a raça, opiniões políticas, filiação sindical, convicções religiosas ou filosóficas, vida sexual ou orientação sexual (al. g).

A preocupação do legislador comunitário ao estabelecer estas limitações funda-se no facto de essas informações consubstanciarem fortes motores de discriminação, impulsionando a indevida intromissão nos direitos e liberdades do trabalhador, acentuando o desequilíbrio já existente nas relações de trabalho.

O incumprimento das proibições de práticas de IA de risco elevado implica o pagamento de coimas até EUR 35.000.000 ou, no caso de empresas, até 7% do volume de negócio anual a nível mundial no exercício anterior, consoante o que for mais elevado – artigo 99.º, n.º 3 e 7 do RIA.

3.1.2.2. Risco elevado

Os sistemas de risco elevado dizem respeito a atividades que podem aportar um risco significativo de danos para a saúde, segurança ou direitos fundamentais – artigo 6.º do RIA.

No âmbito laboral o legislador comunitário estabeleceu que se consideram sistemas de risco elevado quando a IA é utilizada para: (i) o recrutamento e seleção de trabalhadores; (ii) a tomada de decisões que afetem as relações laboral e (iii) a monitorização e avaliação de desempenho e conduta dos trabalhadores.

Apenas assim não o será quando esta utilização não represente um risco significativo de causar danos à saúde, à segurança e aos direitos fundamentais do trabalhador, e não influencie significativamente a tomada de decisões, salvo nos casos em que envolvam a definição de perfis de indivíduo – artigo 6.º, n.º 2 do RIA.

Ademais, é expressamente reconhecido pelo legislador comunitário a influência da aplicação de sistemas de IA nas relações contratuais e pré-contratuais, pelo que a regulamentação destas matérias nos presentes termos visa prevenir práticas discriminatória.

Assim, no âmbito de aplicação de sistemas de IA de risco elevado devem ser verificadas as seguintes condutas pelos responsáveis pela sua implantação (artigo 9.º e seguintes do RIA):

- (i) adoção de medidas técnicas e organizativas adequadas para garantir que a utilização desses sistemas se desenvolve de acordo com as instruções de utilização;
- (ii) conservação dos registos gerados pelos sistemas de IA;
- (iii) garantia de que os dados utilizados são relevantes e representativos da finalidade prosseguida;
- (iv) garantia de supervisão humana adequada;
- (v) cumprimento do dever de informação aos trabalhadores e seus representantes previamente à implementação dos sistemas de IA;¹⁵⁷
- (vi) cumprimento do dever de informação aos trabalhadores diretamente afetados pelos sistemas de IA;
- (vii) investimento na literacia no domínio da IA;
- (viii) cooperação com as autoridades competentes;
- (ix) possível realização de uma avaliação do impacto da utilização de sistemas de IA.¹⁵⁸

Note-se que a Comissão Europeia ainda irá desenvolver orientações específicas referentes aos sistemas de IA de risco elevado no sentido de orientar os seus vários utilizadores.

¹⁵⁷ Confirmar artigo 466.º, n.º 1, al. d) do CT.

¹⁵⁸ Neste sentido veja-se, como referido no artigo 9.º, n.º 9 do RIA, a possibilidade de a implementação dos sistemas de IA terem impactos negativos “sobre pessoas com menos de 18 anos e, se for o caso, outros grupos vulneráveis”.

O incumprimento destas estipulações implica o pagamento de coimas até EUR 15.000.000 ou, no caso de empresas, até 3% do volume de negócio anual a nível mundial no exercício anterior, consoante o que for mais elevado – artigo 99.º, n.º 4 e 7 do RIA.

A mais, a prestação de informações falsas, incorretas ou incompletas às autoridades competentes implica o pagamento de coimas até EUR 7.500.000 ou, no caso de empresas, até 1% do seu volume de negócios anual a nível mundial no exercício anterior, consoante o que for mais elevado – artigo 99.º, n.ºs 5 e 7 do RIA.

3.2. O conceito de algoritmo: notas características

Ao longo das últimas décadas tem-se debatido se será possível criar um conceito único de algoritmo.¹⁵⁹ Apesar das várias definições desaguarem a uma similar conclusão, acreditamos que, atualmente, não é possível criar uma definição estanque, uma vez que, face ao intenso desenvolvimento tecnológico, o conceito de algoritmo tem vindo a expandir-se.¹⁶⁰

Ainda assim, em termos generalistas, é possível definir algoritmo como uma sequência finita de passos/instruções para solucionar um determinado problema. Através da criação de um algoritmo é possível estabelecer um padrão de comportamento que a máquina deverá seguir para alcançar um resultado para um problema.^{161/162}

De mãos dadas com os algoritmos temos a inteligência artificial. Nos termos do artigo 3.º, n.º 1 do RIA, sistema de inteligência artificial é *“um sistema baseado em máquinas concebido para funcionar com níveis de autonomia variáveis, e que pode apresentar capacidade de adaptação após a implantação e que, para objetivos explícitos ou implícitos, e com base nos dados de entrada que recebe, infere a forma de gerar resultados, tais como*

¹⁵⁹ Como refere ANA PAULA DIDIER STUADART, *O poder diretivo algorítmico*, São Paulo, SP: LTr Editora, 2023, p. 27, “Apesar do conceito e do estudo dos algoritmos serem antigos, o tema em questão ganhou destaque e relevância após o início do desenvolvimento de computadores, durante o século XX. Como o objetivo das pesquisas era transferir para a máquina o trabalho de resolver problemas, principalmente na Segunda Guerra Mundial, na qual os algoritmos foram utilizados para análise e descoberta das trajetórias de mísseis, bem como para desvendar códigos criptografados, seria preciso criar algoritmos que pudessem ser usados por uma entidade autômata incapaz de refletir sobre uma maneira diferente de agir”.

¹⁶⁰ YURI GUVERICH, *What is an algorithm?*, M. Bieliková et. Al. (Eds.): SOFSEM 2012, LNCS 7147, p. 32.

¹⁶¹ ANA PAULA DIDIER STUADART, *O poder...* Ob. cit., p. 26.

¹⁶² WOODROW BARFIELD, UGO PAGALLO, *Advanced introduction to law and artificial intelligence*, Edward Elgar Advanced Introductions, 2020, p. 9 a 11.

previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais”.¹⁶³ Por outras palavras, a inteligência artificial é a capacidade que uma máquina tem para reproduzir competências similares às humanas.

Os algoritmos desenvolvem-se, via regra, através de técnicas de *machine learning* que se traduzem num processo segundo o qual o próprio algoritmo aprende com os dados inseridos e com os resultados alcançados, melhorando gradualmente com a experiência.¹⁶⁴ Através deste método os algoritmos são frequentemente treinados para encontrarem padrões e correlações nos dados. Como explicado por ZHI-HUA ZHOU¹⁶⁵

A aprendizagem automática é a técnica que melhora o desempenho do sistema, aprendendo com a experiência através de métodos computacionais. Nos sistemas informáticos, a experiência existe sob a forma de dados e a principal tarefa da aprendizagem automática é desenvolver algoritmos de aprendizagem que criem modelos a partir dos dados. Ao alimentar o algoritmo de conhecimento com dados de experiência, obtém-se um modelo que pode fazer previsões (...) sobre novas observações.

(tradução nossa)

Podemos, pois, afirmar que a barreira entre os seres humanos e as máquinas está, neste momento, na capacidade emotiva à qual o ser humano não se consegue desvincular.¹⁶⁶

¹⁶³ Os sistemas de software com capacidades inferiores encontram-se excluídos da definição de inteligência artificial.

¹⁶⁴ Como explicado por SPENCER MAINKA, *Algorithm-Based Recruitment Technology in the Workplace*, 5 Tex. A&M J. Prop. L. 801 (2018), p. 803: «Machine learning is a type or set of algorithms that can teach itself by analyzing data to increase the accuracy of its solution.11 Instead of a programmer asking, “how can this algorithm solve this problem?” a machine learning algorithm programmer asks, “how can this algorithm learn to solve this problem?” Machine learning enables computers to learn without being specifically programmed».

¹⁶⁵ ZHI-HUA ZHOU, *Machine learning*, Translated by Shaowu Liu, ISBN: 978-981-15-1967-3, p. 2. “Machine learning is the technique that improves system performance by learning from experience via computational methods. In computer systems, experience exists in the form of data, and the main task of machine learning is to develop learning algorithms that build models from data. By feeding the learning algorithm with experience data, we obtain a model that can make predictions (...) on new observations”.

¹⁶⁶ MARIANA ALVES TEIXEIRA, *Da (des)proteção do Candidato a Emprego em Face da Inteligência Artificial*, Almedina, 2023, p. 24.

3.3. O processo de recrutamento

3.3.1. Considerações preliminares

Entre os vários setores afetados pelo desenvolvimento tecnológico os departamentos de recursos humanos são dos que mais necessitam de permanecer voláteis às diferentes alterações tecnológicas e em matéria de proteção de dados, uma vez que são estes que irão proceder à recolha, tratamento, processamento e armazenamento dos dados pessoais dos diversos colaboradores.

Ao contrário do que pode ser entendido comumente, o tratamento de dados pessoais não se inicia com o vínculo contratual, começando ainda na fase de recrutamento.

Atualmente as entidades empregadoras procuram socorrer-se de ferramentas que permitam a agilização dos processos de recrutamento. Um claro exemplo da mecanização destes processos são os sistemas de triagem de candidatos (os *application tracking systems*) cujo principal objetivo assenta na publicação das ofertas de emprego e agilização da visualização dos currículos dos candidatos a emprego pelos recrutadores, facilitando o contacto posterior (e.g., LinkedIn).^{167/168}

Este tipo de tecnologia é muito vantajoso para as entidades empregadoras, uma vez que conseguem, desta forma, agilizar o processo de recrutamento, obtendo de forma simples e rápida diferentes informações sobre o candidato a emprego, o que se mostra fundamental para conseguirem uma melhor captação de talento.^{169/170}

¹⁶⁷ FRANCISCO X. GÓMEZ GARCÍA, *La importancia del e-recruitment en la moderna gestión de recursos humanos*, International Journal of Information Systems and Software Engineering for Big Companies (IJISEBC), 6(2), 2019, p. 34 e 35.

¹⁶⁸ MARIANA ALVES TEIXEIRA, *Da (des)proteção...* Ob. cit., p. 23.

¹⁶⁹ ROBERTO FERNÁNDEZ FERNÁNDEZ, *Selección...* Ob. cit., p. 54.

¹⁷⁰ A este propósito, veja-se o mencionado por OLGA GARCIA COCOA, *La protección de datos de carácter personal en los procesos de búsqueda de empleo*, Laborum, Murcia, 2016, p. 70: “En este sentido, se puede decir que la alta capacidad que tienen las tecnologías informáticas para almacenar y filtrar datos de carácter personal, también se ha trasladado al ámbito de la búsqueda y selección de candidatos al empleo. Así pues, estos mecanismos de recopilación de información personal son utilizados, tanto por las empresas de intermediación públicas y privadas, como por las entidades que realizan su propia selección de personal. Muchos de estos procedimientos, además de ofrecer servicios de registro de datos, se configuran como verdaderas oficinas virtuales de empleo que ofrecen una amplia cartera de servicios para colaborar en la colocación de aquellas personas que estén a la búsqueda de un empleo”.

Também os candidatos a emprego podem beneficiar com estes mecanismos, evitando situações de discriminação (direta ou indireta, consciente ou inconsciente) que poderiam ocorrer numa seleção puramente humana.¹⁷¹

Não obstante, as preocupações em sede de recrutamento de trabalhadores recaem sobre a possibilidade de os sistemas algorítmicos criados incidirem sobre informações pessoais e privadas, pouco relevantes para a seleção do trabalhador para o cargo a que se candidata. Esta é uma realidade próxima, uma vez que os algoritmos funcionam, como previamente explicado, através de uma combinação de dados que, feita de forma errada, poderá proceder à seleção com base em critérios que estariam proibidos pelo legislador ao abrigo de processos de recrutamento tradicionais.¹⁷²

Como bem explicado por MARIANA ALVES TEIXEIRA,¹⁷³

neste contexto, revelar-se-á mais difícil averiguar e provar se os mecanismos utilizados para encontrar ou certificar o candidato ideal vão mais longe do que o necessário. Aliás, a aparente objetividade dos resultados destes sistemas, torna-os quase inquestionáveis gerando uma passividade e aceitação acrítica em relação a estes, quer por parte do candidato, quer por parte do próprio empregador.

Cientes destas limitações, analisemos as vantagens, os riscos e os novos desafios que a utilização algorítmica nos processos de recrutamento aportam.

3.3.2. A legitimidade da entidade empregadora para o tratamento dos dados pessoais do candidato a emprego

Como previamente mencionado, o esbatimento das barreiras que separam a vida pessoal da vida pública dos candidatos a emprego tem permitido às entidades empregadores terem acesso a informações que, noutras épocas, não seriam acessíveis.

¹⁷¹ MILENA DA SILVA ROUXINOL, *O agente algorítmico – licença para discriminar? (um olhar sobre a seleção de candidatos a trabalhadores através de técnicas de inteligência artificial)*, In Mafalda Miranda Barbosa, Felipe Braga Netto, Michael César Silva, José Luiz de Moura Faleiros Júnior, *Direito Digital e Inteligência Artificial: Diálogos Entre Brasil e Europa*, Editora Foco, 2021, ponto 1.

¹⁷² MARIANA ALVES TEIXEIRA, *Da (des)proteção...* Ob. cit., p. 25 e 26.

¹⁷³ MARIANA ALVES TEIXEIRA, *Da (des)proteção...* Ob. cit., p. 26.

Ainda assim, apesar de um candidato a emprego possuir um perfil público, disponível para consulta por qualquer pessoa, tal não deve significar, por si só, que as informações aí partilhadas devem ser objeto de análise aquando da candidatura a emprego.¹⁷⁴

Nos termos do artigo 6.º, n.º 1, al. f) do RGPD e do artigo 8.º, n.º 2 da CDFUE, a entidade empregadora tem legitimidade para recolher e tratar dados pessoais relativos a candidatos a emprego, na medida em que essa recolha se mostre necessária e pertinente para o desempenho da função à qual aquele se candidata, isto é, sempre que exista interesse legítimo.

Ora, mais do que uma simples liberdade de tratamento, a entidade empregadora deverá ter um fundamento jurídico que sustente a análise da informação partilhada, devendo esta se mostrar necessária e pertinente para o desempenho da função à qual o candidato se propõe.¹⁷⁵

Contudo, sempre que exista a necessidade de um tratamento de dados pessoais prévio à celebração do contrato deve o candidato a emprego ser devidamente informado.¹⁷⁶

Não obstante, quando se torne claro que a oferta de emprego não será concluída, deve a entidade empregadora proceder à eliminação dos dados recolhidos durante o processo de recrutamento. Isto acontece uma vez que a fase de recrutamento é uma fase pré-contratual, na qual as partes avaliam os seus interesses em contratar. Findo o processo de recrutamento os dados fornecidos (e.g., CV, informações partilhadas das entrevistas, etc.) perdem o fundamento para a finalidade que legitimou o seu tratamento.¹⁷⁷

A conservação posterior dos dados para ulteriores propostas de trabalho apenas poderá ocorrer mediante prévia autorização do respetivo titular (i.e., através do seu expresse

¹⁷⁴ LURDES DIAS ALVES, *Proteção...* *Ob. cit.*, p. 25.

¹⁷⁵ Confirmar GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2017 sobre o tratamento de dados no local de trabalho*, GT 249, Adotado em 8 de junho de 2017, p. 13.

¹⁷⁶ Confirmar GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS... *Ob. cit.*, p. 13.

¹⁷⁷ TATIANA DUARTE, em comentário ao artigo 88.º do RGPD, ALEXANDRE SOUSA PINHEIRO, CRISTINA PIMENTA COELHO, TATIANA DUARTE, CARLOS JORGE GONÇALVES E CATARINA PINA GONÇALVES, *Comentário ao Regulamento Geral de Proteção de Dados*, Coimbra, Edições Almedina, dezembro 2018, p. 671.

consentimento¹⁷⁸). Assim, sempre que o titular dos dados não pretenda essa conservação, deverá a informação recolhida ser eliminada.¹⁷⁹

3.3.3. A limitação ao prazo de conservação dos dados pessoais dos candidatos a emprego

No ponto anterior observamos que mediante consentimento do candidato a emprego as empresas podem conservar os seus dados para ulteriores propostas. Ainda assim, importa perceber qual o limite temporal para a conservação dessas informações.

Uma das limitações do RGPD e da LGPD assenta na falta de especificação do período em que os dados podem ser conservados. Ora, face a essa ausência, as empresas ficam vinculadas às decisões da CNPD que, nesta matéria, considera que os dados pessoais se encontram desatualizados ao fim de um ano a contar da sua recolha, período no qual devem ser eliminados.¹⁸⁰

Apesar das decisões da CNPD criarem esta limitação temporal, o que acontece na prática é bastante diferente, uma vez que as empresas tendem a conservar os dados recolhidos por períodos bastante maiores, assumindo uma postura totalmente contrária ao princípio da limitação.

Além disso, nos termos da legislação laboral, as empresas são obrigadas a manter o registo dos processos de recrutamento efetuados durante cinco anos – artigo 32.º do CT.

Surge então a questão: deverão os interesses da empresa prevalecer sobre os direitos e liberdades dos titulares dos dados? Entendemos que, ao abrigo do artigo 32.º do CT, conjugado com o artigo 6.º, n.º 1, al. f) do RGPD, é possível estender o prazo de conservação dos dados para um período superior a um ano, alegando para tal a prossecução de um

¹⁷⁸ TATIANA DUARTE, *Ob. cit.*, p. 671. Conforme refere Tatiana Duarte, nestes casos o consentimento pode ser fundamento para a licitude do tratamento dos dados pessoais dos candidatos.

¹⁷⁹ Neste sentido, veja-se a Recomendação CM/Rec(2015)5 do Comité de Ministros aos Estados-Membros sobre o tratamento de dados pessoais no contexto laboral, adotado pelo Comité de Ministro em 01.04.2015, ponto 13.2: “*Personal data submitted in support of a job application should normally be deleted as soon as it becomes clear that an offer of employment will not be made or is not accepted by the job applicant. Where such data are stored with a view to a further job opportunity, the data subject should be informed accordingly and the data should be deleted if he or she so requests*”.

¹⁸⁰ Veja-se, a título de exemplo, as decisões da CNPD proferidas nos processos n.º 766/2013 e 3727/14.

interesse legítimo da empresa.¹⁸¹ Não obstante, parece-nos excessiva uma conservação por um período de cinco anos face à volatilidade da informação na era atual.¹⁸² A mais, os dados estarão, frequentemente, desatualizados, criando um ónus nos responsáveis pelo tratamento em proceder à sua atualização, o que nem sempre representará uma mais-valia para a empresa.

3.3.4. As fases de recrutamento e a influência algorítmica

Podemos dividir o processo de recrutamento em três grandes fases¹⁸³: (i) a procura dos candidatos a emprego; (ii) a avaliação dos candidatos e (iii) a seleção e subsequente contratação.¹⁸⁴

Nesta análise importa não descurar que, nos termos do RIA, a utilização de sistemas de IA – e, desde logo, algoritmos – no processo de recrutamento é classificada como de risco elevado face aos potenciais danos que podem causar à saúde, segurança e/ou direitos fundamentais dos trabalhadores – artigo 6.º, n.º 2, Considerando 57 e Anexo III do RIA.

3.3.4.1. Fase 1: procura dos candidatos

O processo de recrutamento inicia-se com a procura de candidatos (*sourcing*) através da divulgação de anúncios ou do contacto direto com potenciais interessados.

Os algoritmos funcionam nesta fase como selecionadores do leque de eventuais aspirantes a trabalhador.¹⁸⁵ Se é verdade que estas ferramentas dificilmente tomam decisões de contratar¹⁸⁶, também o é que são elas que, frequentemente, procedem à rejeição automática

¹⁸¹ TATIANA DUARTE, *Ob. cit.*, p. 671.

¹⁸² Veja-se que cada vez mais os trabalhadores investem na sua formação e procuram empregos que os satisfaçam económica e pessoalmente, o que implica, em muitos casos, frequentes mudanças de emprego.

¹⁸³ Esta é uma divisão meramente referencial, de forma a facilitar a presente análise.

¹⁸⁴ JOSÉ JOÃO ABRANTES E ISABEL VALENTE DIAS, *Regulação do uso do algoritmo nas relações laborais... Ob. cit.*, p. 42.

¹⁸⁵ JENNY R. YANG, *Ensuring a future that advances equity in algorithmic employment decisions: The future of work: protecting workers' civil rights in the digital era*, Washington DC: Urban Institute, February 5, 2020, p. 5.

¹⁸⁶ MIRANDA BOGEN, AARON RIEKE, *Help wanted: an examination of hiring algorithms, equity and bias*, Washington DC: Upturn, 2018.

dos candidatos, rejeição essa que pode ter origem na utilização de ferramentas de direcionamento dos anúncios assentes em critérios discriminatórios.¹⁸⁷

No que às plataformas diz respeito, podemos fazer uma divisão entre plataformas de publicidade generalizadas (e.g. Facebook) e plataformas especializadas (e.g., LinkedIn). Nestas últimas, além de uma divulgação de forma passiva (partilha da vaga), existe um verdadeiro incentivo aos utilizadores a se candidatarem. Acresce que, comumente, a própria plataforma analisa e sugere potenciais candidatos.

Estas recomendações são desenvolvidas através de dois filtros. O primeiro, o filtro baseado no conteúdo, tem por base preferências expressas pelo próprio utilizador no passado. O segundo, o filtro colaborativo, infere as preferências de outros utilizadores com perfis semelhantes.¹⁸⁸

Desta análise parece-nos que a distribuição dos diferentes anúncios, ainda que tendenciosa, não partirá, na generalidade, da adoção de critérios discriminatórios por parte da entidade empregadora, mas antes da averiguação do conjunto de dados recolhidos no próprio mercado.

3.3.4.2. Fase 2: avaliação dos candidatos

A segunda fase do processo de recrutamento é a fase de avaliação, triagem ou *screening*. É nesta fase que as entidades empregadoras analisam o perfil dos candidatos a emprego.¹⁸⁹

Tradicionalmente, a avaliação das competências dos diferentes candidatos é feita mediante provas de conhecimento e testes de avaliação psicológica.¹⁹⁰ Atualmente estas formas vêm sendo substituídas por diferentes ferramentas, tais como sistemas de classificação de

¹⁸⁷ Neste sentido veja-se o famoso caso da rede Facebook, a qual oferecia a possibilidade de filtrar o direcionamento de anúncio tendo em consideração, por exemplo, a idade, a étnica e as convicções religiosas dos utilizadores. Tendo sido divulgado estudos demonstrando o carácter discriminatório, o Facebook procedeu à exclusão de filtros como a etnia, comprometendo-se a realizar as mudanças necessárias para evitar situações discriminatórias no seio laboral. Cfr.

IFEOMA AJUNWA, *The paradox of automation as anti-bias intervention*, Cardozo law review, 2020, p. 1700 e 1701.

¹⁸⁸ MARIANA ALVES TEIXEIRA, *Da (des)proteção...* Ob. cit., p. 29.

¹⁸⁹ JENNY R. YANG, *Ensuring...* Ob. cit., p. 5.

¹⁹⁰ DAVID CARVALHO MARTINS, *Pre-screening e screening: poder funcional do empregador?*, In MARIA DO ROSÁRIO PALMA RAMALHO E TERESA COELHO MOREIRA, *O regulamento geral de proteção de dados e as relações de trabalho*, 1.ª Edição, Lisboa: AAFDL Editora, 2020, p. 115.

currículos; *chatbots*; testes online ou sistemas de entrevista de vídeo que, em tempo real, analisam o tom de voz do candidato, a expressão facial e a linguagem utilizadas.¹⁹¹

Apesar de possibilitarem um processo de recrutamento mais célere e económico, a utilização destes mecanismos pode gerar condutas, ainda que não intencionais, discriminatórias. Nesta senda, veja-se o famoso caso da *Amazon* em que o motor de contratação utilizado atribuía pontuações diferentes aos candidatos em função do género. O motor de pesquisa tinha “aprendido”, segundo os dados adquiridos, a atribuir classificações mais elevadas a fatores como o género, desvalorizando as capacidades técnicas dos candidatos. Identificando o sistema que o padrão de contratação da empresa incidia, na sua maioria, em candidatos do sexo masculino, “aprendeu” a preferir a seleção de candidatos masculinos, excluindo, consequentemente, os candidatos do sexo femininos.¹⁹²

Não recusando a possível vertente discriminatória que a utilização de algoritmos pode aportar, é importante ter em consideração que, frequentemente, esse desvio deve-se a falaciosos dados de treino – que, no exemplo anterior fora o historial de recrutamento da empresa, assente num estereótipo implícito.¹⁹³

Como referido por MARIANA ALVES TEIXEIRA,¹⁹⁴

O perigo que decorre da utilização destes sistemas reside, portanto, na sua aparente neutralidade e opacidade dos critérios que estão na base da avaliação.

3.3.4.3. Fase 3: seleção e contratação

Por fim, a fase de seleção que, como referido anteriormente, será primordialmente humana.

¹⁹¹ “A propósito de cada uma das referidas tecnologias, vide, a título de exemplo, o sistema de análise de CVs *Textkernel’s Extract! 4.0.*, a tecnologia conversacional *MYA*, o sistema de avaliação de personalidade *Cappfinity*, e a plataforma de entrevistas *HireVue*”. MARIANA ALVES TEIXEIRA, *Ob. cit.*, p. 30, e ROBERTO FERNÁNDEZ FERNÁNDEZ, *Selección...* *Ob. cit.*, p. 50.

¹⁹² JEFFREY DASTIN, *Amazon scraps secret AI recruiting tool that showed bias against woman*, Reuters, October 11, 2018.

¹⁹³ CAROLINA DE FREITAS E SILVA, *A máquina como recrutar, empregador e colega de trabalho: alguns aspectos jurídicos de contratar, gerir e lidar com pessoas na era digital*, *Questões Laborais*, Ano XXXI, n.º 64, Jan/Jun 2024, p. 52.

¹⁹⁴ MARIANA ALVES TEIXEIRA, *Da (des)proteção...* *Ob. cit.*, p. 31.

Atualmente é ainda possível às entidades empregadoras procederem à contratação dos diferentes candidatos através de sistemas automáticos de recrutamento. Estes são *softwares* que permitem prever a probabilidade de o candidato vir a aceitar a proposta de emprego e sugerem o que a entidade empregadora pode fazer para aumentar essas hipóteses (e.g., ajuste salarial, atribuição de benefícios, etc.).¹⁹⁵

A preocupação assenta, mais uma vez, no facto de estes programas poderem ser impulsionadores da acentuação de diferenças (e.g., salariais) assentes no género ou na raça dos candidatos.¹⁹⁶

3.4. Avaliação de desempenho do trabalhador

Iniciada a relação laboral os algoritmos podem ser utilizados como ferramentas auxiliares à avaliação de desempenho dos trabalhadores, facilitando a tomada de decisões das entidades empregadoras quanto a progressões na carreira, atribuições de bónus ou aplicação de sanções.¹⁹⁷

A despeito disso, o recurso a algoritmos para fundamentar uma decisão terá, em última *ratio*, de cumprir os requisitos legalmente consagrados. Não obstante o algoritmo determinar o potencial destinatário da decisão, a sua concretização dependerá sempre do cumprimento das “tradicionais” exigências legais (e.g., não é possível no ordenamento jurídico português proceder ao despedimento de um trabalhador sem um motivo justificativo).¹⁹⁸

3.4.1. Sistemas biométricos para controlo de assiduidade

Dados biométricos são “*dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente*

¹⁹⁵ IFEOMA AJUNWA, *The paradox...* Ob. cit., p. 1704.

¹⁹⁶ IFEOMA AJUNWA, *The paradox...* Ob. cit., p. 1704.

¹⁹⁷ JOSÉ JOÃO ABRANTES E ISABEL VALENTE DIAS, *Regulação do uso do algoritmo nas relações laborais...* Ob. cit., p. 42.

¹⁹⁸ Este também é um corolário do direito à não avaliação com base num tratamento automatizado. Confirmar ponto 2.5.8.

imagens faciais ou dados dactiloscópicos” – artigo 4.º, n.º 14 do RGPD. Falamos de informações como as impressões digitais e o reconhecimento facial.¹⁹⁹

Como estipulado no artigo 28.º, n.º 6 da LPDP, as entidades empregadoras têm legitimidade para proceder ao tratamento de dados biométricos para o controlo da assiduidade e do acesso às instalações.²⁰⁰ Esse tratamento tem de ser, todavia, necessário, adequado e proporcional – artigo 18.º do CT.

Importa, contudo, fazer uma breve contextualização no que aos dados biométricos diz respeito. Previamente à entrada em vigor do RGPD, os dados biométricos não estavam expressamente caracterizados como dados sensíveis, pelo que, à partida, o seu tratamento era legítimo mediante prévia autorização da CNPD²⁰¹ – é exatamente nesta lógica que se encontram redigidos os n.ºs 1 e 4 do artigo 18.º do CT.

Com a ascensão dos dados biométricos a dados sensíveis o seu tratamento passou a ser, *a priori*, proibido. Acresce que este tratamento já não poderia realizar-se com base no interesse legítimo de responsável pelo tratamento dos dados, i.e., o empregador.

Ora, tendo em consideração o supra, entendemos que a legitimidade para o tratamento dos dados biométricos apenas poderá ocorrer ao abrigo do artigo 9.º, n.º 2, al. b) do RGPD, isto é, para efeitos de *“cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria laboral, de segurança social e de proteção social, na medida em que esse tratamento seja permitido pelo direito da União ou dos Estados-Membros ou ainda por uma convenção coletiva nos termos do direito dos Estados-Membros que preveja garantias adequadas dos direitos fundamentais e dos interesses do titular dos dados”*.

Face a esta evolução legislativa, é nosso entendimento que o n.º 1 do artigo 18.º do CT²⁰² não é atualmente aplicável em matéria de controlo de assiduidade e acesso às instalações,

¹⁹⁹ EDUARDO TOMASEVICIUS FILHO, *Reconhecimento facial e lesões aos direitos de personalidade*, In MAFALDA MIRANDA BARBOSA, FELIPE BRAGA NETTO, MICHAEL CÉSAR SILVA, JOSÉ LUIZ DE MOURA FALEIROS JÚNIOR, *Direito Digital e Inteligência Artificial: Diálogos Entre Brasil e Europa*, Editora Foco, 2021.

²⁰⁰ Confirmar artigo 9.º, n.º 4 e Considerando 88 do RGPD.

²⁰¹ JOÃO P. MONJARDINO, *A recolha de dados biométricos no contexto laboral*, E-Report, Outubro 2018, p. 6.

²⁰² Existem autores como SIMÃO DE SANTA’ANA E VITORINO GOUVEIA que entendem que, não obstante a extinção da autorização prévia da CNPD, a entidade empregadora continua com a obrigação de proceder à consulta da comissão de trabalhadores, nos termos do artigo 18.º, n.º 4 do CT. Partilhamos da mesma opinião, uma vez que a participação da comissão de trabalhadores neste processo representa um verdadeiro

devendo a comunicação à CNPD ser substituída por procedimentos eficazes, como a avaliação do impacto da utilização dos dados do trabalhador (artigo 35.º do RGPD).²⁰³

Ainda que o tratamento destes dados seja bastante restrito, a utilização de dados biométricos é tendencialmente vista como não violadora dos direitos dos trabalhadores. Isto deve-se à finalidade desse tratamento que, como referido por LURDES DIAS ALVES²⁰⁴

assenta na necessidade de agilizar o cumprimento de um objetivo – a afixação do horário de trabalho, o controlo da assiduidade, e o registo do tempo de trabalho. Tal objetivo decorre de obrigação legal que recai sobre a Entidade Empregadora – responsável pelo tratamento (artº 202º do CT).

Veja-se, neste sentido, a decisão da CNPD²⁰⁵ que refere expressamente que

[a] operação de recolha das características biométricas com a finalidade de controlo do horário de trabalho não envolve, em si mesmo, uma violação da integridade física do trabalhador, do seu direito à privacidade ou da sua intimidade.

Uma vez que a quantidade de dados biométricos existentes é muito vasta, é importante cingirmos a nossa análise ao dado mais comum no âmbito laboral, i.e., a impressão digital.

A utilização da impressão digital pelas entidades empregadoras apresenta vantagens como o baixo custo e a fácil implementação. Em contrapartida, cortes ou queimaduras podem dificultar a sua leitura.

cumprimento do n.º 3 do artigo 20.º do CT, i.e., do dever de informação. Cfr. SIMÃO DE SANTA'ANA E VITORINO GOUVEIA, *O RGPD...* Ob. cit., p. 255.

²⁰³ Neste sentido veja-se, ainda, o Considerando 89 do RGPD que refere que “A Diretiva 95/46/CE estabelece uma obrigação geral de notificação do tratamento de dados pessoais às autoridades de controlo. Além de esta obrigação originar encargos administrativos e financeiros, nem sempre contribuiu para a melhoria da proteção dos dados pessoais. Tais obrigações gerais e indiscriminadas de notificação deverão, por isso, ser suprimidas e substituídas por regras e procedimentos eficazes mais centrados nos tipos de operações de tratamento suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, devido à sua natureza, âmbito, contexto e finalidades. Os referidos tipos de operações de tratamento poderão, nomeadamente, envolver a utilização de novas tecnologias, ou pertencer a um novo tipo e não ter sido antecedidas por uma avaliação de impacto sobre a proteção de dados por parte do responsável pelo tratamento, ou ser consideradas necessárias à luz do período decorrido desde o tratamento inicial responsável pelo tratamento”.

²⁰⁴ LURDES DIAS ALVES, *Proteção...* Ob. cit., p. 11.

²⁰⁵ COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS, *Princípios sobre a utilização de dados biométricos no âmbito do controlo de acessos e de assiduidade*, 26 de fevereiro de 2004, p. 4. Apesar desta pronúncia ter ocorrido antes da ascensão dos dados biométricos a dados pessoais sensíveis, o entendimento tem-se mantido o mesmo na atualidade, continuando a presente deliberação a ser utilizada para sustentar decisões.

Sobre a legitimidade da utilização das impressões digitais para o controlo de assiduidade dos trabalhadores, a Agência Espanhola de Proteção de Dados (AEPD) pronunciou-se no sentido de que o tratamento deste tipo de dados biométricos para o controlo da assiduidade não consubstancia uma violação aos direitos de personalidade, uma vez que as informações contidas nos mesmos não abrangem qualquer aspeto específico da personalidade do seu titular.²⁰⁶

Em oposição temos a utilização da íris. Apesar de ser um dos dados mais fiáveis, visto que se mantém inalterada ao longo da vida e é única para cada indivíduo, a legitimidade do seu tratamento é mais controversa, uma vez que através da sua leitura é possível aceder a dados da saúde do trabalhador (e.g., consumo de drogas e álcool, existência de doenças, etc.), podendo impulsionar condutas discriminatórias.²⁰⁷

Portanto, a utilização de dados biométricos pelas empresas para o controlo da assiduidade vai sempre depender de dois fatores: (i) da necessidade desse tratamento e (ii) do nível de intromissão na vida privada e nos direitos de personalidade dos seus trabalhadores (cumprimento do princípio da proporcionalidade²⁰⁸).

Entendemos, por isso, que a utilização de dados biométricos que não impliquem uma excessiva intromissão na esfera da vida privada dos trabalhadores (como é o caso das impressões digitais) para o controlo da assiduidade se mostra bastante vantajosa. Além de ser um método confiável e preciso, é uma verdadeira chave única intransmissível. Através da implementação destes sistemas é possível atingir um controlo mais fidedigno²⁰⁹, reduzir custos em recursos (e.g., na criação de cartões pessoais) e evitar a prática de determinado tipo de fraudes (e.g. transmissão de cartões).

²⁰⁶ AGÊNCIA ESPANHOLA DA PROTEÇÃO DE DADOS, *Deliberación 0324/2009*. Em concreto: “*En el caso planteado, tratándose del tratamiento de la huella digital, la información contenida en dicho dato no contiene ningún aspecto concreto de la personalidad y tan sólo cuando dicha información se vincula a la identidad de una persona es posible identificarla con toda certeza, de modo que los datos que se recaban no pueden considerarse de mayor trascendencia que los relativos a un número personal, a una ficha que tan solo pueda utilizar una persona o a la combinación de ambos*”.

²⁰⁷ JAVIER FERNÁNDEZ ORRICO, *Límites a la biometría como medio de identificación y control de los trabajadores: necesidad de su regulación*, In *Vigilancia y control en el Derecho del Trabajo Digital*, 1.ª ed., febrero, 2020, Aranzadi.

²⁰⁸ COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS, *Princípios...* Ob. cit., p. 6 e 7, pontos 41 a 43 e 51.

²⁰⁹ COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS, *Princípios...* Ob. cit., p. 4: “[a] finalidade do tratamento assenta na necessidade de agilizar o cumprimento de um objectivo que a lei reconhece integrar-se no âmbito de poderes de controlo da entidade responsável pelo tratamento: a fixação do horário de trabalho, o controlo da assiduidade e o registo do tempo de trabalho”.

3.4.2. Controlo de alcoolémia e substâncias psicoativas

A condução da atividade laboral deve ser realizada tendo em atenção as normas de saúde e segurança no trabalho. É fundamental garantir um ambiente onde os trabalhadores possam desempenhar as suas funções de forma segura e protegida, minimizando os riscos de acidentes e doenças profissionais.

O problema do consumo de álcool e substâncias psicoativas no contexto laboral é entendido como uma questão de saúde²¹⁰, merecendo um tratamento cuidadoso. A este propósito veja-se o Considerando 53 do RGPD quando refere que

[a]s categorias especiais de dados pessoais que merecem uma proteção mais elevada só deverão ser objeto de tratamento para fins relacionados com a saúde quando tal for necessário para atingir os objetivos no interesse das pessoas singulares e da sociedade no seu todo, nomeadamente no contexto da gestão dos serviços e sistemas de saúde ou de ação social.

Podendo este controlo ser potenciador de condutas discriminatórias, uma vez colocar em causa direitos, liberdades e garantias do trabalhador, a sua testagem deve ser restrita a categorias de trabalhadores cuja atividade possa colocar em perigo quer a sua integridade física, quer a de terceiros.²¹¹ Acresce que estes dados têm necessariamente de ser utilizados para medicina preventiva e curativa, podendo, contudo, ser aproveitados em sede de procedimento disciplinar em curso.

De modo a criar um ambiente saudável, a entidade empregadora deverá adotar procedimentos adequados em regulamentos²¹² onde constem “as substâncias alvo da deteção; as categorias profissionais que se justifica serem alvo dos testes; a oportunidade da contraprova e sua gratuidade; os procedimentos a adotar em caso de teste positivo; a

²¹⁰ Entende LURDES DIAS ALVES que, sendo este um problema de saúde, o trabalhador terá direito a “incapacidade temporária, subsídio de doença e outros benefícios sociais, através de procedimentos integrados exclusivamente no âmbito da medicina do trabalho não devendo existir em qualquer outro contexto”, LURDES DIAS ALVES, *Proteção...* Ob. cit., p. 13.

²¹¹ LURDES DIAS ALVES, *Proteção...* Ob. cit., p. 13.

²¹² Neste sentido, veja-se INSTITUTO DA DROGA E DA TOXICODEPENDÊNCIA, I.P., E AUTORIDADE PARA AS CONDIÇÕES DO TRABALHO, *Segurança e Saúde no Trabalho e a Prevenção do Consumo de Substâncias Psicoativas: Linhas Orientadoras para a Intervenção em Meio Laboral*, 8.ª versão, 13 de janeiro de 2010.

*comunicação à entidade patronal unicamente por ficha de aptidão com a menção de apto ou não apto; a sujeição a processo disciplinar face a uma prestação laboral considerada fraca e inaceitável independentemente do consumo”.*²¹³ Ainda assim, a livre adesão do trabalhador aos mecanismos implementados para esse controlo é indispensável – artigo 29.º da LPDP.

Por fim, importa referir que o consumo de álcool e/ou substâncias psicoativas não é, por si só, fundamento suficiente para justa causa de despedimento. Não obstante, os comportamentos resultantes desse consumo podem, nesse caso, ser objeto de análise e sanção disciplinar, como veremos mais à frente – artigo 351.º, alíneas h) e m) do CT.

3.4.3. Sistemas de geolocalização

A utilização de sistemas de geolocalização no local de trabalho tem crescido de forma exponencial nos últimos anos. Através destes mecanismos as entidades empregadoras conseguem localizar e monitorizar, em tempo real e com uma grande precisão, a posição geográfica dos trabalhadores. Entre as várias tecnologias existentes podemos destacar o uso do *Global Positioning System* (GPS).

No âmbito laboral as empresas utilizam estes sistemas em veículos ou dispositivos móveis (computadores e telemóveis) por si fornecidos para o desenvolvimento da atividade laboral.

Apesar destes dados não se encontrarem expressamente consagrados como dados sensíveis nos termos do artigo 9.º do RGPD, o seu tratamento levanta preocupações quanto à possível violação dos direitos de privacidade dos trabalhadores, uma vez que, consoante a sua extensão, podem elaborar perfis comportamentais e identificar hábitos da vida do trabalhador.^{214/215}

Nos termos do Código do Trabalho, a utilização de sistemas de controlo à distância tem como finalidade a proteção e segurança do trabalhador – artigo 20.º do CT. No mesmo sentido foi a Recomendação do Comité de Ministros sobre o Tratamento de Dados Pessoais

²¹³ LURDES DIAS ALVES, *Proteção...* Ob. cit., p. 13.

²¹⁴ COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS, *Deliberação n.º 7680/2014, Aplicável aos tratamentos de dados pessoais decorrentes da utilização de tecnologias de geolocalização no contexto laboral*, p. 5.

²¹⁵ ANA DE LA PUEBLA PINILLA, *Geolocalización...* Ob. cit., p. 44

no Contexto Laboral que defendeu que os equipamentos de geolocalização só devem ser introduzidos quando necessários para atingir um fim legítimo prosseguido pela entidade empregadora, não se podendo traduzir num objetivo principal, mas apenas numa consequência indireta de uma ação necessária para proteger a produção, saúde e segurança.²¹⁶

Ainda assim, entende-se que em determinadas circunstâncias é possível à entidade empregadora socorrer-se dos mecanismos de geolocalização em automóveis, nomeadamente para (i) gestão de frota em serviço externo (mas apenas nas atividades de assistência técnica externa ou ao domicílio, distribuição de bens, transporte de passageiros, transporte de mercadorias e segurança privada) e (ii) proteção de bens (mas apenas nos casos de veículos que transportem materiais perigosos ou de valor elevado).^{217/218}

Em oposição, por considerado altamente intrusivo na privacidade do trabalhador, os dispositivos móveis devem, sempre que possível, evitar a utilização de sistemas de geolocalização, optando por mecanismos alternativos como a encriptação e a autenticação restrita para o seu acesso.²¹⁹

Face ao exposto, concluímos que a utilização destes sistemas se encontra proibida para controlo (i) do desempenho do trabalhador; (ii) do cumprimento do contrato; (iii) do cumprimento da legislação rodoviária e (iv) da utilização da viatura para fins pessoais.^{220/221} A violação de qualquer uma destas proibições onera o trabalhador no direito de resolver o contrato e receber uma indemnização, nos termos dos artigos 394.º e 396.º do CT.

²¹⁶ Recomendação CM/Rec(2015)5 do Comité de Ministros aos Estados-Membros sobre o tratamento de dados pessoais no contexto laboral, adotado pelo Comité de Ministro em 01.04.2015, ponto 16.1: “*Equipment revealing employees’ location should be introduced only if it proves necessary to achieve the legitimate purpose pursued by employers and their use should not lead to continuous monitoring of employees. Notably, monitoring should not be the main purpose, but only an indirect consequence of an action needed to protect production, health and safety or to ensure the efficient running of an organisation*”.

²¹⁷ Sempre que se mostre legítima a utilização de mecanismos de geolocalização, é dever da entidade empregadora implementar mecanismos que permitam evitar o controlo fora do seu horário de trabalho.

²¹⁸ LURDES DIAS ALVES, *Proteção...* Ob. cit., p. 16.

²¹⁹ LURDES DIAS ALVES, *Proteção...* Ob. cit., p. 17.

²²⁰ No âmbito dos dispositivos móveis, uma vez que a finalidade de proteção é o bem em si, parece-nos, desde logo, desproporcional a utilização destes sistemas de controlo. No mesmo sentido, LURDES DIAS ALVES, *Proteção...* Ob. cit., p. 17.

²²¹ COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS, *Deliberação n.º 7680/2014*, Ob. cit., pontos 52, e 57 a 59.

3.4.4. Sistemas de videovigilância

O controlo dos dados recolhidos por sistemas de videovigilância recebeu enfoque por parte do legislador português aquando da transposição das normas do RGPD para o nosso ordenamento jurídico, tendo este inclusive criado uma disposição específica para esta matéria – artigo 19.º da LPDP.

Dúvidas não surgem de que os dados recolhidos por estes sistemas se enquadram na categoria de dados pessoais, uma vez se tratar de “*informação relativa a uma pessoa singular identificada ou identificável [por] identificadores por via eletrónica*”, nos termos do artigo 4.º, n.º 1 do RGPD. Deste modo, não será necessário que as imagens recolhidas sejam explícitas de pessoas, bastando que as mesmas permitam identificar ou localizá-las (e.g., imagem de um carro na qual se vê a matrícula).²²²

Note-se que a proteção dos direitos de imagem encontra-se consagrada em diversos diplomas, que vão desde a Constituição da República Portuguesa, no artigo 26.º, ao Código Civil, no artigo 79.º e ao Código Penal, no artigo 199.º. Assim, a utilização destes mecanismos tem de desenvolver-se em harmonia com as diversas disposições legais em matéria de direitos de imagem.

A utilização de sistemas de videovigilância tem como finalidade a proteção de pessoas e bens, evitando/controlando possíveis práticas criminosas. Este também foi o entendimento do legislador laboralista que acabou por ir mais longe e estipulou que a implementação destes sistemas no local de trabalho se pode ainda justificar pela natureza da atividade desenvolvida – artigo 20.º, n.º 2 do CT.

No mesmo sentido que os sistemas de geolocalização, o Código do Trabalho determina que o empregador não pode utilizar os meios de videovigilância com a finalidade de controlar o desempenho dos trabalhadores (artigo 20.º, n.º 1 do CT)²²³, devendo a sua legítima utilização ser devidamente informada ao trabalhador (artigo 20.º, n.º 3 do CT).

²²² LURDES DIAS ALVES, *Proteção...* Ob. cit., p. 17.

²²³ Recomendação CM/Rec(2015)5 do Comité de Ministros aos Estados-Membros sobre o tratamento de dados pessoais no contexto laboral, adotado pelo Comité de Ministro em 01.04.2015, ponto 15.1: “*The introduction and use of information systems and technologies for the direct and principal purpose of monitoring employees’ activity and behaviour should not be permitted. Where their introduction and use for other legitimate purposes, such as to protect production, health and safety or to ensure the efficient running of an organisation has for*

No que à utilização diz respeito, e ao contrário do que acontecia até 2018, a instalação de sistemas de videovigilância no local de trabalho não está dependente de autorização prévia da CNPD, bastando, para tanto, que se cumpram os requisitos estipulados no n.º 2 do artigo 21.º do CT, i.e., necessidade, adequação e proporcionalidade ao objetivo a atingir.^{224/225}

Como explicado por LURDES DIAS ALVES,²²⁶

[o] tratamento de dados de videovigilância, de modo sintético, pode absorver em si, por um lado, regras genéricas, por serem aplicáveis ao tratamento de todos os dados pessoais e, por outro lado, regras específicas, por serem aplicáveis em exclusivo à videovigilância.

Relativamente às regras genéricas referimo-nos ao cumprimento dos princípios gerais estipulados ao longo do RGPD, tais como o princípio da licitude, lealdade e transparência, nos termos dos quais o tratamento tem de se desenvolver tendo por base uma fonte de licitude (artigo 6.º do RGPD), e o princípio da limitação das finalidades, segundo o qual a recolha e o tratamento de dados devem ter uma finalidade determinada, explícita e legítima.^{227/228}

Por referências às regras específicas, e em conformidade com o artigo 31.º da Lei n.º 34/2013, de 16 de maio, referimo-nos às seguintes exigências:

- (i) As imagens capturadas por videovigilância são armazenadas em formato codificado pelo prazo de 30 dias a contar da sua gravação devendo, após esse período, ser destruídas no prazo máximo de 48 horas. Em situações específicas, esse prazo pode estender-se a 90 ou 180 dias, nos termos da Lei n.º 51/2006, de 29 de agosto.

indirect consequence the possibility of monitoring employees' activity, it should be subject to the additional safeguards set out in principle 21, in particular the consultation of employees' representatives".

²²⁴ Com a entrada em vigor do RGPD, e nos termos do artigo 62.º, n.º 2 da LPDP, as disposições que previam autorização prévia da CNPD deixaram de se aplicar por incompatibilidade de regime. Excetua-se, contudo, as situações em que os sistemas de videovigilância impliquem a captação de som, nos termos do artigo 19.º, n.º 4 da LPDP. Veja-se, ainda, SIMÃO DE SANTA'ANA E VITORINO GOUVEIA, *O RGPD... Ob. cit.*, p. 239.

²²⁵ Existem autores como SIMÃO DE SANTA'ANA E VITORINO GOUVEIA que entendem que, não obstante a extinção da autorização prévia da CNPD, a entidade empregadora continua com a obrigação de proceder à consulta da comissão de trabalhadores, nos termos do artigo 21.º, n.º 4 do CT. Partilhamos da mesma opinião, uma vez que a participação da comissão de trabalhadores neste processo representa um verdadeiro cumprimento do n.º 3 do artigo 20.º do CT, i.e., do dever de informação. Cfr. SIMÃO DE SANTA'ANA E VITORINO GOUVEIA, *O RGPD... Ob. cit.*, p. 244.

²²⁶ LURDES DIAS ALVES, *Proteção... Ob. cit.*, p. 18.

²²⁷ LURDES DIAS ALVES, *Proteção... Ob. cit.*, p. 18.

²²⁸ Confirmar ponto 2.4. da presente dissertação.

- (ii) As pessoas que tenham acesso às gravações face às suas funções devem guardar sigilo, exceto quando a legislação processual penal permita o seu uso para apuramento de responsabilidade disciplinar, conforme a Lei n.º 51/2006, de 29 de agosto;
- (iii) Em locais monitorados por câmaras, é obrigatório sinalizar visivelmente a presença de videovigilância.^{229/230}

Não obstante a legitimidade para a sua utilização, é expressamente proibida a instalação de câmara que incidam sobre “o interior de áreas reservadas aos trabalhadores, designadamente zonas de refeição, vestiários, ginásios, instalações sanitárias e zonas exclusivamente afetadas ao seu descanso”, como estipulado no artigo 19.º, n.º 2, al. d) da LPDP.^{231/ 232}

Refira-se, também, que é proibida a captação de som juntamente com imagem, exceto no período em que as instalações estejam encerradas ou mediante autorização prévia da CNPD – artigo 19.º, n.º 4 da LPDP.

Note-se que as imagens recolhidas apenas podem ser utilizadas no âmbito do processo penal ou para efeitos de apuramento de responsabilidade disciplinar, na medida em que o sejam no âmbito do processo penal – artigo 28.º, n.ºs 4 e 5 da LPDP.²³³ Contudo, nestas situações deverá o trabalhador obter cópia de quaisquer gravações feitas.²³⁴

²²⁹ LURDES DIAS ALVES, *Proteção... Ob. cit.*, p. 18.

²³⁰ Veja-se, ainda, a análise da CNPD sobre os sistemas de videovigilância, disponível para consulta [aqui](#).

²³¹ Recomendação CM/Rec(2015)5 do Comité de Ministros aos Estados-Membros sobre o tratamento de dados pessoais no contexto laboral, adotado pelo Comité de Ministro em 01.04.2015, ponto 15.2: “*Information systems and technologies that indirectly monitor employees’ activities and behaviour should be specifically designed and located so as not to undermine their fundamental rights. The use of video surveillance for monitoring locations that are part of the most personal area of life of employees is not permitted in any situation*”.

²³² No mesmo sentido, veja-se ainda FILIPA URBANO CALVÃO, *A proteção de dados pessoais no contexto laboral: análise da jurisprudência*, In Caderno de Justiça Administrativa, N.º 128 (mar.- abr.) 2018, p. 5 e 6.

²³³ Recomendação CM/Rec(2015)5 do Comité de Ministros aos Estados-Membros sobre o tratamento de dados pessoais no contexto laboral, adotado pelo Comité de Ministro em 01.04.2015, ponto 15.3: “*In the event of dispute or legal proceedings, employees should be able to obtain copies of any recordings made, when appropriate and in accordance with domestic law. The storage of recordings should be subject to a time limit*”.

²³⁴ LURDES DIAS ALVES, *Proteção... Ob. cit.*, p. 18.

3.4.5. **Sistemas de controlo da utilização de telefones, do correio eletrónico, do acesso à Internet ou do computador**

A utilização de ferramentas tecnológicas, como computadores e telemóveis, na era atual é fundamental para os diferentes sujeitos económicos acompanharem o desenvolvimento. Apesar dos indubitáveis benefícios, a utilização destes recursos não deixa de colocar sérios riscos à privacidade dos trabalhadores.²³⁵

Consciente desta possibilidade, o legislador estipulou, no n.º 1 do artigo 22.º do CT, que “[o] trabalhador goza do direito de reserva e confidencialidade relativamente ao conteúdo das mensagens de natureza pessoal e acesso a informação de carácter não profissional que envie, receba ou consulte, nomeadamente através do correio eletrónico”.²³⁶ Não obstante, é reconhecido ao empregador a possibilidade de estabelecer regras de utilização dos meios de comunicação por si fornecidos – n.º 2 do mesmo artigo.

De forma a balizar a utilização dos instrumentos de trabalho por si disponibilizados deve a entidade empregadora elaborar regulamentos internos nos quais estabeleça, de forma clara e precisa, os limites de uso desses equipamentos – artigo 99.º do CT. Estes regulamentos devem cumprir os princípios da necessidade, proporcionalidade e boa-fé, tendo a sua aplicação o menor impacto possível na vida do trabalhador.²³⁷

Com a disponibilização de computadores e telemóveis as empresas estão à distância de um clique para aceder a informações privadas do trabalhador, nomeadamente através do controlo do e-mail, monitorização do uso da internet, acesso remoto ao computador do trabalhador e controlo de comunicações telefónica e de tráfego. Deste modo, é fulcral que exista uma clara limitação dos poderes das entidades empregadoras de forma a evitar o acesso a informações pessoais dos seus trabalhadores.

²³⁵ SIMÃO DE SANT’ANA E VITORINO GOUVEIA, *O RGPD e os recursos humanos: guia prático para a conformidade*, Almedina, junho 2022, p. 175.

²³⁶ Na mesma ordem veja-se, ainda, o artigo 8.º, n.º 1 da CEDH que estabelece que qualquer pessoa tem direito à reserva da vida privada e familiar, do domicílio e correspondência, e o artigo 7.º da CDFUE que impõe o respeito pela vida privada e família, pelo domicílio e correspondência. Refira-se, ainda, os artigos 8.º do CDFUE e 16.º do TFUE que consagram o direito à proteção dos dados pessoais.

²³⁷ LURDES DIAS ALVES, *Proteção...* Ob. cit., p. 14.

3.4.5.1. Controlo do e-mail do trabalhador

No que ao controlo do e-mail diz respeito, e independentemente das regras aplicadas pela empresa, a entidade empregadora não tem legitimidade para abrir o correio eletrónico dirigido ao trabalhador, quer por motivos de privacidade²³⁸, quer por motivos de segredo profissional específico.^{239/240} A jurisprudência tem sido clara nesta matéria referindo que não é possível ao empregador aceder ao conteúdo das mensagens recebidas pelo trabalhador, mesmo que esteja a correr processo disciplinar contra si. Além disso, não basta que os intervenientes das comunicações se refiram a aspetos da empresa para que tais comunicações assumam, de imediato, natureza profissional e, como tal, permitam um escrutínio da empresa.²⁴¹ Este entendimento é ainda sufragado nos artigos 34.º da CRP, 22.º do CT e 4.º da Lei n.º 41/2004, de 18 de agosto, que garantem a inviolabilidade da correspondência e das comunicações.²⁴²

A fiscalização desenvolvida pela empresa não pode ser sistemática e permanente, mas antes pontual e direcionada para as áreas de maior risco, devendo a escolha dos trabalhadores ser efetuada de forma aleatória.^{243/244}

Como refere a CNPD, o acesso ao correio eletrónico profissional do trabalhador pela entidade empregadora deve ocorrer em última *ratio* e, sempre que aconteça, deve ser realizado na presença do trabalhador e, preferencialmente, de um representante sindical (ou de outra estrutura representativa) ou de alguém indicado pelo trabalhador. Esse acesso deve restringir-se à visualização dos endereços dos destinatários, do assunto, da data e da hora do envio das comunicações. Se necessário, e caso não tenha tido a oportunidade de excluí-las

²³⁸ Como refere GARCIA MARQUES a liberdade de utilização do correio eletrónico pelos trabalhadores justifica-se pelo facto de estes entenderem que têm um determinado nível de privacidade no seu local de trabalho. GARCIA MARQUES E LOURENÇO MARTINS, *Direito da Informática*, 2.ª Edição refundida e atualizada, Coimbra, Almedina, 2006, p. 377.

²³⁹ COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS, *Deliberação n.º 1638/2013*, de 16 de julho de 2013, p. 19.

²⁴⁰ LURDES DIAS ALVES, *Proteção...* *Ob. cit.*, p. 15.

²⁴¹ Neste sentido refiram-se os seguintes Acórdãos: Acórdão do Tribunal da Relação de Lisboa, de 05.06.2008, proferido no âmbito do processo n.º 2970/2008-4; Acórdão do Tribunal da Relação de Lisboa, de 07.03.2012, proferido no âmbito do processo n.º 24163/09.0T2SNT.L1-4; Acórdão do Supremo Tribunal de Justiça, de 05.07.2007, proferido no âmbito do processo n.º 07S043; Acórdão do Tribunal da Relação do Porto, de 08.02.2010, proferido no âmbito do processo n.º 452/08.0TTVFR.P1, todos disponíveis para consulta em www.dgsi.pt.

²⁴² FILIPA URBANO CALVÃO, *A proteção...* *Ob. cit.*, p. 6.

²⁴³ LURDES DIAS ALVES, *Proteção...* *Ob. cit.*, p. 15.

²⁴⁴ SIMÃO DE SANT'ANA E VITORINO GOUVEIA, *O RGPD...* *Ob. cit.*, p. 177.

ou arquivá-las em uma pasta específica, o trabalhador pode identificar mensagens privadas que não deseja que sejam lidas pelo empregador.²⁴⁵

É ainda possível às entidades empregadoras acederem ao correio eletrónico dos seus trabalhadores com fundamento na ausência. Contudo, mesmo nestas situações é necessário existir uma finalidade concreta e explícita (que terá de ser comunicada ao trabalhador), devendo o empregador cumprir os requisitos supramencionados, nomeadamente a presença de um representante dos trabalhadores ou de alguém indicado pelo trabalhador. Se tal não for possível, e sempre que exista um delegado de proteção de dados na empresa, deverá ser este o responsável por garantir o cumprimento da lei e, consequentemente, dos direitos do trabalhador.²⁴⁶

Aquando da saída do trabalhador da empresa o empregador deve disponibilizar um prazo razoável para este retirar o conteúdo de cariz pessoal do seu e-mail. Finalizado esse período deve o empregador eliminar a respetiva conta e evitar atribuir o mesmo endereço de correio eletrónico a outro colaborador.

3.4.5.2. Monitorização do uso da *Internet*

A *Internet* pode ser utilizada para diversas finalidades e nesse sentido tem-se debatido a possibilidade do controlo pela entidade empregadora da navegação realizada pelo trabalhador.

Como previamente referido, o empregador, aquando da elaboração do regulamento interno, deve garantir que os trabalhadores estão devidamente esclarecidos sobre os limites estabelecidos na utilização da *Internet*.²⁴⁷

A finalidade do controlo neste âmbito é principalmente preventiva. Assim, caso pretenda limitar o acesso do trabalhador à *Internet* a entidade empregadora deve adotar sistemas de

²⁴⁵ COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS, *Deliberação n.º 1638/2013*, de 16 de julho de 2013, p. 20.

²⁴⁶ COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS, *Deliberação n.º 1638/2013*, de 16 de julho de 2013, p. 21.

²⁴⁷ Veremos, no ponto 3.4.5.5., um caso paradigmático a este respeito.

filtros que impossibilitem a visita de determinados *websites* que considere não autorizados ou sistemas *proxy* que armazenem e registem os *sites* visitados.^{248/249}

Contudo, e como refere a CNPD²⁵⁰, deve

admitir[-se] um certo grau de tolerância em relação ao acesso à Internet para fins privados, nomeadamente se este ocorrer fora do horário de trabalho.

Note-se, porém, que o controlo realizado pela empresa não deve ser permanente e sistemático, mas antes um controlo parametrizado, com o objetivo de detetar eventuais desvios ou abusos aos limites estabelecidos por si.²⁵¹

Refira-se, por fim, que no regulamento interno elaborado a entidade empregadora pode definir limites à utilização da *Internet* nos instrumentos por si disponibilizados. Contudo, essas regras devem refletir a possibilidade de trabalho por turnos.²⁵²

3.4.5.3. Acesso remoto ao computador do trabalhador

Como previamente desenvolvido no ponto 3.4.3., é proibido o controlo da atividade do trabalhador à distância através de sistemas como *Virtual Network Computing* (sistemas que permitem acompanhar o que o trabalhador faz no seu computador) ou *Electronically Stored Information* (sistemas de registo eletrónico, pesquisa, localização e obtenção de dados).

Assim, como recomendado pela CNPD,²⁵³

[q]uaisquer mecanismos adotados pela entidade empregadora, relativamente à realização de cópias de segurança da informação contida nos computadores individuais atribuídos aos trabalhadores ou à centralização em arquivo geral de documentação profissional dispersa, devem garantir que não é acedida e copiada informação de natureza privada.

²⁴⁸ SIMÃO DE SANT'ANA E VITORINO GOUVEIA, *O RGPD...* Ob. cit., p. 177.

²⁴⁹ FILIPA URBANO CALVÃO, *A proteção...* Ob. cit., p. 8.

²⁵⁰ COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS, *Deliberação n.º 1638/2013*, de 16 de julho de 2013, p. 22.

²⁵¹ COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS, *Deliberação n.º 1638/2013*, de 16 de julho de 2013, p. 22.

²⁵² LURDES DIAS ALVES, *Proteção...* Ob. cit., p. 15.

²⁵³ COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS, *Deliberação n.º 1638/2013*, de 16 de julho de 2013, p. 25.

Para este efeito, tais procedimentos devem prever a existência de uma separação inequívoca de pastas pessoais e profissionais, ser transparentes e claramente descritos aos trabalhadores, com prestação de informação e orientação prática quanto à forma correta de arquivar eventuais documentos privados.

3.4.5.4. Controlo de dados de comunicações telefónicas e de tráfego

No que diz respeito ao controlo de comunicações telefónicas e de tráfego entende-se que a entidade empregadora se encontra vedada de aceder ao seu conteúdo através de qualquer sistema.²⁵⁴

Ainda assim é admissível a gravação de chamadas para as seguintes finalidades: (i) prova da relação contratual; (ii) chamadas de emergência²⁵⁵ e (iii) monitorização da qualidade de atendimento²⁵⁶.²⁵⁷ No que a esta última finalidade diz respeito, a Deliberação 629/2010 da CNPD veio estabelecer alguns limites, nomeadamente:

- (i) As gravações de chamadas objeto de monitorização deverão ser recolhidas de forma aleatória;
- (ii) Apenas 5% do volume total das chamadas efetuadas deverão ser objeto de monitorização;²⁵⁸
- (iii) Deve ser cumprido o direito de informação, quer ao trabalhador²⁵⁹, quer ao cliente;
- (iv) Deve ser obtido o consentimento expresso de todos os intervenientes, não sendo possível o mero exercício do direito de oposição;

²⁵⁴ SIMÃO DE SANT'ANA E VITORINO GOUVEIA, *O RGPD... Ob. cit.*, p. 259.

²⁵⁵ A autorização da gravação das chamadas de emergência encontra-se consagrada no artigo 4.º, n.º 4 da Lei n.º 41/2004, de 18 de agosto.

²⁵⁶ Sobre a diferenciação entre monitorização de qualidade de atendimento e avaliação do desempenho do trabalhador veja-se o Acórdão do Tribunal da Relação de Lisboa, de 22.05.2013, proferido no âmbito do processo n.º 2567/12.1TTLSB.L1-4, disponível para consulta em www.dgsi.pt.

²⁵⁷ COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS, *Deliberação n.º 629/2010*, de 13 de setembro de 2010, p. 3.

²⁵⁸ Apesar de ter estabelecido um limite percentual, a CNPD não estipulou qualquer limite temporal, pelo que parece que o este critério será decidido pelo empregador.

²⁵⁹ Neste sentido veja-se o referido pela CNPD na mesma deliberação, p. 15: “Por um lado, no contrato de trabalho celebrado deverá figurar a possibilidade de gravação de chamadas para efeito de monitorização da qualidade do serviço, bem como as condições decorrentes desse tratamento.

Nos casos de alteração do conteúdo funcional do trabalhador, atentas as implicações na sua privacidade, pugna-se pela redução a escrito, por meio de adenda contratual ou outro meio idóneo que assegure o pleno conhecimento do trabalhador nos termos supra descritos”.

- (v) Não sejam os dados recolhidos utilizados para a avaliação de desempenho do trabalhador.²⁶⁰

Estando consagrada a possibilidade de controlo, esta deve limitar-se a identificar o utilizador, a sua função/categoria, o número de telefone chamado/recebido (com supressão dos últimos quatro dígitos), tipo de chamada (local, regional ou internacional), duração e custo da mesma.²⁶¹

Por fim, e como clarifica a CNPD,²⁶²

[d]eve ser estabelecido um prazo limitado de conservação, que não deve exceder o período legal de contestação da fatura. Os motivos que presidem à liberdade de organização por parte da entidade empregadora não justificam que a conservação dos dados tratados para a finalidade de controlo dos dados de tráfego se estenda para além daquele prazo.

...1. O caso paradigmático do Acórdão do TEDH: BĂRBULESCU V. ROMANIA

Da análise realizada até aqui, e em particular a desenvolvida no ponto 3.4.5., observamos a importância da salvaguarda do direito de privacidade do trabalhador no que diz respeito às suas comunicações. Como vimos, quer a doutrina e jurisprudência, quer a legislação existente (nacional e internacional) são claras nestas questões, defendendo a limitação da atuação da entidade empregadora.

Ainda assim, raras não são as vezes em que, face à difícil conciliação entre os poderes da entidade empregadora e os direitos do trabalhador, estas questões são tema de debate no TEDH, como ocorreu no paradigmático Acórdão de BĂRBULESCU V. ROMANIA.²⁶³

²⁶⁰ COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS, *Deliberação n.º 629/2010*, de 13 de setembro de 2010, p. 18.

²⁶¹ COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS, *Deliberação n.º 1638/2013*, de 16 de julho de 2013, p. 17.

²⁶² COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS, *Deliberação n.º 1638/2013*, de 16 de julho de 2013, p. 17.

²⁶³ Acórdão do TEDH: BĂRBULESCU V. ROMÂNIA, de 05.09.2017, proferido no âmbito do processo n.º 61496/08, disponível para consulta [aqui](#).

Eis os contornos do caso: o trabalhador Bărbulescu teria desempenhado funções de engenheiro numa empresa privada que, aquando do seu início, lhe solicitou a criação de uma conta no *Yahoo Messenger* de forma a facilitar o contacto com os clientes.

Através de regulamento interno a empresa proibiu a utilização dos instrumentos de trabalho para fins pessoais. Note-se que em 3 de julho de 2007 o empregador teria distribuído pelos colaboradores um “aviso informativo” advertindo que a conduta dos trabalhadores seria devidamente monitorizada e punida sempre que violassem o regulamento implementado.

Nesta sequência, em 13 de julho de 2007, o trabalhador teria sido informado que as suas comunicações haviam sido monitorizadas, tendo a empresa concluído pela utilização da sua conta para fins pessoais.²⁶⁴ Face ao exposto, a entidade empregadora cessou o vínculo contratual com fundamento na violação por parte do trabalhador das regras internas que determinavam a proibição do uso dos recursos da empresa para fins pessoais.

Inconformado, o trabalhador contestou a decisão no Tribunal do Condado de Bucareste requerendo (i) a anulação do despedimento; (ii) o pagamento dos salários e de outros direitos desde a data do seu despedimento e (iii) a condenação da empresa no pagamento de uma indemnização. Em 7 de dezembro de 2007 o Tribunal reconheceu a legalidade do despedimento, fundamentando que o artigo 267.º do CT da Romênia permite ao empregador investigar disciplinarmente e supervisionar os seus trabalhadores.

O trabalhador recorreu desta decisão para o Tribunal da Relação, reforçando a sua defesa e argumentando, ainda, que não existia qualquer regulamento interno na empresa e que o empregador não tinha distribuído nenhum “aviso informativo”, o que significava que a monitorização teria ocorrido fora do seu conhecimento.²⁶⁵ Em 17 de junho de 2008 o Tribunal da Relação manteve a legalidade do despedimento, sustentando que, nos termos do

²⁶⁴ A empresa teria apresentado ao trabalhador a transcrição de 45 páginas de mensagens trocadas com o seu irmão e com a sua noiva relacionadas com assuntos privados. LEILIANE PIOVESANI VIDELETTI, *Caso BĂRBULESCU V. ROMÊNIA: Tensão entre o poder diretivo do empregador e o direito à privacidade do empregador no contexto da sociedade tecnológica*, Revista Jurídica Luso-Brasileira, Ano 6, 2020, n.º 4, p. 1698.

²⁶⁵ O Tribunal considerou que não existia qualquer evidência de que o trabalhador tinha sido previamente informado do início da monitorização. Confirmar parágrafo 75 do Acórdão: “*In any event, it does not appear that the applicant was informed in advance of the extent and nature of his employer’s monitoring activities, or of the possibility that the employer might have access to the actual contents of his communications*”.

artigo 40.º do CT da Romênia, o empregador tem a legitimidade para monitorar o uso da *Internet* pelos seus funcionários.

Impossibilitado de recurso nacional, o trabalhador levou o caso ao TEDH que, numa primeira fase, não logrou êxito nas suas pretensões. Entendeu o Tribunal que o despedimento fora lícito uma vez que o trabalhador teria utilizado os instrumentos da empresa para fins diversos e durante o horário de trabalho.

Mais tarde, em 2016, através de revisão, o TEDH defendeu que o trabalhador detinha razoável expectativa de privacidade, independentemente da existência de regulamento interno que vedasse o uso dos instrumentos de trabalho para fins pessoais. Como mencionado pelo Tribunal²⁶⁶

as instruções da entidade empregadora não pode reduzir a zero a vida social privada no local de trabalho. O respeito pela vida privada e pela privacidade da correspondência continua a existir, mesmo que possa ser restringido na medida do necessário.

(tradução nossa)

Esta decisão levantou o debate sobre a aplicabilidade do artigo 8.º da CEDH no âmbito das relações laborais e, em particular, da existência de uma “obrigação positiva” na esfera do trabalhador, uma vez que a relação contratual em controvérsia era privada (entendendo, consequentemente, que dever-se-ia realizar uma interpretação extensiva da aplicabilidade da norma). Através da presente, veio o TEDH clarificar que a noção de correspondência não deve ser limitativa, admitindo na sua interpretação as mensagens enviadas e recebidas a partir de instrumentos fornecidos pela empresa, quer no local de trabalho, quer fora dele.²⁶⁷

Este mostrou-se um caso paradigmático pois, além de ter produzido duas decisões diferentes no TEDH, procedeu à análise de questões fundamentais como a aplicabilidade do artigo 8.º da CEDH no âmbito das relações laborais. Além disso, analisou, pela primeira vez, uma situação que envolveu uma entidade privada.

²⁶⁶ Acórdão do TEDH: BĂRBULESCU V. ROMÊNIA, de 05.09.2017, proferido no âmbito do processo n.º 61496/08, parágrafo 80, disponível para consulta [aqui](#): “*an employer’s instructions cannot reduce private social life in the workplace to zero. Respect for private life and for the privacy of correspondence continues to exist, even if these may be restricted in so far as necessary*”.

²⁶⁷ Confirmar parágrafo 74 do Acórdão.

Apesar desta decisão não representar uma mudança no pensamento tradicional, realça a importância de as empresas aplicarem políticas claras relativamente à utilização e monitorização da *Internet* e correio eletrónico. O Tribunal afirmou, de forma clara, que a entidade empregadora tem legitimidade para tomar medidas de controlo das comunicações e do uso da *Internet*, mas deve fazê-lo de forma adequada e suficiente, devendo as mesmas serem completamente compreendidas pelos seus trabalhadores.²⁶⁸

3.4.6. A utilização algorítmica no processo de avaliação de desempenho do trabalhador

O processo de avaliação de desempenho no ambiente laboral é fundamental para uma equilibrada gestão de equipas. Através da sua implementação é possível identificar pontos forte e áreas de melhoria, permitindo ao trabalhador alinhar-se com os objetivos da empresa.

Com a evolução tecnológicas novos métodos e ferramentas, como os algoritmos baseados em IA, têm sido incorporados de forma a tornar estes processos mais céleres, precisos e justos. Segundo um estudo elaborado pela PWC, cerca de 40% das empresas internacionais utilizam sistemas de IA para funções de recursos humanos.²⁶⁹ Ainda assim, a sua implementação não está isenta de desafios e considerações éticas.

É indiscutível a capacidade dos algoritmos em analisar uma vasta quantidade de dados relativos ao desempenho do trabalhador, tais como a produtividade, a qualidade do trabalho, o cumprimento de horários, etc. Através da sua utilização é possível um processamento de dados de forma detalhada, célere e, alegadamente, imparcial. Contudo, nem sempre é esta a realidade. Como refere um estudo da UGT²⁷⁰

²⁶⁸ Confirmar parágrafo 14 do Acórdão.

²⁶⁹ PWC, *Artificial Intelligence in HR: a No-brainer*, 2018, p. 2.

²⁷⁰ SERVICIO DE ESTUDIOS DE LA CONFEDERACIÓN, *Las decisiones algorítmicas en las relaciones laborales*, 8 febrero 2021, n.º 20, p. 4: “los algoritmos no son empáticos: no descifran, ni comprenderán a corto plazo, los conceptos de humanidad o probidad. No olvidan, no perdonan, no poseen conciencia de su propia falibilidad. No poseen escala de valores, ni distinguen las diferencias culturales o sociales intrínsecas a los mismos. No presentan sentido común e incluso, en determinadas habilidades perceptivas, demuestran la misma capacidad de un bebé. Y por si esto no fuese suficiente, no se autocorrigen bajo criterios de comprensión, equilibrio, justicia, ética, moralidad u otredad. Hoy por hoy, la comprensión humana sigue, y seguirá siéndolo a largo plazo, imprescindible para tomar decisiones bajo criterios justos y equitativos”.

Os algoritmos não são empáticos: não compreendem, nem compreenderão a curto prazo, os conceitos de humanidade ou de probidade. Não esquecem, não perdoam, não têm consciência da sua própria falibilidade. Não possuem uma escala de valores, nem distinguem as diferenças culturais ou sociais que lhes são intrínsecas. Não têm senso comum e até, em certas capacidades preceptivas, demonstram a mesma capacidade de um bebé. E se isto não bastasse, não se autocorrigem sob critérios de compreensão, equilíbrio, justiça, ética, moral ou alteridade. Atualmente, a compreensão humana continua a ser, e continuará a ser a longo prazo, essencial para tomar decisões justas e equitativas. tomar decisões com base em critérios justos e equitativos.

(tradução nossa)

Não podemos discordar deste entendimento sem, contudo, ter algumas reservas. Como referimos anteriormente, os algoritmos desenvolvem-se tendo por base informações previamente fornecidas que, direta ou indiretamente, podem conter referências discriminatórias. É, pois, fundamental a neutralidade aquando do “ensino” do algoritmo, optando por fornecer dados puramente objetivos. Como refere TERESA COELHO MOREIRA²⁷¹

Os algoritmos são, no final, construções humanas: eles são criados, programados e treinados por seres humanos. As escolhas feitas por estes durante a programação de um algoritmo afetam toda a operação e resultados dos mesmos. Assim, os algoritmos não estão livres de inspiração humana. Além disso, os algoritmos são treinados com dados históricos. Se esses dados forem tendenciosos contra certos indivíduos ou grupos, o algoritmo replicará o viés humano e aprenderá a discriminá-los.

Assim, como bem mencionado no Considerando 91 do RIA,

Dada a natureza dos sistemas de IA e os riscos para a segurança e os direitos fundamentais possivelmente associados à sua utilização, nomeadamente no que respeita à necessidade de assegurar um controlo adequado do desempenho de um sistema de IA num cenário real, é apropriado determinar responsabilidades específicas para os responsáveis pela implantação. Em particular, os responsáveis

²⁷¹ TERESA COELHO MOREIRA, *Gestão Algorítmica*, In *Liber Amicorum Benedita Mac Croire*, Volume II, 14 de dezembro de 2022, p. 556 e 557.

pela implantação deverão tomar medidas técnicas e organizacionais adequadas para assegurar que utilizam os sistemas de IA de risco elevado de acordo com as instruções de utilização e deverão ser equacionadas outras obrigações relativas ao controlo do funcionamento dos sistemas de IA e à manutenção de registos, se for caso disso. Além disso, os responsáveis pela implantação deverão assegurar que as pessoas encarregadas de aplicar as instruções de utilização e de supervisão humana, tal como estabelecido no presente regulamento, têm as competências necessárias, em especial um nível adequado de literacia, formação e autoridade no domínio da IA para desempenhar adequadamente essas funções. Essas obrigações não deverão prejudicar outras obrigações do responsável pela implantação em relação a sistemas de IA de risco elevado nos termos do direito da União ou do direito nacional.

Deste modo, é elementar investir numa idónea formação dos responsáveis pela implementação dos sistemas de IA, bem como num forte controlo dos mesmos, através de auditorias realizadas por entidades externas às empresas que os implementam.²⁷²

No que à avaliação de desempenho realizada por algoritmos diz respeito, importa salientar o facto de nos encontrarmos perante dados sensíveis o que, por si só, implica considerações especiais.^{273/274} Além de um tratamento à luz dos princípios do RGPD, e em particular do princípio da transparência, é fundamental garantir o respeito pelos direitos do trabalhador, nomeadamente através da garantia da privacidade e proteção dos dados ao longo de todo o seu tratamento.²⁷⁵

Outra questão fulcral em sede algorítmica são as condutas discriminatórias. É fundamental que o tratamento dos dados recolhidos assente em valores como a imparcialidade e objetividade. Como referido pela Comissão Europeia²⁷⁶

²⁷² TERESA COELHO MOREIRA, *Gestão... Ob. cit.*, p. 558.

²⁷³ Nesta linha atente-se o referido no Considerando 54 do RIA.

²⁷⁴ A este propósito veja-se o Considerando 30 do RIA que refere que: “Deverão ser proibidos os sistemas de categorização biométrica baseados em dados biométricos de pessoas singulares, como o rosto ou as impressões digitais, para deduzir ou inferir as suas opiniões políticas, a filiação sindical, as convicções religiosas ou filosóficas, a raça, a vida sexual ou a orientação sexual de uma pessoa”.

²⁷⁵ GRUPO INDEPENDENTE DE PERITOS DE ALTO NÍVEL SOBRE A INTELIGÊNCIA ARTIFICIAL, *Orientações éticas para uma IA de confiança*, criado pela Comissão Europeia em junho 2018, 2019, p. 22.

²⁷⁶ GRUPO INDEPENDENTE DE PERITOS DE ALTO NÍVEL SOBRE A INTELIGÊNCIA ARTIFICIAL, *Orientações éticas... Ob. cit.*, p. 22.

A inclusão e a diversidade têm de estar presentes em todo o ciclo de vida do sistema de IA para que a IA de confiança se torne uma realidade. Além da consideração e do envolvimento de todas as partes interessadas ao longo do processo, tal implica também que a igualdade de acesso mediante processos de conceção inclusivos e a igualdade de tratamento sejam asseguradas. Este requisito está estreitamente relacionado com o princípio da equidade.

(...)

Os conjuntos de dados utilizados pelos sistemas de IA (tanto para treino como para funcionamento) podem ser afetados pela inclusão de desvios históricos inadvertidos, bem como por lacunas e por maus modelos de governação. A manutenção de tais desvios pode dar origem a discriminação e preconceitos (in)diretos não intencionais contra determinados grupos ou pessoas, agravando o preconceito e a marginalização.

Deste modo, antes de procederem a qualquer análise baseada em sistemas de IA, as empresas devem realizar uma avaliação do impacto da sua utilização, tal como recomendado pelo RIA e consagrado no artigo 35.º do RGPD. Posteriormente, ao decidirem implementar estes sistemas de IA, é importante adotarem tecnologias sofisticadas, de encriptação e segurança cibernética, de modo a se protegerem de eventuais ciberataques.

Por fim, note-se que como desenvolvido no ponto 2.5.8., é expressamente proibida a tomada de decisões automatizadas, salvo nos casos previstos no n.º 2 do artigo 22.º do RGPD, nomeadamente em sede de consentimento. Como melhor desenvolvido no ponto 2.6.1.1., entendemos que a prestação de consentimento pelo trabalhador devidamente informado deve ser fundamento suficiente para o tratamento de dados. Face a este entendimento, o trabalhador pode, efetivamente, estar sujeito a decisões automatizadas. Não obstante, o trabalhador terá sempre a possibilidade de impugnar tais decisões, devendo, consequentemente, ser feita uma análise por entidades externas de forma a verificar se existiram fatores, por exemplo, discriminatórios na tomada de decisões.

Contudo, e uma vez que os sistemas de IA estão numa fase embrionária (tal como a legislação que os regula), entendemos que o mais seguro será proceder, após a decisão tomada pelo sistema de IA, a uma nova análise, agora pelo responsável pelo tratamento dos

dados, garantindo, desta forma, uma abordagem mais holística e compreensiva do desempenho do trabalhador.^{277/ 278}

3.5. O poder disciplinar e sancionatório da entidade empregadora com base numa análise algorítmica

No início da presente dissertação referimos que a relação laboral é caracterizada por ser uma relação de poder, de subordinação. Sendo o empregador o sujeito que detém o domínio dos meios é a ele que compete, nos termos dos artigos 97.º e 98.º do CT, o poder de direção e o poder disciplinar.²⁷⁹

Enquanto o poder de direção se caracteriza pela legitimidade de “*estabelecer os termos em que o trabalho deve ser prestado, dentro dos limites decorrentes do contrato e das normas que o regem*” (o que pode acontecer, desde logo, através de regulamento interno), o poder disciplinar valida a capacidade de julgar e punir dentro dos limites legais.²⁸⁰

No exercício do poder disciplinar o empregador tem a legitimidade de aplicar as sanções previstas no artigo 328.º, n.º 1 do CT, nomeadamente: (i) repreensão; (ii) repreensão registada; (iii) sanção pecuniária; (iv) perda de dias de férias; (v) suspensão do trabalho com perda de retribuição e de antiguidade e (vi) despedimento sem indemnização.²⁸¹

Após abertura de procedimento disciplinar e proferimento de decisão nesses termos (artigo 329.º do CT), deve a entidade empregadora aplicar a sanção decidida no prazo de três meses, sob pena de caducidade (artigo 330.º do CT).²⁸²

²⁷⁷ GRUPO INDEPENDENTE DE PERITOS DE ALTO NÍVEL SOBRE A INTELIGÊNCIA ARTIFICIAL, *Orientações...* Ob. cit., p. 18 e 19.

²⁷⁸ Neste sentido veja-se o referido pela OIT quando referiu ser necessário “[p]otenciar e gerir a tecnologia a favor do trabalho digno. Significa envolver trabalhadores e gestores na negociação da conceção do trabalho. Significa também adotar uma abordagem da inteligência artificial baseada no “ser humano no comando”, que garanta que decisões finais que afetem o trabalho sejam tomadas por seres humanos”. ORGANIZAÇÃO INTERNACIONAL DO TRABALHO, *Trabalhar para um futuro melhor*, Comissão Mundial sobre o futuro do trabalho, 2019, p. 13.

²⁷⁹ JOÃO LEAL AMADO, *Contrato de Trabalho: noções básicas...* Ob. cit., p. 213 a 219.

²⁸⁰ JOÃO LEAL AMADO, *Direito do Trabalho: Relação Individual*, 2.ª Edição, 2023, Almedina, p. 1251 a 1253.

²⁸¹ Refira-se que, sempre que seja intenção da entidade empregadora proceder ao despedimento do trabalhador, tal intenção deve constar de forma expressa na nota de culpa.

²⁸² Para uma análise mais pormenorizada confirmar LURDES DIAS ALVES, *Proteção...* Ob. cit, capítulo 8. O direito disciplinar e sancionatório, p. 37 e 38.

A aplicação de sanções disciplinares com base numa análise algorítmica é um tema de crescente relevância, sobretudo com o aumento da implementação de tecnologias de IA nos processos de recrutamento e avaliação. Da mesma forma que é possível utilizar um algoritmo para recrutar ou promover trabalhadores, também o será para despedir.^{283/284}

A promessa de objetividade e imparcialidade é uma das principais razões pelas quais as empresas estão a considerar o uso de algoritmos para fundamentar a sua utilização nos processos disciplinares.

Para facilitar a nossa análise, suportemo-nos de dois recentes casos que implicaram o despedimento de trabalhadores com base numa análise algorítmica.

O primeiro caso ocorreu com a empresa *Amazon*, que desenvolveu um sistema automatizado para medir a produtividade dos seus trabalhadores de armazém. Através deste sistema a taxa de produtividade de cada trabalhador era constantemente monitorizada, gerando avisos automáticos sobre os níveis de produção. Com base nestas informações, entre 2017 e setembro de 2018 a *Amazon* despediu do seu armazém sito em Baltimore cerca de 300 trabalhadores (o que correspondia, à data, a cerca de 10% do número de trabalhadores anuais).²⁸⁵

O segundo exemplo ocorreu no controverso caso da *TAP*. Aquando do anúncio do processo de reestruturação que implicaria a redução de pessoal, o presidente da administração do grupo *TAP* informou que a seleção de trabalhadores a integrarem o despedimento coletivo seria realizada por um algoritmo desenvolvido pela consultora Boston Consulting Group (BCG). Segundo este sistema de IA a escolha dos trabalhadores elegíveis para a rescisão do vínculo contratual seria feita com base num conjunto de critérios (variáveis do algoritmo) como o absentismo e a senioridade (idade/antiguidade).²⁸⁶

²⁸³ RICHARD A. BALES AND KATHERINE VW STONE, *The Invisible Web at Work: Artificial Intelligence and Electronic Surveillance in the Workplace*, In 41 Berkeley Journal of Employment and Labor Law 1, 10.06.2020, p. 14.

²⁸⁴ JOSÉ JOÃO ABRANTES E ISABEL VALENTE DIAS, *Regulação do uso do algoritmo nas relações laborais... Ob. cit.*, p. 42.

²⁸⁵ COLIN LECHER, *How Amazon automatically tracks and fires warehouse workers for “productivity”*, The Verge, 25.04.2019, disponível para consulta [aqui](#).

²⁸⁶ AGÊNCIA LUSA, *TAP: Boston Consulting Group escolhida para elaboração do plano de reestruturação*, Observador, 11.08.2020, disponível para consulta [aqui](#).

Estes dois exemplos mostram, de forma clara, como a utilização de algoritmos na seleção de trabalhadores se torna uma realidade cada vez mais atual. Ainda assim, note-se que em ambas as situações nos deparamos com problemas similares. No caso da *Amazon*, o processo de decisão que esteve na base do despedimento não foi transparente para os trabalhadores despedidos que, mesmo depois do despedimento, não sabiam quais eram as taxas de produtividade que tinham de atingir, nem como ou porque não as atingiram. Na *TAP*, o algoritmo referenciava as ausências dos trabalhadores, mas não diferenciava os seus motivos (e.g., falta justificada), o que suscitou a contestação dos interessados através do respetivo sindicato.

Refira-se, ainda, que no processo de despedimento promovido pela *Amazon* os trabalhadores não tinham qualquer informação de que os seus dados estavam a ser recolhidos e processados por um algoritmo.

Ora, ambas as situações descritas sofreram de vícios similares: falta de transparência, discriminação, parcialidade e arbitrariedade. Como iremos analisar infra, estes problemas podem gerar desconfiança por parte dos trabalhadores que veem os seus dados recolhidos e tratados de forma desumanizada.

A implementação de sanções assentes numa análise algorítmica deve ser acompanhada de rigorosos mecanismos de supervisão e transparência, como estipulado quer no RGPD, quer no RIA. As empresas devem garantir que os algoritmos são justos, equitativos e livres de qualquer tipo de discriminação. Além disso, é crucial que os trabalhadores tenham acesso às informações sobre como as decisões são tomadas e que possam contestar e apelar decisões que considerem infundadas.

A utilização de algoritmos na aplicação do poder disciplinar pode, de facto, trazer benefícios significativos. A eficiência e a rapidez na análise de grandes volumes de dados são algumas dessas vantagens. Com a capacidade de processar informações de forma quase instantânea, os algoritmos podem identificar padrões de comportamento que poderiam passar despercebidos em avaliações humanas, permitindo uma resposta mais adequada às infrações cometidas.

Contudo, a automatização destes processos não está isenta de riscos. Como explicado previamente, a programação dos algoritmos é realizada por pessoas, o que significa que os próprios preconceitos e limitações dos programadores podem ser incorporados no sistema, resultando em decisões enviesadas, que penalizam injustificadamente determinados grupos. A ausência de uma adequada supervisão pode exacerbar este problema, transformando a promessa de imparcialidade numa criação meramente utópica.²⁸⁷

Outra questão que se levanta diz respeito à responsabilidade. Sendo a decisão disciplinar tomada por um algoritmo, quem deve ser responsabilizado pela mesma? A empresa que utilizou o sistema, os desenvolvedores do algoritmo, ambos ou ninguém? Esta é uma pergunta complexa que implica uma análise cuidadosa, a qual teremos tempo para nos debruçarmos mais a frente neste trabalho.

De igual importância é a realização de auditorias regulares aos algoritmos utilizados para fins disciplinares, como estipulado pelo artigo 5.3 do Anexo VII do RIA. Isso inclui a revisão dos dados de entrada, no sentido de assegurar que não existem preconceitos incorporados, e a análise dos resultados obtidos, para verificar a sua conformidade com as expectativas de imparcialidade e equidade.

Além disso, a colaboração entre empresas e sindicatos é fundamental para o desenvolvimento de um quadro normativo de suporte à utilização destas tecnologias. Esta colaboração deve desenvolver-se através da criação de diretrizes claras sobre a utilização dos sistemas de IA em processos disciplinares, garantindo que os direitos dos trabalhadores são protegidos e que as decisões tomadas são justas e imparciais. Assim, as empresas que pretendam utilizar algoritmos na aplicação do poder disciplinar ou de direção devem adotar

²⁸⁷ Neste sentido veja-se o referido por ALEX J. WOOD, *Algorithmic Management: Consequences for Work Organisation and Working Conditions*, Seville: European Commission, 2021, JRC124874, p. 9: “In summary, this section has highlighted the use of algorithmic management in terms of the auto-matic disciplining of workers. Based on the algorithmic evaluation of workers outlined in the previ-ous section, firms can automatically restrict access to future work. Workers deemed to be perform-ing poorly by algorithmic evaluation systems have been found to have work automatically filtered to higher-performing workers, access to the best shifts blocked and have even been deactivated from a digital labour platform or fired from their job. However, this section has again highlighted that examples of the ideal typical form of algorithmic management in which these systems act autonomously without the input of humans is rare in practice. At a minimum, human managers can review and overrule algorithmic discipline, and in most cases it is the human manager that performs the act of discipline on behalf of the algorithm. These features of algorithmic discipline make it difficult to determine the degree to which a decision should primarily be located with a human or algorithmic actant”.

uma abordagem cautelosa e ética, mostrando-se disponíveis para reavaliar e ajustar os seus sistemas de IA.

3.5.1. A conservação dos dados pessoais do trabalhador após a cessação do vínculo contratual

Os dados coletados durante processos disciplinares e as ações realizadas como resultado são considerados dados pessoais de condenações penais e de infrações – artigo 10.º do RGPD. Como tal, é fundamental as empresas criarem procedimentos que permitam a sua adequada organização e segurança, garantido os direitos e liberdades dos seus titulares.²⁸⁸

No que ao período de conservação diz respeito, quer o RGPD, no artigo 5.º, n.º 1, al. e), quer a LPDP, no artigo 21.º, estipulam que os dados devem ser conservados pelo período estritamente necessário à prossecução da finalidade da recolha. Apesar de não existir um período temporal demarcado, a CNPD tem entendido que o limite máximo da conservação dos dados do trabalhador despedido é de um ano sobre a data da cessação do contrato.²⁸⁹

Entendemos que este também é o prazo estipulado pela lei laboral, nos termos do artigo 337.º, n.º 1 do CT que determina que “[o] crédito de empregador ou trabalhador emergente de contrato de trabalho, da sua violação ou cessação prescreve decorrido um ano a partir do dia seguinte àquele em que cessou o contrato de trabalho”. Assim, o empregador deverá, por exemplo, preservar os recibos de vencimento pelo prazo de um ano, sob pena de não conseguir fazer prova da efetuação desses pagamentos.

Note-se, contudo, que existem determinados dados objeto de tratamento cujo prazo será maior. Refira-se a título de exemplo os dados referentes aos processos de recrutamento, cuja conservação deverá ser de 5 anos, nos termos do artigo 32.º do CT, e os dados referentes a serviços de segurança e de saúde no trabalho quando esteja em causa o património genético, cujo prazo será de 40 anos, nos termos do artigo 46.º, n.º 3 da Lei n.º 102/2009.

²⁸⁸ SIMÃO DE SANT’ANA E VITORINO GOUVEIA, *O RGPD... Ob. cit.*, p. 291.

²⁸⁹ Neste sentido vejam-se as seguintes decisões: Comissão Nacional de Proteção de Dados, Deliberação n.º 5981/2014, de 1 de julho de 2014 e Deliberação n.º 3996/2014, de 22 de abril de 2014.

Assim, apesar da regra geral de conservação dos dados pessoais em matéria laboral ser de um ano, existem determinadas circunstâncias que, face às suas necessidades de proteção, implicam uma conservação por períodos superiores.

Independentemente do prazo, as empresas devem informar os trabalhadores sobre a sua conservação, em que moldes esta ocorre e durante que período. Esta transparência é fundamental para manter a confiança dos trabalhadores e garantir que os seus direitos são respeitados.

Ademais, a empresa deverá garantir a segurança dos dados conservados através da implementação das medidas necessárias para prevenir acessos não autorizados, perdas ou destruições.²⁹⁰

Terminado o período de conservação, a entidade empregadora deverá estabelecer procedimentos específicos para uma correta e segura eliminação dos dados recolhidos.

3.6. Algoritmo como novo desafio legal

Os artigos científicos que abordam a temática algorítmica tendem a iniciar-se com uma frase quase icónica que exprime a novidade e a vantagem que estes novos mecanismos acarretam.

A dependência de sistemas informáticos é cada vez maior nas económicas modernas que os utilizam para serem mais competitivas. A análise de dados tem crescido fortemente nos últimos anos, sendo o recurso a tecnologias de IA crucial para permitir às empresas analisarem quantidades elevadas de dados num curto espaço de tempo.²⁹¹ Através da sua utilização as empresas conseguem prever interesses dos seus clientes e comportamento futuros, antecipando eventuais sucessos ou infortúnio económicos e servindo de base técnico-funcional de novos modelos de negócio.²⁹²

²⁹⁰ Confirmar Considerando 83 e artigo 32.º do RGPD.

²⁹¹ JOSÉ JOÃO ABRANTES E ISABEL VALENTE DIAS, *Regulação do uso do algoritmo nas relações laborais... Ob. cit.*, p. 38.

²⁹² WOLFGANG HOFFMANN -RIEM, *Controle do Comportamento por Meio de Algoritmos: um Desafio para o Direito*, RDP, Edição especial, 2019, p. 126.

Inegáveis são as vantagens que estes sistemas de IA aportam para a economia. Ainda assim, é fundamental não desconsiderar os perigos que a sua utilização implica. Como referido por WOLFGANG HOFFMANN -RIEM²⁹³

Com o uso de algoritmos, inauguram-se chances consideráveis em diversos campos – ou quase todos – do desenvolvimento social. Todavia, essa averiguação também vem acompanhada de riscos consideráveis, p. ex., em virtude das possibilidades de influência e até manipulação de comportamentos, perigos à proteção da privacidade ou da propriedade intelectual, vulnerabilidades crescentes também de organizações vitais como as dos serviços públicos e muito mais. Do mesmo modo que em outros campos de inovação, trata-se, na área de informática, do ajuste correto entre o espírito de inovação e a responsabilidade pela inovação.

3.6.1. As vantagens da utilização algorítmica na relação laboral

A utilização de novas tecnologias no âmbito laboral representa um mecanismo precioso nas diversas fases da relação contratual.

Na fase de recrutamento a utilização de sistemas de IA auxilia os recursos humanos no desenvolvimento da sua atividade, permitindo-lhes que tenham uma atuação cada vez mais estratégica e decisiva na contratação.²⁹⁴ Como referido por MIRANDA BOGEN e AARON RIEKE, as entidades empregadoras optam pela implementação destas ferramentas de forma a (i) reduzir o tempo e os custos gasto com a contratação; (ii) maximizar a qualidade da contratação e (iii) conseguir atingir uma maior diversidade de trabalhadores^{295, 296}.

No desenrolar da relação contratual a utilização algorítmica permite uma gestão automatizada, facilitando a distribuição de tarefas, a avaliação de desempenho, o controlo dos tempos de trabalho, etc. Note-se que todos estes fatores serão analisados de forma

²⁹³ WOLFGANG HOFFMANN -RIEM, *Controle... Ob. cit.*, p. 127.

²⁹⁴ MARYKATE ZUKIEWICZ, MELISSA A CLARK, LIBBY MAKOWSKY, *Implementation of the Teach For America Investing in Innovation Scale-Up*, In Mathematica Policy Research, Princeton, 2015, p. 11-15.

²⁹⁵ Refira-se que o facto de os sistemas de IA funcionarem através de um processo (tendencialmente) neutro, permite afastar o preconceito e a subjetividade humana no processo de recrutamento, aumentando, consequentemente, a diversidade no local de trabalho. Note-se que afirmamos “tendencialmente”, uma vez que existe a possibilidade de o próprio algoritmo assumir uma conduta discriminatório, como iremos analisar melhor infra.

²⁹⁶ MIRANDA BOGEN, AARON RIEKE, *Help wanted... Ob. cit.*, p. 6 e 7.

minuciosa, desde logo pelo facto de o algoritmo desenvolver, produzir e acumular raciocínios aprendidos, aplicando-os de forma exponencialmente mais rápida do que o ser humano.

Por fim, podemos ainda ter um algoritmo que, face à análise dos dados adquiridos durante a relação laboral, permite determinar o trabalhador “mais apto” a ser despedido.

Esta abordagem é conhecida por *People Analysis* ou *HR Analysis* que, segundo MATTHEW BODIE, MIRIAM A. CHERRY, MARIA L. MCCORMICK e JINTONG TANG,²⁹⁷ se traduz

[n]um processo ou método de gestão de recursos humanos baseado na utilização de “grandes volumes de dados” para obter informações sobre o desempenho profissional. A ideia central é que o julgamento subjetivo não estruturado não é rigoroso nem fiável como forma de avaliar o talento ou criar políticas de recursos humanos. Em vez disso, os dados - grandes conjuntos de dados objetivos, geralmente quantitativos - devem constituir a base para a tomada de decisões no espaço de RH.

(tradução nossa)

Através da sua adoção as empresas começam a olhar para os seus problemas internos como correlações em vez de causalidades, permitindo formular verdadeiros cenários probabilísticos. Como explica LAURA SCHERTEL MENDES e MARCELA MATTIUZZO²⁹⁸

Durante muito tempo, a ciência e a descoberta científica funcionaram por meio da busca por causalidades. Esse é um aspeto desenvolvido e estimulado na pesquisa científica, e geralmente é visto como o único modo por meio do qual seria possível compreender o que ocorre ao nosso redor. Com Big Data, contudo, a causalidade perde espaço para as correlações. Uma correlação é a probabilidade de um evento ocorrer caso outro evento também se realize. É uma relação estatística entre tais acontecimentos.

²⁹⁷ MATTHEW BODIE, MIRIAM A. CHERRY, MARIA L. MCCORMICK, JINTONG TANG, *The Law and Policy of People Analytics*, Legal Studies Research Paper Series, Saint Louis University School of Law, No. 2016-6, p. 3: “*People analytics is a process or method of human resources management based on the use of “big data” to capture insights about job performance. The core idea is that unstructured subjective judgment is not rigorous or trustworthy as a way to assess talent or create human resources policies. Instead, data— large pools of objective, generally quantitative data—should form the foundation for decisionmaking in the HR space*”.

²⁹⁸ LAURA SCHERTEL MENDES E MARCELA MATTIUZZO, *Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia*, RDU, Porto Alegre, Volume 16, n.º 90, 2019, p. 44.

(tradução nossa)

Acresce que, como refere JESÚS R. MERCADER UGUINA²⁹⁹

o empresário não tem de adquirir um novo algoritmo cada vez que pretender expandir ou reformar a sua empresa; tem apenas de o adaptar aos novos parâmetros de referência que necessita em cada momento.

(tradução nossa)

É a conjugação de todos estes fatores que torna a implementação destes sistemas aliciante aos empregadores. Contudo, como bem referido por FREDERICO VENTURA SEQUEIRA, não estamos perante cenários infalíveis, pelo que³⁰⁰

é necessário não nos deixarmos iludir com a ideia de que os números, rectius, os algoritmos não mentem, antes atendendo efetivamente ao conteúdo, à substância que transparece uma realidade bastante diferente e, até certo ponto, assustadora.

São inúmeras as fragilidades da utilização de algoritmos, pelo que a sua implementação deve ser devidamente ponderada e o controlo frequente. Passemos à análise de algumas delas.

3.6.2. A discriminação algorítmica

Não obstante as vantagens da utilização algorítmica abordadas no ponto anterior, importa percebermos se, na prática, estes sistemas de IA são capazes de cumprir o que prometem, nomeadamente, eliminar o preconceito humano e oferecer decisões objetivas.³⁰¹

É fundamental não cair no erro de coisificar a pessoa humana, reduzindo os seus direitos, liberdades e garantias.³⁰² Neste sentido, os algoritmos devem ser utilizados enquanto meios

²⁹⁹ JESÚS R. MERCADER UGUINA, *Algoritmos e inteligencia artificial en el derecho digital del trabajo*, tirant lo blach, Valencia, 2022, p. 70.

³⁰⁰ FREDERICO VENTURA SEQUEIRA, *O algoritmo no tecido empresarial: Das vicissitudes de contratação ao despedimento de trabalhadores – Uma arma nociva que necessita de ser desarmada?*. In *Anuário da Proteção de Dados*, 2022, Coordenado por FRANCISCO PEREIRA COUTINHO e GRAÇA CANTO MONIZ, Lisboa: CEDIS, p. 77 e 78.

³⁰¹ TERESA COELHO MOREIRA, *Direito do Trabalho: Relação Individual*, 2.^a Edição, 2023, Almedina, p. 354.

³⁰² ROBERTO FERNÁNDEZ FERNÁNDEZ, *Selección...* Ob. cit., p. 57.

para chegar a um fim, facilitando a atuação humana em processos que, sem a sua ajuda, seriam menos céleres e mais complexos.

Na atualidade, o pináculo dos valores de uma vivência em sociedade assenta na antidiscriminação, ou seja, na aceitação da diferença. A consagração da proibição da discriminação é transversal a todas as áreas do Direito, encontrando-se consagrada, desde logo, na Constituição da República Portuguesa no seu artigo 13.º com a denominação “princípio da igualdade”. Em matéria laboral, o princípio da igualdade está reconhecido no artigo 24.º do CT, tendo expressão ao longo de todo o diploma.

O ato discriminatório pode ocorrer de forma direta ou indireta.^{303/ 304} No primeiro caso falamos de uma conduta motivada pelo facto de o sujeito discriminado estar inserido num grupo diferenciado (e.g., ser mulher ou homem, ser negro ou caucasiano; ser de uma determinada faixa etária, etc.). No segundo, referimo-nos a uma conduta que, embora aparentemente neutra, tem um efeito discriminatório para determinadas pessoas, pelo que a intenção do agente tem pouca relevância.³⁰⁵ É na discriminação indireta que inserimos, regra geral, a análise algorítmica, o que coloca diversas questões.

Um dos principais problemas referentes às condutas discriminatórias promovidas por algoritmos diz respeito aos temas de prova, uma vez que não é uniforme a necessidade de verificação de “consciência” e/ou “intencionalidade” para que o ato praticado se considere discriminatório. Ainda assim, é do nosso entendimento que tais elementos não são fundamentais para a categorização de uma conduta nesses termos, desde logo pelo facto destes mecanismos não possuírem subconsciência. É, pois, elementar concluir, como refere MILENA DA SILVA ROUXINOL,³⁰⁶ que

os atos deliberados de discriminação só podem ocorrer através de sistemas algorítmicos se a máquina for dolosamente instruída nesse sentido pelo humano que a funcionaliza em seu proveito.

³⁰³ BRUNO MESTRE, *Direito Antidiscriminação – uma perspetiva europeia e comparada*, Vida Económica, 2020, p. 51 a 73.

³⁰⁴ TERESA COELHO MOREIRA, *Direito do Trabalho: Relação Individual... Ob. cit.*, p. 350.

³⁰⁵ MILENA DA SILVA ROUXINOL, *O agente algorítmico... Ob. cit.*, ponto 2.2.

³⁰⁶ MILENA DA SILVA ROUXINOL, *O agente algorítmico... Ob. cit.*, ponto 2.2.

Isto acontece uma vez que os algoritmos são sistemas de *machine learning*, que aprendem através de dados previamente inseridos e da própria prática decisória, facilitando decisões enviesadas.^{307/308} Por se desenvolverem nestes termos os sistemas algorítmicos tornam-se obscuros, pois a única forma de existir um verdadeiro controlo pelas autoridades reguladoras é descobrindo quais as informações providas em primeira linha. Como refere JOÃO LUÍS NOGUEIRA MATIAS e RICARDO ANTÓNIO MAIA DE MORAIS JÚNIOR³⁰⁹

*não é à toa que os algoritmos são denominados, muitas vezes, de caixas pretas, pois, dependendo da metodologia utilizada para o aprendizado da máquina, será praticamente impossível verificar seus critérios ou sua árvore de decisão.*³¹⁰

A discriminação algorítmica ocorre pela influência de diversos fatores, sendo possível, no entendimento de LAURA SCHERTEL MENDES e MARCELA MATTIUZZO,³¹¹ identificarmos quatro tipos de discriminação:

- (i) discriminação por erro estatístico, decorrente de uma errada contabilização dos dados devida a falhas na criação do algoritmo (e.g., *credit score*);
- (ii) discriminação por generalização, segundo a qual o algoritmo teoricamente funciona corretamente, mas, por algum motivo, relaciona os indivíduos a grupos por possuírem determinadas características (e.g., o número de trabalhadores despedidos por má conduta eram todas de uma determinada nacionalidade e o algoritmo associa a nacionalidade do candidato a emprego como um possível trabalhador com má conduta);

³⁰⁷ SPENCER MAINKA, *Algorithm-Based...* Ob. cit., p. 811 a 814.

³⁰⁸ No mesmo sentido veja-se TERESA COELHO MOREIRA, *Direito do Trabalho: Relação Individual...* Ob. cit., p. 357.

³⁰⁹ JOÃO LUÍS NOGUEIRA MATIAS, RICARDO ANTÓNIO MAIA DE MORAIS JÚNIOR, *Discriminação algorítmica na relação de emprego: eficiência económica, inteligência artificial e fragilidade do emprego*, Revista do Tribunal Superior do Trabalho, Porto Alegre, n.º 90, n.º 2, 2024, p. 137 e 138.

³¹⁰ TERESA COELHO MOREIRA, *Direito do Trabalho: Relação Individual...* Ob. cit., p. 350.

³¹¹ LAURA SCHERTEL MENDES E MARCELA MATTIUZZO, *Discriminação Algorítmica...* Ob. cit., p. 51 a 53.

- (iii) discriminação pelo uso de informação sensível. Apesar do algoritmo, matematicamente, atuar corretamente, a utilização de dados sensíveis promove discriminação (e.g., a discriminação das minorias pode perpetuar-se);^{312/313} e
- (iv) discriminação limitadora do exercício de direitos. Também neste tipo de discriminação podemos observar que os cálculos algoritmos estão corretos, mas, ainda assim, reduzem os direitos dos seus titulares. Aqui não está em causa o tipo de dados tratados, mas a correlação entre a informação utilizada pelo algoritmo e o exercício de um direito.

São inúmeras as decisões discriminatórias tomadas por algoritmos, remontando o primeiro caso relatado à década de 70. Nesse período apenas organizações importantes utilizavam sistemas de IA, mas a Faculdade de Medicina do Hospital de St. George, em Londres, decidiu proceder à criação do seu próprio algoritmo visto que anualmente recebia mais de 12 candidaturas para cada uma das suas 150 vagas.³¹⁴

O problema do algoritmo criado pelo Hospital de St. George incidiu nos dados inseridos, que se mostravam racistas e xenófobos, uma vez que, por exemplo, interligavam os motivos de rejeição de candidaturas passadas para determinarem a rejeição de candidaturas atuais (e.g., motivos de maternidade, local de nascimento, nomes de nascimento³¹⁵, etc.).

³¹² Como referem LAURA SCHERTEL MENDES E MARCELA MATTIUZZO, *Discriminação Algorítmica... Ob. cit.*, p. 54, «[a]qui, a necessidade de proteção difere da necessidade advinda da discriminação por generalização, na medida em que não se trata simplesmente de uma violação decorrente da categorização incorreta de uma pessoa “atípica”; ao contrário, nesse caso, todas as pessoas do grupo são afetadas. Isso porque a discriminação resultante do uso de informações sensíveis pode ser, e muitas vezes é, estatisticamente consistente. Contudo, por tratar-se de grupos historicamente discriminados, é um dos tipos mais perversos de discriminação, ao reforçar o tratamento discriminatório e automatizá-lo, tornando mais difícil para os membros de tais agrupamentos superarem determinada situação prejudicial. Esse uso de características discriminatórias pode ser encontrado especialmente no setor de seguros, onde nacionalidade e gênero, por exemplo, podem ser utilizados como critérios negativos em uma avaliação de risco de crédito».

³¹³ TERESA COELHO MOREIRA, *Direito do Trabalho: Relação Individual... Ob. cit.*, p. 350 a 352.

³¹⁴ FREDERICO VENTURA SEQUEIRA, *O algoritmo... Ob. cit.*, p. 82.

³¹⁵ A este propósito, veja-se o estudo realizado por RUPA BANERJEE, JEFFREY G. REITZ, PHIL OREOPOULOS, *Do Large Employers Treat Racial Minorities More Fairly? An Analysis of Canadian Field Experiment Data*, In *Canadian Public Policy*, University of Toronto Press, Vol. 44, no. 1, 2018, p. 2 e 3, que demonstrou que candidatos com nomes indianos, paquistaneses e chineses tendem a ter cerca de 28% menos chances de obter um convite de entrevista a emprego.

Por fim, em 1988 a Comissão de Igualdade Racial do governo britânico considerou o Hospital culpado de discriminação de cerca de 72.000 candidatos.³¹⁶

Este caso mostra, de forma evidente, a necessidade de uma atuação proativa de todas as entidades reguladoras e, em particular, de auditores, de modo que a aplicação destas novas tecnologias atuem de forma isenta e igualitária na análise dos dados. Este também deve ser um esforço posto em prática pelas empresas, adotando sistemas de IA atuais e competitivos.

3.6.3. As decisões automatizadas

Previamente³¹⁷ abordamos o direito do titular dos dados em não ficar sujeito a nenhuma decisão tomada exclusivamente com base num tratamento de dados automatizado, i.e., sem qualquer intervenção humana – artigo 22.º, n.º 1 do RGPD. Esta limitação está intrinsecamente ligada com a intenção do legislador em prevenir possíveis condutas discriminatórias levadas a cabo por algoritmos.

Como analisado, apenas nas situações elencadas no artigo 22.º, n.º 2 do RGPD é que há a possibilidade da tomada de decisões sem qualquer interferência humana, nomeadamente: (i) se se mostrarem necessárias para a celebração ou execução de um contrato entre o titular dos dados e um responsável pelo tratamento; (ii) se autorizadas pelo direito da União ou pelo Estado-Membro a que o tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou (iii) se baseadas no consentimento explícito do titular dos dados.

No que concerne à autorização da utilização das decisões automatizadas pelo direito da União Europeia ou pelo Estado-Membro dificuldades de compreensão não surgem. Por outro lado, relativamente ao consentimento, partilhamos o mesmo entendimento desenvolvido no ponto 2.6.1.1.

Assim, as dúvidas poderão surgir por referência à primeira exceção, i.e., a possibilidade de utilização das decisões automatizadas com fundamento na necessidade das mesmas para a

³¹⁶ Para um maior desenvolvimento das consequências para o Hospital de St. George, confirmar SOLON BAROCAS & ANDREW D. SELBST, *Big Data's Disparate Impact*, California Law Review, Vol. 104, 2016, p. 682.

³¹⁷ Recuperar o desenvolvido no ponto 2.5.8.

celebração ou execução de um contrato entre o titular dos dados e o responsável pelo tratamento (entre o trabalhador e o empregador). Façamos uma análise concreta sobre a possibilidade da sua utilização nas diferentes fases contratuais.

...2. Fase de recrutamento

Das três fases que de seguida iremos analisar, a utilização de decisões automatizadas é de mais fácil compreensão na fase de recrutamento.

O processo de seleção e recrutamento de trabalhadores sempre foi alvo de críticas por se mostrar, via regra, tendencioso. (In)conscientemente os responsáveis pelos recursos humanos praticam atos discriminatórios tendo por base fatores como a idade, raça, sexo, etc.

Apesar de na atualidade características como a diversidade, *soft-skills* e domínio linguístico serem valorizadas, a verdade é que existem fatores que, nos dias de hoje, ainda têm um forte peso (e.g., a cunha). Assim, quando a fase de seleção é desenvolvida apenas por humanos, frequentemente currículos que seriam, objetivamente, de maior relevância, acabam por ser colocados em segundo plano.

A utilização de decisões automatizadas nesta fase é, no nosso entender, muito vantajosa quer para os recursos humanos, quer para o próprio candidato a emprego.

Relativamente aos primeiros é importante referir que a atuação humana se pode mostrar pouco viável face ao elevado número de dados para tratamento. Para uma empresa que receba centenas de currículos não é humanamente rentável analisar, individualmente, cada uma das candidaturas de forma a selecionar os potenciais candidatos a emprego. Deste modo, é inquestionável que a utilização de sistemas de IA permite, desde logo, a redução do tempo gasto na análise de currículos e na procura de candidatos, tornando todo o processo de recrutamento mais célere e económico.³¹⁸ Como explicado por JÉSUS R. MERCADER UGUINA³¹⁹

³¹⁸ “Y además las TIC permiten acceder a un gran volumen de información y a su tratamiento rápido y barato mediante la creación de los correspondientes algoritmos que a través de la elaboración de perfiles acceden al conocimiento detallado de cuándo, cómo, dónde y con qué resultado se ha trabajado”, Tribunal do Trabalho, n.º 33 de Madrid, sentença 53/2019, de 11 de fevereiro de 2019, disponível para consulta [aqui](#).

³¹⁹ JESÚS R. MERCADER UGUINA, *Algoritmos...* Ob. cit., p. 76: «Las funciones algorítmicas permiten, una vez definido en detalle un perfil profesional determinado (titulación, años de experiencia, etc., y unos pesos

As funções algorítmicas permitem, uma vez definido em pormenor um determinado perfil profissional (qualificações, anos de experiência, etc., e pesos associados a cada uma destas características), extrair as informações pertinentes dos “CV” dos candidatos e calcular a correspondência mais exata com o perfil desejado.

(tradução nossa)

Quanto aos segundos, os candidatos a emprego conseguem obter uma maior objetividade referente ao processo decisório (evitando condutas discriminatórias), elemento fundamental quando a possibilidade de contratação acontece nesta fase. Além disso, o facto de os dados serem analisados por um sistema de IA permite que um maior número de candidatos participe no processo de seleção. Não obstante o aumento das candidaturas, o processo torna-se mais célere.

Note-se que falamos de decisões automatizadas referentes à seleção de trabalhadores e não à sua contratação. Assim, entendemos que o processo de escolha de candidatos a emprego poderá ser realizado por um algoritmo criado pela empresa com esse intuito, mas a execução de entrevistas para apurar qual o melhor candidato para finalizar a contratação deverá ser cumprida por um humano. Isto porque, não obstante existirem sistemas de IA com capacidade de análise de expressões faciais e reconhecimento de comportamentos, os sistemas utilizados para este efeito nas empresas não são os mais adequados uma vez se tratarem de sistemas de *machine learning* e não de *deep learning*.³²⁰

Além disso, a contratação de um trabalhador implica, frequentemente, a sua inserção numa equipa com a qual se terá de relacionar. É, pois, fundamental que os representantes dessa equipa consigam analisar diretamente (e não através de um sistema informático) o perfil, a postura e a sinergia do seu potencial colega. Apesar de estarmos a caminhar para um mundo cada vez mais partilhado com a inteligência artificial, não podemos descurar da autonomia

asociados a cada una de esas características), extraer de los "currícula" de los candidatos la información relevante y calcular el más preciso ajuste al perfil deseado».

³²⁰ A este propósito, é importante ter em consideração que os diversos sistemas de IA que atualmente utilizamos para conversar e/ou fazer questões, como é o caso do ChatGPT, são sistemas de *deep learning*. A implementação de sistemas de IA de *deep learning* implicariam um grande investimento por parte das entidades empregadoras pelo que, frequentemente, os sistemas utilizados no âmbito laboral são apenas de *machine learning* (menos desenvolvidos).

e singularidade humanas, caracterizadas, em grande parte, pelas relações interpessoais partilhadas.³²¹

Assim, através da conjugação da tecnologia e da análise humana entendemos ser possível realizar processos de recrutamento mais justos, eficazes e eficientes.

...3. Fase de avaliação de desempenho

Para analisarmos a possível aplicabilidade das decisões automatizadas nos processos de avaliação de desempenho devemos fazer uma divisão entre processos de avaliação quantitativos e processos de avaliação qualitativos.

Os processos de avaliação quantitativos correspondem a sistemas de avaliação por escala, i.e., o avaliando recebe uma cotação para cada parâmetro a avaliar (e.g., uma avaliação numa escala de 1 a 5 para elementos como assiduidade, pontualidade, trabalho em equipa, etc.). São, portanto, processos puramente métricos e objetivos. A atuação algorítmica nestes sistemas é unicamente aritmética, ou seja, o algoritmo limita-se a realizar um cálculo em conformidade com o peso de cada elemento da avaliação e com a cotação atribuída. Através desse cálculo é adjudicada uma nota ao trabalhador.

Face à objetividade destes sistemas entendemos que a inexistência de atuação humana durante o processo de análise e decisão é aceitável, não colocando em causa a objetividade da decisão. Compreenda-se que, como iremos referir mais à frente neste trabalho, isto não significa dizer que não é necessário um controlo contínuo quer por parte dos responsáveis pelo tratamento dos dados, quer pelos responsáveis pela implementação do sistema algorítmico.

Por outro lado, no que diz respeito aos processos de avaliação subjetivos, assentes na apresentação de um comentário sobre o trabalho realizado pelo trabalhador, a utilização de um algoritmo para atribuir uma cotação (quantitativa ou qualitativa³²²) pode mostrar-se desafiante.

³²¹ Refira-se, ainda, que os algoritmos com capacidade de leitura de expressões faciais podem discriminar, ainda que involuntariamente, um candidato a emprego quando, por exemplo, o mesmo sofra de paralisia facial.

³²² Não obstante a avaliação ser subjetiva a nota final a atribuir ao trabalhador poderá ser quantitativa (e.g., numa escala de 1 a 5) ou qualitativa (e.g., cumpriu as expectativas, ficou aquém das expectativas).

Os sistemas utilizados para analisar elementos subjetivos (como texto e imagem) denominam-se algoritmos de processamento de linguagem natural (NPL).³²³ Através destes mecanismos é possível, no âmbito empresarial, determinar se os trabalhadores expressam opiniões positivas, negativas ou neutras sobre os diversos temas questionados.³²⁴

A implementação de mecanismos de NPL podem ter duas finalidades: (i) a apresentação de resumos sobre as avaliações realizadas³²⁵ ou (ii) a atribuição de uma avaliação (qualitativa ou quantitativa) tendo por base o *feedback* recebido. Apesar de na primeira situação não falarmos de uma decisão puramente automatizada – uma vez que para a atribuição de uma avaliação final o responsável de recursos humanos terá de intervir analisando o resumo apresentado pelo sistema de IA –, o mesmo não acontece no segundo caso, no qual a máquina além de analisar os diversos *feedbacks* atribui uma nota final tendo por base essa avaliação.

Apesar da ausência de intervenção humana, entendemos que, ainda assim, é possível admitir decisões automatizadas nestes moldes. Para tanto é necessário um adequado desenvolvimento do algoritmo a aplicar, o qual deverá ter capacidade para analisar texto e compreender um diverso leque de palavras³²⁶, de modo a não bloquear ou desconsiderar determinadas realidades quando confrontado com assuntos para os quais não tenha sido devidamente programado.

É importante destacar que a aplicação de sistemas de NPL nos locais de trabalho tem recebido particular aderência nos últimos anos, permitindo aos trabalhadores intervirem em questões importantes no seio laboral e empresarial. A título de exemplo, refira-se a implementação dos denominados “*pulse survey*” que se traduzem em curtos questionários,

³²³ Os métodos de NPL podem utilizar técnicas de aprendizagem de *machine learning* ou *deep learning*.

³²⁴ Em termos muito sumários, o algoritmo é treinado de forma a “compreender” o significado das palavras: analisa, individualmente, cada palavra e o seu significado e, posteriormente, chega a um resultado no qual determina se a frase apresentada é positiva ou negativa. Para uma melhor compreensão sobre o funcionamento dos mecanismos NPL veja-se: DATA SKILL UP LLC, *Natural Language Processing in Employee Sentiment Analysis, How NPL Transforms Unstructured Data into Actionable Employee Insights*, Sep 27, 2024 e ELIZABETH D. LIDDY, *Natural Language Processing*, In *Encyclopedia of Library and Information Science*, 2nd Ed. NY. Marcel Decker, Inc.

³²⁵ ADITYA JAIN, GANDHAR KULKARNI, VRAJ SHAH, *Natural Language Processing*, International Journal of Computer Sciences and Engineering, Volume 6, Issue 1, E-ISSN: 2347-2693, p. 165 e 166.

³²⁶ ERIK CAMBRIA, SOUJANYA PORIA, ALEXANDER GELBUKH, MIKE THELWALL, *Sentiment Analysis Is a Big Suitcase*, IEEE Intelligent Systems, Volume 32, Issue 6, November/December 2017, p. 74-80.

realizados com uma determinada frequência, que visam monitorizar o estado de satisfação e envolvimento dos trabalhadores na empresa.³²⁷

...4. Fase de despedimento

Por último, é essencial compreendermos se é possível a aplicação de decisões automatizadas em sede de despedimento. Para tanto, vamos dividir esta análise entre (i) despedimento coletivo e (ii) despedimento por facto imputável ao trabalhador (justa causa de despedimento).

O despedimento coletivo, previsto e regulado a partir do artigo 359.º do CT, é uma das três modalidades de despedimento por motivos objetivos.³²⁸ A entidade empregadora recorre a este mecanismo quando verificadas circunstâncias externas às partes, nomeadamente flutuações no mercado que exijam ao empregador uma reestruturação da empresa no sentido de a manter ativa.³²⁹

A utilização de algoritmos para processos de despedimento coletivo tem vindo a receber significativa adesão por parte das empresas que encontram nestes mecanismos a objetividade necessária para determinar quais os trabalhadores a serem selecionados tendo por base um conjunto de fatores (e.g., produtividade, assiduidade, antiguidade, etc.).

Partilhamos a mesma opinião nesta matéria. O despedimento coletivo, como o próprio nome indica, é um despedimento assente em motivos objetivos. A utilização de um sistema algorítmico para determinar quais os trabalhadores a serem selecionado parece-nos bastante eficaz, permitindo uma análise mais eficiente, pormenorizada e objetiva.

³²⁷ RACHIT GARG, ARVIND W KIWELEKAR, LAXMAN D NETAK, AKSHAY GHODAKE, *I-Pulse: A NPL based novel approach for employee engagement in logistics organization*, International Journal of Information Management Data Insights, 2021, p. 4.

³²⁸ A nossa análise não incidirá sobre as restantes modalidades de despedimento coletivo, i.e., despedimento por extinção de posto de trabalho e despedimento por inadaptação, por não se mostrarem eficientes para a aplicação algorítmica. A primeira, porque a eventual aplicação algorítmica seria apenas para proceder à análise dos setores menos produtivos e que poderiam ser absorvidos por outros (e não concretamente para determinar os trabalhadores a serem despedidos), a segunda, por ser uma modalidade de despedimento que, apesar de legalmente consagrada, não existir verdadeiramente no ordenamento jurídico português.

³²⁹ PEDRO FURTADO MARTINS, *Cessação do Contrato de Trabalho*, Princípiã, Cascais, 4.ª edição, setembro de 2017, p. 262 a 272.

É, contudo, necessário aquando da elaboração do algoritmo proceder a uma consciente e cuidada inserção dos dados a analisar de forma que os trabalhadores sejam avaliados em conformidade com a legislação vigente. A título de exemplo refira-se a importância de o algoritmo ter em consideração os motivos das ausências dos trabalhadores, de modo a não rotular da mesma forma um trabalhador que falta frequentemente sem motivo justificativo e um trabalhador que se encontra ausente por, por exemplo, baixa médica.

No verso da moeda temos os despedimentos por facto imputável ao trabalhador. Nos termos do artigo 351.º, n.º 1 do CT “*constitui justa causa de despedimento o comportamento culposos do trabalhador que, pela sua gravidade e consequência, torna imediata e praticamente impossível a subsistência da relação de trabalho*”. O n.º 2 deste preceito faz um elenco taxativo das causas de despedimento, nomeadamente:

- a) desobediência ilegítima às ordens dadas por responsáveis hierarquicamente superiores;
- b) violação de direitos e garantias de trabalhadores da empresa;
- c) provocação repetida de conflitos com trabalhadores da empresa;
- d) desinteresse repetido pelo cumprimento, com a diligência devida, de obrigações inerentes ao exercício do cargo ou posto de trabalho a que está afeto;
- e) lesão de interesses patrimoniais sérios da empresa;
- f) falsas declarações relativas à justificação de faltas;
- g) faltas não justificadas ao trabalho que determinem diretamente prejuízos ou riscos graves para a empresa, ou cujo número atinja, em cada ano civil, cinco seguidas ou 10 interpoladas, independentemente de prejuízo ou risco;
- h) falta culposa de observância de regras de segurança e saúde no trabalho;
- i) prática, no âmbito da empresa, de violências físicas, injúrias ou outras ofensas punidas por lei sobre trabalhador da empresa, elemento dos corpos sociais ou empregador individual não pertencente a estes, seus delegados ou representantes;
- j) sequestro ou em geral crime contra a liberdade das pessoas referidas na alínea anterior;
- k) incumprimento ou oposição ao cumprimento de decisão judicial ou administrativa;
- l) reduções anormais de produtividade.

Da análise deste elenco é possível retirar, quase de imediato, uma conclusão: a maioria dos motivos apresentados não admitem uma análise algorítmica ou, quando muito, uma vantajosa e económica análise. Façamos um exame concreto.

Abordemos, em primeiro lugar, as alíneas que, inquestionavelmente, admitiriam uma intervenção algorítmica. As alíneas g) e l), porque delimitadas por elementos objetivos (número de faltas e redução de atividade), teriam resultados positivos com a aplicação algorítmica. Através da determinação de valores específicos, o algoritmo permitiria um controlo contínuo e eficaz da assiduidade e da produtividade dos trabalhadores, informando-os e às empresas quando se encontrassem a atingir esses limites. Ultrapassados esses valores o algoritmo informaria a empresa da possibilidade de despedimento do trabalhador em causa.

Atente-se que o n.º 1 do artigo 351.º do CT refere que o despedimento apenas poderá ocorrer caso o comportamento do trabalhador torne *“imediata e praticamente impossível a subsistência da relação de trabalho”*. Para obtermos uma admissível decisão automatizada o algoritmo deve ser programado tendo por base limites que a entidade empregadora considere suficientes para proceder a um despedimento (caso contrário será necessária uma intervenção humana).

No que concerne às alíneas j) e k) entendemos que não existem vantagens na intervenção algorítmica, uma vez se tratarem de situações cuja prática determinam, quase de forma imediata, o despedimento. Recorde-se que os algoritmos funcionam tendo por base dados fornecidos, pelo que não seria benéfico para as empresas fornecerem dados sobre, por exemplo, o incumprimento de uma decisão judicial para, posteriormente, o algoritmo determinar o despedimento do trabalhador quando essa decisão já seria de se esperar. Por outras palavras, nestas situações o algoritmo não irá otimizar a decisão, pelo que não se mostra economicamente proveitoso.

Por fim, as alíneas a) a f), h) e i) são as que geram maior controvérsia quanto à aplicação algorítmica em sede de despedimento individual. Cada uma destas alíneas demonstra um certo nível de subjetividade. Como referimos anteriormente, a análise de elementos subjetivos é possível através da utilização de sistemas de NPL, mas seria essa análise benéfica neste contexto? Depende. A implementação de algoritmos nas empresas, além de fornecer respostas objetivas, tem como objetivo primordial otimizar o tempo gasto. Nos

casos elencados nestas alíneas nem sempre é possível atingir essa otimização. Vejam-se os dois exemplos que de seguida elaboramos:

- (i) Exemplo A: O trabalhador A provoca, frequentemente, conflitos na empresa. Pelo menos uma vez por semana os seus superiores têm de o advertir sobre o cumprimento das regras implementadas no local de trabalho. Sempre que é advertido é preenchido um documento no qual é explicado, pormenorizadamente, o ocorrido. Esse documento é, posteriormente, analisado pelo algoritmo implementado na empresa que o avalia numa escala de 1 a 10, sendo 1 pouco grave e 10 extremamente grave. Atingido um determinado nível de mau comportamento o algoritmo envia um aviso ao empregador informando-o da possibilidade de despedir o trabalhador.

Neste exemplo entendemos que a intervenção algorítmica poderá ser positiva.

- (ii) Exemplo B: O trabalhador B faltou 5 vezes ao trabalho, tendo apresentado, em 2 delas, justificações de comparência no centro de saúde. Uma semana mais tarde a entidade empregadora tomou conhecimento de que as justificações apresentadas teriam sido forjadas, não correspondendo a documentos verdadeiros.

No exemplo agora apresentado entendemos que, não obstante a possibilidade da intervenção de um sistema de IA, o mesmo mostrar-se-ia menos eficaz do que uma intervenção humana. A exigência da programação de um sistema para a análise de questões deste calibre é imensa e, apesar da possibilidade da sua criação, entendemos que seria sempre necessária uma intervenção humana no sentido de fiscalizar, *a posteriori*, essa decisão.

Assim, é do nosso entendimento que a decisão pela utilização de algoritmos para as situações descritas nas alíneas a) a f), h) e i) deve ser feita tendo em consideração cada situação em concreto, avaliando os eventuais benefícios que essa implementação possa aportar.

3.6.4. A importância dos sindicatos na “negociação algorítmica”

A negociação coletiva continua a ser, nos dias de hoje, um dos instrumentos mais eficazes na salvaguardar dos direitos dos trabalhadores, em particular no que diz respeito aos rápidos avanços tecnológicos. Como referido por ROBERTO FERNÁNDEZ FERNÁNDEZ,³³⁰

... os instrumentos ligados ao direito coletivo são tradicionalmente essenciais para limitar as prerrogativas das empresas, podendo oferecer soluções bastante flexíveis, tanto a nível setorial como empresarial, e tentando compatibilizar os interesses dos trabalhadores e dos empregadores, aplicando os princípios gerais previstos na legislação e conciliando-os quando estão em conflito.

(tradução nossa)

O reconhecimento da importância da intervenção das estruturas representativas dos trabalhadores nestas matérias é abonado quer pela legislação nacional, quer pela internacional.³³¹

A nível internacional, o artigo 88.º do RGPD determina que

[o]s Estados-Membros podem estabelecer, no seu ordenamento jurídico ou em convenções coletivas, normas mais específicas para garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral, nomeadamente para efeitos de recrutamento, execução do contrato de trabalho, incluindo o cumprimento das obrigações previstas no ordenamento jurídico ou em convenções coletivas, de gestão, planeamento e organização do trabalho, de igualdade e diversidade no local de trabalho, de saúde e segurança no trabalho, de proteção dos bens do empregador ou do cliente e para efeitos do exercício e gozo, individual ou coletivo, dos direitos e benefícios relacionados com o emprego, bem como para efeitos de cessação da relação de trabalho.

³³⁰ ROBERTO FERNÁNDEZ FERNÁNDEZ, *Selección...* Ob. cit., p. 113: “En efecto, las normas paccionadas siguen siendo, sin duda, la herramienta más eficaz para ofrecer salvaguardas contra la rápida evolución tecnológica de la gestión algorítmica, no en vano los instrumentos vinculados al derecho colectivo han demostrado tradicionalmente ser esenciales en aras a limitar las prerrogativas empresariales, pudiendo llegar a ofrecer soluciones bastante flexibles tanto a nivel sectorial como de empresa y tratar de compatibilizar, aplicando los principios generales previstos legislativamente, los intereses de trabajadores y empresarios, compaginando los mismos cuando estuvieran distanciados”.

³³¹ TERESA COELHO MOREIRA, *Direito do Trabalho: Relação Individual...* Ob. cit., p. 360 e 361.

Este artigo demonstra de forma clara a importância das convenções coletivas como fonte essencial para garantir um tratamento justo e legal dos dados pessoais no contexto laboral. Note-se que este preceito faz referência expressa ao processamento de dados para fins de recrutamento e gestão, ilustrando a importância destes instrumentos na regulação de matérias que envolvam a utilização de sistemas de IA e de gestão algorítmica em sede laboral.³³²

De encontro a este entendimento vai o Considerando 92 do RIA que reforça a ideia de que

Continua a ser necessário garantir a informação dos trabalhadores e dos seus representantes sobre a implantação prevista de sistemas de IA de risco elevado no local de trabalho quando não estiverem cumpridas as condições para essas obrigações de informação ou de informação e consulta previstas noutros instrumentos jurídicos.

A nível nacional o Código do Trabalho determina, no artigo 466.º, n.º 1, al. d), que o delegado sindical tem direito à informação e consulta sobre os “*parâmetros, critérios, regras e instruções em que se baseiam os algoritmos ou outros sistemas de inteligência artificial que afetam a tomada de decisões sobre o acesso e a manutenção do emprego, assim como condições de trabalho, incluindo a elaboração de perfis e o controlo da atividade profissional*”. Mais uma vez reforça-se o valor da intervenção das estruturas de representação dos trabalhadores em matéria algorítmica.

É elementar concluir que a atuação destes agentes terá agora de ir além das suas tradicionais funções, adotando uma postura mais ativa na proteção dos direitos e liberdades dos trabalhadores.³³³ Para tanto, devem ser adotadas medidas como:

- (i) Promoção da formação e educação dos trabalhadores em matéria de IA, permitindo-os compreender o alcance e a atuação das novas tecnologias, adaptando-se, mais facilmente, ao mercado;
- (ii) Aumento do envolvimento dos trabalhadores nas decisões sobre a eventual implementação de sistemas de IA no âmbito laboral;

³³² VALERIO DE STEFANO, SIMON TAES, *Algorithmic management and collective bargaining*, ETUI aisbl, Brussels, 2021, ISSN 2507-1548, p. 9.

³³³ PAWEŁ NOWIK, *New challenges for trade unions in the face of algorithmic management in the work environment.*, Studies on Labour Law and Social Policy, 2022, 29, nr 2, p. 122.

- (iii) Elaboração de políticas internas que garantam uma maior proteção dos direitos dos trabalhadores quando confrontados com sistemas de IA;
- (iv) Incentivo à implementação consciente de sistema de IA, permitindo que os mesmos se traduzam em mecanismos de otimização do trabalho em vez de uma eventual ameaça;
- (v) Monitorização dos sistemas de IA e análise do seu impacto em âmbito laboral;
- (vi) Criação de mecanismos de feedback onde os trabalhadores possam expressar as suas preocupações;
- (vii) Desenvolvimento de diretrizes éticas para o uso da IA, garantindo que as novas tecnologias respeitem a dignidade do trabalhador e não perpetuem condutas discriminatórias.

Em suma, não obstante as vantagens da implementação de sistemas de IA no seio laboral, é importante ter em consideração os riscos que os mesmos podem esboçar. Neste sentido, é fundamental o envolvimento das estruturas coletivas na tomada de decisões que conduzam à implementação de algoritmos, em particular a sua atuação *ex ante*, prévia à produção de eventuais danos, não descurando, ainda assim, uma atuação *ex post*.

3.6.5. Decisões algorítmicas: a quem responsabilizar?

Aqui chegados surge a questão: na eventual violação dos direitos, liberdades e garantias do trabalhador, quem deve ser responsabilizado?

Como bem explicado por JOSÉ VIDA FERNÁNDEZ,³³⁴

Embora o novo modelo de governação dos riscos digitais esteja ainda em formação e deva ser definido nos próximos anos, é já evidente que não é comparável aos modelos de governação de outros riscos globais. De facto, a natureza única destes riscos digitais (...) torna muito difícil a implementação de um sistema de intervenção

³³⁴ JOSÉ VIDA FERNÁNDEZ, *La gobernanza de los riesgos digitales: desafíos y avances en la regulación de la inteligencia artificial*, Cuadernos de Derecho Transnacional. 2022, Vol. 14, n.º 1, p. 496: “*Aunque el nuevo modelo de gobernanza de los riesgos digitales se encuentra en proceso de formación y tendrá que definirse en los próximos años, ya es posible constatar que no es equiparable a los modelos de gobernanza de los demás riesgos globales. En efecto, la naturaleza singular de estos riesgos digitales que se ha descrito anteriormente hace que sea muy difícil desplegar un sistema de intervención similar al que se ha venido desarrollando frente a los riesgos que amenazan el medio ambiente, la salud o la seguridad, por lo que deberá desarrollar unas características propias que aún están por definir*”.

semelhante ao que foi desenvolvido para os riscos ambientais, sanitários ou de segurança, pelo que terá de desenvolver características próprias que ainda não foram definidas.

(tradução nossa)

A criação e solidificação de medidas que permitam a salvaguarda dos direitos dos eventuais lesados por sistemas de IA tem vindo a ser defendida a nível internacional. A este propósito, a Comissão Europeia pronunciou-se afirmando que³³⁵

As pessoas que sofreram danos causados pela intervenção de sistemas de IA devem beneficiar do mesmo nível de proteção que as pessoas que sofreram danos causados por outras tecnologias, sem que tal impeça a inovação tecnológica de se continuar a desenvolver.

Neste sentido, em 20 de outubro de 2020 foi aprovada a Resolução do Parlamento Europeu que contém recomendações à Comissão sobre o regime de responsabilidade civil aplicável à inteligência artificial, assinalando a importância da regulação desta matéria a nível europeu – Resolução n.º 2020/2014 (INL).

Do mesmo modo que o RIA, a abordagem adotada pela Resolução do Parlamento Europeu assentou no risco. Assim, como explica JESÚS R. MERCADER UGUINA,³³⁶

o cálculo da responsabilidade entre os diferentes intervenientes dependerá da interação entre o objetivo de utilização para o qual o sistema de IA é comercializado, a forma como o sistema de IA é utilizado, a gravidade dos potenciais danos ou prejuízos, o grau de autonomia da tomada de decisões que pode resultar em danos e a probabilidade de materialização do risco.

(tradução nossa)

³³⁵ COMISSÃO EUROPEIA, *Livro Branco sobre a inteligência artificial – Uma abordagem europeia virada para a excelência e confiança*, Bruxelas, 19.02.2020, p. 17.

³³⁶ JESÚS R. MERCADER UGUINA, *Algoritmos...* Ob. cit., p. 195: «el cálculo de la responsabilidad entre los distintos agentes dependerá de la interacción entre la finalidad de uso para la que se comercializa el sistema de IA, la forma en que se usa el sistema de IA, la gravedad del daño o perjuicio potencial, el grado de autonomía de la toma de decisiones que puede resultar en daños y de la probabilidad de que el riesgo se materialice”.

No sentido de proceder a uma diferenciação dos diversos agentes que intervêm no processo de criação e implementação dos sistemas de IA, a Resolução prevê dois tipos de sujeitos: os operadores de *frontend* ou operadores finais e os operadores de *backend* ou operadores iniciais – artigo 3.º, al. e) e f). O operador final corresponde a “qualquer pessoa singular ou coletiva que exerça um grau de controlo sobre um risco relacionado com a operação e o funcionamento do sistema de IA e que beneficie da sua operação”. Em contrapartida, o operador inicial será “qualquer pessoa singular ou coletiva que, de forma contínua, defina as características da tecnologia, forneça dados e preste serviços essenciais de apoio de backend e, por conseguinte, exerça igualmente algum controlo sobre o risco ligado à operação e ao funcionamento do sistema de IA”.³³⁷

A Resolução estipula ainda a noção de controlo, o qual corresponderá a “qualquer ação de um operador que influencie a operação de um sistema de IA e, por conseguinte, a medida em que o operador expõe terceiros aos riscos potenciais associados à operação e ao funcionamento do sistema de IA; essas ações podem ter impacto na operação, determinando os dados introduzidos, os dados de saída ou os resultados, ou modificar funções ou processos específicos no sistema de IA; o grau em que esses aspetos da operação do sistema de IA são determinados pela ação depende do nível de influência que o operador tem sobre o risco ligado à operação e ao funcionamento do sistema de IA” – artigo 3.º, al. g).

Desta análise é possível depreender que o operador final corresponderá, no âmbito laboral, à entidade empregadora, e o operador inicial ao criador do algoritmo (via regra, um informático). Destaque-se que, no entendimento do Parlamento Europeu, ambos os operadores têm uma atuação ativa e de controlo sob o sistema de IA (o que terá claros reflexos a nível de responsabilidade). Esse é um dos motivos pelo qual a Resolução impõe a adesão a seguros de responsabilidade civil nos termos dos artigos 4.º, n.º 4, 5.º e 6.º

Em matéria de responsabilidade a Resolução do Parlamento Europeu optou por um regime de responsabilidade objetiva, independente da culpa, tendo o operador os encargos pelos prejuízos ou danos causados por uma atividade, dispositivo ou processamento físico ou

³³⁷ Nos termos do Considerando 8 “deverá ser sempre claro que quem cria, mantém, controla o sistema de IA, ou nele interfere, deverá ser responsável pelos danos ou prejuízos causados pela atividade, o dispositivo ou o processo”.

virtual baseado na IA – artigo 4.º, n.º 1.³³⁸ Note-se que não é evidenciada qualquer diferenciação entre operador inicial ou operador final, pelo que, na existência de ambos, a responsabilidade será solidária – artigo 11.º.³³⁹

Importa, ainda, mencionar que os operadores de sistemas de IA de alto risco, como o são os implementados no âmbito laboral, não podem eximir-se da sua responsabilidade alegando que atuaram com a devida diligência ou que os prejuízos ou danos foram causados por uma atividade, um dispositivo ou um processo autónomo baseado no seu sistema de IA. Contudo, os operadores não serão considerados responsáveis pelos prejuízos ou danos se estes tiverem sido causados por motivos de força maior – artigo 4.º, n.º 3.

A opção por um regime de responsabilidade objetiva parece justificar-se pelo Considerando 3 que explica que

... a ascensão da IA constitui um desafio significativo para os quadros de responsabilidade existentes. A utilização de sistemas de IA no nosso quotidiano conduzirá a situações em que a sua opacidade (elemento de caixa negra) e a série de intervenientes no seu ciclo de vida tornem extremamente dispendioso, ou mesmo impossível, identificar quem exercia o controlo do risco de utilização do sistema de IA em questão ou qual foi o código ou entrada que provocou a operação danosa. Essa dificuldade é agravada pela conectividade entre um sistema de IA e outros sistemas de IA e sem IA, pela sua dependência de dados externos, pela sua vulnerabilidade a violações da cibersegurança e ainda pela crescente autonomia dos sistemas de IA desencadeados pelas capacidades de aprendizagem automática e aprendizagem profunda. Para além destas características complexas e potenciais vulnerabilidades, os sistemas de IA também podem ser utilizados para causar danos graves – como comprometer a dignidade humana e os valores e liberdades europeus – através da localização de pessoas contra a sua vontade, da introdução de sistemas

³³⁸ A este propósito refira-se o artigo 4.º, n.º 4 da Resolução que determina que quer o operador de *frontend*, quer o operador de *backend* devem estar cobertos por seguros de responsabilidade civil adequados, nos termos dos artigos 5.º e 6.º.

³³⁹ A respeito desta questão destaque-se o final do artigo 11.º que determina que “*se o operador de frontend for também o produtor do sistema de IA, o presente regulamento prevalece sobre a Diretiva relativa à responsabilidade decorrente dos produtos. Se o operador de backend também for considerado produtor na aceção do artigo 3.º da Diretiva relativa à responsabilidade decorrente dos produtos, a presente Diretiva é aplicável. Se houver apenas um operador e esse operador for também o produtor do sistema de IA, o presente regulamento prevalece sobre a Diretiva relativa à responsabilidade decorrente dos produtos*”.

de crédito social, de decisões enviesadas em matérias relacionadas com seguros de doença, concessão de crédito, decisões judiciais, recrutamento ou emprego, ou da construção de sistemas de armas letais autónomas.

É importante referir que o regime agora exposto se traduz, como mencionado previamente, numa recomendação do Parlamento Europeu e não num regulamento. Ainda assim, a aplicação de um regime de responsabilidade objetiva assente no risco parece-nos o mais lógico, quer por se compactuar com o estipulado no RIA, quer por se mostrar mais favorável ao lesado. Além disso, confrontamo-nos com a impossibilidade de atribuir culpa aos sistemas de IA o que implica, desde logo, a desconsideração da aplicabilidade do regime de responsabilidade subjetiva.³⁴⁰

Outra solução viável seria conduzir a responsabilidade dos sistemas de IA ao regime dos danos causados por coisas, animais ou atividades, o qual implicaria a inversão do ónus da prova para o detentor do sistema de IA. Por outras palavras, caberia ao detentor do sistema de IA demonstrar que atuou com zelo e diligência adequadas, pelo que os danos se teriam produzido independentemente da sua atuação – artigo 493.º, n.º 1 do CC.³⁴¹

3.6.6. Diretiva (UE) 2024/2831 do Parlamento Europeu e do Conselho, de 23 de outubro

No passado dia 11 de novembro de 2024 foi publicada no Jornal Oficial da União Europeia a Diretiva (UE) 2024/2831 do Parlamento Europeu e do Conselho, de 23 de outubro de 2024, relativa à melhoria das condições de trabalho em plataformas digitais – Considerando 16. Através deste diploma é regulada pela primeira vez a utilização de algoritmos pelas plataformas de trabalho digital.³⁴²

³⁴⁰ A este propósito refira-se a inicial proposta apresentada pelo Parlamento Europeu à Comissão Europeia [Proposta 2015/2103 (INL)] no sentido de atribuir personalidade jurídica aos robôs dotados de capacidades decisória – artigo 59.º, al. g) da proposta. Disponível para consulta [aqui](#).

³⁴¹ Falamos de uma inversão do ónus da prova nos termos do n.º 1 do artigo 493.º do CC (dever de vigilância), mas já não do n.º 2 (atividades perigosas), uma vez que entendemos excessivo catalogar a atuação algorítmica como perigosa. Note-se que uma caracterização nestes termos pode ser condicionadora do desenvolvimento tecnológico.

³⁴² A diretiva entra em vigor a partir de 1 de dezembro de 2024 e deve ser transposta até ao dia 2 de dezembro de 2026.

Apesar deste documento respeitar ao trabalho nas plataformas digitais é do nosso entendimento que as medidas aí estabelecidas poder-se-ão estender à “comum” relação de trabalho, pelo que a sua análise se mostra pertinente.

Por referência à presente dissertação destacamos a regulamentação de dois temas: (i) a gestão algorítmica (artigos 7.º a 15.º) e (ii) as medidas de proteção a implementar (artigos 22.º e 23.º).

Em matéria de gestão algorítmica a Diretiva impõe a realização de avaliações de impacto sobre a proteção de dados pessoais sempre que exista a utilização de sistemas automatizados de monitorização e de tomada de decisões – artigo 8.º.

As plataformas de trabalho digital que utilizem estes sistemas necessitam de informar devidamente as pessoas que trabalham nas mesmas, os representantes dos trabalhadores e, mediante pedido, as autoridades nacionais sobre a sua utilização³⁴³ – artigo 9.º.

O legislador estabeleceu ainda, no artigo 7.º, a proibição de sistemas automatizados de monitorização e tomada de decisões (desde o início do processo de recrutamento ou seleção) para:³⁴⁴

- (i) tratar dados pessoais sobre o estado emocional ou psicológico de uma pessoa que trabalha em plataformas digitais;
- (ii) tratar dados pessoais relacionados com conversas privadas, incluindo intercâmbios com outras pessoas que trabalham em plataformas digitais e os representantes das pessoas que trabalham em plataformas digitais;
- (iii) recolher dados pessoais de uma pessoa que trabalha em plataformas digitais quando esta não esteja a disponibilizar ou efetuar um trabalho em plataformas digitais;
- (iv) tratar dados pessoais para prever o exercício dos direitos fundamentais;

³⁴³ Caso não existam representantes dos trabalhadores deve ser assegurado que as plataformas informam diretamente os trabalhadores em causa sobre as decisões suscetíveis de conduzir à introdução, ou a alterações substanciais na utilização, de sistemas automatizados de monitorização ou sistemas automatizados de tomada de decisões. As informações são prestadas sob a forma de documento escrito, ainda que em formato eletrónico. Na prestação de informações devem ser salvaguardados valores como a transparência, inteligibilidade e facilidade no acesso, utilizando uma linguagem clara e simples – artigo 14.º e Considerando 53.

³⁴⁴ Neste sentido, confirmar o Considerando 39, 40 e 41.

- (v) tratar quaisquer dados pessoais para inferir a origem racial ou étnica, o estatuto migratório, as opiniões políticas, as convicções religiosas ou filosóficas, a deficiência, o estado de saúde, incluindo a doença crónica ou o estatuto serológico VIH, o estado emocional ou psicológico, a filiação sindical, a vida sexual ou a orientação sexual;
- (vi) tratar quaisquer dados biométricos de uma pessoa que trabalha em plataformas digitais para determinar a identidade dessa pessoa, comparando esses dados com os dados biométricos de pessoas singulares armazenados numa base de dados.

É importante destacar que, no sentido de atingir um efetivo controlo destes sistemas, se estabeleceu a necessidade de supervisão e avaliação humanas do impacto das decisões tomadas – artigos 10.º e 12.º. Ora, é mais uma vez reforçada a ideia de que, não obstante a sua eficiência, os sistemas de IA ainda necessitam de um “apoio” humano de forma a garantir que os direitos, liberdades e garantias dos que com eles podem ser afetados sejam salvaguardados.

Por outro lado, no que concerne à proteção das pessoas que trabalham nas plataformas digitais, a Diretiva procurou evidenciar a necessidade da tomada de medidas no sentido de salvaguardar essas pessoas contra formas de tratamento desfavorável ou consequências adversas – artigo 22.º.

Em vista disso foi consagrado o direito a que as decisões tomadas por sistemas de IA sejam explicadas e reapreciadas sempre que requerido – artigo 11.º.

Além disso, o legislador determinou a implementação de medidas adequadas para proibir o despedimento ou a cessação do contrato das pessoas que trabalham em plataformas digitais, ou ação equivalente, bem como qualquer ação preparatória nesse sentido – artigo 23.º e Considerando 47 e 66. Assim, as pessoas que trabalham em plataformas digitais que considerem terem sido (i) despedidas, (ii) alvo de cessação do seu contrato ou (iii) sujeitas a ações de efeito equivalente podem solicitar à plataforma de trabalho digital que exponha de forma devidamente fundamentada os motivos do despedimento, da cessação do contrato ou da ação equivalente – n.º 2 do artigo 23.º.

Este diploma procurou ainda reforçar a negociação coletiva de modo a facilitar o exercício dos direitos relacionados com a gestão algorítmica – artigo 25.º.

Apesar desta Diretiva regular, ainda que de forma generalizada, a utilização de algoritmos pelas plataformas de trabalho digital, as medidas aí estabelecidas podem facilmente estender-se às comuns formas de trabalho – como explicado infra e de seguida melhor desenvolvido.

3.6.7. Soluções

A implementação de tecnologias de IA no âmbito laboral apresenta inúmeros desafios, especialmente no que concerne ao cumprimento dos direitos, liberdades e garantias dos trabalhadores, ao combate à discriminação e à atribuição de responsabilidade por danos causados por estes mecanismos. Citando ROBERTO FERNÁNDEZ FERNÁNDEZ,³⁴⁵

A este respeito, é aconselhável não se deixar levar pelo brilho provocado pela Inteligência Artificial e por todas as ferramentas ligadas às novas tecnologias, uma vez que uma das suas atrações é a sua aparência de neutralidade, naquilo a que se chamou a “fachada da tecnologia objetiva”, provocando “preconceitos de automação” ou “complacência induzida”, de modo que “muitas pessoas querem acreditar que uma máquina que imita as funções do cérebro humano pode estar livre de limitações humanas, incluindo preconceitos económicos, sociais, culturais e políticos específicos [; no entanto], é a ética e os valores dos humanos que constroem os sistemas e os sistemas de IA”

(tradução nossa)

O regime de responsabilidade objetiva recomendado pelo Parlamento Europeu é um passo importante para mitigar os riscos associados ao uso da inteligência artificial. No entanto, além do enquadramento legal, é crucial que as empresas adotem medidas práticas que assegurem o respeito pela lei e pela ética no uso desses sistemas. As soluções que se seguem

³⁴⁵ ROBERTO FERNÁNDEZ FERNÁNDEZ, *Selección... Ob. cit.*, p. 57 e 58: «A este respecto, es conveniente no dejarse llevar por el brillo provocado por la Inteligencia Artificial y todos los instrumentos vinculados a las nuevas tecnologías, pues no de su atractivo es su apariencia de neutralidad, en lo que se ha denominado la "fachada de la tecnología objetiva", causante de "sesgos de automatización" o "complacencia inducida", de manera que "muchas personas quieren creer que una máquina que imita las funciones del cerebro humano puede estar libre de limitaciones humanas, incluyendo sesgos económicos, sociales, culturales y políticos particulares [;sin embargo], la ética y los valores de los seres humanos que construyen sistemas de Inteligencia Artificial y de los sistemas"».

visam oferecer diretrizes claras e eficazes para uma adequada implementação dos sistemas de IA no contexto laboral, garantindo uma abordagem que privilegie tanto os direitos dos trabalhadores quanto os interesses das empresas.

a. Sistemas de IA como um complemento laboral

A utilização de mecanismos de IA no âmbito laboral é vista, regra geral, como uma ferramenta de apoio às empresas que visa reduzir os gastos e aumentar os lucros. Permanece a ideia de que a implementação destes sistemas acarretará consequências como a redução da empregabilidade e o aumento da taxa de desemprego.

Esta visão deve ser destruída e, no seu lugar, edificada a ideia de que os sistemas de IA vieram para, além de ajudar as empresas, apoiar os trabalhadores, permitindo-lhes melhorar a qualidade do trabalho.³⁴⁶

Assim, à medida que as empresas ponderam se e como devem adotar tecnologias de IA, devem simultaneamente considerar quais os sistemas que melhor ajudarão à sua força de trabalho. Deste modo, previamente à aquisição de tecnologias de IA, as entidades empregadoras devem considerar de que forma as mesmas afetariam o normal desenvolvimento do trabalho e respetivas oportunidades de emprego e decidirem em conformidade com essas conclusões.

b. Envolvimento de trabalhadores

O primeiro passo para um adequado desenvolvimento dos sistemas de IA e uma melhor receção dos mesmos por partes dos trabalhadores passa pelo envolvimento destes, bem como dos seus representantes, na conceção, desenvolvimento, testagem, formação, utilização e supervisão daqueles.^{347/ 348}

³⁴⁶ Nesta senda veja-se a proposta apresentada pelo U.S. DEPARTMENT OF COMMERCE, U.S. DEPARTMENT OF LABOR, *Good Job Principles*, disponível para consulta [aqui](#).

³⁴⁷ U. S. DEPARTMENT OF LABOR, *Artificial Intelligence and worker well-being: principles and best practices for developers and employers*, October 2024, p. 8.

³⁴⁸ TERESA COELHO MOREIRA, *Direito do Trabalho: Relação Individual...* Ob. cit., p. 360 e 361.

As empresas devem garantir que os trabalhadores e os seus representantes são devidamente informados sobre quais os dados recolhidos, bem como quais os parâmetros, critérios e regras na base da tomada de decisões do sistema de IA – artigo 466.º do CT e Considerando 92 do RIA.

Para uma consciente compreensão do alcance de atuação dos sistemas implementados, as entidades empregadoras devem promover formações adequadas, com linguagem clara, em matéria de inteligência artificial.

Este envolvimento deve passar, ainda, pela criação de canais nos quais os trabalhadores possam relatar problemas associados aos sistemas de IA (e.g., violação de direitos, erros, etc.).

c. Desenvolvimento e implementação dos sistemas de IA em conformidade com os valores éticos e legais

O desenvolvimento e implementação de sistemas de IA no local de trabalho deve realizar-se em conformidade com os valores éticos. Mais do que um apoio económico para as empresas, estes mecanismos devem ser criados e formados de modo a proteger os trabalhadores.³⁴⁹ Para uma boa aceitação destas novas tecnologias é elementar que os trabalhadores não se sintam atacados, oprimidos ou coagidos pelas mesmas.

Como fomos referindo ao longo da presente dissertação, a recolha e tratamento de dados pessoais tem de se fundar num interesse legítimo. Cumprindo esse requisito, a utilização de sistemas de IA desenvolver-se-á tendo por base diversos pilares. Um dos mais importantes é a transparência. É fulcral que os trabalhadores compreendam a atuação e o alcance dos sistemas implementados, acompanhando a sua criação, desenvolvimento e funcionamento.³⁵⁰

Simultaneamente, estas tecnologias devem mostrar-se objetivas, mantendo-se neutras e imparciais, atingindo respostas justas para cada realidade. Para tanto é necessário que aquando da criação algorítmica seja seguida uma política de antidiscriminação, incorporando

³⁴⁹ RAY EITEL-PORTER, *Beyond the promise: implementing AI*, AI and Ethics (2021), p. 75 e 76.

³⁵⁰ TERESA COELHO MOREIRA, *Direito do Trabalho: Relação Individual... Ob. cit.*, p. 358 e 359.

uma diversidade de dados que permitam que o algoritmo não diferencie os diversos candidatos a emprego/trabalhadores em função do gênero, raça, origem, etc. A salvaguarda pela objetividade destes sistemas aumenta a confiabilidade e credibilidade nos mesmos.

Assim, as empresas devem, mais do que contratar um sistema existente, desenvolver algoritmos especificamente direcionados para os seus interesses e para a sua realidade, garantindo uma adequada atuação da inteligência artificial.

d. Realização de avaliações de impacto e auditorias

Previamente à implementação de um sistema de IA as empresas devem realizar avaliações de impacto e auditorias aos mesmos. Como refere CARLA REGINA THOMÉ WEDY,³⁵¹

Tendo em vista que a eficácia de qualquer algoritmo está intrinsecamente ligada à qualidade dos dados que o sustentam, o cuidado com a base de dados sob a qual o modelo matemático irá ser processado é crucial. Em outras palavras, a excelência do resultado automatizado gerado por um algoritmo (output) está diretamente relacionada à qualidade das informações que ele recebe como entrada (input). Dessa forma, se o algoritmo se fundamenta em bases de dados históricos permeados por vieses discriminatórios, ele reproduzirá automaticamente os mesmos padrões tendenciosos que formaram a base de seu processamento.

Ora, é fundamental uma meticulosa análise prévia do sistema a implementar no sentido de assegurar que o mesmo cumpre com as diretrizes éticas e legais. Para tanto devem ser criadas estruturas independentes, com profissionais devidamente formados, para a realização de auditorias, as quais devem avaliar as taxas de erro, os riscos de potencial discriminação ou viés algorítmico, a acessibilidade, identificar impactos nos direitos dos trabalhadores e documentar impactos negativos na qualidade e no bem-estar dos mesmos.³⁵²

³⁵¹ CARLA REGINA THOMÉ WEDY, *As decisões automatizadas no processo de recrutamento e seleção de empregados: entre o poder empregatício e os vieses discriminatórios*, In *Novas tecnologias e o princípio da centralidade da pessoa humana*, Anais do XIII Congresso Iberoamericano de Investigadores y Docentes de Derecho e Informática, Casa Leiria São Leopoldo/RS, 2023 p. 175.

³⁵² U. S. DEPARTMENT OF LABOR, *Artificial*,,, *Ob. cit.*, p. 9.

Além de um controlo prévio, as empresas devem promover um controlo contínuo e regular (por períodos com um maior ou menor afastamento temporal tendo em consideração o tipo de sistemas de IA implementado).³⁵³

e. Assegurar a proteção dos dados recolhidos

Como previamente mencionado na análise do RGPD e dos seus princípios subjacentes, é imprescindível criar medidas de segurança técnicas e organizativas sólidas para evitar violações de dados e garantir o cumprimento da legislação em matéria de proteção de dados.

Deste modo, as empresas podem optar pelo controlo de acesso aos dados, acautelando que apenas pessoas autorizadas os consultem. A utilização da criptografia pode representar um forte mecanismo para atingir esse objetivo.

Além disso, as empresas devem cumprir com o princípio da minimização do tratamento, recolhendo e tratando apenas os dados que se mostrem estritamente necessários para as finalidades específicas e legítimas. Esses dados devem, sempre que possível, ser anonimizados evitando, desta forma, o risco do seu reconhecimento.

f. Responsabilização

A responsabilidade por atos de sistemas de IA é uma questão complexa e crucial, especialmente no contexto europeu, onde a regulamentação procura equilibrar a inovação tecnológica e a proteção dos direitos dos cidadãos – e, aqui em particular, dos trabalhadores.

Apesar de não existir (ainda) um documento legal que regule, especificamente, a responsabilidade por danos causados por sistemas de IA, a Comissão Europeia começa, como observamos supra, a dar os primeiros passos nesse sentido.

Esta temática deve ser uma prioridade nas políticas europeias, garantindo que a inovação não ocorra às custas da segurança, da ética e dos direitos dos cidadãos. Um quadro regulatório claro, que inclua mecanismos de responsabilização, transparência e proteção dos

³⁵³ TERESA COELHO MOREIRA, *Direito do Trabalho: Relação Individual... Ob. cit.*, p. 357 e 358.

direitos humanos é fundamental para promover um desenvolvimento tecnológico que beneficie a sociedade como um todo.

Conclusão

O avanço tecnológico, sobretudo no que concerne à utilização de sistemas de IA, tem vindo a impactar significativamente o Direito Laboral, impondo novos desafios e exigindo uma adaptação contínua da legislação às novas realidades.

Apesar das inegáveis vantagens proporcionadas pela utilização de tecnologias de IA – e, em particular, algoritmos –, como a objetividade e a eficiência nos processos de decisão, não se podem ignorar os riscos associados, nomeadamente o potencial de discriminação e a opacidade dos processos automatizados. A possibilidade de as decisões laborais serem tomadas sem intervenção humana levanta questões éticas e jurídicas relevantes, nomeadamente no que toca à transparência, à equidade e à proteção dos direitos dos trabalhadores.

Não obstante, o eventual risco da implementação destes mecanismos não pode traduzir-se numa barreira para o avanço tecnológico no seio laboral. Em sentido inverso, as dificuldades apresentadas devem servir de impulso para o legislador – nacional e internacional – investir na regulamentação destas matérias.

O RGPD e, recentemente, o RIA constituem diplomas fundamentais para um adequado enquadramento legal da utilização das novas tecnologias no contexto laboral. Ainda assim, a complexidade inerente à aplicação dessas normas, aliada ao rápido desenvolvimento tecnológico, exigem que o legislador continue a adaptar e a reforçar o quadro normativo de modo a garantir uma efetiva proteção dos direitos fundamentais dos trabalhadores.

Em matéria legislativa é importante reforçar a necessidade de uma correta regulação do regime de responsabilidade por danos causados por sistemas de IA. Apesar de caminharmos nesse sentido, dúvidas continuam a surgir quanto aos sujeitos a quem responsabilizar.

Contudo, é indispensável ter em consideração que o acompanhamento deste avanço não pode passar apenas pelo legislador. Também as empresas têm um papel vital em todo este processo. O investimento na formação de trabalhadores, a inclusão destes e dos seus representantes sindicais, a adoção de medidas éticas, a realização de auditorias e a restrição da utilização de todos e quaisquer dados pessoais devem ser algumas das medidas a implementar pelas empresas no sentido de facilitar a integração da inteligência artificial no local de trabalho.

Conclui-se, deste modo, que o uso de algoritmos no âmbito laboral deve ser cuidadosamente regulado e monitorizado, garantido que os benefícios trazidos pela tecnologia não se sobrepõem aos direitos dos trabalhadores. O desafio que se coloca às sociedades modernas, em especial ao Direito, é o de encontrar um equilíbrio entre a inovação tecnológica e a preservação dos princípios éticos e jurídicos fundamentais, assegurando que a tecnologia seja uma aliada na construção de um mercado de trabalho mais justo, inclusivo e transparente.

Bibliografia

- ADITYA JAIN, GANDHAR KULKARNI, VRAJ SHAH, *Natural Language Processing*, International Journal of Computer Sciences and Engineering, Volume 6, Issue 1, E-ISSN: 2347-269, disponível para consulta [aqui](#)
- AGÊNCIA ESPANHOLA DA PROTEÇÃO DE DADOS, *Deliberação 0324/2009*, disponível para consulta [aqui](#)
- AGÊNCIA LUSA, *TAP: Boston Consulting Group escolhida para elaboração do plano de reestruturação*, Observador, 11.08.2020, disponível para consulta [aqui](#)
- ALEX J. WOOD, *Algorithmic Management: Consequences for Work Organisation and Working Conditions*, Seville: European Commission, 2021, JRC124874
- ALEXANDRE SOUSA PINHEIRO, CRISTINA PIMENTA COELHO, TATIANA DUARTE, CARLOS JORGE GONÇALVES E CATARINA PINA GONÇALVES, *Comentário ao Regulamento Geral de Proteção de Dados*, Coimbra, Edições Almedina, dezembro 2018
- ANA DE LA PUEBLA PINILLA, *Geolocalización y control biométrico*, III Encuentro Internacional sobre Transformaciones del Derecho del Trabajo Ibérico, ISBN 978-84-697-0418-9, disponível para consulta [aqui](#)
- ANA PAULA DIDIER STUDART, *O poder diretivo algorítmico*, São Paulo, SP: LTr Editora, 2023, disponível para consulta [aqui](#)
- ANTÓNIO BARRETO MENEZES CORDEIRO, *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*, Coimbra, Almedina, 2021
- A. BARRETO MENEZES CORDEIRO, *Direito da Proteção de Dados à Luz do RGPD e da Lei n.º 58/2019*, Almedina, 2022
- ANTÓNIO MENEZES CORDEIRO, *Direito do Trabalho II – Direito Individual*, Almedina, 2019
- ANTÓNIO MONTEIRO FERNANDES, *Direito do Trabalho*, 20.^a Edição, Almedina, 2020
- BERNARDO DA GAMA LOBO XAVIER, *Manual de Direito do Trabalho*, com colaboração de P. Furtado Martins, A. Nunes de Carvalho e Joana Vasconcelos, 4.^a Edição, Revista e Actualizada, Rei dos Livros, 2020

- BRUNO MESTRE, *Direito Antidiscriminação – uma perspetiva europeia e comparada*, Vida Económica, 2020
- CARLA REGINA THOMÉ WEDY, *As decisões automatizadas no processo de recrutamento e seleção de empregados: entre o poder empregatício e os vieses discriminatórios*, In *Novas tecnologias e o princípio da centralidade da pessoa humana*, Anais do XIII Congresso Iberoamericano de Investigadores y Docentes de Derecho e Informática, Casa Leiria São Leopoldo/RS, 2023, disponível para consulta [aqui](#)
- CAROLINA DE FREITAS E SILVA, *A máquina como recrutar, empregador e colega de trabalho: alguns aspectos jurídicos de contratar, gerir e lidar com pessoas na era digital*, *Questões Laborais*, Ano XXXI, n.º 64, Jan/Jun 2024,
- COLIN J. BENNETT, *Regulating Privacy: Data Protection and Public Policy in the Europe and the United States*, Cornell University Press, Ithaca, 1992, disponível para consulta [aqui](#)
- COLIN LECHER, *How Amazon automatically tracks and fires warehouse workers for “productivity”*, The Verge, 25.04.2019, disponível para consulta [aqui](#)
- COMISSÃO EUROPEIA, *Livro Branco sobre a inteligência artificial – Uma abordagem europeia virada para a excelência e confiança*, Bruxelas, 19.02.2020, disponível para consulta [aqui](#)
- COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS, *Deliberação/2019/494*, disponível para consulta [aqui](#)
- COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS, *Deliberação n.º 1638/2013*, de 16 de julho de 2013, disponível para consulta [aqui](#)
- COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS, *Deliberação n.º 3996/2014*, de 22 de abril de 2014, disponível para consulta [aqui](#)
- COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS, *Deliberação n.º 5981/2014*, de 1 de julho de 2014, disponível para consulta [aqui](#)
- COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS, *Deliberação n.º 629/2010*, de 13 de setembro de 2010, disponível para consulta [aqui](#)
- COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS, *Deliberação n.º 7680/2014, Aplicável aos tratamentos de dados pessoais decorrentes da utilização de tecnologias de geolocalização no contexto laboral*, disponível para consulta [aqui](#)

- COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS, *Princípios sobre a utilização de dados biométricos no âmbito do controlo de acessos e de assiduidade*, 26 de fevereiro de 2004, disponível para consulta [aqui](#)
- DANIEL ALVES DA CUNHA, ANA HIERRO E DIOGO ROFRIGUES DA SILVA, *Guia do Processo da Adequação ao Regulamento Geral de Proteção de Dados – Implementação e Auditoria*, Almedina, 2021
- DATASKILLUP LLC, *Natural Language Processing in Employee Sentiment Analysis, How NPL Transforms Unstructured Data into Actionable Employee Insights*, Sep 27, 2024, disponível para consulta [aqui](#)
- DAVID CARVALHO MARTINS, *Pre-screening e screening: poder funcional do empregador?*, In MARIA DO ROSÁRIO PALMA RAMALHO E TERESA COELHO MOREIRA, *O regulamento geral de proteção de dados e as relações de trabalho*, 1.^a Edição, Lisboa: AAFDL Editora, 2020
- DGERT, *Teletrabalho no contexto da negociação coletiva*, Coleção: Negociação coletiva em foco, n.º 1 de 2020, 25 de novembro de 2020, Direção-Geral do Emprego e das Relações de Trabalho, Divisão de Promoção do Diálogo Social, disponível para consulta em [aqui](#)
- Diretrizes EDPB 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679, adotadas em 4 de maio de 2020, disponível para consulta [aqui](#)
- EDUARDO TOMASEVICIUS FILHO, Reconhecimento facial e lesões aos direitos de personalidade, In Mafalda Miranda Barbosa, Felipe Braga Netto, Michael César Silva, José Luiz de Moura Faleiros Júnior, *Direito Digital e Inteligência Artificial: Diálogos Entre Brasil e Europa*, Editora Foco, 2021.
- ELISA SIERRA HERNÁIZ, *Las categorías especiales de datos del trabajador: Estudio de los límites y garantías legales para su tratamiento em la relación laboral*, Pamplona: Aranzadi-Thomson Reuters, 2021
- ELIZABETH D. LIDDY, *Natural Language Processing*, In Encyclopedia of Library and Information Science, 2nd Ed. NY. Marcel Decker, Inc., disponível para consulta [aqui](#)
- Eurostat, *8% of EU enterprises used AI technologies in 2023*, 29 May 2024, disponível para consulta [aqui](#)
- FILIPA URBANO CALVÃO, *A proteção de dados pessoais no contexto laboral: análise da jurisprudência*, In Caderno de Justiça Administrativa, N.º 128 (mar.- abr.) 2018

- FILOMENA VIEIRA, *RGPD para cidadãos atentos: manual de curso online*, Direção-Geral da Qualificação dos Trabalhadores em Funções Públicas (INA), Lisboa, novembro de 2018, disponível para consulta [aqui](#)
- FRANCISCO X. GÓMEZ GARCÍA, *La importancia del e-recruitment en la moderna gestión de recursos humanos*, International Journal of Information Systems and Software Engineering for Big Companies (IJISEBC), 6(2), 2019, disponível para consulta [aqui](#)
- FREDERICO VENTURA SEQUEIRA, *O algoritmo no tecido empresarial: Das vicissitudes de contratação ao despedimento de trabalhadores – Uma arma nociva que necessita de ser desarmada?*. In *Anuário da Proteção de Dados*, 2022, Coordenado por FRANCISCO PEREIRA COUTINHO e GRAÇA CANTO MONIZ, Lisboa: CEDIS, disponível para consulta [aqui](#)
- GARCIA MARQUES E LOURENÇO MARTINS, *Direito da Informática*, 2.^a Edição refundida e atualizada, Coimbra, Almedina, 2006
- GEMMA GALDON CLAVELL, *AI Auditing: Checklist for AI Auditing*, Support Pool of Experts Programme, European Data Protection Board, 2023, disponível para consulta [aqui](#)
- GEMMA GALDON CLAVELL, *AI Auditing: Proposal for AI leaflets*, Support Pool of Experts Programme, European Data Protection Board, 2023, disponível para consulta [aqui](#)
- GEMMA GALDON CLAVELL, *AI Auditing: Proposal for Algo-scores*, Support Pool of Experts Programme, European Data Protection Board, 2023, disponível para consulta [aqui](#)
- GRUPO INDEPENDENTE DE PERITOS DE ALTO NÍVEL SOBRE A INTELIGÊNCIA ARTIFICIAL, *Orientações éticas para uma IA de confiança*, criado pela Comissão Europeia em junho 2018, 2019 disponível para consulta [aqui](#)
- GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Documento de trabalho sobre questões relativas à protecção de dados no âmbito da tecnologia RFID*, WP 105, adotado em 19 de janeiro de 2005, disponível para consulta em [aqui](#)
- GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 02/2016 sobre a publicação de dados pessoais para efeitos de transparência no setor público*, WP239, Adotado em 8 de junho de 2016, disponível para consulta [aqui](#)

- GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 15/2011 sobre a definição de consentimento*, WP187, adaptado em 13 de julho de 2011, disponível para consulta [aqui](#)
- GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 2/2017 sobre o tratamento de dados no local de trabalho*, GT 249, Adotado em 8 de junho de 2017, disponível para consulta [aqui](#)
- GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Parecer 4/2007 sobre o conceito de dados pessoais*, WP 136, Adotado em 20 de junho, disponível para consulta [aqui](#)
- GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679*, adotadas em 28 de novembro de 2017, Última redação revista e adotada em 10 de abril de 2018, WP259 rev. 01, disponível para consulta [aqui](#)
- GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (EU) 2016/679*, adotadas em 3 de outubro de 2017, com a última redação revista e adotada em 6 de fevereiro de 2018, disponível para consulta [aqui](#)
- GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Orientações sobre o direito à portabilidade dos dados*, WP 242 rev.01, adotadas em 13 de dezembro de 2016 e revistas em 5 de abril de 2017, disponível para consulta [aqui](#)
- GRUPO DE TRABALHO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS, *Orientações sobre os encarregados da proteção de dados (EPD)*, WP 243 rev.01, Adotadas em 13 de dezembro de 2016, Com a última redação revista e adotada em 5 de abril de 2017, disponível para consulta [aqui](#)
- IFEOMA AJUNWA, *The paradox of automation as anti-bias intervention*, Cardozo law review, 2020, disponível para consulta [aqui](#)
- INSTITUTO DA DROGA E DA TOXICODEPENDÊNCIA, I.P., E AUTORIDADE PARA AS CONDIÇÕES DO TRABALHO, *Segurança e Saúde no Trabalho e a Prevenção do Consumo de Substâncias Psicoactivas: Linhas Orientadoras para a Intervenção em Meio Laboral*, 8.ª versão, 13 de janeiro de 2010, disponível para consulta [aqui](#)

- JAMES BEVERAGE, *The Privacy Act of 1974: An Overview*, Duke Law Journal, Vol. 1976, No. 2 Seventh Annual Administrative Law Issue (May, 1976), disponível para consulta [aqui](#)
- JAVIER FERNÁNDEZ ORRICO, *Límites a la biometría como medio de identificación y control de los trabajadores: necesidad de su regulación*, In *Vigilancia y control en el Derecho del Trabajo Digital*, 1.ª ed., febrero, 2020, Aranzadi, disponível para consulta [aqui](#)
- JEFFREY DASTIN, *Amazon scraps secret AI recruiting tool that showed bias against woman*, Reuters, October 11, 2018, disponível para consulta [aqui](#)
- JENNY R. YANG, *Ensuring a future that advances equity in algorithmic employment decisions: The future of work: protecting workers' civil rights in the digital era*, Washington DC: Urban Institute, February 5, disponível para consulta [aqui](#)
- JESÚS R. MERCADER UGUINA, *Algoritmos e inteligencia artificial en el derecho digital del trabajo*, tirant lo blach, Valencia, 2022
- JOANA MAGINA, *Fundamentos de licitude do tratamento de dados pessoais em contexto laboral*, In MARIA DO ROSÁRIO PALMA RAMALHO E TERESA COELHO MOREIRA, *O regulamento geral de proteção de dados e as relações de trabalho – Estudos APODIT 6*, Lisboa, AAFDL Editora, 2020
- JOÃO LEAL AMADO, *Contrato de Trabalho: noções básicas*, 4.ª Edição, 2023, Almedina
- JOÃO LEAL AMADO, *Direito do Trabalho: Relação Individual*, 2.ª Edição, 2023, Almedina
- JOÃO LUÍS NOGUEIRA MATIAS, RICARDO ANTÓNIO MAIA DE MORAIS JÚNIOR, *Discriminação algorítmica na relação de emprego: eficiência económica, inteligência artificial e fragilidade do emprego*, Revista do Tribunal Superior do Trabalho, Porto Alegre, n.º 90, n.º 2, 2024, disponível para consulta [aqui](#)
- JOÃO P. MONJARDINO, *A recolha de dados biométricos no contexto laboral*, E-Report, Outubro 2018, disponível para consulta [aqui](#)
- JORGE MIRANDA, RUI MEDEIROS, *Constituição Portuguesa Anotada*, Tomo I, Introdução Geral, Preâmbulo, Artigos 1.º a 79.º, Coimbra Editora, 2005

- JOSÉ JOÃO ABRANTES E ISABEL VALENTE DIAS, *Regulação do uso do algoritmo nas relações laborais*, In Questões Laborais N.º 63: Agenda do Trabalho Digno, Ano XXX – n.º 63 – Jul/Dez 2023 – Periodicidade Semestral
- JOSÉ VIDA FERNÁNDEZ, *La gobernanza de los riesgos digitales: desafíos y avances en la regulación de la inteligencia artificial*, Cuadernos de Derecho Transnacional. 2022, Vol. 14, n.º 1, disponível para consulta [aqui](#)
- LAURA SCHERTEL MENDES E MARCELA MATTIUZZO, *Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia*, RDU, Porto Alegre, Volume 16, n.º 90, 2019, disponível para consulta [aqui](#)
- LEILIANE PIOVESANI VIDELETTI, *Caso BĂRBULESCU V. ROMÊNIA: Tensão entre o poder diretivo do empregador e o direito à privacidade do empregador no contexto da sociedade tecnológica*, Revista Jurídica Luso-Brasileira, Ano 6, 2020, n.º 4, disponível para consulta [aqui](#)
- LENORE COOPER GARON, *Protecting Privacy in Credit Reporting*, Journal Article, Stanford Law Review, Vol. 24, no. 3 (Feb., 1972), disponível para consulta [aqui](#)
- LURDES DIAS ALVES, *Proteção de Dados Pessoais no Contexto Laboral: o direito à privacidade do trabalhador*, Almedina, 2020
- *Manual da Legislação Europeia sobre Proteção de Dados*, Edição de 2018, Agência dos Direitos Fundamentais da União Europeia e Conselho da Europa, 2022, disponível para consulta [aqui](#)
- MARIA DEL MAR CRESPI FERRIOL, *El tratamiento de los datos personales relativos a salud de los trabajadores*, Revista General de Derecho del Trabajo y de la Seguridad Social 52, 2019, disponível para consulta [aqui](#)
- MARIA DO ROSÁRIO PALMA RAMALHO, *Tratado de Direito do Trabalho, Parte I – Dogmática Geral*, 5.ª Edição, Almedina, 2020
- MARIA DO ROSÁRIO PALMA RAMALHO, *Tratado de Direito do Trabalho, Parte II – Situações Laborais Individuais*, 8.ª Edição, Almedina, 2021
- MARIANA ALVES TEIXEIRA, *Da (des)proteção do Candidato a Emprego em Face da Inteligência Artificial*, Almedina, 2023
- MARYKATE ZUKIEWICZ, MELISSA A CLARK, LIBBY MAKOWSKY, *Implementation of the Teach For America Investing in Innovation Scale-Up*, In Mathematica Policy Research, Princeton, 2015

- MATTHEW BODIE, MIRIAM A. CHERRY, MARIA L. MCCORMICK, JINTONG TANG, *The Law and Policy of People Analytics*, Legal Studies Research Paper Series, Saint Louis University School of Law, No. 2016-6, disponível para consulta [aqui](#)
- MILENA DA SILVA ROUXINOL, *O agente algorítmico – licença para discriminar? (um olhar sobre a seleção de candidatos a trabalhadores através de técnicas de inteligência artificial)*, In Mafalda Miranda Barbosa, Felipe Braga Netto, Michael César Silva, José Luiz de Moura Faleiros Júnior, *Direito Digital e Inteligência Artificial: Diálogos Entre Brasil e Europa*, Editora Foco, 2021
- MIRANDA BOGEN, AARON RIEKE, *Help wanted: an examination of hiring algorithms, equity and bias*, Washington DC: Upturn, 2018, disponível para consulta [aqui](#)
- OLGA GARCIA COCOA, *La protección de datos de carácter personal en los procesos de búsqueda de empleo*, Laborum, Murcia, 2016
- ORGANIZAÇÃO INTERNACIONAL DO TRABALHO, *Trabalhar para um futuro melhor*, Comissão Mundial sobre o futuro do trabalho, 2019
- PAWEŁ NOWIK, *New challenges for trade unions in the face of algorithmic management in the work environment.*, Studies on Labour Law and Social Policy, 2022, 29, nr 2, disponível para consulta [aqui](#)
- PEDRO FURTADO MARTINS, *Cessação do Contrato de Trabalho*, Princípia, Cascais, 4.^a edição, setembro de 2017
- PER LUNDIN, *Computers and Welfare: The Swedish Debate on the Politics of Computerization in the 1970s and the 1980s. 4th History of Nordic Computing (HiNC4)*, Aug 2014, Copenhagen, Denmark, disponível para consulta [aqui](#)
- PRODATA, *Taxa de analfabetismo segundo os Censos: total e por sexo*, disponível para consulta [aqui](#).
- PWC, *Artificial Intelligence in HR: a No-brainer*, disponível para consulta [aqui](#)
- RACHIT GARG, ARVIND W KIWELEKAR, LAXMAN D NETAK, AKSHAY GHODAKE, *I-Pulse: A NPL based novel approach for employee engagement in logistics organization*, International Journal of Information Management Data Insights, 2021, disponível para consulta [aqui](#)
- RAY EITEL-PORTER, *Beyond the promise: implementing AI*, AI and Ethics (2021), disponível para consulta [aqui](#)

- Recomendação CM/Rec(2015)5 do Comité de Ministros aos Estados-Membros sobre o tratamento de dados pessoais no contexto laboral, adotado pelo Comité de Ministro em 01.04.2015, disponível para consulta [aqui](#)
- *Records, Computers and the Rights of Citizens*, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Department of Health, Education & Welfare, July 1973, DHEW Publication NO. (OS) 73-94, disponível para consulta [aqui](#)
- RICHARD A. BALES AND KATHERINE VW STONE, *The Invisible Web at Work: Artificial Intelligence and Electronic Surveillance in the Workplace*, In 41 Berkeley Journal of Employment and Labor Law 1, 10.06.202, disponível para consulta [aqui](#)
- RICHARD H. GOLDSTEIN/ MARK S BRODIE, *Commercial Credit Bureaus: The Rights to Privacy and State Actions*, 24 AM. U. L. REV. 421, 1975
- ROBERTO FERNÁNDEZ FERNÁNDEZ, *Selección de trabajadores y algoritmos: desafíos ante las nuevas formas de reclutamiento*, Thomson Reuters, 2022
- RODRIGO SERRA LOURENÇO, *Consentimento e acordo do trabalhador para tratamento dos seus dados pessoais – Comentário ao Acórdão da RC de 19/06/2021*, In REVISTA DO CENTRO DE ESTUDOS JUDICIÁRIOS, *Privacidade e Dados Pessoais*, 2023 - II
- RUPA BANERJEE, JEFFREY G. REITZ, PHIL OREOPOULOS, *Do Large Employers Treat Racial Minorities More Fairly? An Analysis of Canadian Field Experiment Data*, In Canadian Public Policy, University of Toronto Press, Vol. 44, no. 1, 2018, disponível para consulta [aqui](#)
- SANDRA WACHTER, BRENT MITTELSTADT E CHRIS RUSSEL, *Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI*, Computer Law & Security Review, n.º 41, 2021, disponível para consulta [aqui](#)
- SERVICIO DE ESTUDIOS DE LA CONFEDERACIÓN, *Las decisiones algorítmicas en las relaciones laborales*, 8 febrero 2021, n.º 20, disponível para consulta [aqui](#)
- SIMÃO DE SANT'ANA E VITORINO GOUVEIA, *O RGPD e os recursos humanos: guia prático para a conformidade*, Almedina, junho 2022
- SOLON BAROCAS & ANDREW D. SELBST, *Big Data's Disparate Impact*, California Law Review, Vol. 104, 2016, disponível para consulta [aqui](#)

- SPENCER MAINKA, *Algorithm-Based Recruitment Technology in the Workplace*, 5 Tex. A&M J. Prop. L. 801 (2018), disponível para consulta [aqui](#)
- TERESA COELHO MOREIRA, *Algumas Implicações Laborais do Regulamento Geral de Proteção de Dados Pessoais no Trabalho 4.0*, Revista Questões Laborais, n.º 51, dezembro, 2017
- TERESA COELHO MOREIRA, *Gestão Algorítmica*, In *Liber Amicorum Benedita Mac Croire*, Volume II, 14 de dezembro de 2022, disponível para consulta [aqui](#)
- TERESA COELHO MOREIRA, *Dados pessoais: breve análise do art. 28.º da lei n.º 58/2019*, de 8 de agosto, Revista Questões Laborais (Ano XXVI, n.º 55, julho/dezembro 2019), 2020
- TERESA COELHO MOREIRA, *Direito do Trabalho: Relação Individual*, 2.ª Edição, 2023, Almedina
- U.S. DEPARTMENT OF COMMERCE, U.S. DEPARTMENT OF LABOR, *Good Job Principles*, disponível para consulta [aqui](#),
- U.S. DEPARTMENT OF LABOR, *Artificial Intelligence and worker well-being: principles and best practices for developers and employers*, October 2024, disponível para consulta [aqui](#)
- VALERIO DE STEFANO, SIMON TAES, *Algorithmic management and collective bargaining*, ETUI aisbl, Brussels, 2021, ISSN 2507-1548, disponível para consulta [aqui](#)
- VERN COUNTRYMAN, *The Diminishing Right of Privacy: The personal Dossier and the Computer*, In *Law in Contemporary Society, The Orgain Lectures*, The University of Texas Press, Austin and London, disponível para consulta [aqui](#)
- *What is personal data? Key definitions*, The General Data Protection Regulation, Information Commissioner's Office, 17 October 2022 – 1.0.11
- WOLFGANG HOFFMANN -RIEM, *Controle do Comportamento por Meio de Algoritmos: um Desafio para o Direito*, RDP, Edição especial, 2019, disponível para consulta [aqui](#)
- WOODROW BARFIELD, UGO PAGALLO, *Advanced introduction to law and artificial intelligence*, Edward Elgar Advanced Introductions, 2020, disponível para consulta [aqui](#)
- YURI GUVERICH, *What is an algorithm?*, M. Bielíková et. Al. (Eds.): SOFSEM 2012, LNCS 7147, disponível para consulta [aqui](#)

- ZHI-HUA ZHOU, *Machine learning*, Translated by Shaowu Liu, ISBN: 978-981-15-1967-3, disponível para consulta [aqui](#)