FACULDADE DE DIREITO
UNIVERSIDADE DE LISBOA

MESTRADO EM DIREITO E PRÁTICA JURÍDICA

ESPECIALIDADE EM DIREITO DA EMPRESA

Patricia Gurzone

A PROTEÇÃO DE DADOS E AS NOVAS TECNOLOGIAS

Orientador:
Professor Doutor Diogo Neves Pereira Duarte

Lisboa
2022

UNIVERSIDADE DE LISBOA
FACULDADE DE DIREITO

Patricia Gurzone

A PROTEÇÃO DE DADOS E AS NOVAS TECNOLOGIAS

Dissertação de Mestrado, como requisito parcial à obtenção do grau de Mestre em Direito da Empresa pela Faculdade de Direito da Universidade de Lisboa – curso de Mestrado em Direito e Prática Jurídica, realizada sob a orientação do Professor Doutor Diogo Neves Pereira Duarte.

Lisboa
2022

UNIVERSIDADE DE LISBOA
FACULDADE DE DIREITO

Patricia Gurzone

A PROTEÇÃO DE DADOS E AS NOVAS TECNOLOGIAS

Dissertação de Mestrado, como requisito parcial à obtenção do grau de Mestre em Direito da Empresa pela Faculdade de Direito da Universidade de Lisboa – curso de Mestrado em Direito e Prática Jurídica, realizada sob a orientação do Professor Doutor Diogo Neves Pereira Duarte.

Banca Examinadora:

_____

_____

_____

Lisboa
2022

RESUMO

Esta dissertação visa analisar a questão da Proteção de Dados em razão das novas tecnologias, buscando-se responder quais são as limitações e direcionamentos impostos pelas normas de proteção de dados para as atividades de tratamento de dados, vislumbrando os riscos e consequências para a sociedade como um todo, sendo este o problema de pesquisa. Tendo-se como objetivo geral apresentar características, vantagens e desafios inerentes à proteção de dados e a utilização de novas tecnologias, trazendo à discussão as limitações e direcionamentos impostos pelas normas de proteção de dados para as atividades de tratamento de dados, vislumbrando os riscos e consequências para a sociedade como um todo. O estudo norteou-se por uma pesquisa qualitativa e descritiva e análise dos dados coletados sobre o tema com base em fundamentos para o tratamento de dados e na legislação aplicada à proteção de dados. Concluindo-se que a tecnologia avança a cada dia e com ela as formas de uso dos dados pessoais. É facto que a utilização de novas tecnologias pode trazer inúmeros benefícios, redução de custos, maior eficiência e celeridade em vários sentidos, contudo, quanto aos avanços seria viável rever e redefinir limites, de modo a não haver brechas, atualizando as formas de proteção a fim de assegurar ao titular dos dados a proteção de seus dados pessoais.

Palavras-chave: Proteção de dados. *Compliance*. *Big Data*. Novas tecnologias.

ABSTRACT

This dissertation analyzes the issue of Data Protection due to new technologies, seeking to answer what are the limitations and directions imposed by the data protection rules for data processing activities, foreseeing the risks and consequences for society as a whole, this being the research problem. The general objective is to present the characteristics, advantages and challenges inherent to data protection and the use of new technologies, bringing to discussion the limitations and directions imposed by the data protection regulations for data processing activities, glimpsing the risks and consequences for society as a whole. The study was guided by a qualitative and descriptive research and analysis of the data collected on the subject based on fundamentals for data processing and on the legislation applied to data protection. It is concluded that technology advances every day and with it the forms of use of personal data. It is a fact that the use of new technologies can bring numerous benefits, cost reduction, greater efficiency and speed in several ways, however, as to advances it would be feasible to review and redefine limits, so that there are no gaps, updating the forms of protection in order to ensure the data subject the protection of his personal data.

Keywords: Data protection. Compliance. Big data. New technologies.

LISTA DE SIGLAS E ABREVIATURAS

AIP	Avaliação de Impacto de Privacidade
CC	Código Civil
CNPD	Comissão Nacional de Proteção de Dados
GDPR	Regulamento Geral sobre a Proteção de Dados
IA	Inteligência Artificial
LGPD	Lei Geral de Proteção de Dados
MiFID	Diretiva de Instrumentos Financeiros
MIT	Massachusetts Institute of Technology
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
PIA	Avaliação de Impacto de Privacidade
RGIC	Regime Geral das Instituições de Crédito e Sociedades Financeiras
RGPD	Regulamento Geral sobre a Proteção de Dados
SEC	Securities and Exchange Commission
TJUE	Tribunal de Justiça da União Europeia
UE	União Europeia

ÍNDICE GERAL

INTRODUÇÃO

Esta dissertação visa analisar a questão da proteção de dados em função das novas tecnologias. A escolha desta análise deve-se ao facto de ser um tema atual e de grande relevância para a área do conhecimento em que se insere diretamente o estudo, bem como para as demais áreas evolvidas. Leva-se em consideração que o não cumprimento do Regulamento Geral sobre a Proteção de Dados (RGPD, ou GDPR em inglês) pode gerar uma grande exposição e risco à reputação daqueles que descumprirem a legislação, nomeadamente no que se refere aos dados pessoais.

Importante ponderar que o tema "proteção a dados pessoais" trouxe e ainda traz grande discussão e relevo ao cenário europeu após a publicação do RGPD, entretanto, não se trata de uma absoluta novidade, mas, sim, de um tema que já vinha sendo discutido em legislações anteriores ao RGPD e até mesmo na Constituição da República Portuguesa. Apesar disso, vale referir outro papel fundamental do RGPD na atualidade, por continuar trazendo discussões regulares e importantes sobre o tema da proteção de dados, levando-se em conta a velocidade da evolução tecnológica, nunca imaginada. O tratamento de dados deve ser realizado de forma lícita, sendo imperioso ao respetivo responsável que comprove o cumprimento dos princípios relativos ao tratamento dos dados pessoais.

Em função deste cenário, levantou-se o seguinte problema de pesquisa: Quais são as limitações e direcionamentos impostos pelas normas de proteção de dados para as atividades de tratamento de dados, vislumbrando os riscos e as consequências para a sociedade como um todo?

O objetivo geral centrou-se em apresentar características, vantagens e desafios inerentes à proteção de dados e a utilização de novas tecnologias, trazendo à discussão as limitações e os direcionamentos impostos pelas normas de proteção de dados para as atividades de tratamento, vislumbrando os riscos e as consequências para a sociedade como um todo.

No tocante aos objetivos específicos, buscou-se: a) levantar as legislações portuguesa e brasileira, como um olhar em paralelo, e suas aplicações à proteção de dados; b) levantar os fundamentos de legitimidade para tratamento de dados e análise acerca do consentimento; c) conhecer e angular o panorama das novas tecnologias e entender a sua relação com a proteção de dados – conforme a legislação em vigor; e d) analisar o tema acerca das decisões automatizadas e tratamento automatizado à luz do RGPD.

Este estudo norteou-se por uma pesquisa qualitativa e descritiva, cuja coleta de dados contou com um levantamento bibliográfico sobre o tema, apoiando-se no conhecimento publicado em material impresso e *on-line* por pesquisadores em livros, artigos, legislação e jurisprudência. Mediante os dados coletados, a construção desta dissertação, para melhor compreensão do assunto abordado, foi dividida em 5 capítulos, como elencados a seguir.

No Capítulo 1, aborda-se a Legislação aplicada à Proteção de Dados, em termos gerais, trazendo considerações acerca do Regulamento Geral sobre a Proteção de Dados (RGPD), e sobre a Lei n.º 58, de 8 de agosto de 2019, que assegura a execução, na ordem jurídica portuguesa do RGPD e aplicam-se aos tratamentos de dados pessoais realizados no território português, independentemente da natureza pública ou privada do responsável pelo tratamento ou do subcontratante; também são apresentados os conceitos de anonimização e pseudonimização, considerando-se inclusive o direito de todo cidadão ao acesso de seus respetivos dados informatizados. Na sequência, abordam-se os princípios relativos ao tratamento de dados pessoais. Discorre-se sobre o papel do encarregado de proteção de dados, as questões de portabilidade e interoperabilidade, prazo de conservação dos dados e anonimização.

Ainda, o Capítulo 1 traz considerações a respeito da Lei Geral de Proteção de Dados Pessoais brasileira (LGPD), n.º 13.709, de 14 de agosto de 2018, iniciando pelos princípios relativos ao tratamento dos dados pessoais previstos na referida lei, quais sejam: boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e, por fim, responsabilização e prestação de contas; e as bases legais para o tratamento dos dados pessoais previstos na LGPD, no que concerne a consentimento e legítimo interesse.

No Capítulo 2, entra-se no âmbito da adequação à regulamentação de Proteção de Dados, passando pelas respetivas ações: realização de auditoria inicial, definição das medidas de adequação e implementação das referidas medidas de adequação. Aborda-se também o tema de *compliance* e a respectiva avaliação de impacto sobre a proteção de dados.

No Capítulo 3, expõem-se os fundamentos de legitimidade para o tratamento de dados e analisa-se a definição de consentimento e o seu desdobramento em consentimento livre, específico e informado, bem como a análise acerca do interesse legítimo.

No Capítulo 4, abre-se o panorama das novas tecnologias e sua relação com a proteção de dados, trazendo um entendimento geral sobre *big data* e seus 3 Vs – volumetria, variedade e velocidade; os princípios e fundamentos da proteção de dados e utilização do *big data*; entra-se no âmbito da inteligência artificial e nesse ponto, fala-se sobre *machine learning*, consultoria robótica, ética e inteligência artificial, proposta de regulamento do Parlamento Europeu e do Conselho sobre Regras Harmonizadas em Matéria de inteligência artificial; finalizando o capítulo com considerações acerca da *blockchain*.

No Capítulo 5, discorre-se sobre decisões automatizadas e tratamento automatizado, exclusivamente com base em definição de perfis, cujo uso dispensa a intervenção humana no processo de tomada de decisão, respeitadas algumas previsões do RGPD; as exceções à utilização de tratamento automatizado; o direito à explicação; o uso de decisões automatizadas e discriminação; o direito à portabilidade de dados e tratamento automatizado.

Por fim, desenvolve-se uma análise conclusiva sobre a utilização de novas tecnologias em relação à proteção de dados, depreendendo-se que tais tecnologias podem gerar oportunidades de negócios, redução de custos de conservação dos dados e a capacidade de tratar elevado volume de informação. A economia digital trará cada vez mais desafios ao mercado, e este deve estar preparado de maneira satisfatória para esta jornada. A regulamentação deve evoluir no sentido de que seja considerada uma aliada ao desenvolvimento tecnológico e desenvolvimento do mercado digital, nomeadamente no que se refere à busca pela proteção dos dados, de forma que a evolução esteja aliada à segurança, bem como à solidez e transparência.

1 LEGISLAÇÃO APLICADA À PROTEÇÃO DE DADOS

Este capítulo destina-se a apresentar a legislação aplicada à proteção de dados, quais sejam o Regulamento Geral sobre a Proteção de Dados (RGPD), a Lei n.º 58, de 8 de agosto de 2019, da República Portuguesa, bem como considerações sobre a Lei Geral de Proteção de Dados (LGPD) brasileira. Serão analisados os seus conceitos, aplicabilidade, amplitude, de modo a ter um panorama macro da legislação aplicada à proteção de dados.

1.1 Regulamento Geral sobre a Proteção de Dados (RGPD)

O Regulamento Geral sobre a Proteção de Dados (RGPD) (UE) n.º 679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, está em vigor desde o dia 25 de maio de 2018.

O principal objetivo do RGPD é "contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união económica, para o progresso económico e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares"[1]. Desta forma, as empresas tiveram obrigatoriamente de passar a proteger eficazmente os dados dos seus clientes, entre diversas outras responsabilidades, devendo inclusive informar ao órgão regulador obre qualquer vazamento de dados pessoais, caso ocorram.

O RGPD, portanto, estabelece regras relativas à proteção das pessoas singulares, no que diz respeto ao tratamento de dados pessoais e à livre circulação desses mesmos dados; defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o direito à proteção dos dados pessoais; e, estabelece que a proteção das pessoas singulares, relativamente ao tratamento de seus dados pessoais, é um direito fundamental, como trata o seu Considerando 1.[2]

[1] REGULAMENTO (UE) 2016/679 do Parlamento Europeu e do Conselho da União Europeia de 27 de abril de 2016. [Em linha]. **Jornal Oficial da União Europeia**. 4 maio 2016. [Consult. 8 jan. 2022]. Disponível em WWW:<URL:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>.
[2] Ibidem. p.1.

O Artigo 8.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia[3] e o Artigo 16.º, n.º 1 do Tratado sobre o Funcionamento da União Europeia[4] determinam que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeto.

O RGPD busca compatibilizar princípios e valores preservando os direitos individuais. A forma de alcançar esse propósito é conservando a privacidade ajustada à lei, à ética e à moral que regem a sociedade.[5]

Importante destacar que o direito à proteção de dados pessoais não é uma regra absoluta, isto é, deve sempre ser considerado e ponderado em relação à sua função na sociedade e, ainda, equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade.

O RGPD consagra o respeto pela vida privada e familiar, o domicílio e as comunicações, a proteção dos dados pessoais, a liberdade de pensamento, de consciência e de religião, a liberdade de expressão e de informação, a liberdade de empresa, o direito à ação e a um tribunal imparcial, bem como à diversidade cultural, religiosa e linguística.[6]

Lurdes Dias Alves entende que o RGPD alterou por completo o paradigma da regulação em matéria de proteção de dados pessoais, passando de hétero regulação para autorregulação.[7]

O RGPD extinguiu o controle prévio exercido pela Autoridade Nacional, em Portugal, a Comissão Nacional de Proteção de Dados (CNPD). Nesse sentido, não existe a necessidade de comunicação ou autorização prévia para realização do tratamento de dados pessoais. Isso significa maior liberdade às empresas, desde que respeitados os direitos dos titulares dos dados, viabilizando uma evolução constante e inúmeras possibilidades em face das novas tecnologias. Relativamente a esse ponto, o regulamento considera que as novas tecnologias podem permitir que as empresas privadas e as entidades públicas utilizem os

---

[3] CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA. [Em linha]. **Jornal Oficial da União Europeia**. 7 jun. 2016. 2016/C 202/02. [Consult. 08 jan. 2022]. Disponível em WWW:<URL:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/ TXT&from=FR>.

[4] TRATADO SOBRE O FUNCIONAMENTO DA UNIÃO EUROPEIA (versão consolidada). [Em linha]. **Jornal Oficial da União Europeia**. 7 jun. 2016. 2016/C 202/47. [Consult. 12 jan>]. Disponível em WWW:<URL:https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF>.

[5] ANTUNES, Luis - **Pôr em prática o RGPD**. Lisboa, Portugal: FCA, 2018. p. 51.

[6] REGULAMENTO (UE), 2016.

[7] ALVES, Lurdes Dias - **Regulamento geral de proteção de dados: principais dificuldades e dúvidas das organizações e dos titulares de dados pessoais na adaptação ao atual regime.** Lisboa: Cyberlaw, 1(6) (2018). p. 13.

dados pessoais numa escala nunca vista anteriormente no exercício das suas atividades. Desse modo, as referidas tecnologias transformaram a economia e a vida social e devem contribuir para facilitar a livre circulação de dados pessoais, assegurando elevado nível de proteção dos dados das pessoas singulares.[8]

Neste sentido, Hanna Arendt afirma:

> Uma crise [mudança de época] obriga-nos a voltar às perguntas originais e exige de nós respostas sejam elas novas ou velhas, mas que respondam diretamente à questão. Uma crise apenas se transformará num desastre se for respondida com juízos preconcebidos, ou seja, preconceitos.[9]

O RGPD pode ser visto como uma oportunidade de transformação digital para a União Europeia, desenvolvendo a economia digital. Importa destacar que referida transformação poderia culminar num desastre, a depender de como a norma seria interpretada, utilizada e aplicada.[10]

Em vista desta questão, não basta verificar apenas a existência das normas, sendo de extrema importância a implementação de procedimentos sólidos e robustos que façam com que os titulares dos dados confiem na economia digital. Tanto os titulares dos dados pessoais como as empresas devem adquirir uma consciência real acerca da economia pautada em dados, e saber o quanto é essencial para o desenvolvimento futuro.[11]

O RGPD deve ser visto como uma grande oportunidade de modernização para empresas e organizações, sendo que a adequação é vista como uma vantagem competitiva uma vez que os titulares dos dados terão uma confiança adicional nos processos de tratamento e utilização de seus dados.[12]

De forma a assegurar um nível de proteção coerente das pessoas singulares e eliminar os obstáculos à circulação de dados pessoais na União Europeia, o nível de proteção dos direitos e liberdades das pessoas singulares relativamente ao tratamento desses dados deve ser equivalente em todos os Estados-Membros.[13]

---

[8] REGULAMENTO (UE), 2016.
[9] ARENDT, Hanna - **Between Past and Future:** Eight exercises in Political Thought. Londres: Penguin Books, 1993. p. 141.
[10] SANTOS, Sofia Berberan; GABRIEL, João - **Regulamento Geral de Protecção de Dados, Legislação e Algumas Notas.** Lisboa: CPA Academy, 2017. pp. 15-16.
[11] TRIBUNAL CONSTITUCIONAL - **Estudos em homenagem ao Conselheiro Presidente Joaquim de Sousa Ribeiro.** Coimbra: Almedina, 2019. p. 504.
[12] Ibidem. p. 503.
[13] REGULAMENTO (UE), *op cit.*

No que se refere ao tratamento de dados pessoais para cumprimento de uma obrigação jurídica, para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento, os Estados-Membros estão autorizados a aprovar disposições nacionais para especificar a aplicação das regras do RGPD.[14]

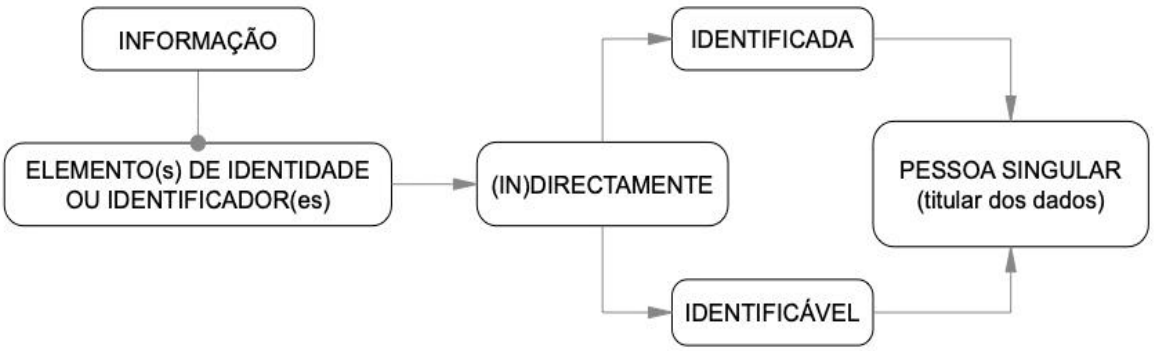
1.1.1 Dado pessoal de acordo com o RGPD

Dado pessoal pode ser entendido como a informação relativa a uma pessoa singular identificada ou identificável, como mostra a Figura 1. Portanto, é importante referir que para ser considerado um dado pessoal, a informação deve ser relativa a uma pessoa.

De acordo com o disposto no RGPD:

> É considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.[15]

Figura 1. Dados pessoais[16]



O Considerando 26 do RGPD estabelece que os princípios da proteção de dados aplicam-se a qualquer informação relativa a uma pessoa singular identificada ou identificável.

[14] REGULAMENTO (UE), 2016.
[15] Ibidem.
[16] UNIVERSIDADE DE COIMBRA - **Informação Administrativa e Proteção de Dados. Dados Pessoais**. [Em linha]. 2020 (a). [Consult. 15 abr. 2022]. Disponível em WWW:<URL:https://www.uc.pt/protecao-de-dados/protecao_dados_pessoais/conceitos_basicos_protecao_de_dados/dados_pessoais>.

Os dados pessoais que tenham sido pseudonimizados, que possam ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares, deverão ser considerados informações sobre uma pessoa singular identificável.[17]

1.1.1.1 Conceito de anonimização e pseudonimização

1.1.1.1.1 Anonimização

No tocante à anonimização, os princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, isto é, às informações que não digam respeto a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado.[18,19]

> […] Os princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeto a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz, por isso, respeto ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação.[20]

Acerca da anonimização o Anuário de Protecção de Dados dos autores Francisco Pereira Coutinho e Graça Canto Moniz explica:

> *As a started principle, when data is rendered anonymous (Recital 26 of the GDPR) all identifying elements have been irreversibly eliminated from a set of personal data, and allows no possibility to re-identify the person(s) concerned. Consequently, it is deemed to be no longer personal data. Later, anonymized data might be aggregated in order to be analyzed and to gain insights about the population, as well as combined*

[17] UNIVERSIDADE DE COIMBRA, 2020 (a).

[18] Concessão do anonimato no âmbito dos processos entrados no Tribunal de Justiça. Quando uma parte considerar necessário que alguns dos seus dados pessoais não sejam divulgados no âmbito das publicações relacionadas com um processo entrado no Tribunal de Justiça, pode dirigir-se a este último para, se for caso disso, requerer que lhe seja concedido o anonimato no âmbito desse processo. Para preservar a sua eficácia, esse pedido deve, no entanto, ser apresentado o mais cedo possível no processo. Devido à crescente utilização das novas tecnologias da informação e às obrigações que incumbem ao Tribunal de Justiça em matéria de publicações, a anonimização será com efeito muito mais difícil de se concretizar – e pode, assim, ficar privada de efeito útil – se a comunicação relativa à entrada do processo em causa já tiver sido publicada no Jornal Oficial da União Europeia.

[19] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA - **A proteção de dados pessoais no âmbito das publicações relativas aos processos judiciais no Tribunal de Justiça**. [Em linha]. 2015. [Consult. 13 jan. 2022]. Disponível em WWW:<URL:https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-11/tra-doc-pt-div-c-0000-2015-201508723-05_00.pdf>.

[20] Considerando 26 do RGPD.

with data from any other sources. At this stage, IoT developers can analyze, share, sell or publish the data without any data protection requirements. [21,22]

O RGPD não diz respeto ao tratamento de informações anónimas, inclusive para fins estatísticos ou de investigação. Toda informação é considerada relevante para efeitos de aplicação do Direito da proteção de dados.[23] O objetivo do legislador é atribuir um sentido amplo ao conceito de dado pessoal, não estando limitado às informações sensíveis ou de ordem privada. Assim, deve considerar qualquer tipo de informação que diga respeto a uma determinada pessoa.

1.1.1.1.2 Pseudonimização

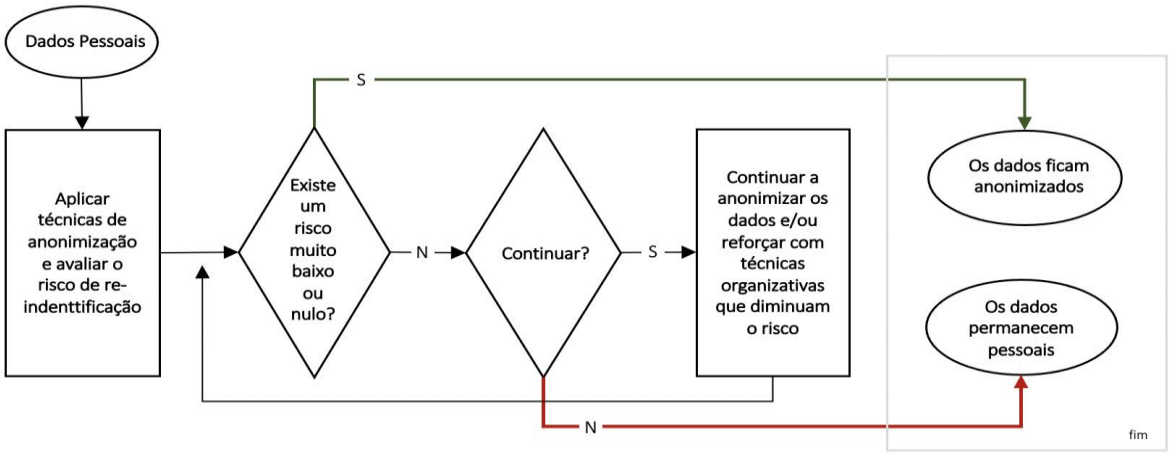
O RGPD determina o conceito de pseudonimização, ou seja, o tratamento de dados pessoais para que não possam mais ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que tais informações sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas, de modo a garantir que os dados pessoais não sejam atribuídos a uma pessoa singular identificada ou identificável.[24]

Ainda de acordo com o RGPD, 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. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica.[25]

A Figura 2, ilustra o conceito de anonimização e pseudonimização.

[21] PEREIRA COUTINHO, Francisco; CANTO MONIZ, Graça (Coords.) - **Anuário de Proteção de Dados - 2019**. Lisboa: CEDIS, 2019. p. 103.
[22] Como princípio inicial, quando os dados são tornados anónimos (considerando 26 do RGPD) todos os elementos de identificação foram eliminados de um conjunto de dados pessoais, e não permite qualquer possibilidade de reidentificar a pessoa em causa. Consequentemente, considera-se que já não se trata de dados pessoais. Mais tarde, os dados anonimizados poderão ser agregados para serem analisados e para se obterem informações, bem como combinados com dados de quaisquer outras fontes. Nesta fase, os programadores podem analisar, partilhar, vender ou publicar os dados sem quaisquer requisitos de proteção de dados. (Tradução livre)
[23] KLAR, Manuel; KÜHLING, Jürgen - **Anotação ao artigo 4.º do RGPD** em Kühling/Buchner, DatenschutzGrundverordnung. 2.ª ed. Beck, Munique, 2018. Rn.9.
[24] REGULAMENTO (UE), 2016.
[25] Ibidem.

Figura 2. Anonimização e Pseudonimização[26]



> Acerca do conceito de informação, A. Barreto Menezes Cordeiro explica que:
>
> A noção de informação (pessoal) vai muito além do significado tradicionalmente atribuído a ela no contexto dos direitos da personalidade, ainda que pressuponha, como faz o Tribunal Europeu dos Direitos do Homem, uma conceção mais flexível. Privacidade não deve ser considerado como sinónimo de direitos pessoais, nem a proteção concedida pelo regime jurídico previsto no Artigo 80.º do Código Civil (CC) é idêntica à prevista pelo Direito da proteção de dados.[27]

Deverá, então, entender como sendo pessoal, toda informação relativa à vida privada e à vida profissional e social de uma pessoa singular. Relativamente ao conceito de informação, A. Barreto Menezes Cordeiro afirma que "o conceito de informação pessoal abrange, consequentemente, todos os aspetos relativos à nossa pessoa, quer sejam familiares ou sociais, privados ou públicos, físicos ou mentais".[28]

Neste sentido e no que diz respeto ao conceito de dado pessoal, Nuno Saldanha explica que:

> Qualquer tipo de informação, se for relativa a uma pessoa, pode ser considerado dado pessoal e estes dados pessoais conter informações sobre a vida privada (mas não da esfera privada) ou profissional. Para além dos óbvios dados pessoais, como números de contribuinte, de segurança social, de identificação etc., está também incluída informação referente, por exemplo, a uma avaliação profissional ou de outro género.[29]

---

[26] UNIVERSIDADE DE COIMBRA - **Informação Administrativa e Proteção de Dados. Anonimização e Pseudonimização**. [Em linha]. 2020 (b). [Consult. 2 fev. 2022]. Disponível em WWW:<URL:https://www.uc.pt/protecao-de-dados/protecao_dados_pessoais/anonimizacao>.

[27] CORDEIRO, A. Barreto Menezes - **Dados Pessoais: Conceito, Extensão e Limites. Lisboa, Portugal: Centro de Investigação de Direito Privado**. [Em linha]. 2018 (a). [Consult. 12 fev. 2022]. Disponível em WWW:<URL:https://blook.pt/publications/publication/e38a9928dbce/>. p. 05.

[28] Idem. **Direito da Proteção de Dados**. Coimbra: Almedina, 2020. p. 108.

[29] SALDANHA, Nuno - **Novo Regulamento Geral de Proteção de Dados**. Lisboa: FCA, 2018. p. 31.

1.1.1.2 Direito de acesso do cidadão aos seus respetivos dados informatizados

Importa referir que a Constituição da República Portuguesa, em seu Artigo 35.º, n.º 1, dispões que "todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeto, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos previstos na lei".[30]

O texto constitucional culmina, principalmente, em três direitos: o direito de acesso do titular dos dados aos registos informáticos, bem como a sua retificação, atualização ou eliminação; o direito ao sigilo de dados; e o direito ao não tratamento de alguns tipos de dados pessoais.[31]

O alcance do direito de acesso é regulado no Artigo 15.º, não se limitando, entretanto, ao simples acesso aos dados, sendo possível ao interessado obter do responsável pelo tratamento a confirmação da existência ou inexistência do tratamento, bem como a respetiva finalidade, categoria dos dados, destinatários, período de conservação, entre outras informações. Nos casos em que os dados pessoais ultrapassam as fronteiras da UE, aumenta o risco de o titular dos dados não conseguir exercer os seus direitos.[32]

De acordo com o Artigo 35.º, n.º 2, da Constituição da República Portuguesa, 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 por intermédio de uma entidade administrativa independente.[33] O mesmo Artigo aduz que é proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei, e define a proibição de atribuir um número nacional único aos cidadãos.[34]

[30] CONSTITUIÇÃO DA REPÚBLICA PORTUGUESA - Sétima Revisão Constitucional. [Em linha]. [Em linha]. **Diário da República**. n.º 155, I Série-A, 12 ago. 2005. [Consult. 12 jan 2022]. Disponível em WWW:<URL:https://dre.pt/legislacao-consolidada/-/lc/34520775/view>.
[31] LEAL, Ana Alves. Aspetos jurídicos da análise de dados na internet (Big data analytics) nos setores bancário e financeiro: proteção de dados pessoais e deveres de informação. In CORDEIRO, António Menezes; DUARTE, Diogo Pereira; OLIVEIRA, Ana Perestrelo de - **FinTech: desafios da tecnologia**. Coimbra: Almedina, 2017. pp. 124-125.
[32] PEREIRA COUTINHO, Francisco; CANTO MONIZ, Graça (Coords.). **Anuário da Proteção de Dados - 2018**. Lisboa: CEDIS, 2018. p. 16.
[33] CONSTITUIÇÃO DA REPÚBLICA PORTUGUESA, *op cit.* Artigo 35.º, n.º 2.
[34] Ibidem.

1.1.2 Princípios relativos ao tratamento de dados pessoais

Os princípios relativos ao tratamento de dados pessoais encontram-se plasmados no Artigo 5.º do RGPD, sendo os dados pessoais:

"a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados."[35]

Do *supra* exposto, resulta claro que o tratamento dos dados pessoais deve ser lícito, leal e transparente.

Tratamento lícito é aquele que deve ser entendido como permitido, legítimo e realizado de acordo com a lei.

De acordo com o Considerando 40 do RGPD:

> Para que o tratamento seja lícito, os dados pessoais deverão ser tratados com base no consentimento do 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. [36]

O tratamento leal, por sua vez, deve ser entendido como um tratamento fiel, que esteja de acordo com as informações prestadas ao titular no momento da recolha dos dados pessoais. O Artigo 8.º, n.º 2, da Carta dos Direitos Fundamentais da União Europeia, dispões que os dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeto e de obter a respetiva retificação.[37] A lealdade impõe aos responsáveis pelo tratamento a obrigação de perseguirem a todo tempo os interesses e as expectativas dos titulares dos dados.[38]

Já o tratamento transparente é aquele que deve ser entendido como um tratamento claro, evidente, que se percebe facilmente. O Considerando 39 do RGPD dispões que o tratamento de dados pessoais deverá ser efetuado de forma lícita e equitativa, ser transparente para as pessoas singulares, cujos dados pessoais tenham sido recolhidos, utilizados,

[35] REGULAMENTO (UE), 2016.
[36] Ibidem.
[37] CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA, 2016.
[38] CORDEIRO, 2020. p. 154.

consultados ou sujeitos a qualquer outro tipo de tratamento, e à medida que os dados pessoais são ou virão a ser tratados.

O princípio da transparência exige que as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples. Esse princípio diz respeto, em particular, às informações fornecidas aos titulares dos dados sobre a identidade do responsável pelo tratamento, aos fins a que o tratamento se destina, bem como às informações que se destinam a assegurar que seja efetuado com equidade e transparência com as pessoas singulares em causa, inclusive a proteger o seu direito de obter a confirmação e a comunicação dos dados pessoais que lhes dizem respeto e que estão sendo tratados.[39]

A transparência corresponde a um princípio geral de proteção de dados, conforme previsto no Artigo 5.º, n.º 1, alínea a), e é diretamente implementado nos Artigos 12.º a 15.º do RGPD. Este princípio estipula que as informações ou comunicações relacionadas com o tratamento de dados pessoais devem ser facilmente acessíveis, de fácil entendimento pelo titular dos dados e concisas, diretas, completas e verdadeiras.[40]

De acordo com o Artigo 12.º, n.º 1, do RGPD, o responsável pelo tratamento toma as medidas adequadas para fornecer ao titular as informações a respeto do tratamento de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças. As informações são prestadas por escrito ou por outros meios, incluindo, se for caso disso, por meios eletrônicos. Se o titular dos dados o solicitar, a informação pode ser prestada oralmente, desde que a identidade do titular seja comprovada por outros meios.[41] As informações sobre o tratamento devem estar à disposição do titular dos dados no momento da coleta, conforme Artigo 13.º. Em todos os casos, o legislador fornece o conteúdo mínimo das informações que devem ser prestadas, que incluem: identidade e dados de contato da pessoa responsável pelo tratamento; finalidade do tratamento; fundamento jurídico; destinatário dos dados; o direito de acesso, retificação, portabilidade, entre outros.[42]

"b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades".[43]

[39] REGULAMENTO (UE), 2016.
[40] LEAL, 2017. pp. 126-127.
[41] REGULAMENTO (UE), *op.cit.*
[42] PEREIRA COUTINHO; CANTO MONIZ, 2018. p. 15.
[43] REGULAMENTO (UE), *op.cit.*

Os dados pessoais devem ser recolhidos para finalidades que estejam determinadas. Portanto, deve ser realizada uma análise cuidadosa e adequada dos dados pessoais necessários ao tratamento e que, como tal, precisam ser utilizados, não sendo assim permitida a recolha de dados pessoais que não sejam relevantes e necessários ao tratamento. O princípio da especificação e da limitação das finalidades significa que a legitimidade do tratamento de dados pessoais dependerá da finalidade do tratamento[44], que deverá estar definida antes das operações de tratamento terem início. Importante destacar que a finalidade deve ser claramente informada pelo responsável pelo tratamento ao titular dos dados pessoais antes do início do tratamento de dados.

A expressão finalidade legítima deve ser interpretada de forma ampla, sendo imperioso que haja o cumprimento das disposições legais aplicáveis. Portanto, todas as finalidades que violarem a lei deverão ser consideradas ilegítimas.[45]

No que se refere à análise para saber se a finalidade de uma nova operação de tratamento dos dados é ou não compatível com a finalidade, para que os dados pessoais foram inicialmente recolhidos, importa avaliar o Considerando 50 do RGPD, que dispões que o responsável pelo seu tratamento, após ter cumprido todos os requisitos para a licitude do tratamento inicial, deverá ter em atenção à existência de uma ligação entre a primeira finalidade e aquela a que se destina a nova operação de tratamento que se pretende efetuar, o contexto em que os dados pessoais foram recolhidos, em especial as expectativas razoáveis do titular dos dados quanto à sua posterior utilização, baseadas na sua relação com o responsável pelo tratamento; a natureza dos dados pessoais; as consequências que o posterior tratamento dos dados pode ter para o seu titular; e a existência de garantias adequadas tanto no tratamento inicial como nas outras operações de tratamento previstas.[46]

Acerca de um eventual tratamento posterior, considerando as finalidades para as quais os dados foram inicialmente recolhidos, deve-se verificar se o processamento posterior é compatível com a finalidade para a qual os dados pessoais foram inicialmente coletados; inclusive, avaliar os seguintes fatores: existência de um vínculo entre a finalidade inicial e a finalidade do tratamento subsequente, contexto da recolha de dados pessoais, nomeadamente no que diz respeto à relação entre o titular dos dados e o responsável pelo tratamento, à natureza dos dados pessoais, com particular atenção às categorias especiais de dados

[44] Convenção 108, Artigo 5.º, alínea. b); Diretiva Proteção de Dados, Artigo 6.º, n.º 1, alínea. b).
[45] CORDEIRO, 2020. p. 156.
[46] REGULAMENTO (UE), 2016.

pessoais[47], às possíveis consequências do subsequente tratamento e à existência de salvaguardas adequadas, cifragem ou pseudonimização, por exemplo.[48]

De uma leitura atenta ao Considerando 50 do RGPD, pode-se compreender que as finalidades e os tratamentos compatíveis com os originalmente assinalados não necessitam de qualquer controle extraordinário.[49] Importa ainda ressalvar que o tratamento posterior para fins de arquivo de interesse público ou para fins de investigação científica ou histórica, bem como para fins estatísticos, não é considerado incompatível com as finalidades iniciais, conforme dispões o Artigo 89.º, n.º 1 do RGPD.

"c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados".[50]

Os dados pessoais recolhidos, devem ser limitados ao que é necessário no que se refere às finalidades para as quais são tratados. Não poderão ser recolhidos dados que não sejam necessários à finalidade para a qual o tratamento é realizado em primeira instância. Acerca desse princípio, importa analisar o disposto no Considerando 39 do RGPD, segundo o qual:

> Os dados pessoais deverão ser adequados, pertinentes e limitados ao necessário para os efeitos para os quais são tratados. Para isso, é necessário assegurar que o prazo de conservação dos dados seja limitado ao mínimo. Os dados pessoais apenas deverão ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios. A fim de assegurar que os dados pessoais sejam conservados apenas durante o período considerado necessário, o responsável pelo tratamento deverá fixar os prazos para o apagamento ou a revisão periódica. Deverão ser adotadas todas as medidas razoáveis para que os dados pessoais inexatos sejam retificados ou apagados. Os dados pessoais deverão ser tratados de uma forma que garanta a devida segurança e confidencialidade, incluindo para evitar o acesso a

[47] 8 CATEGORIAS ESPECIAIS DE DADOS. 8.1 O que constitui uma categoria especial de dados. O RGPD prevê proteção específica para dados pessoais que são especialmente sensíveis no que toca aos direitos e liberdades fundamentais das pessoas singulares. Esses dados encontram-se definidos no artigo 9.º do RGPD como categorias especiais de dados pessoais e incluem dados sobre a saúde, a origem racial ou étnica, as convicções religiosas ou filosóficas, as opiniões políticas, a filiação sindical, bem como dados biométricos e relativos à vida sexual ou à orientação sexual de uma pessoa singular. Os responsáveis pelo tratamento só podem tratar categorias especiais de dados se cumprirem uma das condições estabelecidas no artigo 9.º, n.º 2, do RGPD, como terem obtido o consentimento explícito do titular dos dados ou se os dados tiverem sido manifestamente tornados públicos pelo seu titular. Para além das condições do artigo 9.º do RGPD, o tratamento de categorias especiais de dados deve recorrer a um fundamento jurídico estabelecido no artigo 6.º do RGPD e ser efetuado de acordo com os princípios fundamentais estabelecidos no artigo 5.º do mesmo regulamento. Diretrizes 8/2020 sobre o direcionamento para os utilizadores das redes sociais. Versão 2.0. Adotadas em 13 de abril de 2021.

[48] MAGALHÃES, Filipa Matias; PEREIRA, Maria Leitão - **Regulamento Geral de Proteção de Dados – Manual Prático**. Porto: Vida Económica, 2018. p. 30.

[49] CORDEIRO, 2020. p. 158.

[50] REGULAMENTO (UE), 2016.

> dados pessoais e equipamento utilizado para o seu tratamento, ou a sua utilização por pessoas não autorizadas.[51]

"d) Exatos e atualizados sempre que necessário".[52]

Os dados pessoais devem ser atualizados sempre que necessário, sendo certo que o responsável pelo tratamento deve tomar as medidas necessárias para verificar se os dados pessoais fornecidos pelo titular estão corretos e exatos.

"Os direitos de retificação e ao apagamento dos dados são aplicáveis tanto aos «dados pessoais de entrada» (os dados pessoais utilizados para criar o perfil) como aos «dados de saída» (o próprio perfilou a «pontuação» atribuída à pessoa)."[53]

É importante destacar ainda que devem ser adotadas todas as medidas adequadas para que os dados inexatos sejam apagados ou retificados sem demora. Cabe ao responsável pelo tratamento dos dados optar pela solução mais adequada ao caso, de forma que complete ou apague parte da informação.[54]

De acordo com o Manual da Legislação Europeia sobre Proteção de Dados:

> Um responsável pelo tratamento que tenha em seu poder informações pessoais não deverá utilizar essas informações sem tomar medidas para se certificar, com um grau de certeza razoável, que os dados são exatos e estão atualizados. A obrigação de assegurar a exatidão dos dados tem de ser interpretada no contexto da finalidade do tratamento dos dados.[55]

"e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados".[56]

Os dados pessoais serão identificados apenas durante o período necessário ao tratamento, diante das finalidades. Existe, pois, claramente, um limite para a conservação dos dados pessoais.

De acordo com o Considerando 63 do RGPD:

> Cada titular de dados deverá ter o direito de conhecer e ser informado, nomeadamente, das finalidades para as quais os dados pessoais são tratados, quando possível do período durante o qual os dados são tratados, da identidade dos destinatários dos dados pessoais, da lógica subjacente ao eventual tratamento

[51] REGULAMENTO (UE), 2016.
[52] Ibidem.
[53] GRUPO DE TRABALHO DO ARTIGO 29.º. Comissão Europeia, Direção-Geral de Justiça para a Proteção de Dados. **Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679**. 6 fev. 2018. p. 19
[54] CORDEIRO, 2020. p. 272.
[55] AGÊNCIA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA. Conselho da Europa - **Manual da Legislação Europeia sobre Proteção de Dados**. 2014. p. 76.
[56] REGULAMENTO (UE), *op.cit.*

> automático dos dados pessoais e, pelo menos quando tiver por base a definição de perfis, das suas consequências.[57]

Os responsáveis pelo tratamento devem implementar políticas para manter, arquivar e excluir dados, garantindo que os dados não sejam retidos por mais tempo do que o necessário.[58]

Cabe destacar que os dados pessoais podem ser conservados durante períodos mais longos, no caso de serem tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o Artigo 89.º, n.º 1, do RGPD. Neste caso, devem ser aplicadas medidas técnicas e organizativas adequadas à finalidade última, que é a de proteger os direitos e liberdades do titular dos dados.

No tocante à obrigação de eliminação das informações. Quando deixam de ser necessárias, Luis Antunes afirma:

> O princípio da conservação dos dados exige que os dados sejam apagados logo que deixem de ser necessários para as finalidades para que foram recolhidos. O Artigo da lei portuguesa (Lei n.º 67/98 de 26 de outubro, Artigo 5.º) que regula este princípio refere que o prazo de conservação de dados pessoais é o que estiver fixado por lei ou, na falta desta, o que se revele necessário para a prossecução da finalidade. Mas quando, pela natureza e finalidade do tratamento, não seja possível determinar antecipadamente o momento em que o mesmo deixa de ser necessário, é lícita a conservação dos dados pessoais. No entanto, quando a finalidade que motivou o tratamento, inicial ou posterior, de dados pessoais termina, o responsável pelo tratamento deve proceder à sua destruição. Por último, nos casos em que existe um prazo de conservação de dados imposto por lei, só pode ser exercido o direito ao apagamento previsto no Artigo 17.º do RGPD findo esse prazo.[59]

É importante notar que o direito de oposição e o direito de apagamento numa fase inicial obedecem a uma lógica facultativa: a composição desses direitos no domínio do interessado. Mecanismos opcionais para esses direitos podem prever proteções para as partes interessadas contra a conduta do responsável pelo tratamento. Em sendo o tratamento proibido, o seu responsável será obrigado a não apresentar qualquer comportamento que predisponha ao referido tratamento.[60]

Por fim, ainda sobre o direito de apagamento e antecipando as dificuldades técnicas de controle da informação em ambiente *on-line*, o legislador introduziu critérios de

[57] REGULAMENTO (UE), 2016.
[58] MAGALHÃES; PEREIRA, 2018. p. 31.
[59] ANTUNES, 2018. p. 47.
[60] LEAL, 2017. p. 133.

razoabilidade, disponibilidade tecnológica e custos, flexibilizando esta obrigação e aproximando-a de uma obrigação de meio e não de resultado.[61]

Com base no princípio da autonomia, a regulamentação sobre a proteção de dados pessoais reconhece um lugar importante para o desejo individual. O acompanhamento das atividades de tratamento constitui um controle pessoal sobre os dados pessoais, independentemente da base jurídica do tratamento.[62]

"f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas".[63]

Os dados pessoais devem permanecer seguros, sendo dever do responsável pelo tratamento dos dados pessoais zelar pela respetiva confidencialidade, bem como pela sua guarda de forma segura.

Acerca das medidas de segurança e período de conservação dos dados, Nuno Saldanha afirma:

> Igualmente aliado ao tema do período de conservação dos dados está a questão da existência de medidas de segurança adequadas. Com efeito, quanto mais tempo os dados são conservados maior é o risco de perda, destruição ou mesmo de fraude sobre essa informação. Será que o ambiente físico ou lógico é o adequado para a manutenção dessa informação? Será que os ficheiros em papel estão devidamente fechados em salas, armários, gavetas, com acesso restrito com registo de acesso etc.? E quanto aos sistemas informáticos? Estão devidamente protegidos com *passwords*, firewalls, pseudonimizações, cifragens etc.?[64]

No caso de violação de dados, o responsável pelo tratamento é obrigado a garantir que está sempre atento a qualquer violação para que as medidas adequadas possam ser tomadas rapidamente. O mais importante no caso de uma violação de dados, não seria apenas comprovar o momento que o responsável tomou conhecimento da violação, mas sim as medidas implementadas de forma rápida sobre o motivo que levou à referida violação, a fim de determinar se os dados pessoais foram realmente violados, tomando todas as ações corretivas e notificações necessárias.[65]

Por último, importante referir que o responsável pelo tratamento deve cumprir os princípios relativos aos dados pessoais e pode ser chamado a comprovar referidas

[61] PEREIRA COUTINHO; CANTO MONIZ, 2018. pp. 17-18.
[62] Ibidem. p. 13.
[63] REGULAMENTO (UE), 2016.
[64] SALDANHA, Nuno - **RGPD - Guia para uma auditoria de conformidade – Dados, privacidade, implementação, controlo, compliance**. Lisboa: FCA, 2019. p. 56.
[65] ALVES, 2018. p. 15.

obrigações; deve ser capaz de demonstrar respeto aos princípios, garantindo o tratamento dos dados de acordo com o RGPD. Este é o princípio da responsabilidade que implica a necessidade de implementação de uma política de gestão e governança de dados.[66]

1.1.3 Comentários a Lei n.º 58/2019

A Lei n.º 58, de 8 de agosto de 2019, assegura a "execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares em relação ao tratamento de dados pessoais e à livre circulação desses dados".[67]

A execução do RGPD na ordem jurídica portuguesa é assegurada pela Lei n.º 58/2019, e de acordo com o seu Artigo 2.º:

> a lei aplica-se aos tratamentos de dados pessoais realizados no território nacional, independentemente da natureza pública ou privada do responsável pelo tratamento ou do subcontratante, mesmo que o tratamento de dados pessoais seja efetuado em cumprimento de obrigações legais ou no âmbito da prossecução de missões de interesse público, aplicando-se as exclusões previstas no Artigo 2.º do RG.[68]

Aplica-se a lei em questão aos tratamentos de dados pessoais realizados fora do território português quando forem efetuados no âmbito da atividade de um estabelecimento situado no território português; ou afetarem titulares de dados que se encontrem no território português, quando as atividades de tratamento estejam subordinadas ao disposto no Artigo 3.º, n.º 2, do RGPD, sobre o tratamento de dados pessoais de titulares residentes no território da União; ou afetarem dados que estejam inscritos nos postos consulares de que sejam titulares portugueses residentes no estrangeiro.[69]

A Lei n.º 58/2019 explicita que a Comissão Nacional de Proteção de Dados (CNPD) é a autoridade de controle nacional para efeitos do RGPD. Cumpre destacar que *a CNPD "*é uma entidade administrativa independente, com personalidade jurídica de direito público e poderes de autoridade, dotada de autonomia administrativa e financeira, que funciona junto da Assembleia da República".

---

[66] MAGALHÃES; PEREIRA, 2018. p. 32.
[67] LEI Nº 58/2019, de 8 de agosto, da Assembleia da República Portuguesa. [Em linha]. **Diário da República**. 1.ª série. n.º 151. 2019. [Consult. 8 jan. 2022]. Disponível em WWW:<URL:https://dre.pt/pesquisa/-/search/123815982/details/maximized>.
[68] Ibidem. Art. 2.º, n. 1.
[69] Ibidem.

A CNPD controla e fiscaliza o cumprimento do RGPD, bem como das demais disposições legais e regulamentares em matéria de proteção de dados pessoais, a fim de defender os direitos, liberdades e garantias das pessoas singulares no âmbito dos tratamentos de dados pessoais.[70]

1.1.3.1 Encarregado de proteção de dados conforme a Lei n.º 58/2019

A Lei n.º 58/2019 dispões que o encarregado de proteção de dados é designado com base nos requisitos previstos no RGPD, não sendo necessária certificação profissional para o efeito. Importante referir que o encarregado de proteção de dados exerce a sua função com autonomia técnica perante a entidade responsável pelo tratamento ou subcontratante.[71]

Assim como determinado no RGPD, a Lei n.º 58/2019 também delibera que o encarregado de proteção de dados está obrigado a um dever de sigilo profissional em tudo o que se refira ao exercício da função, que se mantém inclusive após o termo das funções que lhes deram origem.

O Artigo 11.º da Lei n.º 58/2019 determina que além do disposto no RGPD, são funções do encarregado de proteção de dados:

> (i) assegurar a realização de auditorias, quer periódicas, quer não programadas;
> (ii) sensibilizar os utilizadores para a importância da detecção atempada de incidentes de segurança e para a necessidade de informar imediatamente o responsável pela segurança;
> (iii) assegurar as relações com os titulares dos dados nas matérias abrangidas pelo RGPD e pela legislação nacional em matéria de proteção de dados.[72]

Importante destacar que o tratamento sob a autoridade do responsável por esta atividade, o encarregado, ou sob a autoridade do subcontratante, de acordo com o Artigo 29.º do RGPD, comentado por Francisco Rodrigues Rocha, assim dispões:

> O subcontratante ou qualquer pessoa que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, tenha acesso a dados pessoais, não procede ao tratamento desses dados exceto por instrução do responsável pelo tratamento, salvo se a tal for obrigada por força do direito da União ou dos Estados-Membros.[73]

Rocha explica que os dados só poderão ser tratados mediante instruções para isso por parte do responsável e sob sua autorização. Sendo exceção o caso em que seja requerido pelo

[70] LEI nº 58, 2019. Art. 2.º, n. 1.
[71] Ibidem. Art. 9.º, p. 3.
[72] Ibidem. Art. 11.º, p. 3.
[73] ROCHA F. R. - Responsável pelo tratamento e subcontratante. In CORDEIRO, A.B.M (Coord.) - **Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 58/2019**. Faculdade de Direito. Universidade de Lisboa. Almedina, 2021. p. 257.

direito da UE ou do Estado-membro que "qualquer pessoa, responsável pelo tratamento ou não seja obrigada a tratar dados sem ou mesmo contrariamente às instruções do responsável pelo tratamento".[74]

1.1.3.2 A portabilidade e interoperabilidade dos dados

Sobre a portabilidade dos dados, esta deve, sempre que possível, ter lugar em formato aberto. No que se refere à Administração Pública, sempre que a interoperabilidade dos dados não seja tecnicamente possível, o titular dos dados tem o direito de exigir que estes lhe sejam entregues num formato digital aberto, de acordo com o Regulamento Nacional de Interoperabilidade Digital em vigor.

O direito à portabilidade reconhece duas opções para o titular: a de receber um conjunto de dados pessoais e a de transmitir esses dados entre controladores privados de dados, sem necessariamente seguir a sua transmissão imediata a outro titular, não apenas nas situações em que o titular pretenda transferir todos os seus dados para outro provedor, mas também os casos em que deseja garantir a interoperabilidade, entre os sistemas que utiliza.[75]

1.1.3.3 Prazo de conservação dos dados

O prazo de conservação dos dados pessoais é o que estiver fixado por norma legal ou, na falta desta, o que se revele necessário para a prossecução da finalidade. Quando, pela natureza e finalidade do tratamento, designadamente para fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos, não seja possível determinar antecipadamente o momento em que ele deixa de ser necessário, é lícita a conservação dos dados pessoais, desde que sejam adotadas medidas técnicas e organizativas adequadas a garantir os direitos do titular dos dados, designadamente a informação da sua conservação.[76]

Os dados pessoais podem ser conservados enquanto não decorrer o prazo de prescrição, no caso de serem necessários para o responsável pelo tratamento, ou o subcontratante, comprovar o cumprimento de obrigações contratuais ou de outra natureza.

[74] ROCHA, 2021. p. 258.
[75] PEREIRA COUTINHO; CANTO MONIZ, 2018. p. 25.
[76] LEI Nº 58, 2019. Art. 21.º, n.º 2.

No momento que cessar a finalidade que motivou o tratamento, inicial ou posterior, de dados pessoais, o responsável pelo tratamento deve proceder à sua destruição ou anonimização.

Considerando que referida lei assegura a execução do RGPD na ordem jurídica portuguesa, importa realizar uma análise da mencionada regulamentação, permitindo vislumbrar questões específicas aplicáveis ao ordenamento jurídico português. No mesmo sentido, nos casos em que se analisa o tratamento de dados sob a ótica da legislação brasileira, importa observar a Lei n.º 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais Brasileira (LGPD).

1.2 Considerações acerca da Lei Geral de Proteção de Dados Pessoais brasileira

A Lei n.º 13.709, de 14 de agosto de 2018, dispões sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.[77]

A LGPD estabelece que dado pessoal é toda informação relacionada à pessoa natural identificada ou identificável e determina que o tratamento desses dados deve considerar os princípios de privacidade descritos na lei. Acerca desse tema, Anderson Schreiber afirma que a nova lei brasileira de proteção de dados pessoais reconhece o direito específico à proteção de dados pessoais. O Artigo 5.º, item I, da lei define dados pessoais como "dados relacionados com uma pessoa singular identificada ou identificável". A limitação da proteção aos dados relativos a pessoas singulares confirma a ligação de direito entre proteção de dados, privacidade e dignidade humana, tal como defendida pela doutrina jurídica brasileira.[78]

A lei trouxe a questão dos dados pessoais "sensíveis" que abrangem registos sobre raça, opiniões políticas, crenças, dados de saúde e características genéticas e biométricas. A lei condiciona o tratamento destes dados a um consentimento específico e sublinhado do titular, vinculado a finalidades específicas. Este consentimento só pode ser revogado em

[77] LEI N.º 13.709, de 14 de agosto de 2018, do Congresso Nacional. [Em linha]. **Diário Oficial da União**. 15 ago. 2018. [Consult. 8 jan. 2022]. Disponível em WWW:<URL:http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>.

[78] VICENTE, Dario Moura; CASIMIRO, Sofia de Vasconcelos - Data Protection in the Internet, Ius Comparatum. **Global Studies in Comparative Law**. Vol. 38, Alemanha: Springer, 2020, p. 46.

circunstâncias preestabelecidas enumeradas pela lei, por exemplo quando os dados são essenciais para a proteção da saúde ou para estudos por instituto de pesquisa.[79]

A LGPD prevê como fundamentos da proteção de dados pessoais:

> i) o respeto à privacidade;
> ii) a autodeterminação informativa;
> iii) a liberdade de expressão, de informação, de comunicação e de opinião;
> iv) a inviolabilidade da intimidade, da honra e da imagem;
> v) o desenvolvimento económico e tecnológico e a inovação;
> vi) a livre iniciativa, a livre concorrência e a defesa do consumidor;
> vii) os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.[80]

A LGPD aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

> i) a operação de tratamento seja realizada no território nacional;
> ii) a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;
> iii) ou os dados pessoais, objeto do tratamento, tenham sido coletados no território nacional.[81]

A lei em discussão não é aplicável ao tratamento de dados pessoais:

> (i) realizado por pessoa natural para fins exclusivamente particulares e não económicos;
> (ii) realizado para fins exclusivamente: jornalístico e artísticos ou acadêmicos;
> (iii) realizado para fins exclusivos de: segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais; ou
> (iv) provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na Lei.[82]

O direito à privacidade, após o tratamento promissor reservado pela Constituição de 1988[83], brasileira, que sancionava um forte compromisso em favor da proteção da vida privada, foi suspenso pelo legislador, entretanto, a extraordinária evolução tecnológica mostrou que a privacidade estava em perigo. A aprovação da lei brasileira de proteção de dados pessoais reforça o compromisso do Congresso brasileiro em realizar o projeto

[79] VICENTE; CASIMIRO, 2020. p. 46.
[80] LEI N.º 13.709, 2018.
[81] Ibidem.
[82] Ibidem.
[83] BRASIL - **Constituição da República Federativa do Brasil de 1988**. [Em linha]. 1988. [Consult. 10 fev. 2022]. Disponível em WWW:<URL:http://www.planalto.gov.br/ ccivil_03/constituicao/constituicao.htm>.

constitucional, bem como em aproximar o Brasil das melhores experiências internacionais no assunto. A criação de uma agência independente responsável pela proteção de dados pessoais é urgente. Só assim será possível evitar que todos os esforços para a criação da nova lei se tornem ineficazes na transformação da realidade brasileira.[84]

1.2.1 Princípios relativos ao tratamento dos dados pessoais previstos na LGPD

As atividades de tratamento de dados pessoais deverão observar a boa-fé e os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

(i) Boa-fé:

No que se refere especificamente às atividades de tratamento de dados pessoais, a boa-fé está prevista no Artigo 6.º da LGPD, no qual se verifica a obrigatoriedade de observar a boa-fé objetiva, como regra de conduta, do qual se extrai a norma de comportamento que exige lealdade, honestidade e respeto aos interesses da outra parte.[85]

Como ensina Silvio Rodrigues, "a boa-fé é um conceito ético, moldado nas ideias de proceder com correção, com dignidade, pautando sua atitude pelos princípios da honestidade, da boa intenção e no propósito de a ninguém prejudicar".[86] Caio Mario da Silva Pereira, por sua vez, aduz que "trata-se de cláusula geral de observância obrigatória, veiculadora de conceito jurídico indeterminado, a ser concretizada segundo as peculiaridades de cada caso".[87]

A boa-fé objetiva deve ser observada para legitimar o tratamento de dados pessoais, que deve corresponder às razoáveis expectativas de seu titular, que confia seus dados à outra parte. Resta claro que os dados pessoais devem ser utilizados com lealdade, mediante a implementação de medidas efetivas com o objetivo de minimizar os riscos inerentes às atividades de tratamento de dados pessoais e ainda tendo em vista as finalidades previamente estabelecidas, considerando que os dados pessoais e as informações extraídas a partir de seu tratamento, "constituem-se em uma representação virtual da pessoa perante a

[84] VICENTE; CASIMIRO, 2020. pp. 53-54.
[85] LEI N.º 13.709, 2018. Art. 6.º.
[86] RODRIGUES, Silvio - **Direito civil. Dos contratos e das declarações unilaterais de vontade**. Vol. 3. 30.ª ed. São Paulo: Saraiva, 2004. p. 61.
[87] PEREIRA, Caio Mario da Silva. **Instituições de direito civil**. Vol. III. atual. 19.ª ed. Rio de Janeiro: Forense, 2015. p. 19.

sociedade, ampliando ou reduzindo as suas oportunidades no mercado, conforme sua utilização".[88]

No que se refere às atividades de tratamento de dados pessoais, que impõe deveres, limita e orienta a interpretação e aplicação da norma aos casos concretos, resta claro que a boa-fé exerce função importante, refletindo maior segurança e confiabilidade aos titulares dos dados pessoais em relação aos interessados em tratar referidas informações, bem como direcionando a aplicação dos demais princípios inerentes ao tratamento de dados pessoais.

(ii) Finalidade:

O princípio da finalidade indica que o tratamento de dados pessoais deve ser realizado para finalidades legítimas, específicas, explícitas, que devem ser informadas ao seu titular, sendo vedada a utilização dos dados pessoais de maneira incompatível com as finalidades previamente estabelecidas, conforme também previsto no RGPD.[89]

De acordo com Danilo Doneda, "toda a utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes de sua coleta".[90]

O atendimento ao princípio da finalidade exige a definição clara quanto à utilização e quanto aos limites do tratamento a que os dados pessoais serão submetidos, inclusive no que se refere ao acesso aos dados pessoais. O princípio da finalidade limita a transferência de dados pessoais a terceiros sem que seu titular tenha conhecimento de tal prática.

Importa referir que as políticas de privacidade, os termos e condições de uso devem ser claros, redigidos de maneira direta e sem qualquer ambiguidade quanto à extensão das atividades voltadas ao tratamento de dados pessoais, visto que "raramente o cidadão é capaz de perceber o sentido que a coleta de determinadas informações pode assumir em organizações complexas e dotadas de meios sofisticados para tratamento de dados".[91]

As atividades de tratamento de dados pessoais e todo o relacionamento com o titular dos dados devem ser sempre pautados pela boa-fé, refletindo a realidade com exatidão ao titular dos dados pessoais, afastando generalidades e abstrações, que permitiriam a flexibilização ou a sobreposição aos limites impostos pela finalidade do tratamento dos dados pessoais previamente determinada.

---

[88] MENDES, Laura Shertel - **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental.** São Paulo: Saraiva, 2014. p. 198.
[89] LEI N.º 13.709, 2018. Art. 6.º.
[90] DONEDA, Danilo - **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 216.
[91] RODOTÀ, Stefano - **A vida na sociedade da vigilância: a privacidade hoje.** Celina Bodin de Moraes (Org.). Danilo Doneda e Lucianda Cabral Doneda (Trad.). Rio de Janeiro: Renovar, 2008. p. 37.

(iii) Adequação:

O princípio da adequação estabelece que o tratamento deve ser compatível com as finalidades estabelecidas e com as legítimas expectativas do titular dos dados pessoais, ou seja, segundo o que dispões a LGPD, deve haver "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento".[92]

Os dados pessoais devem ser coletados apenas para finalidades específicas e lícitas e não devem ser tratados posteriormente para qualquer finalidade incompatível com esse propósito. Assim, no caso de as organizações realizarem outras atividades de tratamento de dados pessoais, deverão verificar se as operações são compatíveis com as finalidades previamente informadas ao titular dos referidos dados. No mesmo entendimento, tem-se o Considerando 50 do RGPD, que afirma:

> 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. Nesse caso, não é necessário um fundamento jurídico distinto do que permitiu a recolha dos dados pessoais.[93]

Ainda o Considerando 50 do RGPD, a fim de apurar se a finalidade de uma nova operação de tratamento dos dados é ou não compatível com a finalidade para o recolhimento inicial dos dados pessoais, o responsável pelo seu tratamento, depois de ter cumprido todos os requisitos para a licitude do tratamento inicial, deverá ter em atenção, entre outros aspetos, como a existência de uma ligação entre a primeira finalidade e aquela a que se destina à nova operação de tratamento que se pretende efetuar; o contexto em que os dados pessoais foram recolhidos, em especial as expectativas razoáveis do titular dos dados quanto à sua posterior utilização, baseadas na sua relação com o responsável pelo tratamento; a natureza dos dados pessoais; as consequências que o posterior tratamento dos dados pode ter para o seu titular; e a existência de garantias adequadas tanto no tratamento inicial como nas outras operações de tratamento previstas.[94]

Dessa forma, para que seja efetivamente cumprido o princípio da adequação, deve-se avaliar se os dados pessoais tratados são adequados para que as finalidades previamente informadas aos seus titulares sejam alcançadas. Importante verificar se os dados pessoais são

[92] LEI N.º 13.709, 2018. Art. 6.º, II.
[93] REGULAMENTO (UE), 2016.
[94] Ibidem.

relevantes para as atividades de tratamento dos dados pessoais, de acordo com as finalidades previamente estabelecidas.

(iv) Necessidade:

O princípio da necessidade limita o tratamento de dados pessoais ao mínimo necessário para a prossecução das finalidades estabelecidas, não devendo ultrapassar os limites impostos pelos princípios da finalidade e adequação. Assim, o tratamento de dados pessoais deve estar limitado "ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos".[95] O princípio da necessidade tem como objetivo fazer com que as atividades de tratamento de dados pessoais estejam voltadas exclusivamente ao que é essencial para realização dos objetivos a serem atingidos.

Importante ainda ressaltar que os dados pessoais tratados para qualquer finalidade não devem ser mantidos por mais tempo do que o necessário para que se atinja a finalidade pretendida. As atividades relacionadas ao tratamento de dados pessoais devem ser adequadas, relevantes e limitadas ao que é de facto necessário em relação aos propósitos para os quais foram coletados.

Assim, tem-se uma obrigação de minimização do tratamento de dados pessoais ao nível adequado, considerando a finalidade a ser atingida, o que exige uma avaliação de proporcionalidade das atividades a serem adotadas.[96] Esta avaliação de proporcionalidade das atividades envolve a necessidade de introduzir procedimentos de avaliação de impacto sobre a privacidade adequados.

(v) Livre acesso:

O princípio do livre acesso assegura aos titulares dos dados pessoais a "consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais".[97] O princípio do livre acesso surge como instrumento de tutela dos interesses individuais, permitindo a fiscalização quanto à qualidade dos dados e o cumprimento dos princípios da finalidade, da adequação, da necessidade, bem como o acesso facilitado a uma série de informações sobre o tratamento dos dados pessoais, de maneira clara, adequada e ostensiva, que são colocadas à disposição do titular.

[95] LEI N.º 13.709, 2018. Art. 6.º, III.
[96] VOIGT, Paul; BUSSCHE, Axel von dem. **The UE general data protection regulation (GDPR): a practical guide.** Alemanha: Springer International Publishing, 2017. p. 90.
[97] LEI N.º 13.709, *op cit.* Art. 6.º, IV.

O responsável pelo tratamento dos dados pessoais deve disponibilizar aos seus titulares meios técnicos de acesso direto às informações, estabelecendo uma capacidade de controle dos interessados sobre seus dados pessoais. Esses mecanismos disponibilizados aos titulares dos dados pessoais devem permitir, de facto, o livre acesso e, quando necessário, a correção das informações imprecisas ou sua exclusão, ainda que por requerimento feito ao controlador da base de dados pelo titular dos dados pessoais.

Portanto, o princípio do livre acesso corresponde à oportunidade concedida ao indivíduo para aceder seus dados pessoais, inseridos em bases de dados e de exigir que os titulares dessas bases de dados corrijam informações incorretas ou excluam informações não necessárias ou armazenadas de forma inadequada. O livre acesso aos dados é essencial para assegurar que as informações pessoais permaneçam precisas e completas.

(vi) Qualidade dos dados:

O princípio da qualidade dos dados trata da garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.[98] Exige-se, assim, que os dados pessoais sejam exatos e atualizados sempre que necessário, devendo ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora[99], conforme disposto no Artigo 5.º, n.º 1, do RGPD.

Importa referir que os dados pessoais devem ser precisos, no intuito de proporcionar uma ilustração adequada dos fatos e do perfil de seu titular. Assim, o tratamento de dados pessoais deve sempre buscar a verdade, sendo possível atingi-la quando assegurada a exatidão dos referidos dados pessoais. O princípio da qualidade dos dados pessoais traz uma garantia ao titular dos dados quanto ao direito de correção de dados pessoais imprecisos e o direito de concluir dados pessoais incompletos. Deve-se assegurar ainda aos respetivos titulares, mecanismos pelos quais possam solicitar a correção ou a complementação de seus dados pessoais.

O princípio do livre acesso e o princípio da qualidade dos dados promovem em conjunto um ambiente mais justo e leal, tanto sob o ponto de vista do titular dos dados pessoais, que, por meio de tais princípios, é contemplado por mecanismos que permitem

[98] LEI N.º 13.709, 2018. Art. 6.º, V.
[99] REGULAMENTO (UE), 2016.

medidas proativas, visando ao acesso e controle aos seus dados, quanto sob o ponto de vista da administração pública ou das empresas, já que uma base de dados contendo dados imprecisos, que não apenas ferem direitos dos seus titulares, como conduzem a decisões equivocadas, mostra-se de nenhum valor.

(vii) Transparência:

O princípio da transparência assegura aos titulares dos dados pessoais, informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respetivos agentes de tratamento, observados os segredos comercial e industrial. [100] O objetivo principal do princípio da transparência consiste em assegurar que os indivíduos compreendam facilmente o que ocorre com seus dados pessoais. Assim, é preciso estar claro que dados pessoais estão sendo coletados, analisados, utilizados, consultados, bem como a dimensão em que isso ocorre. No mesmo sentido, tem-se o que dispões o Considerando 58 do RGPD.

Por um lado, o ideal de transparência de mercado acaba invertendo os papéis tradicionais, quem estava na posição ativa e menos confortável, quem precisava agir, se informar, questionar, adquirir conhecimentos técnicos ou informação suficiente para a realização de bons negócios, o consumidor entrava na confortável posição de titular de um direito subjetivo à informação (Artigo 6.º, III) enquanto aquele que se encontrava em posição passiva de segurança, o fornecedor, passava a ser objeto de novo dever de informação, dever de conduta ativa (para informar), o que significa, na prática, uma reversão de papéis.[101]

Relativamente ao tratamento dos dados pessoais, a transparência aliada ao princípio da finalidade traduzem-se no dever de informação clara ao titular dos dados pessoais, de maneira que seja possível conhecer como seus dados pessoais serão utilizados, se haverá a utilização secundária dos dados, assegurando que o titular dos dados pessoais tenha conhecimento da finalidade que se busca atingir por meio do tratamento de seus dados pessoais, sendo ainda possível optar se permitirá ou não esse tratamento, não podendo presumir tal aceitação.

Como brilhantemente afirmado por James R. Kalyvas e Michael R. Overly, ao encomendar produtos *on-line*, os consumidores entendem que seu endereço de correspondência e informações do cartão de crédito são necessários para que o vendedor processe e conclua a compra. O indivíduo, no entanto, não necessariamente compreenderia

[100] LEI N.º 13.709, 2018. Art. 6.º, VI.
[101] MARQUES, Claudia Lima - **Contratos no código de defesa do consumidor: o novo regime das relações contratuais**. 7.ª ed., São Paulo: Revista dos Tribunais, 2014. p. 785.

ou gostaria que essas informações fossem utilizadas pela empresa para futuras comunicações de *marketing* ou compartilhadas com terceiros para seus próprios fins de *marketing*.[102]

Ao titular é atribuída uma possibilidade de decisão acerca da utilização de seus dados pessoais decorrente das informações que lhe são fornecidas, não apenas no que se refere à extensão desta utilização ou finalidade a ser atingida, mas também no que se refere aos riscos, efeitos, possibilidades, procedimentos inerentes a tais atividades e demais informações essenciais para que o titular dos dados pessoais possa exercer seu direito de escolha.

(viii) Segurança:

O princípio da segurança estabelece a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.[103] A imposição de um direito ao tratamento seguro e responsável dos dados pessoais,[104] que deve ser realizado de maneira que garanta a segurança apropriada, incluindo a proteção contra tratamento não autorizado ou ilegal e contra vazamentos e danos decorrentes, por intermédio de medidas técnicas e organizacionais apropriadas.[105]

O exercício das atividades de tratamento de dados pessoais deve buscar a proteção contra riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado. Imperioso destacar que aqueles que controlam dados pessoais devem adotar medidas técnicas e organizacionais apropriadas para manter um nível adequado de segurança para si. Tais medidas devem ser desenhadas para impedir o tratamento de dados em desacordo com a regulamentação, bem como proteger contra possível vazamento dos dados pessoais.

O nível apropriado de segurança e proteção dos dados pessoais representa um dever de cuidado razoável, que resulta no estabelecimento de obrigações aos responsáveis pelo tratamento de dados pessoais, que acarretam sua responsabilização em caso de negligência. A proteção aos dados pessoais deve estar inserida nas práticas empresariais, necessitando assim de medidas técnicas e organizacionais que busquem ferramentas para proteção antes que eventos de invasão de sistemas ou vazamento de dados ocorram.

---

[102] KALYVAS, James R.; OVERLY, Michael R. - **Big data: a business and legal guide.** New York: 2015. p. 36.
[103] LEI N.º 13.709, 2018. Art. 6.º, VII.
[104] AGNELLUTTI, Cody - **Big data: an exploration of opportunities, values, and privacy issues**. New York: Nova Science Publishers, 2014. p. 20.
[105] VOIGT; BUSSCHE, 2017. p. 92.

(ix) Prevenção:

O princípio da prevenção indica a necessidade de "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais".[106] O tratamento dos dados pessoais deve ser realizado de maneira que garanta a segurança apropriada, incluindo a proteção contra tratamento não autorizado ou ilegal e contra os vazamentos e danos decorrentes, por intermédio de medidas técnicas e organizacionais apropriadas.

Ameaças às bases de dados estão em constante desenvolvimento, ao mesmo tempo em que falhas nos recursos de segurança são regularmente descobertas. Portanto, uma tecnologia nova e revolucionária no mercado logo se tornará um requisito de segurança padrão e com o tempo proporcionará pouca segurança.

Os princípios da segurança e da prevenção representam princípios extremamente importantes sob a perspetiva económica daqueles que usufruem de dados pessoais para o direcionamento de suas políticas ou atividades empresariais. Um incidente de vazamento de dados pessoais atinge não apenas os direitos dos titulares dos dados, mas também poderá responsabilizar o responsável pelo tratamento de referidos dados.

Atualmente, a ocorrência de falhas na segurança e na prevenção de riscos no tratamento de dados pessoais, que resultam no vazamento ou no acesso ilegítimo às informações, acarretam não apenas a responsabilização, mas também impactam diretamente a reputação e o valor da empresa no mercado, gerando inúmeras consequências negativas à empresa, uma vez que a confiança é um fator fundamental que determina a preferência dos consumidores em determinada empresa e direciona suas escolhas.

(x) Não discriminação:

O princípio da não discriminação trata da impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.[107]

Acerca desse assunto, Fábio Konder Comparato, em análise sobre a Declaração Universal de Direitos Humanos, afirma que o princípio da igualdade essencial do ser humano, apesar das numerosas diferenças biológicas e culturais que o distinguem, consta do Artigo II. A isonomia ou igualdade perante a lei, proclamada no Artigo VII, é uma simples consequência deste princípio. Atentar contra a dignidade humana consiste precisamente em considerar e tratar o outro – um indivíduo, uma classe social, um povo – como um ser inferior

[106] LEI N.º 13.709, 2018. Art. 6º, VIII.
[107] Ibidem. Art. 6º, IX.

a pretexto de diferenças de etnia, sexo, costumes ou riqueza patrimonial. Algumas diferenças, não são deficiências, mas, pelo contrário, fontes de valores positivos e, como tais, devem ser protegidas e incentivadas.[108]

A não discriminação no tratamento de dados pessoais é colocada no intuito de assegurar o tratamento igualitário entre cidadãos, seja nas relações privadas e comerciais ou perante o Estado, visando evitar o tratamento mediante o estabelecimento de critérios injustos, violadores da dignidade da pessoa humana, de cunho exclusivamente discriminatório. Em certos casos, a promoção da igualdade implica o tratamento desigual de certas situações, conforme proposto por Aristóteles, sendo o entendimento que se deve tratar igualmente os iguais e desigualmente os desiguais, na medida de sua desigualdade.[109]

O tratamento de dados pessoais, nomeadamente através de processos automatizados, é, ao mesmo tempo, uma atividade que apresenta riscos cada vez mais evidentes, risco que se materializa na possibilidade de exposição e utilização indevida ou abusiva de dados pessoais; no caso de esses dados estarem incorretos e deturparem seu proprietário; na sua utilização por terceiros sem o conhecimento ou autorização do seu titular; no caso de uso para fins discriminatórios. Diante desse cenário, vê-se a importância e necessidade de mecanismos que permitam à pessoa o conhecimento e o controle de seus dados.[110]

O princípio da não discriminação objetiva garantir direitos iguais entre todos os cidadãos, eliminando práticas desleais, abusivas e contrárias à boa-fé. As práticas de tratamento de dados pessoais exigem cautela, especialmente diante de processos automatizados, impedindo a criação ou elevação de barreiras económicas e sociais.

(xi) Responsabilização e prestação de contas:

O princípio da responsabilização e prestação de contas impõe a demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.[111] O responsável pelo tratamento dos dados pessoais deverá zelar pelo cumprimento dos demais princípios, portanto, deverá observar a boa-fé na utilização de dados pessoais, assegurar que o seu tratamento seja realizado para finalidade específica, com

[108] COMPARATO, Fábio Konder. **A afirmação histórica dos direitos humanos**. 9.ª ed., rev. e atual. São Paulo: Saraiva, 2015. p. 241.
[109] ARISTÓTELES. **Ética a Nicômaco**. 4.ª ed. São Paulo: Nova Cultura, 1991. p.120.
[110] MAGALHÃES, Guilherme Martins (Coord**.). Direito privado e internet – atualizado pela Lei nº 12.965/2014**. São Paulo Atlas 2014. p. 62.
[111] LEI N.º 13.709, 2018. Art. 6.º, X.

transparência e adequação, de acordo com a necessidade, assegurando a qualidade dos dados e o livre acesso aos seus titulares, a não discriminação e implementando medidas de segurança e prevenção para o tratamento dos dados pessoais. As medidas adotadas pelo responsável pelo tratamento dos dados pessoais devem permitir que seja realizada a efetiva demonstração de seu cumprimento e eficácia.

Referidas obrigações não se restringem aos controladores dos dados pessoais, uma vez que são aplicáveis também aos operadores, que devem estar vinculados por contrato e regras corporativas, a atender aos padrões de tratamento de dados pessoais estabelecidos pelo controlador para total conformidade com a norma jurídica, incluindo-se os princípios, que devem ser observados em todas as fases do tratamento dos dados.

Estar em conformidade com as normas de proteção de dados pessoais traduz-se na capacidade de atender às normas de tratamento de dados pessoais, e ainda comprovar documentalmente tal conformidade, devendo os princípios ora tratados e as demais normas estarem completamente inseridos no desenvolvimento das atividades de tratamento dos dados pessoais. O princípio da responsabilização e prestação de contas fortalece o comprometimento daqueles que exercem as atividades de tratamento de dados pessoais buscando o respeto às normas e à privacidade dos titulares dos dados.

1.2.2 Bases legais para o tratamento dos dados pessoais previstos na LGPD

De acordo com o previsto no Artigo 7.º da LGPD, o tratamento de dados pessoais somente será considerado lícito mediante a indicação das bases legais.

Assim sendo, o tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: mediante o fornecimento de consentimento pelo titular; para o cumprimento de obrigação legal ou regulatória pelo controlador; pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas; para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; para a execução de contrato do qual o titular seja parte; para o exercício regular de direitos em processo judicial, administrativo ou arbitral; para a proteção da vida e integridade física do titular ou de terceiros; para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; quando necessário para atender aos interesses legítimos do controlador

ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, e para a proteção do crédito.[112]

A seguir, analisam-se o consentimento e o legítimo interesse:

(i) Consentimento:

É uma das bases legais mais utilizadas para legitimar o tratamento de dados pessoais, sendo assim, a base legal que traz o maior número de discussões. Conforme definido na LGPD, consentimento deve ser conceituado como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada." [113]

O consentimento deve ser fornecido por escrito ou por qualquer outro meio que demonstre a manifestação de vontade do titular.[114] De acordo com a LGPD, "caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais".[115] A legislação impede que o tratamento de dados pessoais seja realizado mediante qualquer vício de consentimento, atribuindo o ônus da prova ao controlador dos dados pessoais, que deverá possuir meios de comprovar que o consentimento foi obtido em conformidade com o previsto na lei.

Qualquer alteração quanto à finalidade específica, forma e duração do tratamento, na identificação do controlador dos dados pessoais e acerca do uso compartilhado dos dados, deve ser informada ao titular, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração. O fornecimento de informações com conteúdo enganoso, abusivo ou sem clareza por parte do responsável pelo tratamento dos dados pessoais, resulta na nulidade do consentimento fornecido pelo seu titular, que poderá ainda revogá-lo a qualquer tempo, caso discorde de alterações na finalidade para a qual os dados estão sendo tratados. A revogação poderá operar-se pela mera manifestação realizada por meio de um procedimento gratuito e facilitado, que deve ser disponibilizado pelo responsável pelo tratamento dos dados aos titulares dos dados pessoais.

A lei determina que o consentimento deve ser livre, uma vez que o titular dos dados pessoais poderá aceitar ou recusar o tratamento de seus dados, ou até mesmo retirar seu consentimento, sem ser penalizado ou sofrer interferências na qualidade do serviço ou

[112] LEI N.º 13.709, 2018. Art. 7.º.
[113] Ibidem. Art. 5.º, XII.
[114] Ibidem. Art. 8.º, §1.º.
[115] Ibidem.

produto contratados. No que se refere ao consentimento informado, traduz-se no facto de o titular dos dados pessoais ter à sua disposição todas as informações necessárias para que possa decidir se deseja ou não aceitar as condições de tratamento de seus dados pessoais. Por consentimento inequívoco, entende-se que não devem existir dúvidas acerca da intenção do titular dos dados pessoais de permitir o seu tratamento.

A obtenção de consentimento do titular dos dados pessoais é dispensada, nas hipóteses em que os dados foram tornados manifestamente públicos pelo seu titular, exigindo-se, entretanto, a observância dos princípios previstos na legislação. Importante referir que o silêncio do titular dos dados pessoais e as opções pré-assinaladas não constituem consentimento válido.

(ii) Legítimo interesse:

O legítimo interesse deve ser avaliado através da análise de proporcionalidade entre os interesses do controlador ou de terceiros e as legítimas expectativas dos titulares dos dados pessoais. Caso exista conflito entre o legítimo interesse do controlador e as legítimas expectativas, direitos e liberdades do titular dos dados pessoais, os direitos dos titulares dos dados devem prevalecer.

O legítimo interesse nem sempre será a base legal mais apropriada e exige do responsável pelo tratamento dos dados cautela no que se refere à proteção dos interesses e direitos dos titulares dos dados. O responsável pelo tratamento dos dados pessoais deverá manter registo da avaliação de legítimo interesse para que se possa demonstrar conformidade com as normas de proteção de dados pessoais. De acordo com o que dispões a LGPD, a autoridade nacional de proteção de dados poderá solicitar o relatório de impacto à proteção de dados pessoais ao controlador, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.[116]

[116] LEI N.º 13.709, 2018. Art. 10.º, § 3.º.

2 ADEQUAÇÃO À REGULAMENTAÇÃO DE PROTEÇÃO DE DADOS

Para atender à legislação de proteção de dados pessoais, tanto a europeia quanto a brasileira, as empresas deverão promover e executar internamente um planejamento estratégico estruturado que deve passar por alguns passos principais. O primeiro passo para adequação é realizar um mapeamento detalhado dos dados pessoais tratados e o seu ciclo de vida. Trata-se de uma auditoria inicial. Posteriormente, deve-se identificar as medidas necessárias à adequação à lei de proteção de dados. Por fim, as medidas de adequação devem ser implementadas pela organização.

2.1 Realização da auditoria inicial

Para adequar-se à legislação de proteção de dados pessoais, as empresas devem realizar uma auditoria inicial. É extremamente importante conhecer todos os procedimentos e métodos da organização em relação à coleta e tratamento de dados. Imperioso nesse ponto conhecer o ciclo de vida dos dados pessoais, ou seja, identificar como é feito o registo; o local que esses registos se encontram; o responsável pelo gerenciamento dos registos; os dados pessoais que são coletados pela organização no conjunto das operações de tratamento que realizam.

A organização deve avaliar se os tratamentos realizados e os dados coletados estão em sintonia com as finalidades pretendidas e com a base legal correta para cada operação de tratamento de dados pessoais. A avaliação da licitude do tratamento é o primeiro passo da análise uma vez que se não há tratamento lícito não pode existir tratamento de dados pessoais. O resultado dessa auditoria inicial deve resultar na elaboração de relatório com a identificação de todas as operações de tratamento de dados pessoais, independentemente do grau de complexidade, devendo constar desde as operações de tratamento de dados pessoais simples até as extremamente complexas.

2.2 Definição das medidas de adequação

Durante todo o processo de adequação à legislação de proteção de dados, deve estar presente o direito à informação e transparência perante o titular dos dados pessoais. O direito à informação deve ser implementado de forma que o titular dos dados pessoais tenha clareza quanto às operações realizadas com seus dados pessoais. Imperioso também estar presente

o princípio da limitação das finalidades, sendo que os dados pessoais devem ser recolhidos para finalidades determinadas, explícitas e legítimas.

De acordo com o Artigo 32.º, n.º 1 do RGPD:

> Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado:
> a) A pseudonimização e a cifragem dos dados pessoais;
> b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;
> c) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico;
> d) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.[117]

Importante que sejam adotadas medidas de segurança proporcionais à operação da organização, levando em consideração os riscos apresentados pelo tratamento, em particular devido à destruição, perda e alteração acidentais ou ilícitas, e à divulgação ou ao acesso não autorizado, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.[118] Nesse ponto, importante verificar as medidas que deverão ser adotadas no que se refere aos contratos em vigor na organização, uma vez que os prestadores de serviço contratados também devem garantir a adoção de todas as medidas de proteção de dados em vigor na organização.

Acerca do registo de todas as atividades de tratamento, importante analisar o que dispões o Artigo 30.º, n.º 1, do RGPD:

> Cada responsável pelo tratamento e, sendo caso disso, o seu representante conserva um registo de todas as atividades de tratamento sob a sua responsabilidade. Desse registo constam todas seguintes informações:
> a) O nome e os contatos do responsável pelo tratamento e, sendo caso disso, de qualquer responsável conjunto pelo tratamento, do representante do responsável pelo tratamento e do encarregado da proteção de dados;
> b) As finalidades do tratamento dos dados;
> c) A descrição das categorias de titulares de dados e das categorias de dados pessoais;
> d) As categorias de destinatários a quem os dados pessoais foram ou serão divulgados, incluindo os destinatários estabelecidos em países terceiros ou organizações internacionais;
> e) Se for aplicável, as transferências de dados pessoais para países terceiros ou organizações internacionais, incluindo a identificação desses países terceiros ou organizações internacionais e, no caso das transferências referidas no Artigo 49.º, n.º

[117] REGULAMENTO (UE), 2016.
[118] Ibidem.

> 1, segundo parágrafo, a documentação que comprove a existência das garantias adequadas;
> f) Se possível, os prazos previstos para o apagamento das diferentes categorias de dados;
> g) Se possível, uma descrição geral das medidas técnicas e organizativas no domínio da segurança referidas no Artigo 32.º, n.º 1. [119]

Deve ser realizado o acompanhamento constante das atividades de tratamento, de forma que a organização não seja exposta a riscos devido a possíveis alterações das atividades de tratamento realizadas. As políticas e procedimentos internos da organização devem refletir as atividades efetivamente realizadas pela organização, devendo ser atualizadas conforme existam novas atividades de tratamento e caso haja alteração nas atividades de tratamento em vigor.

2.3 Implementação das medidas de adequação

A implementação das medidas de adequação deve ser realizada de forma que o responsável pelo tratamento possa assegurar e comprovar que o tratamento é realizado em conformidade com a legislação de proteção de dados. Obviamente que a organização além de cumprir a regulamentação em vigor deve ser capaz de comprovar referido cumprimento, tendo a área de *compliance* da organização extrema importância nesse tema.

Sobre o assunto, importa referir o disposto no Artigo 24.º, n.º 1, do RGPD:

> Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades. [120]

Os procedimentos internos acerca de proteção de dados precisam estar claros para todos os colaboradores da organização, o que é concretizado por meio de treinamento e conscientização. Não basta ter as regras apenas em políticas e procedimentos internos, referidos procedimentos devem ser amplamente difundidos para real conhecimento da organização. É importante que os parceiros e prestadores de serviços da organização também sejam conscientizados, visto que devem contribuir com o cumprimento das práticas e políticas da organização que se referem ao tratamento de dados pessoais.

[119] REGULAMENTO (UE), 2016.
[120] Ibidem. Artigo 24.º, n.º 1.

Relativamente a criação de códigos de conduta, de forma a tornar mais eficaz o cumprimento das disposições dos diversos setores, tendo em conta as suas especificidades, bem como a certificação no campo de proteção de dados, o RGPD incentiva a elaboração de códigos de conduta por associações ou outros organismos representativos de categorias de responsáveis pelo tratamento ou de subcontratantes.[121] Associações ou outros organismos representativos de um setor têm capacidade de elaborar códigos de conduta que façam real sentido em virtude da operação de tratamento realizada. No que se refere à política de privacidade, importa dizer que:

> *Privacy policies consist of documents which set forth an organization's data practices on processing activities of personal data to it users, such as collection, use, sharing, and retention. They serve as a basis for decision-making and as a 'tool for preference matching' for consumers, as consumers tend to place a higher value on a product/service, after learning more about its attributes and tradeoffs. As such, Privacy Policies constitute the locus where consequences are produced, the 'technically most feasible place to protect privacy and personal data'.*[122,123]

A implementação de sistemas de gestão de segurança da informação tem como objetivo evitar violações de dados pessoais. Além da implementação dos sistemas de gestão de segurança da informação, a organização precisa possuir um sistema para gerenciamento de violações de dados pessoais. Qualquer violação de dados deve ser reportada e formalizada em relatórios internos à organização, além de eventual comunicação à Autoridade de Controle e aos titulares, para estabelecimento de histórico, para reparação dos danos presentes e para a mitigação de danos futuros. O relatório final de implementação das medidas de adequação à legislação de proteção de dados, com as políticas internas e a política de privacidade, correspondem aos principais instrumentos para comprovação de conformidade à legislação.

2.4 *Compliance*

Compliance significa conhecer as normas, seguir os procedimentos recomendados, e agir em conformidade. Significa obedecer, cumprir, satisfazer, estar em conformidade com

[121] PEREIRA COUTINHO; CANTO MONIZ, 2018. p. 47.
[122] Ibidem. p.104.
[123] "As políticas de privacidade consistem em documentos que estabelecem as práticas de uma organização sobre as actividades de tratamento de dados pessoais dos seus utilizadores, tais como a recolha, utilização, partilha e retenção. Servem como base para a tomada de decisões e como ferramenta para os consumidores, uma vez que os consumidores tendem a atribuir um valor mais elevado a um produto/serviço, depois de saberem mais sobre os seus atributos. Como tal, as Políticas de Privacidade constituem o "local tecnicamente mais viável para proteger a privacidade e os dados pessoais". (Tradução livre)

o que foi imposto, ou seja, observar, ser responsável, e cumprir regulamentos internos e externos impostos às atividades da organização.[124] Em geral, as empresas têm a responsabilidade de promover uma cultura que promova a ética e o exercício do objeto social em conformidade com a lei.[125] O RGPD traz especial enfoque no cumprimento devido a medidas mais rigorosas de governação e responsabilidade para os responsáveis pelo tratamento ou subcontratantes.[126]

Quanto à origem do termo *compliance*, a ideia surgiu da legislação americana, com a criação da Prudential Securities em 1950, e com a regulamentação da Securities and Exchange Commission (SEC), de 1960, que sugeria a necessidade de institucionalizar programas de *compliance*, a fim de criar procedimentos internos para controlar e monitorar transações entre pessoas. Alguns anos depois, precisamente em 9 de dezembro de 1977, foi registada na Europa a Convenção Relativa à Obrigação de Diligência dos Bancos no Marco da Associação de Bancos Suíços, onde foram instituídas as bases de um sistema de autorregulação de conduta, vinculando as instituições, cujo incumprimento levaria à aplicação de sanções como multas e outras penalidades.[127]

Antonio Barreto Menezes Cordeiro traz para discussão o tema "*data compliance*", afirmando que a complexidade do RGPD, bem como as elevadas coimas desencadearam o estudo da conformidade de dados, sendo que a experiência empírica indica três pontos estruturantes:

> (i) identificação clara do que se pretende e de quem é internamente responsável pelo seu cumprimento;
> (ii) implementação de sistemas de gestão de dados (*Data Protection Management Systems*);
> (iii) implementação de procedimentos uniformes. [128]

Para Marcelo de Aguiar Coimbra e Vanessa Manzi, os programas de *compliance* referem-se ao "ato de cumprir, de estar em conformidade e executar regulamentos internos e externos, impostos às atividades da instituição, buscando mitigar o risco atrelado à reputação e ao regulatório/legal".[129] O conceito de *compliance* é muito mais amplo do que

---

[124] BLOK, Marcella - **Compliance e governança corporativa: atualizado de acordo com a Lei Anticorrupção Brasileira (Lei 12.846) e o decreto-lei 8.421/15.** Rio de Janeiro: Freitas Bastos, 2017. p. 15.
[125] ASSI, Marcos. **Compliance: como implementar**. São Paulo: Trevisan, 2018. p. 19.
[126] PEREIRA COUTINHO; CANTO MONIZ, 2018. p. 46.
[127] GABARDO, Emerson; CASTELLA, Gabriel Morettini - A nova lei anticorrupção e a importância do compliance para as empresas que se relacionam com a Administração Pública. **A&C - Revista de Direito Administrativo & Constitucional**. Belo Horizonte: Fórum. 15(60) (abr./jun.2015). p. 134.
[128] CORDEIRO, 2020. pp. 162-163.
[129] COIMBRA, Marcelo de Aguiar; MANZI, Vanessa Alessi. **Manual de compliance: preservando a boa governança e a integridade das organizações**. São Paulo: Atlas, 2010. p. 2.

pura e simplesmente a busca pela implementação e pelo cumprimento das exigências legais, pois se presta, fundamentalmente, a preservar os princípios éticos.[130]

O *compliance* pode ser dividido em dois campos de atuação, um subjetivo, que inclui normas internas, como a implementação de boas práticas dentro e fora da organização e a aplicação de mecanismos de acordo com a legislação, com o objetivo de prevenir ou minimizar riscos, práticas ilegais e melhorar o relacionamento com clientes e fornecedores, já a segunda área é objetiva, exigida por lei.[131]

Compliance não deve ser entendido apenas e tão somente no que se refere ao cumprimento da legislação e regulamentação em vigor, bem como o desenvolvimento, implementação e cumprimento de políticas e procedimentos internos da organização. A área de *compliance* é responsável por implementar e manter uma cultura de conformidade e ética na operação da organização, por meio de treinamentos, conscientização de todos os empregados, prestadores de serviço e fornecedores que mantenham relacionamento com a organização, de forma que realmente compreendam a necessidade de cumprimento de políticas e procedimentos internos, bem como de normas e regulamentações.

2.4.1 Avaliação de impacto sobre a proteção de dados

Pilar de extrema importância quando se refere ao *compliance*, trata-se da governação corporativa. A governação corporativa corresponde aos processos, sistemas e controles utilizados pela organização. Os princípios que devem estar presentes quando se fala em governação corporativa são: transparência, equidade, prestação de contas e responsabilidade corporativa.

No tocante à dificuldade e forma das organizações comprovarem que efetivamente cumprem o RGPD, Lurdes Dias Alves entende que uma das inovações introduzidas pelo RGPD é o conceito de avaliação de impacto de proteção de dados denominado Avaliação de Impacto de Privacidade (AIPD ou PIA). Trata-se de um processo que visa descrever o tratamento, avaliar a necessidade e proporcionalidade desse tratamento, gerir e prevenir os riscos aos direitos e liberdades dos titulares dos dados decorrentes do tratamento, avaliá-los e determinar as necessárias ações. As AIPDs constituem ferramentas importantes de responsabilidade que ajudam os responsáveis pelo tratamento de dados não apenas a cumprir

[130] ESPÍNDOLA, Maria Fernanda; TOMAZ, Roberto Epifanio - Compliance: o que é, objetivo, aplicação e benefícios. **Revista Síntese de Direito Empresarial**, São Paulo. 10(57) (jul./ago. 2017) 9-20. p. 11.
[131] GABARDO; CASTELLA, 2015. pp. 134-135.

os requisitos do RGPD, mas também a demonstrar que medidas adequadas foram tomadas para garantir a conformidade com o regulamento RGPD.[132]

A avaliação de impacto sobre a proteção de dados deve ser realizada quando o tratamento for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares. Assim, de acordo com o Considerando 91 do RGPD, a avaliação de impacto sobre a proteção de dados deverá ser aplicada às operações de tratamento de grande escala que visem ao tratamento de uma quantidade considerável de dados pessoais em âmbitos regional, nacional ou supranacional e sejam suscetíveis de implicar um elevado risco.

Deverá ser realizada, também, uma avaliação de impacto sobre a proteção de dados nos casos em que os dados pessoais são tratados para tomar decisões relativas a determinadas pessoas singulares, na sequência de qualquer avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares baseada na definição dos perfis desses dados ou na sequência do tratamento de categorias especiais de dados pessoais, de dados biométricos ou de dados sobre condenações penais e infrações ou medidas de segurança conexas.[133]

Ainda de acordo com o RGPD, é igualmente exigida uma avaliação do impacto sobre a proteção de dados para o controle de zonas acessíveis ao público em grande escala, nomeadamente se forem utilizados mecanismos optoelectrónicos ou para quaisquer outras operações quando a autoridade de controle competente considere que o tratamento é suscetível de implicar um elevado risco para os direitos e liberdades dos titulares dos direitos, em especial por impedirem estes últimos de exercer um direito ou de utilizar um serviço ou um contrato ou por serem realizadas sistematicamente em grande escala.[134]

Medidas relacionadas com a realização de uma avaliação de impacto da proteção de dados e a subsequente consulta prévia às autoridades de supervisão, o registo das atividades de processamento, a notificação de violações de dados pessoais, bem como a obrigação de nomear um responsável pela proteção de dados, que deve garantir de forma independente a conformidade com as obrigações legais de cada organização, sendo o ponto de contato com as autoridades de supervisão em questões de proteção de dados pessoais.[135]

[132] ALVES, 2014. p. 13.
[133] REGULAMENTO (UE), 2016.
[134] Ibidem.
[135] PEREIRA COUTINHO; CANTO MONIZ, 2018. p. 47.

A Avaliação de Impacto sobre a Proteção de Dados é uma ferramenta que pode identificar e mitigar riscos de privacidade antes do tratamento de dados pessoais. Esta avaliação envolve a descrição das operações de processamento previstas e a avaliação dos riscos de privacidade e das medidas em virtude desses riscos.[136]

Diante do exposto, para estar em conformidade com a legislação referente à proteção de dados, as organizações devem conhecer detalhadamente toda regulamentação e legislação aplicáveis, de forma a implementar de forma eficiente as políticas de coleta, uso, tratamento, proteção e segurança dos dados dos titulares, sendo de grande valia a utilização da Avaliação de Impacto sobre a Proteção de Dados de forma a identificar e mitigar riscos de privacidade antes do tratamento dos dados pessoais, sempre que o tratamento for possa implicar elevado risco para os direitos dos titulares dos dados pessoais.

[136] PEREIRA COUTINHO; CANTO MONIZ, 2019. p. 105.

3 FUNDAMENTOS DE LEGITIMIDADE PARA O TRATAMENTO DE DADOS À LUZ DO RGPD

Os fundamentos de legitimidade para o tratamento de dados, conforme o RGPD, baseiam-se em consentimento (livre, específico e informado) e em Interesse legítimo, cujos conceitos estão apresentados a seguir.

3.1 Consentimento

Consentimento é um dos conceitos básicos de proteção de dados. O Artigo 4.º, n.º 11, do RGPD define consentimento 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 respeto sejam objeto de tratamento.[137] Portanto, torna-se claro que deve haver expressa manifestação de vontade do titular dos dados. Importa referir que a expressão explícita apenas consta na versão portuguesa do Regulamento. A expressão explícita não pode ser entendida como a forma escrita.[138]

Conforme previsto no Considerando 32 do RGPD, 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 respeto, por exemplo, mediante uma declaração escrita, inclusive em formato eletrônico ou uma declaração oral. O consentimento pode ser dado validando uma opção ao visitar um site na Internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais.[139]

Acerca desta temática, Luis Antunes afirma que:

> Por ‘ato’ não se entenda um simples ‘sim, sem problema’ durante uma chamada telefónica feita por alguém da empresa que pretende tratar os nossos dados. Também não podemos estar sob qualquer pressão de quem requer o consentimento. Assim, e se estivermos a visitar um site, terá de haver uma opção em que tenhamos de colocar uma cruz de consentimento; pois as opções pré-validadas ou a omissão não deverão constituir um consentimento; se estivermos presencialmente com um representante

[137] REGULAMENTO (UE), 2016.
[138] CORDEIRO, 2020. pp. 171-172.
[139] REGULAMENTO (UE), *op cit*.

> da entidade, teremos de assinalar algo que mencione ‘autorizo que’ ou ‘consinto que’ ou, em último caso, por declaração oral.[140]

O consentimento refere-se à principal causa de legitimidade e de licitude do tratamento de dados pessoais, conforme se encontra estipulado no Artigo 6.º, n.º 1, a) do RGPD. O pedido de consentimento tem de ser apresentado de forma clara e objetiva, utilizando uma linguagem fácil de compreender, e de uma forma que o distinga claramente de outras informações, como os termos e condições. O consentimento garante uma proteção dos titulares dos dados, mesmo que a informação empírica demonstre um desinteresse efetivo por parte da maioria da população.

Com relação à validade do consentimento, é importante analisar o quanto referido no Manual da Legislação Europeia sobre Proteção de Dados:

> Outros requisitos de validade do consentimento previstos no direito civil, tais como a capacidade jurídica, também serão naturalmente aplicáveis no contexto da proteção de dados, na medida em que são requisitos jurídicos fundamentais. O consentimento inválido de pessoas sem capacidade jurídica não constitui uma base legal para o tratamento de dados sobre essas pessoas.[141]

Importa destacar que referida manifestação de vontade do titular dos dados deve ser: livre, específica, informada e explícita. A seguir, são explorados em detalhe cada um destes elementos.

3.1.1 Consentimento Livre

O elemento livre deve implicar uma ação do titular de dados, ou seja, este deve poder escolher se dará o consentimento para o tratamento de dados ou não. O referido consentimento não será considerado válido, caso o titular dos dados se sinta coagido a consentir no tratamento dos seus dados pessoais ou, ainda, sofra consequências negativas caso não consinta.

É importante referir que, caso o consentimento esteja agregado a uma parte não negociável nas condições gerais do contrato, presume-se que não foi dado livremente. Portanto, não há consentimento livre ao se verificar que o titular dos dados não tem possibilidade de recusar ou retirar o consentimento sem prejuízo. O desequilíbrio entre o responsável pelo tratamento e o titular dos dados também é ponderado no RGPD.

[140] ANTUNES, 2018. p. 42.
[141] AGÊNCIA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA, 2014. p. 59.

Nesse sentido, o Manual da Legislação Europeia sobre Proteção de Dados dispões:

> A liberdade do consentimento também poderá estar ameaçada em situações de subordinação, em que exista um desequilíbrio económico ou de outro tipo significativo entre o responsável pelo tratamento que obtém o consentimento e a pessoa em causa que dá o consentimento.[142]

Acerca desta temática, torna-se imperioso analisar o Considerando 32 do RGPD:

> O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento. O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins. Se o consentimento tiver de ser dado no seguimento de um pedido apresentado por via eletrônica, esse pedido tem de ser claro e conciso e não pode perturbar desnecessariamente a utilização do serviço para o qual é fornecido.[143]

Assim, importa referir que não será válida qualquer opção pré-assinalada em que o titular de dados não teve qualquer opção. Mas quantas vezes se depara com esse tipo de situação? Está sendo realizada a contratação de um serviço ou a compra de um determinado produto, e novamente aparecem as opções referentes ao tratamento de dados já preenchidas ou previamente validadas. Nestes casos, configura-se o tratamento ilícito dos dados pessoais, uma vez que ao respetivo titular não foi dada a verdadeira opção de aceitar ou não referido tratamento de seus dados pessoais. Os estudos comportamentais e económicos disponíveis sobre a realidade da Internet são claros no sentido de que a maioria das pessoas não lê as condições *on-line*, não tem capacidade ou conhecimento para assimilar o que lê, e caso todos os utilizadores o decidissem fazer, os custos económicos seriam extremamente elevados.[144]

Há, também, situações em que o consentimento é fornecido a finalidades amplas e gerais, sem deixar claro quais são as finalidades específicas e objeto daquele tratamento. Ainda, deve ser vedada qualquer intimidação, coação ou desdobramento negativo se o consentimento for negado pelo titular dos dados. O consentimento será acatado como fundamento para o tratamento de dados pessoais se, ao titular dos dados for oferecida a opção de aceitar ou de recusar os termos propostos. Os responsáveis pelo tratamento devem avaliar os requisitos para obter um consentimento válido.

---

[142] AGÊNCIA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA, 2014. p. 59.
[143] REGULAMENTO (UE), 2016.
[144] CORDEIRO, 2020. p. 169.

O Artigo 7.º, n.º 4, foi redigido de forma não exaustiva, deixando claro que pode haver uma variedade de outras situações, que se enquadram nesta disposição:

> Ao avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato.[145]

Em termos gerais, qualquer elemento que constitua influência desadequada ou coação sobre o titular dos dados, impedindo o exercício livre de sua vontade, tornará, consequentemente, o consentimento inválido.

3.1.2 Consentimento específico

O consentimento deve ser específico, ou seja, deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Caso o tratamento seja necessário para diversas finalidades, o responsável pelo tratamento deverá permitir que o titular dos dados forneça o consentimento para cada finalidade específica. O tratamento de dados pessoais para finalidades ilimitadas ou indeterminadas deve ser considerado um tratamento ilícito.

Destaca-se o que consta no Considerando 33 do RGPD: "Os titulares dos dados deverão ter a possibilidade de dar o seu consentimento unicamente para determinados domínios de investigação ou partes de projetos de investigação, na medida permitida pela finalidade pretendida."[146] Assim, o consentimento pode abranger diversas operações, desde que as referidas operações sirvam à mesma finalidade.

De acordo com o Artigo 5.º, n.º 1, alínea b), do RGPD, a obtenção de consentimento válido deverá ser precedida de uma finalidade determinada, explícita e legítima para o tratamento desejado.[147]

3.1.3 Consentimento informado

O consentimento deve ser informado, tendo em vista os princípios da transparência, lealdade e licitude.

O Manual da Legislação Europeia sobre Proteção de Dados recomenda que:

[145] REGULAMENTO (UE), 2016.
[146] Ibidem.
[147] Ibidem.

> Os responsáveis pelo tratamento devem documentar o modo como se propõe tratar os dados de forma lícita e transparente e colocar esses documentos à disposição das pessoas em causa e do público em geral. As operações de tratamento não podem ser realizadas em segredo e não devem ter efeitos negativos imprevistos. Os responsáveis pelo tratamento devem certificar-se de que os clientes ou cidadãos são informados sobre a utilização dos seus dados. Os responsáveis pelo tratamento devem ainda, na medida do possível, atuar de forma a cumprir prontamente os desejos da pessoa em causa, especialmente quando a base legal do tratamento de dados for o seu consentimento.[148]

O pedido de consentimento tem de deixar clara a finalidade ao tratamento dos dados pessoais e incluir os contatos da empresa responsável por efetuar o tratamento dos dados. A parte interessada deve ser plenamente informada antes de se tomar uma decisão. A integralidade ou incompletude das informações fornecidas pode ser determinada no caso concreto, sendo de extrema importância que a linguagem utilizada seja adaptada ao destinatário pretendido das informações.[149]

Conforme previsto no Artigo 13.º do RGPD, quando os dados pessoais são recolhidos com o titular, o consentimento informado significa que o titular dos dados tem de receber, pelo menos, as seguintes informações acerca do tratamento de seus dados pessoais:

> a) A identidade e os contatos do responsável pelo tratamento e, se for caso disso, do seu representante; b) Os contatos do encarregado da proteção de dados, se for caso disso; c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento; d) Se o tratamento dos dados se basear no artigo 6.º, n.º 1, alínea f), os interesses legítimos do responsável pelo tratamento ou de um terceiro; e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver; f) Se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas.[150]

De acordo com o estatuído no Artigo 14.º do RGPD, quando os dados pessoais não são recolhidos com o titular, as seguintes informações devem ser facultadas:

> a) A identidade e os contatos do responsável pelo tratamento e, se for caso disso, do seu representante; b) Os contatos do encarregado da proteção de dados, se for caso disso; c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento; d) As categorias dos dados pessoais em questão; e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver; f) Se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, a

[148] AGÊNCIA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA, 2014. p. 79.
[149] Ibidem. p. 62.
[150] REGULAMENTO (UE), 2016.

> referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas; [151]

O Artigo 7.º, n.º 2, do RGPD determina que se o consentimento do titular dos dados for dado no contexto de uma declaração escrita que diga também respeto a outros assuntos, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente desses outros assuntos numa linguagem clara e simples.[152]

O Considerando 42 do RGPD aduz que o titular de dados deve conhecer a identidade do responsável pelo tratamento dos dados pessoais:

> Para que o consentimento seja dado com conhecimento de causa, o titular dos dados deverá conhecer, pelo menos, a identidade do responsável pelo tratamento e as finalidades a que o tratamento se destina. Não se deverá considerar que o consentimento foi dado de livre vontade se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado.[153]

Nos casos em que for necessário o tratamento posterior dos dados pessoais para um fim que não seja aquele para o qual os dados tenham sido inicialmente obtidos, o responsável deverá fornecer ao titular dos dados informações claras sobre essa nova finalidade e todas as informações pertinentes a respeto desse tratamento.

O RGPD determina que o consentimento válido exige uma manifestação explícita mediante declaração ou ato positivo inequívoco. Ou seja, o titular dos dados deve agir para permitir o tratamento de seus dados pessoais. O consentimento poderá ser obtido por meio de declaração escrita, oral (gravada), inclusive em formato eletrónico. Como mencionado anteriormente, utilizar opções pré-assinaladas não é considerado válido pelo RGPD.

Acerca da questão da prova do consentimento, Filipa Matias Magalhães e Maria Leitão Pereira entendem que:

> O responsável pelo tratamento deve conseguir demonstrar que o titular dos dados pessoais consentiu livremente e de forma esclarecida. Um consentimento dado de forma oral ou até mediante um consentimento tácito ou outro não oferece estas garantias, porquanto não permite fazer prova de ter sido obtido de forma livre, específica, informada, explícita e através de ato inequívoco.[154]

Quanto ao prazo de validade do consentimento, o RGPD não trouxe uma definição. Assim, deve-se analisar o contexto, a extensão do consentimento e as expectativas do titular dos dados pessoais. Claro que se as operações de tratamento se alteraram de forma relevante,

[151] REGULAMENTO (UE), 2016.
[152] Ibidem.
[153] Ibidem.
[154] MAGALHÃES; PEREIRA, 2018. p. 32.

será necessário obter um novo consentimento do titular dos dados pessoais. No que se refere à revogação do consentimento, vale ressaltar que referida ação pode ser concretizada a todo tempo, total ou parcialmente e não produz efeitos retroativos.[155] Por fim, resta esclarecer que o Artigo 7.º, n.º 3, do RGPD prevê que o responsável pelo tratamento deve garantir que o consentimento deverá ser tão fácil de retirar como fora a ação de autorização de tratamento pelo titular dos dados, a qualquer momento. O RGPD não refere que o ato de dar ou retirar o consentimento deva sempre ser executado pela mesma ação.

3.2 Interesse legítimo

A alínea f do Artigo 6.º, n.º 1, do RGPD determina a licitude do tratamento se este for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.[156]

Apesar de não definir o que entende por interesse legítimo, o legislador europeu traz nos Considerandos de 47 a 49 alguns exemplos. Pode existir um interesse legítimo quando há uma relação relevante e apropriada entre o titular dos dados e o responsável pelo tratamento, em situações como quando o titular dos dados é um cliente ou está ao serviço do responsável pelo tratamento. A existência de um interesse legítimo exige uma avaliação cuidadosa, incluindo se o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados pessoais são recolhidos, que podem ser tratados para esse fim.

Os interesses e direitos fundamentais do titular dos dados podem, em particular, prevalecer sobre os interesses do responsável pelo tratamento, quando os dados pessoais são tratados em circunstâncias em que os titulares dos dados já não esperam um tratamento adicional. O fundamento jurídico não deverá ser aplicável aos tratamentos efetuados pelas autoridades públicas na prossecução das suas atribuições.

O tratamento de dados pessoais, estritamente necessário para efeitos de prevenção e controle da fraude, constitui também um interesse legítimo do responsável pelo tratamento dos dados. O tratamento de dados pessoais realizado para fins de comercialização direta pode ser considerado um interesse legítimo.[157] Poderá ser considerado interesse legítimo caso

[155] CORDEIRO, 2020. p. 189.
[156] REGULAMENTO (UE), 2016.
[157] LEI Nº 58, 2019. Art. 34.º.

possa ser demonstrado que o tratamento une um direito fundamental, corresponde total ou parcialmente a um interesse público, se identifica com outros fundamentos de licitude que constam no Artigo 6.º, n.º 1, do RGPD ou no caso de haver reconhecimento jurídico.

O tratamento de dados pessoais fundado em interesses legítimos do responsável ou de terceiro se apresenta como o fundamento de licitude mais complexo dentre os que constam no Artigo 6.º, n.º 1 do RGPD. Esta complexidade reflete a multiplicidade de fatores a considerar pelo intérprete aplicador:

a) Dados: (i) o tipo ou natureza dos dados pessoais tratados, (ii) o grau de identificação do titular dos dados, (iii) a quantidade de dados processados, (iv) a origem dos dados, e (v) qualidade dos dados.

b) Partes: (i) o titular dos dados em questão, (ii) o número de titulares envolvidos no processamento, (iii) o número de entidades envolvidas no tratamento, (iv) a natureza da relação entre titular e responsável, (v) as expectativas quanto às finalidades do tratamento, e (vi) eventual participação no processamento de responsáveis não estabelecidos na União.

c) Tratamento: (i) o método de realização do tratamento, (ii) o tipo de tratamento realizado, (iii) a duração do tratamento, (iv) frequência do tratamento, (v) as finalidades subjacentes, e (vi) o impacto do tratamento na esfera jurídica do titular.[158]

[158] CORDEIRO, A. Barreto Menezes - O tratamento de dados pessoais fundado em interesses legítimos. [Em linha]. **Revista de Direito e Tecnologia**. (1)1 (2019). [Consult. 13 fev. 2022]. Disponível em WWW:<URL:https://blook.pt/publications/publication/29c85b840a65/>. pp. 28-29.

4 AS NOVAS TECNOLOGIAS E SUA RELAÇÃO COM A PROTEÇÃO DE DADOS

Neste capítulo, dá-se uma ideia geral a respeto de algumas das ferramentas e novas tecnologias uma vez que, em plena era digital, a grande questão está na preocupação acerca da violação de direitos, bem como acerca das formas que são definidas para coletar, armazenar, manipular dados dos titulares. Dada a necessidade de proteger essas informações e a privacidade dos titulares, as normas jurídicas brasileiras e europeias buscam caminhos para lidar com o uso crescente de sistemas inteligentes.

4.1 Big Data

Big data pode ser conceituado pelo enorme volume de dados, que resulta na obtenção de informações a uma velocidade quase impossível de se imaginar. Refere-se ao conjunto de dados cujo tamanho está além da capacidade de uma ferramenta tradicional de banco de dados capturar, armazenar, gerenciar e analisar, representando a próxima fronteira para inovação, concorrência e produtividade.[159]

Big data pode ser entendido através da habilidade de coletar, processar e analisar um grande volume de dados em tempo suficiente para proporcionar ao detentor de tais informações uma maior capacidade e eficiência no direcionamento de suas decisões e atividades. Também pode ser entendido como um processo capaz de estabelecer critérios para tomada de decisões, que utiliza pessoas e tecnologias para analisar rapidamente uma grande quantidade de diferentes tipos de dados coletados a partir de fontes variadas, no intuito de produzir conhecimentos e informações úteis, a partir deste grande fluxo de dados.[160]

No campo da tecnologia da informação, o termo *big data* (em português, megadados, dados massivos ou dados em grande escala) é usado para se referir a conjuntos de informações em grande escala, incluindo tamanho que excede a capacidade e torna impossível, ou ao menos dificulta a adequação das ferramentas de *software* tradicionais para coletar, arquivar, gerenciar e analisar bases de dados.[161]

---

[159] BAGNOLI, Vicente - **Direito econômico e concorrencial**. 7.ª ed. rev., atual e ampl. São Paulo: Revista dos Tribunais, 2017. p. 397.
[160] KALYVAS; OVERLY, 2015. p. 1.
[161] LEAL, 2017. pp. 79-80.

A constante inovação, especialmente no setor de tecnologia, plataformas *on-line*, e na capacidade de analisar dados, elevam as possibilidades de contínua e rápida evolução em termos de *big data*. No universo atual, orientado por dados, as inovações disruptivas e a crescente disponibilidade de dados pessoais, resultaram na crescente implementação de técnicas avançadas para explorar (*mining*) e prospectar (*learning*) grandes conjuntos de dados. O *modus operandi* desses modelos de análise pressupõe a coleta exponencial de dados, a maior parte de matriz pessoal, pois a precisão será maior. Atualmente, é possível dizer que são os dados que comandam a operação.[162]

Embora a Internet tenha sido originalmente concebida como um fenômeno de livre interconexão entre redes globais, um espaço virtual no qual todos os usuários se apresentam, a verdade é que hoje o ciberespaço é uma verdadeira plataforma de transação eletrônica na qual os dados pessoais de seus usuários passam a ser o maior patrimônio económico do mundo *on-line*, tornando-se a nova "moeda" digital. A preocupação no que se refere à enorme quantidade, complexidade e variabilidade de informações disponíveis *on-line*, denominada de *big data*, reside não apenas no facto da sua existência, mas o uso que grandes provedores de serviço fazem dele *on-line* como Google, Amazon, Apple e Facebook.[163]

O conceito de *big data* não se baseia apenas na observação da existência de grandes conjuntos de dados, mas também se fala em *big data* para referenciar as tecnologias e processos envolvidos na coleta, armazenamento, processamento e análise desse grande volume de dados, realizados em períodos de tempo muito curtos. Estes processos envolvem a exploração e prospecção de dados com vista à criação de novas informações. Esta combinação de tecnologias e processos corresponde, portanto, a uma técnica para converter fluxos de dados em conhecimento muito específico (conhecimento intensivo em dados).[164]

Big data é representado pelo enorme conjunto de dados mantidos por empresas, órgãos governamentais, organizações públicas e privadas, que os analisam por meio de algoritmos, capazes de permitir a visualização, a compreensão e o efetivo consumo dos dados coletados. Um algoritmo é definido como uma sequência finita de operações que, executada em uma determinada ordem para atingir um objetivo específico em um tempo finito. O algoritmo deve atender aos seguintes requisitos: possuir um estado inicial, assim

[162] CALVÃO, Filipa. **Fórum de Proteção de Dados. Comissão Nacional de Proteção de Dados**. Lisboa, 2019, n.º 06, novembro de 2019. p. 61.
[163] PEREIRA COUTINHO, Francisco e CANTO MONIZ, Graça (coord.). **Anuário de Proteção de Dados 2019**. Lisboa: CEDIS, 2019. p. 111.
[164] LEAL, 2017. p. 81.

como uma sequência lógica finita de ações claras e precisas, produzindo resultados precisos, possuindo ainda um estado final previsível. Podem ser desenvolvidos algoritmos convertidos total ou parcialmente em um programa e executados em um computador, desde que seja possível definir claramente quais ações uma determinada máquina pode executar.[165]

O RGPD oferece uma importante reflexão acerca dos algoritmos, quando são implementados em uma sociedade, poucas decisões podem ser consideradas puramente técnicas. Há uma preocupação sobre a existência de algoritmo ético, o que requer uma combinação de métodos filosóficos e dispositivos do mais alto padrão. Ainda há muito trabalho a ser percorrido nesse sentido.[166]

A utilização de *big data* tem grande importância para o desenvolvimento da economia e da inovação, de maneira que, no cenário atual da sociedade, viabilizando fomentar o desenvolvimento e crescimento económico, é imprescindível contribuir de forma que a coleta, o processamento e a análise desse grande volume e variedade de dados possa proporcionar ao detentor das informações uma maior eficiência na tomada de decisões, pautadas sempre em questões éticas e de forma a evitar prejuízo em razão desse processamento.

A seguir, serão analisadas algumas questões que se referem ao volume, variedade e velocidade em termos de *big data*.

4.1.1 Volumetria, variedade e velocidade

Quando se fala em *big data*, o assunto remete aos seus 3Vs: volumetria, variedade e velocidade. Assim, tem-se um grande volume e variedade de dados, coletados em alta velocidade.

No que se refere à volumetria, entende-se que o crescimento no volume de dados é reflexo do avanço da tecnologia e a consequente redução de custos para a sua coleta, processamento, análise e armazenamento. O crescimento do *big data* provém especialmente das atividades diárias dos indivíduos, principalmente aquelas relacionadas aos serviços prestados por empresas na Internet. Marco Aurélio Florêncio Filho afirma que "vivemos, hoje, a era da informação. As pessoas passaram a realizar na internet várias atividades do

[165] EDELWEISS, Nina - **Algoritmos e programação com exemplos em Pascal e C.** Porto Alegre, RS: Bookman, 2014. pp. 34-35.
[166] GOODMAN, Bryce; FLAXMAN, Seth - **European Union regulations on algorithmic decision-making and a "right to explanation"**. Oxford Internet Institute. United Kingdom, 2016. p. 7.

seu cotidiano. Em regra, tem-se que toda vez que uma pessoa pretende buscar uma informação, vai-se à Internet".[167]

Entretanto, é importante ter em mente que os dados podem ser obtidos por meio de dispositivos que não possuem efetiva ligação com a Internet, no caso de câmaras de videovigilância, através da análise de passagens de veículos nos serviços de portagem eletrónica, e outros dispositivos que têm um importante conjunto de dados, inclusive para definição de perfis.

Acompanhando o crescimento do volume e fluxo de dados, houve no decorrer do tempo o aumento da velocidade em que esses dados são coletados, analisados e armazenados. A velocidade em *big data* consiste na rapidez com que se pode coletar, analisar e utilizar um grande volume de dados, viabilizada por avanços tecnológicos que permitem o melhor aproveitamento, de maneira extremamente rápida e, por vezes, em tempo real, o que, consequentemente, permite influenciar decisões de maneira instantânea, ou ainda fazer previsões de interesse público ou privado com maior rapidez, mantendo-se consideravelmente elevado os índices de acertos.

A variedade em termos de *big data* indica a incorporação de dados em diversos formatos, incluindo dados estruturados e não estruturados, dados provenientes de e-mails, redes sociais, sensores de ambiente, câmaras, microfones, dentre outros mecanismos que permitem sua coleta. A variedade em *big data* não se trata apenas de uma maior variedade de dados, mas também de maior variedade e amplitude de fontes e formatos de dados explorados.

Atualmente, tem-se discutido muito sobre a veracidade dos dados e que é uma característica do *big data* que é frequentemente discutido como seu quarto "V", em linha com a volumetria, a variedade e a velocidade. A veracidade diz respeto à integridade e à precisão dos dados, de forma a buscar que resultados corretos serão gerados.

O crescimento das atividades de tratamento de dados traz inúmeros desafios, tais como questões operacionais para a coleta, armazenamento, gerenciamento e análise dos dados. O uso eficiente de *big data* depende cada vez mais do aperfeiçoamento de tecnologias e do desenvolvimento de mecanismos que viabilizem sua organização e exploração.

Em *big data*, em termos muito simplificados, três modelos analíticos são normalmente usados: análise descritiva, análise preditiva e análise prescritiva. O que os

[167] FLORÊNCIO FILHO, Marco Aurélio - Aspectos criminais do ECA na sociedade da informação. In ABRUSIO, Juliana. (Coord.) - **Educação digital.** São Paulo: Revista dos Tribunais, 2015. p. 157.

diferencia fundamentalmente são as perguntas que cada um dos modelos pretende responder. Na análise descritiva, a questão central é a de saber o que aconteceu e por que razão aconteceu. Na análise preditiva, o objetivo é responder à pergunta sobre o que acontecerá ou poderá acontecer. Na análise prescritiva, dados os resultados da análise preditiva ou descritiva, trata-se de responder à questão do que necessariamente deverá fazer. O resultado obtido por estes processos será necessariamente distinto, ainda que seja utilizado o mesmo conjunto de dados.[168]

A análise preditiva é o modelo de análise mais utilizado em *big data*. A análise preditiva identifica padrões a partir de conjuntos de dados, sendo assim possível prever resultados, comportamentos, preferências ou tendências futuras.[169] *Big data* representa uma importante fonte de conhecimento, constituindo um processo de direcionamento de inovação por meio de informações obtidas a partir do tratamento de grande volume e variedade de dados. Trata-se de uma fonte capaz de alimentar o desenvolvimento de atividades económicas em diversos segmentos, por meio da formação de bases de dados que possuem importante valor económico e social.

Importante referir a relevância da utilização de *big data* num plano regulatório, utilizar a informação obtida através da análise de *big data* para melhorar ou facilitar o cumprimento dos requisitos regulatórios e de *compliance* a que estão sujeitas as instituições. Esta utilização está atualmente ancorada numa área cada vez mais importante dentro da FinTech: RegTech, tecnologia regulatória, que se refere à criação, por empresas de tecnologia, de soluções para atender e se adaptar aos requisitos regulatórios de cada setor. As empresas da RegTech usam principalmente tecnologias como computação em nuvem, *big data* e *blockchain*, e são amplamente utilizadas no setor bancário e financeiro. [170]

Nas instituições financeiras, a utilização de *big data* tem por objetivo melhorar os processos de detecção de fraudes e operações ilegais, os processos de identificação e categorização dos clientes, e os processos de gestão de riscos.[171] *Big data* é muito utilizado atualmente na identificação de clientes, no que se refere ao cumprimento de exigências regulatórias conhecidas pela expressão em inglês "*know your customer*" e por "*customer due diligence*". A identificação e categorização de clientes integra um processo que assenta no

[168] LEAL, 2017. p. 82.
[169] Ibidem. p. 82.
[170] Ibidem. pp. 91-92.
[171] Ibidem. p. 92.

fornecimento de informações e que possui para as instituições financeiras custos relevantes. O *big data* possibilita uma considerável diminuição desses custos.[172]

A utilização de *big data* pode trazer inúmeros benefícios, redução de custos, maior eficiência e rapidez na realização de diversas análises, sendo, entretanto, importante que sejam definidos certos limites a esse processamento. Em termos de *big data* é possível ter grandes dificuldades na aplicação dos princípios da finalidade, adequação e necessidade.

4.1.2 Princípios e fundamentos da proteção de dados e utilização de big data

Os princípios da finalidade, adequação e necessidade colocam-se em um grande impasse, apresentando-se em oposição às práticas de tratamento de grande volume e variedade de dados pessoais. Inúmeras ferramentas utilizadas em *big data* são baseadas na reunião de dados coletados das mais diferentes formas, origens, momentos, contextos e para finalidades diversas, muitas vezes sequer conhecidas no momento da coleta dos dados. Não raramente, a finalidade ou mesmo a utilidade dos dados são conhecidas apenas depois do tratamento, tornando a observância a tais princípios uma tarefa difícil.

Impõe-se, assim, uma análise crítica devido à falta de criação de regime próprio aplicável ao *big data* no RGPD. O facto de o Regulamento não ter criado um regime próprio de tratamento de dados através de *big data*, optando-se, pelo contrário, apesar do mérito de algumas inovações introduzidas nesta área, por comprimir as peculiaridades reveladas nos enquadramentos clássicos do regime de tratamento de dados. Estas críticas assentam na constatação de que *big data*, graças à sua forma de operação e às especificidades de que necessita, questionam de imediato um conjunto de aspetos fundamentais do regime de proteção de dados, tais como os seus requisitos básicos: transparência, consentimento, limitação de propósito e minimização de dados.[173]

No que se refere ao princípio da limitação das finalidades, *big data* traduz-se numa ameaça por várias razões: seja porque os dados são frequentemente processados e armazenados sem que, naquele momento, esteja definida ou conhecida a real finalidade, seja porque a reutilização de dados pode levar a processamento que geralmente é realizado por diferentes responsáveis, seja porque podem ser utilizados para fins incompatíveis que não eram conhecidos, nem foram comunicados ao interessado na época da recolha, sendo

[172] LEAL, 2017. p. 93.
[173] Ibidem. pp. 140-141.

impossível perceber o alcance das finalidades do tratamento de dados, nem as suas consequências.[174]

A utilização do *big data* também se traduz num problema quando se analisa o princípio da minimização de dados, por um lado, porque as suas técnicas se baseiam na ideia de maximização, ou seja, num incentivo para recolher o máximo de dados possível, e, por outro lado, os procedimentos de *big data* promovem a coleta, o processamento e o armazenamento de dados por longos períodos, mesmo que esses processamentos sejam inúteis. [175]

A proteção à privacidade deve estar inserida em todas as atividades que envolvam o tratamento de dados pessoais, sendo que no decorrer do desenvolvimento dos negócios, as organizações devem assegurar que a atividade é desenvolvida de acordo com o que foi informado ao titular dos dados pessoais e de acordo com o consentimento, caso este seja a base legal referente ao tratamento de dados. Entretanto, importa referir que a obtenção do consentimento nem sempre condiz com a realidade no tocante ao *big data*, pois na grande maioria dos casos, nesta fase, ainda não existe informação suficiente sobre o tratamento e suas finalidades, que possa ser fornecida ao titular dos dados para acreditar que este teve acesso a informações essenciais para se autodeterminar e, portanto, conceder consentimento informado.

A falta de informação suficiente ocorre principalmente por dois motivos: porque muitas vezes o próprio detentor da responsabilidade pelo tratamento não tem conhecimento das complexas fórmulas algorítmicas, que são a base do modelo de análise usado no processamento, e porque, na maioria dos casos, na data da coleta, ainda não é possível determinar todas as finalidades para as quais o tratamento daqueles dados servirão, em particular, no que diz respeto à reutilização de dados ao longo do tempo, pelos vários controladores de dados.[176]Assim, em grande parte dos casos, quando se fala em *big data*, o consentimento prestado pelo titular dos dados não se mostra um consentimento efetivamente válido.

[174] LEAL, 2017. pp. 173-174.
[175] Ibidem. p. 175.
[176] Ibidem. pp. 150-151.

Ocorre que nem todos os dados utilizados em *big data* são dados pessoais. Deste modo, caso os dados utilizados não sejam dados pessoais, não serão aplicáveis os regimes de proteção. Neste ínterim, no conjunto existem dados que não são pessoais, primeiro, porque se referem a elementos identificadores de pessoas coletivas; e segundo, por se tratar de meros dados operacionais, que não são associados a qualquer pessoa, e por fim, nem remotamente, permitem o reconhecimento de qualquer pessoa singular.[177]

Contudo, distinguir dados pessoais e dados não pessoais nem sempre é uma tarefa simples. Isso porque deve-se ponderar a anonimização e pseudonimização de dados pessoais, bem como a reversibilidade destas operações para a reutilização desses dados.[178]

Também é importante analisar os conceitos de anonimização e pseudonimização:

A anonimização, como explicado na secção 1.1.3.4 deste estudo, ocorre quando os dados pessoais se tornam anónimos de tal forma que o proprietário não seja mais ou não possa mais ser identificado. Por esta razão, não se emprega ao tratamento desses dados o Regulamento, uma vez ter sido realizado em conformidade com as elevadas exigências e critérios que lhe foram fixados.[179]

A pseudonimização, como também já mencionado neste estudo, na secção 1.1.1.1, corresponde a uma técnica de "desidentificação" e conduz à criação de dados que se situam entre dados pessoais e dados não pessoais, de modo que não possam mais ser atribuídos a um determinado titular dos dados sem recurso a informações adicionais. Esses dados tornam o seu titular identificável quando combinados com essas informações adicionais e se baseiam na possibilidade de reidentificar os dados. Ao contrário do que acontece com o anonimato, a pseudonimização - a técnica, por excelência, da Privacy by Design - não exclui a aplicação do Regulamento.[180]

Importante referir que a aplicação do regime de proteção de dados de forma mais branda em razão da pseudonimização será possível desde que essas informações sejam mantidas separadamente e sujeitas a medidas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável.

[177] LEAL, 2017. p. 110.
[178] Ibidem. p. 112.
[179] Ibidem. p. 112.
[180] Ibidem. p. 112.

Em termos de *big data*, existem propostas no sentido de criação de um regime especial acerca do tratamento dos dados. O que se propõe é a criação de um regime especial para o tratamento de *big data* que, ignorando a distinção entre dados pessoais e dados não pessoais, ficaria entre a não regulação e a regulação existente acerca do tratamento de dados pessoais. Esta proposta assenta na ideia de que a distinção entre dados pessoais e dados não pessoais já não é factível em face de determinados tipos de dados. Perante a possibilidade de identificação do titular com a utilização das técnicas de *big data*, surge um dilema regulamentar quanto a saber se os regimes de proteção de dados devem se aplicar apenas ao tratamento de dados pessoais ou se devem abranger também o tratamento de dados não pessoais que, quando relacionados com outros dados, permitem a identificação do titular. Neste último caso, o problema é que não há limites para o âmbito do regime de proteção de dados. Outra questão relevante é que grande parte da mineração de dados escapa dessa disciplina.[181]

O mau uso de tecnologias em *big data* é capaz de gerar não apenas danos à privacidade, mas também tratamento discriminatório, caso medidas preventivas não sejam tomadas pelos responsáveis pelo tratamento dos dados. As tecnologias utilizadas podem causar danos sociais, como discriminação de indivíduos ou grupos, além dos danos à privacidade, em decorrência do modo como essas tecnologias são estruturadas e utilizadas.

Neste sentido, é problemático que os usuários da Internet estejam sujeitos, especialmente quando lhes é desfavorável, a informações sobre eles resultantes de uma análise de dados coletados na Internet e essa sujeição muitas vezes envolve a exclusão do usuário de determinados atos ou negócios.[182] Não restam dúvidas quanto aos perigos do *big data*. É possível afirmar que tais perigos são de natureza diferente, convergem todos para a mesma ideia: as decisões são tomada, na maioria das vezes de forma totalmente automatizada, ou seja, sem intervenção humana no processo de tomada de decisão, sobre certas pessoas e empresas, com base nos resultados gerados pela análise de dados na Internet e, muitas vezes, esses resultados são a razão determinante para a tomada de decisão.[183] A utilização de *big data* deve ser pautada em certos limites para esse processamento.

[181] LEAL, 2017. pp. 143-144.
[182] Ibidem. p. 100.
[183] Ibidem.

No próximo capítulo abordam-se alguns temas relevantes e que demonstram que essa preocupação está em análise pelo Parlamento Europeu, no sentido de estabelecer normas harmonizadas para a inteligência artificial.

4.2 Inteligência Artificial

Inteligência artificial, conhecida pela sigla IA, ou AI, em inglês, trata-se do funcionamento de dispositivos eletrónicos, com sua capacidade de perceber variáveis e ajudar a decidir e a solucionar de diversos problemas, simulando a inteligência humana em uma máquina. Uma tecnologia que ocupa o topo da Revolução 4.0.

A União Europeia contou com o Grupo Europeu de Ética em Ciência e Novas Tecnologias para criar um conjunto de princípios democráticos embasados em valores fundamentais nos tratados da UE e na Carta dos Direitos Fundamentais da União Europeia, denominado Declaração sobre Inteligência Artificial, Robótica e Sistemas Autônomos, com o objetivo de responder a questões relativas à proteção da humanidade.

Taisa Macena de Lima e Maria de Fátima Sá, sobre a IA e a proteção da pessoa humana, explicam que:

> Sem intervenção humana direta e controle de fora, sistemas inteligentes podem conduzir diálogos com clientes em centros de atendimento *on-line*, pegar e manipular objetos com precisão, classificar as pessoas e seu comportamento, entre outras tarefas. Mais que isso: máquinas podem 'ensinar a si próprias' novas estratégias e procurar novas evidências para analisar. Por executarem tarefas sem direção humana ou sem supervisão, são denominados 'autônomos' e, por serem capazes de aprender, *machine learning*.[184]

Proteção da pessoa humana refere o respeito à sua dignidade e autonomia, ao exercício de suas responsabilidades, às questões de justiça, equidade e solidariedade, democracia, estado de direito e prestação de contas, e no tocante à segurança, proteção e integridade física e mental, inclusive em prol da proteção de seus dados e sua privacidade, entre outros direitos.[185]

[184] LEAL, 2017. p. 238.
[185] LIMA, Taisa Maria Macena de; SÁ, Maria de Fátima Freire de - Inteligência Artificial e Lei Geral de Proteção de Dados Pessoais. **Revista Brasileira de Direito Civil – RBDCivil,** Belo Horizonte, 26(4); (2020) 227-246.

4.2.1 Machine learning

Machine learning (ou aprendizado de máquina, em português) é uma vertente da inteligência artificial (IA) que prepara máquinas para aprender com dados. Nasceu do reconhecimento de padrões e da teoria de que os computadores podem aprender para realizar tarefas específicas. O seu aspeto iterativo é importante porque, conforme os modelos são expostos a novos dados, eles podem ser ajustados de forma independente, aprendendo com cálculos anteriores para tomar decisões confiáveis e passíveis de serem replicáveis. O *machine learning* já exista há algum tempo, a capacidade de aplicar cálculos matemáticos complexos o *big data* de forma automática, iterativa e cada vez mais rápida é um desenvolvimento recente. Trata-se de uma área que desenvolve algoritmos projetados para serem aplicados a um enorme conjunto de dados, com foco em predição, classificação e agrupamento.

Existe uma controvérsia acerca do entendimento sobre a possibilidade de um *software* "aprender". Alguns dizem que não há aprendizagem real devido à falta de consciência real, uma vez que somente os seres humanos podem aprender. *Machine learning* é um processo estatístico que pode ser usado para uma variedade de operações, mas a operação básica geralmente é o reconhecimento de padrões. Os algoritmos podem identificar padrões ou regras nos dados e usar esses padrões ou regras para interpretar os dados e fazer previsões sobre questões futuras.[186]

O *machine learning* usa um conjunto de recursos ou covariáveis (X) para prever o resultado (Y). Ao usar a previsão, a estrutura não está focada na previsão, mas existem observações rotuladas, em que onde X e Y são observados (dados de treinamento), e o objetivo é prever o resultado, construindo o (x). As suposições são as variáveis básicas necessárias para que a maioria dos métodos de *machine learning* funcione.[187]

Houve uma enorme evolução nas áreas de visão computacional, processamento de linguagem natural e análise de *big data* usando *machine learning*. Atualmente, o *machine learning* tem sido utilizado para o processamento de linguagem natural com base na análise de fala. A visão computacional e o reconhecimento facial baseados no aprendizado profundo podem ser usados para fins de vigilância.

[186] COECKELBERGH Mark - **AI ethics**. Cambridge, MA: The MIT Press, 2020. p. 83.
[187] ATHEY Susan; CATALINI, Christian; TUCKER, Catherine - **The Impact of Machine Learning on Economics**. Stanford, 2018. p. 4.

Machine learning é realmente útil como uma etapa intermediária no trabalho empírico em economia, gerando variáveis que podem ser utilizadas em análises económicas. Pode ser usado para avaliar um modelo de demanda de um consumidor para produtos, sendo possível modelar o impacto das relações do consumidor sobre as características daquele produto, encontrando produtos potencialmente relacionados e subgrupos de produtos similares. Os economistas também combinam suposições comportamentais e estatísticas para construir modelos mais sofisticados que estimam o impacto de políticas anteriormente não utilizadas. A aplicação de previsões a questões políticas tem sido bem-sucedida de várias maneiras, sendo importante para a tomada de decisão. Em um sentido ainda mais amplo, as novas oportunidades criadas por imagens e sensores em grande escala podem levar a novos tipos de análises de bem-estar e produtividade.

A economia, de modo geral, será profundamente transformada pela inteligência artificial e pelo *machine learning*. Os modelos estatísticos serão otimizados e mais robustos, e possuirão propriedades desejáveis de proteção devido à não manipulação, garantindo a equidade. Uma variedade de novas áreas de pesquisa é iniciada com melhores medições, novos métodos diferenciais e questões essenciais.

A futura força de trabalho terá de ser treinada com habilidades empíricas e de ciência de dados. É provável que surjam alguns problemas políticos decorrentes do *machine learning* e da inteligência artificial para estudar, incluindo questões que se referem a trabalhadores que tenham seus empregos eliminados devido à automação.[188] Entretanto, o *machine learning* deve ser considerado uma ferramenta importante e de extrema relevância para a seleção de modelos orientados por dados. Obter a melhor forma para utilizar dados de forma funcional e flexível tem uma importância cada vez maior nos dias atuais.

4.2.2 Consultoria robótica

A definição de consultoria financeira robótica tem como premissas as seguintes definições: "(i) consultoria financeira; (ii) automática; (iii) diretamente acedida pelos investidores, sem ou com mínima intervenção humana."[189]

Há ferramentas de consultoria de investimento digital que aliam usuários tendo por base as suas preferências com relação a determinados produtos financeiros.

[188] ATHEY; CATALINI; TUCKER, 2018. p. 27.
[189] LEAL, 2017. p. 205.

O uso de modelos algorítmicos não é algo específico para a consultoria robótica ou tecnologia financeira, é uma solução que tem sido utilizada no setor financeiro em geral. Pode ser utilizado no cálculo do risco das seguradoras, apresentação de prêmios de seguradoras, cálculo de taxas de juros sobre empréstimos bancários. Importa referir ainda que este modelo é também utilizado na assessoria tradicional, de forma a garantir maior objetividade às soluções apresentadas aos investidores. Percebe-se aqui a ausência de intervenção humana e utilização de algoritmos matemáticos.

O conselho dado pelo robô é baseado principalmente em dois elementos: a informação de entrada fornecida pelo usuário e certos dados de investimento, por exemplo, experiência de investimento, aversão ao risco, objetivos de investimento. O algoritmo constrói uma proposta de portfólio com produtos de investimento, nos quais o usuário pode investir, baseado em suas respostas.[190]

Os utilizadores dos serviços vislumbram uma redução de custos e maior eficiência operacional, maior facilidade de acesso e eficiências institucional e alocativa e, por fim, maior qualidade do serviço prestado, quando da utilização da consultoria robótica. A necessidade de deslocação a uma agência ou dependência do intermediário financeiro, principalmente em uma geração que tem todos os acessos e facilidades, obviamente, fazem com que a consultoria financeira robótica, que pode ser realizada a distância, seja priorizada pelos utilizadores. Outro ponto são os consultores financeiros robóticos, que estão disponíveis vinte e quatro horas por dia, sete dias por semana. Para as instituições financeiras, a implementação da consultoria robótica permite reduzir os custos com a mão de obra, entretanto, a implementação de um modelo de consultoria robótica exige um investimento inicial significativo.

Relativamente aos riscos para os investidores, pode-se elencar três principais riscos: informações insuficientes; disfunções das plataformas; e o uso generalizado de plataformas de consultoria robótica. A ausência de contato humano reduz a informação disponível, maioritariamente para investidores comuns, que possuem conhecimento limitado sobre o funcionamento dos mercados financeiros. O risco mais prevalente para o usuário pode ser considerado o aconselhamento individual insuficiente, o que significa que o resultado não corresponde à situação real e às preferências de risco do indivíduo em questão. Dentro da

[190] RINGE, Wolf-Georg; RUOF, Christopher - A Regulatory Sandbox for Robo Advice, ILE University of Hamburg, Institute of Law and Economics (ILE), Hamburg. **Working Paper Series**. (14) (2018) 04-05.

complexa estrutura do *software* de consultoria em robótica, sempre existe o risco de ocorrer um erro, devido a erros no processo de desenvolvimento.

Importante ter em mente, ainda, o risco sistêmico, uma vez que maioria dos consultores de robótica atua de forma semelhante ao processamento e avaliação dos dados de seus clientes, visto que a composição de seu portfólio e o algoritmo subjacente que aloca recursos são semelhantes. Considerando que os padrões de risco são altamente correlacionados, a consultoria robótica tem o potencial de exibir um comportamento de agregação maior do que os consultores de portfólio tradicionais e de levar ao risco de concentração, já que os participantes do mercado podem agir de forma a elevar o impacto das flutuações económicas, podendo aumentar as flutuações nos preços dos ativos e levar a uma maior incidência de mudanças unilaterais na carteira.

Muito se discute hoje sobre a responsabilidade civil relativamente ao funcionamento das plataformas e imputação de responsabilidade civil, no caso de a gestão das plataformas ser realizada por terceiros. Esta questão é uma realidade comum as empresas digitais e não pode ser considerado um problema específico do mercado de Fintech e/ou consultoria robótica, vez que é uma realidade constante em grande parte das empresas dos mais diversos setores.

Em termos de União Europeia, as normas regulamentares para aconselhamento robótico se encontram na Diretiva de Instrumentos Financeiros (MiFID). A estrutura original datada de 2004 foi revisada com a implementação da MiFID II em 2018. O objetivo da reforma era fortalecer a proteção do investidor e melhorar o funcionamento dos mercados financeiros, tornando-os mais eficientes e transparentes.

De acordo com o Artigo 289.º, n.º 2 do Código dos Valores Mobiliários [191], apenas os intermediários financeiros podem exercer atividades de intermediação financeira e assessoria financeira. Mencionada exclusividade se aplica às instituições de crédito, conforme Artigo 8.º do Regime Geral das Instituições de Crédito e Sociedades Financeiras[192]

[191] MINISTÉRIO DAS FINANÇAS. Código dos Valores Mobiliários. Decreto-Lei n.º 486/99. [Em linha]. **Diário da República** n.º 265/1999, Série I-A, 13 nov. 1999. [Consult. 16 jan. 2022]. Disponível em WWW:<URL:https://dre.pt/dre/legislacao-consolidada/decreto-lei/1999-34575175>.

[192] Idem. Regime Geral das Instituições de Crédito e Sociedades Financeiras. Decreto-Lei n.º 298/92. [Em linha]. **Diário da República** n.º 301/1992, 6º Suplemento, Série I-A, 31 dez. 1992. [Consult. 16 jan. 2022]. Disponível em WWW:<URL:https://dre.pt/dre/legislacao-consolidada/decreto-lei/1992-70072322>.

(RGIC), e às sociedades seguradoras, de acordo com o Artigo 3.º da Lei n.º 147 de 9 de setembro de 2015.[193]

O regime jurídico aplicável ao exercício de consultoria financeira robótica depende do setor e produtos ofertados: seguros, a Lei n.º 147/2015 e a Lei n.º 72 de 16 de abril de 2008, no caso de instrumentos financeiros, o Código dos Valores Mobiliários, e no caso de produtos bancários, o Regime Geral das Instituições de Crédito e Sociedades Financeiras.

A consultoria robótica trouxe novos desafios para o setor financeiro. Como geralmente não há interação, os investidores confiam nas informações escritas, como prospectos de produtos de investimento. Estudos sobre educação financeira mostram que os investidores costumam ter dificuldade em entender até mesmo os termos financeiros básicos. O *design* de informações pode ajudar os provedores de serviços robóticos a envolver seu público, a chamar a atenção para o que é importante e melhorar a interação humana robótica. Dessa forma, eles podem estar mais bem equipados não apenas para cumprir os requisitos regulamentares, mas também para fornecer melhores conselhos e uma melhor experiência aos seus clientes. Os benefícios podem ser substanciais tanto para investidores quanto para as empresas.[194]

No âmbito da consultoria financeira robótica importante que os respetivos regimes se acomodem às modernas plataformas de negociação. O desafio, portanto, é desenhar um ambiente regulatório no qual possam prosperar novos modelos de negócios, no qual sejam monitorados os riscos potenciais para os investidores e a estabilidade financeira, e que simultaneamente crie segurança jurídica para todos os participantes do mercado.

4.2.3 Ética e inteligência artificial

A ética no cenário da inteligência artificial deve ser vista de forma a promover uma reflexão e requer discussão, uma vez que as mudanças impactam os valores humanos. Considerando-se a ética no contexto da inteligência artificial, no meio de conversas sobre a possibilidade de máquinas que tomam decisões que podem impactar a vida da sociedade como um todo, deve-se atentar às discussões e contribuir para que a evolução tecnológica possa caminhar de forma positiva e alinhada com valores éticos importantes.

---

[193] ASSEMBLEIA DA REPÚBLICA. Lei n.º 147/2015. [Em linha]. **Diário da República** n.º 176/2015, Série I, 9 set. 2015, 7342-7500 [Consult. 16 jan. 2022]. Disponível em WWW:<URL:https://dre.pt/dre/detalhe/lei/147-2015-70237675>.

[194] SALO, Marika; HAAPIO, Helena - Robo-Advisors and Investors: Enhancing Human-Robot Interaction Through Information Design. **Associate Professor of Business Law.** 2017. 441-448. ISBN 978390303515-7.

Estratégias para tornar a inteligência artificial mais segura ou livre de erros são elementos de extrema importância na abordagem da demanda ética. Verificar se um produto final atende a especificações de *design* e validar se também atende as necessidades do usuário tem inúmeras implicações. Devem ser utilizadas habilidades para alinhar a inteligência artificial em atenção aos valores humanos, sendo em tese, inclusive, possível de implementar o controle humano na inteligência artificial, o que tem se discutido se realmente será possível diante de técnicas cada vez mais modernas de inteligência artificial.

Deve haver confiança entre os seres humanos e a utilização da inteligência artificial, para que possa funcionar.[195]

Desenvolver e implementar códigos de ética para a inteligência artificial tem relevância nesse cenário. A maneira como é gerenciado o desenvolvimento de códigos de ética para inteligência artificial, assim como a forma que esses códigos são implementados, são elementos importantes da integridade organizacional. É preciso ter a cautela para que esses códigos de ética não funcionem apenas como regras escritas e que não sejam efetivamente aplicados. O controle e a governança fazem parte de uma questão de grande relevância nesse cenário.[196]

É necessário ir além do que é divulgado, não devendo embasar apenas em preocupações futuras. Deve-se utilizar a filosofia e a ciência para verificar e discutir as hipóteses da inteligência artificial, o papel desempenhado nesses cenários, verificando-se como a inteligência artificial será utilizada num futuro próximo, bem como a análise ética de sua utilização, de forma a ser possível contribuir e participar da evolução tecnológica de forma positiva.

4.2.4 Direitos de imagem e inteligência artificial

A revolução industrial 4.0 ampliou o universo digital com tecnologias como a inteligência artificial e também revolucionou os direitos da personalidade, direitos à privacidade, assim como a proteção aos dados pessoais. Essa realidade trouxe importantes questões sobre até que ponto a IA afeta os direitos de imagem e como o direito de personalidade deve ser tratado, relacionado ao uso de imagem, sendo a inteligência artificial um dois muitos elementos associados ao uso de sistema inteligentes.

[195] BODDINGTON, Paula - Artificial Intelligence: Foundations, Theory, and Algorithms, Towards a Code of Ethics for Artificial Intelligence. Oxford, United Kingdom. **Springer International Publishing**, 2017. p. 05.
[196] Ibidem. pp. 99-100.

Entre os exemplos de tais usos, que oferecem oportunidades e, ao mesmo tempo, riscos, tem-se: a captação e utilização de imagens em sites de buscas, divulgação indevida de imagens de pessoas públicas, captação de imagens por câmaras em determinados ambientes, entre outras possibilidades promovidas por sistemas de captação facial.

Ferramentas artificialmente inteligentes estão espalhadas em espaços públicos, o que pode ser interpretado como uso que ofende a privacidade das pessoas, se não for regulado conforme determina a lei. "Não obstante, a proteção do direito à imagem nunca recairá sobre os objetos em si, em termos isolados. Terão de ser sempre enquadrados com alguma representação da pessoa humana para que haja proteção."[197]

> A captação e reprodução de imagens em massa (*big data*), cuja principal fonte é a internet. No seu tratamento são utilizadas tecnologias baseadas em *data mining* e algoritmos assentes em técnicas de *machine learning*, tendo como objetivo a criação de nova informação, que poderá consistir, eventualmente, num perfil de uma determinada pessoa. [198,199]

Além do acesso em massa a imagens expostas, há também casos de manipulação indevida e modificações de imagens estáticas e em movimento, inclusive de voz, por meio de *softwares* de edição de vídeo e imagens, em técnicas baseadas em IA, que impactam o direito da pessoa.[200]

> David Oliveira Festas, citado por Vitor Palmela Fidaldo, explica que:
>
> Qualquer forma de exposição ou reprodução, digital ou não, que seja tecnicamente possível, estará abrangida pela norma, onde se incluem, naturalmente, as fotomontagens. O limite será apenas que a exposição ou reprodução permita a identificação da pessoa retratada, ainda que seja apenas pelas pessoas do seu círculo íntimo.[201]

---

[197] FIDALGO, Vitor Palmela - **Inteligência Artificial e Direitos de Imagem**. [Em linha]. 2018. p. 12. [Consult. 16 jan. 2022]. Disponível em WWW:<URL:https://blook.pt/publications/fulltext/c73d596c5b9b/>.
[198] Ibidem. pp. 12-13.
[199] Com efeito, constituindo a imagem uma informação relativa a uma pessoa singular, capaz de a identificar e que, por esse motivo, cabe no conceito de dados pessoais presente no art. 4.º do Regulamento Geral de Proteção de Dados (RGDP), esta será protegida enquanto tal. III. O regime jurídico da proteção de dados pessoais torna-se, assim, mais um instrumento a ter em conta na proteção do direito à imagem, por vezes, até um instrumento mais expedito do que aquele estabelecido no Código Civil. Numa perspectiva prática, a invocação de regras presentes no regime jurídico da proteção de dados constitui muitas vezes um caminho mais direto para o objetivo que se pretende obter. Permitirá, por exemplo, o apagamento da imagem por parte do responsável pelo tratamento dos dados pessoais, nos termos do art. 17.º do RGDP. IV. A imagem da pessoa humana está sujeita ainda a um regime mais exigente, dado que caberá na categoria de dados sensíveis presente no art. 9.º, n.º 1, do RGDP. A leitura biométrica do rosto, igualmente denominada reconhecimento fácil, tem-se tornado cada vez mais comum. A disciplina da proteção de dados proporciona, uma vez mais, vantagens no que diz respeto à tutela civil. Enquanto nos arts. 79.º, n.º 1, e 82.º do CC, ainda que se exclua o mero consentimento tolerante, se admite que o consentimento seja tácito, no caso do tratamento de dados sensíveis, onde se inclui a imagem da pessoa humana, o consentimento terá de ser 'explícito'.
Ibidem. pp. 12-13.
[200] Ibidem. p. 11.
[201] Ibidem. p. 10.

Tendo-se em vista o campo diversificado e abrangente em que são usadas ferramentas artificialmente inteligentes, a abordagem jurídica sobre a imagem como dado pessoal[202] entra no âmbito interdisciplinar do direito de proteção de dados, privacidade e personalidade, estando coberta pelo RGPD em seu Artigo 4.º, que conceitua dados pessoais.[203]

> A revolução tecnológica redimensionou em diversos aspectos o que se entendia por direito à imagem, pois '[o] desenvolvimento das chamadas tecnologias de informação e comunicação (TICs) causam um impacto considerável na pesquisa e na aplicação desse direito, cujos próprios contornos vão se amoldando de acordo com as tendências do progresso tecnológico'[204]

Pode-se incluir nas questões de direito de imagem as *deepfakes*[205], que é a reconstrução digital de imagens a partir de tecnologias de inteligência artificial. Entende-se que esta, que é uma prática de *fakenews*, represente fator de risco à segurança de dados, sendo uma violação ao RGPD e demais leis de proteção de dados. Diante desta situação, vale ressaltar o Artigo 35.º do RGPD, que pode ser usado em praticamente todos os casos de uso das ferramentas de IA, por meio de avaliações de impacto sobre a proteção de dados.[206]

---

[202] FIDALGO, 2018. pp. 11-14.

[203] O art. 4.º, 1), refere a definição legal de "dados pessoais" como "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular".

[204] MEDON, F. O direito à imagem na era das *deepfakes*. **Revista Brasileira de Direito Civil. RBDCivil**. Belo Horizonte. 27 (jan./mar., 2021) 251-277. pp. 252-3.

[205] "*Deepfakes* são imagens ou vídeos falsos, onde as imagens de pessoas são sobrepostas através de técnicas baseadas na inteligência artificial, que permitem uma autenticidade aparente muito genuína. A visualização desses vídeos, além de prejudicar a imagem do visado, é uma fonte de lucro fácil para quem os coloca na rede. FIDALGO, *op.cit.* p. 10.

[206] "1) Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação. [...] 3) A realização de uma avaliação de impacto sobre a proteção de dados a que se refere o n.º 1 é obrigatória nomeadamente em caso de: a) Avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar; b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9.º, n.º 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.º ; ou c) Controlo sistemático de zonas acessíveis ao público em grande escala."

> Proteger a imagem de uma pessoa é, em última análise, proteger a sua personalidade. [...] E a imagem, como parte integrante da construção da dignidade da pessoa humana, não pode ser tratada de maneira dissociada da dimensão do reconhecimento, presente nesta.[207]

A IA traz muitos benefícios aos usuários, mas também muitos riscos, para além do processamento dos dados pessoais. Em vista dessa realidade, Hoffmann-Riem explica que cada área do ordenamento jurídico enfrenta diferentes desafios, os quais exigem regras abrangentes[208].

Depreende-se, portanto, que as tecnologias digitais, como a IA, podem ter efeitos desejados ou indesejados a partir de uma perspectica ética e sócioeconômica, daí a importância de avaliar o contexto em que se insere o uso de IA, e este requer uma estrutura específica, somando-se à imposição de limites regulatórios, a fim de prover os interesses legais e públicos para proteger a pessoa contra efeitos negativos do uso de sua imagem.[209]

4.2.5 Proposta de regulamento do parlamento europeu e do conselho sobre regras harmonizadas em matéria de inteligência artificial

Está em andamento uma proposta de regulamento do Parlamento Europeu e do Conselho que estabelece normas harmonizadas para a inteligência artificial (Regulamento de Inteligência Artificial).

Inteligência artificial é um conjunto de tecnologias em constante evolução que pode oferecer inúmeros benefícios económicos e sociais para todas as indústrias e atividades sociais. Por meio da IA é possível melhorar as previsões, otimizar as operações e a alocação de recursos e personalizar a prestação de serviços. A utilização de inteligência artificial pode contribuir para resultados sociais e ambientais positivos e proporcionar vantagens competitivas às empresas e à economia europeia. Entretanto, importa referir que os mesmos elementos e técnicas que produzem os benefícios socioeconómicos da inteligência artificial também podem levar a novos riscos ou consequências negativas para os cidadãos e a sociedade. Diante desse cenário, a União Europeia busca adotar uma abordagem equilibrada, de forma a preservar a liderança tecnológica da União Europeia e garantir que as novas

[207] MEDON, *op cit.* p. 257.
[208] HOFFMANN-RIEM, W. Artificial Intelligence as a Challenge for Law and Regulation WISHMEYER T; RADEMACHER R. (Eds) - **Regulating Artificial Intelligence.** [Online]. Switzerland: Springer, 2020. pp. 1-29. [Consult. 2 feb. 2022]. Available from WWW:<URL:https://doi.org/10.1007/978-3-030-32361-5>. pp. 2/12.
[209] Ibidem. p. 5.

tecnologias, desenvolvidas e utilizadas em respeto aos valores, direitos e princípios fundamentais da União.[210]

A citada proposta constitui uma parte fundamental da estratégia para o mercado único digital da União Europeia e tem como objetivos:

> (i) garantir que os sistemas de inteligência artificial utilizados na União são seguros e cumprem a legislação em vigor em matéria de direitos fundamentais e os valores da União;
> (ii) garantir a segurança jurídica para facilitar o investimento e a inovação em matéria de inteligência artificial;
> (iii) melhorar a governação e aplicação efetiva da legislação existente sobre direitos fundamentais e requisitos aplicáveis aos sistemas de inteligência artificial;
> (iv) permitir o desenvolvimento de um mercado único para as aplicações de inteligência artificial legítimas, seguras e de confiança.[211]

É dada preferência a uma estrutura regulatória mais robusta aplicável a sistemas de inteligência artificial de alto risco, com a possibilidade de os fornecedores de sistemas de inteligência artificial livres de risco seguirem um código de conduta. Os requisitos dirão respeto aos dados, documentação e rastreabilidade, à prestação de informações e à transparência, à supervisão humana, à exatidão e à solidez e seriam obrigatórios para os sistemas de inteligência artificial de risco elevado.[212]

O Artigo 1.º da proposta de Regulamento de Inteligência Artificial estabelece:

> (i) regras harmonizadas para a colocação no mercado, a colocação em serviço e a utilização de sistemas de inteligência artificial na União;
> (ii) proibições de certas práticas de inteligência artificial;
> (iii) requisitos específicos para sistemas de inteligência artificial de risco elevado e obrigações para os operadores desses sistemas;
> (iv) regras de transparência harmonizadas para sistemas de [IA] concebidos para interagir com pessoas singulares, sistemas de reconhecimento de emoções e sistemas de categorização biométrica, bem como para sistemas de inteligência artificial usados para gerar ou manipular conteúdo de imagem, áudio ou vídeo;
> (v) regras relativas à fiscalização e vigilância do mercado. [213]

[210] COMISSÃO EUROPEIA - **Regulamento do Parlamento Europeu e do Conselho** que estabelece regras harmonizadas em matéria de Inteligência Artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da União, Bruxelas, 21 abr. 2021.
[211] Ibidem.
[212] LEI Nº 58, 2019. p. 3.
[213] Ibidem.

A proposta de Regulamento de Inteligência Artificial proíbe as seguintes práticas de inteligência artificial:[214]

> (i) a colocação no mercado, a colocação em serviço ou a utilização de um sistema de inteligência artificial que empregue técnicas subliminares que contornem a consciência de uma pessoa para distorcer substancialmente o seu comportamento de uma forma que cause ou seja suscetível de causar danos físicos ou psicológicos a essa ou a outra pessoa;
> (ii) a colocação no mercado, a colocação em serviço ou a utilização de um sistema de inteligência artificial que explore quaisquer vulnerabilidades de um grupo específico de pessoas associadas à sua idade ou deficiência física ou mental, a fim de distorcer substancialmente o comportamento de uma pessoa pertencente a esse grupo de uma forma que cause ou seja suscetível de causar danos físicos ou psicológicos a essa ou a outra pessoa;
> (iii) a colocação no mercado, a colocação em serviço ou a utilização de sistemas de inteligência artificial por autoridades públicas ou em seu nome para efeitos de avaliação ou classificação da credibilidade de pessoas singulares durante um certo período com base no seu comportamento social ou em características de personalidade ou pessoais, conhecidas ou previsíveis, em que a classificação social conduz a tratamento prejudicial ou desfavorável;
> (iv) a utilização de sistemas de identificação biométrica a distância em tempo real em espaços acessíveis ao público para efeitos de manutenção da ordem pública, salvo se essa utilização for estritamente necessária para alcançar um dos seguintes objetivos: a investigação seletiva de potenciais vítimas específicas de crimes, nomeadamente crianças desaparecidas; a prevenção de uma ameaça específica, substancial e iminente à vida ou à segurança física de pessoas singulares ou de um ataque terrorista; e a detecção, localização, identificação ou instauração de ação penal relativamente a um infrator ou suspeito de uma infração penal.

Deve ser criado, implantado, documentado e mantido um sistema de gestão de riscos em relação a sistemas de inteligência artificial de risco elevado. O sistema de gestão de riscos deve consistir num processo iterativo contínuo, executado ao longo de todo o ciclo de vida de um sistema de inteligência artificial de risco elevado, o que requer atualizações regulares sistemáticas. Os sistemas de inteligência artificial de risco elevado devem ser concebidos e desenvolvidos de maneira que assegure que o seu funcionamento seja suficientemente transparente para permitir aos utilizadores interpretar o resultado do sistema e utilizá-lo corretamente.[215]

[214] LEI Nº 58, 2019. p. 3.
[215] Ibidem.

4.3 *Blockchain*

Blockchain "surgiu em 2008 para dar suporte ao *bitcoin* (moedas virtuais criptografadas)"[216]. É um sistema tecnológico que permite armazenar dados com segurança, uma cadeia ou corrente de blocos, como se fossem páginas de um livro-razão, compartilhado e imutável, tendo como função registar transações e habilitar o rastreamento de ativos de organizações.[217] É introduzido pelo uso da tecnologia disruptiva, que se tornou imprescindível para entregar informações com celeridade, advindas do mencionado livro-razão, ao qual apenas os membros de uma rede autorizada têm acesso.[218,219]

> A classe de tecnologia *blockchain* é usualmente identificada em dois sistemas. O sistema público é executado na rede pública e é aberto a todos que quiserem dele participar. O sistema privado, por sua vez, é executado em rede privada, em regra com um propósito específico e que tem um *gatekeeper* que controla a entrada de pessoas. A distinção está na liberdade de entrada e no conhecimento dos dados do banco pelo *gatekeeper*.[220]

As redes *blockchain* trafegam transações comerciais e vão além do bitcoin, computam dados pessoais de clientes e guardam qualquer tipo de dados (documentos, arte, registos entre outros). As informações de transações guardadas em blocos (*blocks*), recebem um código matemático único, por meio de impressão digital, chamada *hash*, inteligando "um

---

[216] NEW LAW - **O blockchain**. [Em linha]. [Consult. 15 jan. 2022]. Disponível em WWW:<URL:https://newlaw.com.br/direito-ao-esquecimento/>.

[217] "Um ativo pode ser tangível (uma casa, um carro, dinheiro, terras) ou intangível (propriedade intelectual, patentes, direitos autorais e criação de marcas). Praticamente qualquer item de valor pode ser rastreado e negociado em uma rede de *blockchain*, o que reduz os riscos e os custos para todos os envolvidos. Uma rede *blockchain* pode acompanhar pedidos, pagamentos, contas, produção e muito mais. Como os membros compartilham uma visualização única dos fatos, é possível ver todos os detalhes de uma transação de ponta a ponta, o que oferece maior confiança, eficiência e novas oportunidades."
IBM - **O que é a tecnologia blockchain?** [Em linha]. 2021. [Consult. 2 fev. 2022]. Disponível em WWW:<URL:https://www.ibm.com/br-pt/topics/what-is-blockchain>.

[218] BRITO, Beatriz Gontijo de; CAMPO, Aline França. Instituto Iberoamericano de Estudos Jurídico**.** [Em linha]. **Revista Ibérica do Direito**. 1(2) (jul./dez., 2020). p. 99. [Consult. 15 jan. 2022]. Disponível em WWW:<URL:https://revistaibericadodireito.pt/index.php/capa/article/view/8/10>.

[219] "Nos termos do artigo, n. 2. da UE General Data Protection Regulation (GDPR) e do artigo 1. da Lei Geral de Proteção de Dados (LGPD), é objetivo a proteção do direito fundamental à proteção dos dados pessoais, no que se refere ao tratamento e à livre circulação. Consideram-se dados pessoais a «informação relativa a uma pessoa singular identificada ou identificável («titular dos dados)». O direito à proteção de dados contempla não somente a privacidade, mas todas as situações existenciais que são afetadas pelo tratamento das informações pessoais. Associado a esse objetivo, a regulação tem por fim promover a confiança necessária para o desenvolvimento especialmente do mercado digital, eliminando-se obstáculos para o fluxo de dados necessários à consecução desse fim.".

[220] Ibidem. pp.119-120.

conjunto em ordem cronológica, formando uma linha contínua de blocos – uma corrente (daí o termo '*chain*')".[221]

> A tecnologia *blockchain* [...] é uma concatenação de blocos, sendo cada um deles composto por um certo número de data, relacionados de tal modo que cada novo bloco que se acrescenta à sequência contém uma imagem criptográfica do anterior. Noutras palavras, é uma base de dados digital, partilhada e sincronizada.[222]

Sua funcionalidade apresenta-se em três momentos:[223]

(i) O registro das informações como blocos de dados, que têm um movimento ativo tangível (produto) ou intangível (intelectual). Esses blocos registram informaçõs como quem, o que, quando, onde quanto e até mesmo a condição de uma transação.

(ii) Um bloco está conectado a outro, anteriores e posteriores, formando uma cadeia de dados segura, de modo que um não afete toda a movimentação, registrando hora e sequência de cada transação.

(iii) As transações são bloqueadas em conjunto, irreversivelmente. Cada bloco em si fortlece a sequência anterior e posterior da cadeia, o que torna a *blockchain* inviolável, sendo este o aspecto da imutabilidade, o que evita adulterações mal-intencionadas, daí a confiabilidade gerada pelo sistema como um todo.

Entre as vantagens da *blockchain*, a IBM destaca três: confiança, segurança e eficiência:[224]

(i) "Maior confiança" – os membros de uma *blockchain* têm a garantia de obter dados corretos e pontuais e que seus registros confidenciais serão compartilhados apenas com os membros da rede a que foi concedido acesso específico.

(ii) "Maior segurança" – os membros de uma *blockchain* fazem questão de dados precisos em todas as transações validadas, que são imutáves e registradas permanentemente, não havendo como excluí-las, nem mesmo o administrador.

(iii) "Mais eficiência" – para acelerar as transações, há um contrato denominado inteligente, que dispões de um conjunto de regras, o qual fica armazenado na *blockchain* e é executado automaticamente.

---

[221] COMO FUNCIONA A TECNOLOGIA BLOCKCHAIN. [Em linha]. **Exame Online**. Future of Money. 23 dez. 2021. [Consult. 10 fev. 2022]. Disponível em WWW:<URL:http://exame.com/future-of-money/como-funciona-a-tecnologia-blockchain/>.

[222] REBELO, M.P. - Os desafios do RGPD perante as novas tecnologias blockchain. [Em linha]. **Rev Bio y Der**. 46 (2019) 117-131. p. 119. [Consult. 15 jan. 2022]. Disponível em WWW:<URL:https://scielo.isciii.es/pdf/bioetica/n46/1886-5887-bioetica-46-00117.pdf >. ISSN 1886-5887.

[223] IBM, 2021.

[224] Ibidem.

> O RGPD surgiu num contexto em que a *blockchain* não era ainda um fenómeno no mundo digital; as suas principais preocupações centravam-se nos serviços em cloud e nas redes sociais, que se organizam sobretudo por sistemas centrais com as quais os usuários interagem e assume normalmente o papel de data processor/controller.[225]

São inúmeras as aplicações da tecnologia *blockchain*, depreendendo-se que tal realidade em contribuído positivamente para o seu crescimento no mercado digital, contudo, é indispensável observar o cumprimento das normas protetivas dos dados pessoais que são cadastrados nesse sistema.

Também deve-se considerar que, em princípio, por um lado, dada a inviolabilidade dos dados que são regitrados e armazenados em uma "cadeia de blocos", a respectiva exclusão não é uma opção. Por outro lado, sendo o funcionamento desta tecnologia caracterizada pela descentralização, não há um controle único e central da "informação numa entidade determinada", e isso acaba afetando a assimilação das partes quanto "às regras previstas no Regulamento, o apuramento de responsabilidades e a aplicação das respetivas sanções."[226]

> É inegável a existência de uma grande tensão entre a arquitetura descentralizada desta tecnologia e o novo regulamento europeu, que acaba por refletir um idêntico conflito de objetivos entre a necessidade de proteger dados pessoais e acautelar os direitos dos seus titulares, por um lado, e ao mesmo tempo a necessidade de promover a inovação tecnológica, por outro.[227]

Como as transações realizadas e registradas nesse sistema, como mencionado, não podem ser apagadas, "então, que em princípio todos os dados lançados no blockchain seriam tendencialmente indestrutíveis, imutáveis e impassíveis de modificação; o que claramente representa um problema na óptica do RGPD".[228]

A indestrutibilidade e imutabilidade tornam qualquer modificação ou uma *erasure* (apagamento) tecnicamente impossível, este foi o princípio inicial do registro em *blockchain*, impossibilitá-lo.[229]

Rebelo ainda ressalta que "no âmbito do sistema *blockchain* uma *erasure* é tecnicamente impossível", até porque, esse foi o foco da sua criação. Entretanto, a autora explica que a "criação de alternativas tecnológicas" com o objetivo de limitar o "processamento dos dados ou que estes façam alguma relação com dados anteriores como

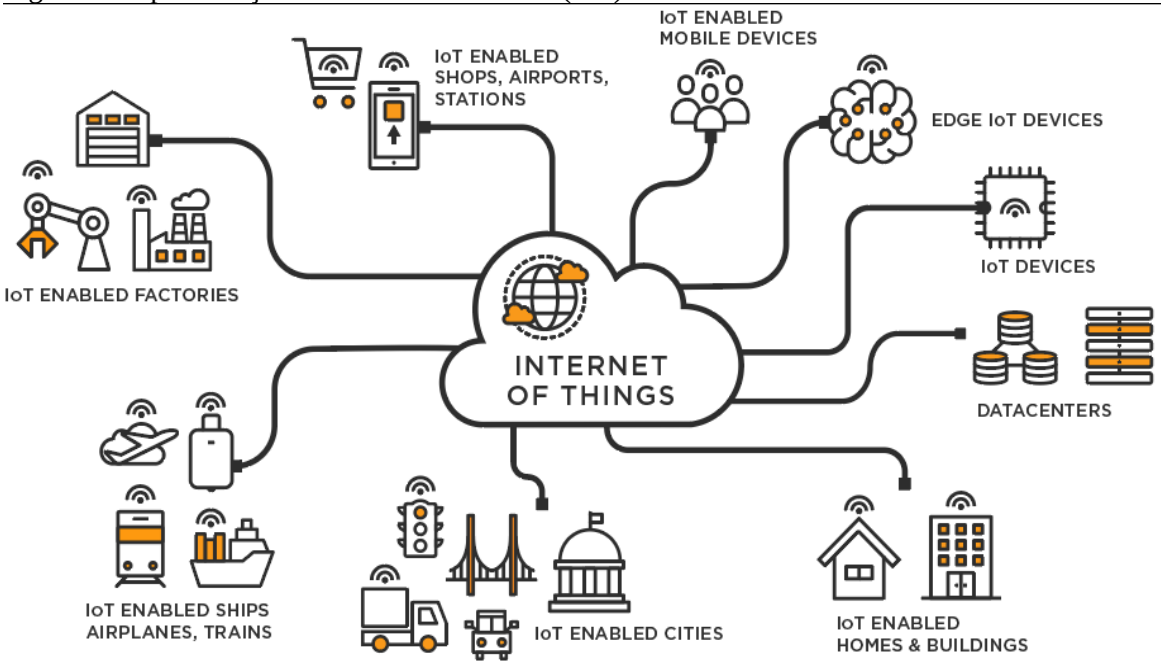
[225] REBELO, 2019. p. 119.
[226] Ibidem. p. 125.
[227] Ibidem. p. 125.
[228] Ibidem. p. 126.
[229] REBELO, 2019. p. 121.

não mais consideráveis", poderá desencadear um questionamento "como sendo suficiente para efeitos de acautelar este direito".[230]

4.4 Internet das Coisas (IoT)

Internet das Coisas é um termo que representa todos os dispositivos de computação conectados à Internet. É normalmente entendida como a "rede de dispositivos responsivos e objetos do dia a dia [...] integrados a sensores ambientais e outras tecnologias que permitem coletar e trocar dados sem intervenção humana"[231], como ilustrado pela figura 2.

Figura 2. Representação da Internet das Coisas (IoT)[232]



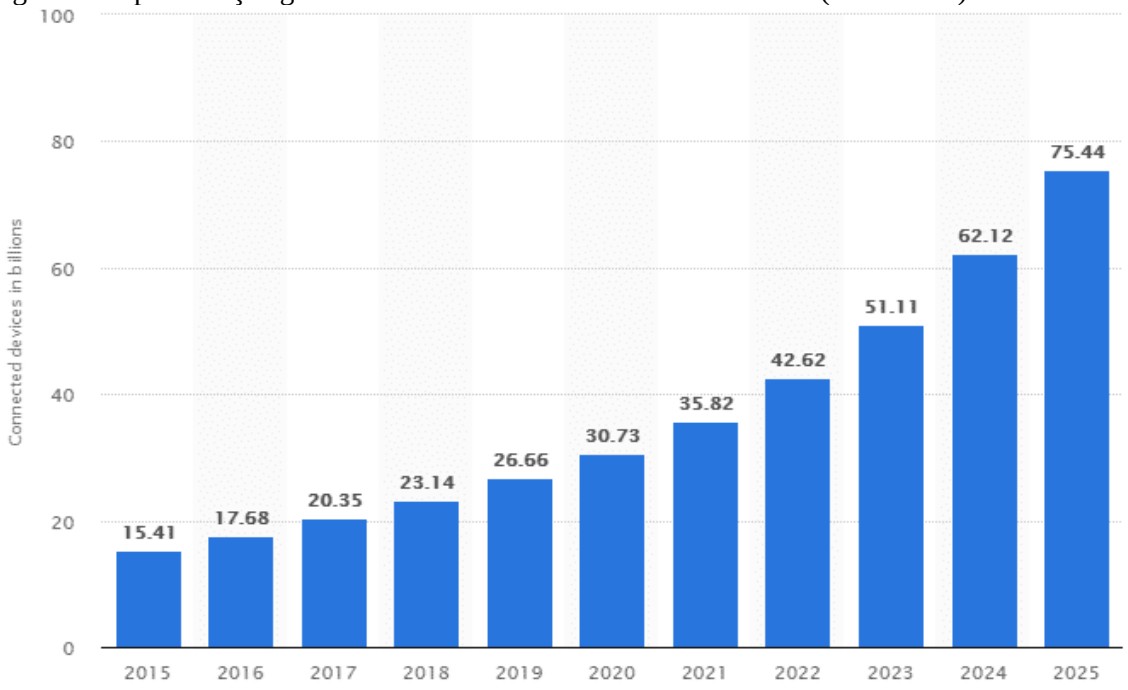
De acordo com o Grupo de Trabalho do Artigo 29.º, no campo da IoT, os dados pessoais são generalizadamente disponibilizados, e são criadas correlações e relações, sendo um mecanismo que possibilita que se determinem, analisem e prevejam aspectos inerentes à personalidade e ao comportamento, bem como aos interesses e hábitos das pessoas.[233,234]

[230] REBELO, 2019. pp. 126-7.
[231] TIBCO SOFTWARE - **O que é a internet das coisas**. [Em linha]. 2020. [Consult. 12 fev. 2022]. Disponível em WWW:<URL:https://www.tibco.com/pt-br/reference-center/what-is-the-internet-of-things-iot>.
[232] Ibidem.
[233] DIAS, Carlos André Ferreira. **A Privacidade na Era da Internet das Coisas. Direito de Personalidade e Proteção de Dados.** [Em linha]. Ciências Jurídico-Civilísticas. Faculdade de Direito. Universidade do Porto. out. 2019. Dissertação de Mestrado em Direito, p. 49. [Consult. 10 fev. 2020]. Disponível em WWW:<URL:https://repositorio-aberto.up.pt/bitstream/10216/124801/2/370854.pdf>.
[234] GRUPO DE TRABALHO DO ARTIGO 29.º, 2018.

No universo da Internet das Coisas (IoT), o RGPD busca dar um reforço à proteção dos dados pessoais aos seus titulares e confere direitos e deveres também aos responsáveis pelo tratamento desses dados, de modo a gerar um grau elevado de segurança, o que gera confiabilidade quanto aos dispositivos inteligentes e ser possível compreender a sua viabilidade.

De acordo com um relatório publicado pela empresa Statista[235], especializada em dados de mercado de consumidores, a IoT está crescendo exponencialmente, tanto que há uma projeção para o final do ano de 2022 de quase 43 bilhões de *smartphones*, *wearables*, relógios inteligentes, carros e outros dispositivos conectados, tendendo chegar no ano de 2025 com 75 bilhões, como mostra a projeção gráfica entre os anos de 2015 (início do levantamento) e 2025 apresentada na Figura 4.

Figura 4. Representação gráfica do crescimento da Internet das Coisas (em bilhões).[236]



> A internet das coisas, a inteligência artificial e a aprendizagem automática, que estão em expansão [contínua], representam grandes fontes de dados não pessoais, por exemplo, em consequência da sua utilização em processos automatizados de produção industrial. [Concluindo que] Se os progressos tecnológicos permitirem transformar dados anonimizados em dados pessoais, esses dados devem ser tratados

[235] STATISTA. **Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions).** [Online]. 2016. [Consult. 10 fev. 2022]. Available from: WWW:<URL:https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>.
[236] Ibidem.

como dados pessoais, e o Regulamento (UE) 2016/679 deve ser aplicado em conformidade.[237]

A IoT está por toda parte, uma realidade global sem volta, em que todos os indivíduos acabam sendo registrados, deixando suas marcas. A legislação deve facultar garantias legais para que esses indivíduos não se tornem seus próprios reféns ou de terceiros com a sua vida privada divulgada indevidamente.

[237] MASSENO, Manuel David; MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. A Segurança na Proteção de Dados – Entre o RGPD Europeu e a LGPD Brasileira. [Em linha]. **Rev. do Cejur: Prestação Jurisdicional**. Florianópolis, 8(1)e346, (jan./dez. 2020) 1-28. [Consult. 10 fev. 2022]. Disponível em WWW:<URL:https://revistadocejur.tjsc.jus.br/cejur/article/download/346/181/614>. ISSN Eletrônico 2319-0884. p.16

5 DECISÕES AUTOMATIZADAS E TRATAMENTO AUTOMATIZADO

5.1 Definição de perfis e uso de decisões automatizadas

De acordo com o Considerando 72 do RGPD, a definição de perfis está sujeita às regras do regulamento que regem o tratamento de dados pessoais, como o fundamento jurídico do tratamento ou os princípios da proteção de dados.[238] Importa referir que o conceito de definição de perfis não deve se confundir com o conceito de procedimento de decisão automatizada, isso porque as decisões automatizadas correspondem à capacidade de tomar decisões através de meios tecnológicos e sem intervenção humana.[239]

Profiling é qualquer forma de processamento automatizado de dados pessoais que envolva o uso dos dados para avaliar aspetos pessoais de um indivíduo. Assim, o processamento é automatizado e utilizado para fins de avaliação. A definição de perfis agrupa as partes interessadas em categorias de acordo com diferentes variáveis e as decisões poderão ser tomadas com base nesses perfis. Há uma preocupação com a discriminação que pode ocorrer em função da definição de perfis e tomada de decisões.[240]

Com relação à definição de perfis, o Regulamento determina uma obrigação de informar o titular quando se trata de decisões automatizadas, incluindo a definição de perfis. Nestes casos, o responsável pelo tratamento deve fornecer informações úteis sobre a lógica subjacente, bem como sobre a importância e as consequências esperadas desse tratamento para o titular dos dados (Artigo 13.º, n.º 2, alínea f).[241]

De acordo com o Artigo 22.º, n.º 1 do RGPD, o titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar. [242]

O Artigo 22.º do RGPD é semelhante ao Artigo 15.º da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeto ao tratamento dos dados pessoais e à livre circulação desses dados, especificamente no que se refere aos direitos e proibições que definem.

[238] REGULAMENTO (UE), 2016.
[239] CORDEIRO, 2020. p. 149.
[240] GOODMAN; FLAXMAN, 2016. p. 3.
[241] LEAL, 2017. p. 127.
[242] REGULAMENTO (UE), *op cit.*

A diferença mais relevante entre os artigos não se enquadra no âmbito dos direitos e proibições, mas nas possibilidades de derrogações. A comprovação da obtenção de consentimento explícito, poderia, em regra, minimizar riscos devido a possíveis violações ao Artigo 22.º do RGPD. Trata-se de prática padrão, pelo menos no contexto da internet, que as empresas exijam que os titulares dos dados forneçam o seu consentimento com relação às atividades de processamento de dados. Assim, nos relacionamentos entre o titular dos dados pessoais e as grandes empresas, verifica-se um nível de proteção reduzido, considerando a possibilidade de referidas empresas demonstrarem o consentimento explícito fornecido pelo titular dos dados.[243]

O grau de proteção previsto no Artigo 22.º do RGPD dependerá também das medidas de proteção que o controlador deve tomar em conformidade com o Artigo 22.º, n.º 3 do RGPD. Portanto, resta claro que o Artigo 22.º do RGPD proporciona um nível de proteção superior ao da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, uma vez que o interessado terá sempre o direito de contestar a decisão.[244]

Relativamente aos dados sensíveis, a versão final do RGPD introduziu uma nova disposição com um nível de proteção adicional para esses tipos de dados no contexto da tomada de decisão automatizada e, portanto, inclui as exceções estabelecidas no Artigo 22.º, n.º 2 do RGPD. Os dados sensíveis são aqueles baseados em dados pessoais que revelam raça ou origem étnica, opiniões políticas, crenças religiosas ou políticas, afiliação a um sindicato, processamento de dados genéticos, dados biométricos para identificar um indivíduo de forma única, dados relacionados à saúde, vida sexual ou orientação sexual de um indivíduo.[245]

Quanto maior o volume e a variedade de dados introduzidos, sejam eles indexadores diretos ou indiretos da identidade do titular a quem se referem, maior é a precisão da previsão. Atualmente, são os dados que impulsionam a operação, os próprios dados que decidem o que acontece a seguir.[246] Sempre que se aplicam sistematicamente as decisões com base em perfis gerados automaticamente, sem qualquer interferência no resultado final, a decisão é considerada como tendo sido tomada exclusivamente com base no processamento

[243] MENDOZA, Isak; BYGRAVE, Lee A. The Right not to be Subject to Automated Decisions based on Profiling. University of Oslo Faculty of Law Legal Studies. **Research Paper Series**, 2017-20, p. 19.
[244] Ibidem. p. 20.
[245] PETKOVA, Bilyana; BOEHM, Franziska - Profiling and the Essence of the Right to Data Protection. **Forthcoming in Cambridge Handbook of Consumer Privacy**. 2017. p. 6.
[246] CALVÃO, Filipa. Comissão Nacional de Proteção de Dados. **Fórum de Proteção de Dados**. Lisboa. n.º 6, nov. 2019. p. 77.

automatizado. No caso de qualquer supervisão significativa, manifestada além de gestos puramente simbólicos, haverá uma real interferência humana no resultado final do processo de tomada de decisão.[247]

O titular de dados tem o direito de não ficar sujeito a decisões exclusivamente automatizadas, ainda que o tratamento em causa seja permitido. Os pressupostos desse direito são:

> (i) a existência de uma decisão tomada sem intervenção humana direta, ou de uma decisão tomada com intervenção humana, mas cuja motivação é baseada em resultados de processamento, seja ou não uma decisão baseada em perfis;
> (ii) uma decisão relativa a uma pessoa e não a um grupo de pessoas;
> (iii) que produza ou venha a produzir efeitos em sua esfera jurídica (positivos ou negativos) ou que por qualquer forma a afete de maneira significativa e semelhante.[248]

As operações de processamento de inteligência artificial automatizam a resolução de problemas complexos da vida real e o fazem por meio de sistemas autônomos que manipulam o conhecimento adquirido para a resolução de problemas e que dispensam total ou parcialmente a intervenção humana no processo de tomada de decisão. As categorias de algoritmos focam o conjunto de modelos ou padrões extraídos de exemplos anteriores (mineração), a fim de projetar no presente a execução otimizada de soluções futuras. A abordagem paradigmática será, portanto, principalmente *soft computing*, que mecaniza a ciência do pensamento humano em código, permeando inferências cujas conclusões aproximadas exteriorizam argumentações difusas.[249]

Com o tempo e devido à disponibilidade de conjunto de dados experimentais e seu rápido processamento, a comparação das características passadas, o comportamento daquela pessoa e o comportamento de outras pessoas desempenha um papel realmente importante. A lógica é que pessoas semelhantes e pertencentes ao mesmo grupo estatisticamente relacionado devem se comportar semelhante à sua confiabilidade e solvência. Nos últimos anos, surgiram novos métodos de pontuação de crédito. Novos operadores estão usando tipos frequentemente atípicos de dados, tanto de fontes *on-line* e como *off-line* para medir a confiança das pessoas.[250]

---

[247] CALVÃO, 2019. p. 83.
[248] LEAL, 2017. pp. 136-138.
[249] CALVÃO, *op cit.* p. 90.
[250] WIEDEMANN, Klaus. - Automated Processing of Personal Data for the Evaluation of Personality Traits: Legal and Ethical Issues. **Max Planck Institute for Innovation & Competition Research Paper**.18(04) (January 16, 2018), [Online]. [Consult. 12 fev. 2022]. Available from WWW:<URL: https://ssrn.com/abstract=3102933 or http://dx.doi.org/10.2139/ssrn.3102933>.

Decisões tomadas exclusivamente com base em definição de perfis e uso de decisões automatizadas que dispensam a intervenção humana no processo de tomada de decisão apenas poderão ser utilizadas em caráter excecional, respetadas algumas previsões tratadas pelo RGPD. Nestes casos, o responsável pelo tratamento dos dados pessoais deverá demonstrar a inexistência de métodos alternativos que sejam eficazes e possam ser utilizados no caso concreto.

5.1.1 Tratamento automatizado de dados

O tratamento automatizado é um processo que soma uma série e ações em relação aos dados pessoais, envolve do cadastramento de dados até a organização, conservação, consulta, utilização, até chegar ao apagamento ou destruição.[251]

O titular tem total controle sobre seus dados, obedecendo-se as determinações do RGPD. Para que seus dados sejam comercializados, no momento da recolha, os responsáveis pelo tratamento deverão explicitar aos titulares o seu direito a se negar a esse tipo de utilização. Essa conformidade está determinada no Artigo 12.º, n.º 2 do RGPD.

O Regulamento determina que decisões automatizadas podem proporcionar muitas consequências às pessoas, e o Artigo 22.º prevê essa gravidade.

Ainda de acordo com o Artigo 22.º, n.º 1, é proibido de forma geral a tomada de decisões "com base exclusivamente no tratamento automatizado". Esta proibição aplica-se independentemente de o titular dos dados adotar uma medida relativa ao tratamento dos seus dados pessoais.[252]

"O responsável pelo tratamento não pode eximir-se do disposto no Artigo 22.º fabricando uma intervenção humana."[253] Para que uma intervenção humana seja considerada, o responsável pelo tratamento deve registar o grau da intervenção e assegurar

[251] "30. No atual contexto, as definições amplas de dados pessoais, tratamento de dados pessoais e responsável pelo tratamento abrange potencialmente um leque sem precedentes de novas situações de facto resultante do desenvolvimento tecnológico. Isto porque muitos, se não a maior parte, dos sítios web e dos ficheiros que são acessíveis através desses sítios incluem dados pessoais, como nomes de pessoas singulares vivas. Isto obriga o Tribunal de Justiça a aplicar uma regra de razão (<<rufe of reason>>), ou seja, o princípio da proporcionalidade, ao interpretar o âmbito da diretiva, a fim de evitar consequências jurídicas irrazoáveis e excessivas. Esta abordagem moderada já foi aplicada pelo Tribunal no acórdão Lindqvist, no qual rejeitou uma interpretação que poderia conduzir a um âmbito de aplicação excessivamente amplo do artigo 25. 0 da diretiva relativa à transferência de dados pessoais para países terceiros, no contexto da Internet."
INFOCURIA JURISPRUDÊNCIA. [Em linha]. 25 jun. 2013. p. 4. [Consult. 10 fev, 2022]. Disponível em WWW:<URL:https://curia.europa.eu/juris/document/document.jsf?docid=138782&doclang=PT>.
[252] REGULAMENTO (UE), 2016. Artigo 22.º, n.º 1.
[253] Ibidem.

que qualquer supervisão da decisão, por alguém com competência e autoridade para isso, seja relevante e não um mero gesto simbólico.

E ao afetar direitos de algum titular, sofre-se os efeitos jurídicos do RGPD, entretanto somente no âmbito do tratamento automatizado. Tais efeitos podem resultar em rescisão contratual; "atribuição ou recusa de uma prestação social específica prevista na legislação [...]; na recusa de admissão num país ou no indeferimento de um pedido de aquisição de nacionalidade".

5.2 Exceções à utilização de tratamento automatizado

O responsável pelo tratamento não deve efetuar o tratamento automatizado, salvo se for aplicável uma das exceções estabelecidas no Artigo 22.º, n.º 2, do RGPD.

A primeira exceção refere-se ao tratamento automatizado necessário para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento. Os responsáveis pelo tratamento poderão utilizar processos de decisões exclusivamente automatizadas para efeitos contratuais se comprovadamente demonstrarem ser esta a forma mais eficaz de tratamento, devendo-se comprovar que a intervenção humana resta praticamente impossível, devido à elevada quantidade de dados objeto de tratamento.

Assim, cabe ao responsável pelo tratamento demonstrar que o tratamento automatizado é indispensável. Caso existam métodos alternativos eficazes e menos invasivos, esse tratamento não será considerado necessário, conforme definido no RGPD.

A segunda exceção refere-se ao tratamento automatizado autorizado pelo direito da União Europeia ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados.

E a terceira e última exceção refere-se ao tratamento automatizado baseado no consentimento explícito do titular dos dados.

O RGPD exige um consentimento explícito, uma vez que o tratamento automatizado pode acarretar prejuízos para o titular de dados, sendo importante garantir um elevado nível de controle sobre referidos dados pessoais. Importa referir ainda que o RGPD não define o consentimento explícito. O termo explícito refere-se ao modo como o consentimento é expresso pelo titular dos dados. Isso significa que o titular dos dados deve fornecer uma

declaração expressa de consentimento. Uma maneira óbvia de garantir que o consentimento seja explícito seria confirmar o consentimento em uma declaração escrita.[254]

Entretanto, no contexto digital ou *on-line*, nem sempre uma declaração escrita seria factível. Assim, o titular de dados pode emitir a declaração requerida preenchendo um formulário eletrônico, enviando um e-mail, ou usando uma assinatura eletrônica. Em teoria, o uso de declarações orais também pode ser considerado como suficientemente expresso para obter consentimento explícito válido, no entanto, pode ser difícil provar que todas as condições para consentimento explícito válido foram atendidas quando a declaração foi gravada.[255]

A verificação do consentimento em duas etapas também pode ser uma maneira de garantir que o consentimento explícito seja válido.[256] O responsável pelo tratamento que utilizar o consentimento como fundamento para a definição de perfis deverá comprovar que o titular dos dados compreende exatamente a lógica envolvida ao tratamento automatizado e as consequências previstas em tal tratamento. Importante que o titular dos dados deve dispor de informação clara e precisa acerca da utilização dos seus dados e as consequências do tratamento, a fim de assegurar que o consentimento representa uma escolha informada.

Foi realizado um estudo que contemplou as atitudes do consumidor, relativamente às preferências de privacidade digital para os estudantes universitários do Massachusetts Institute of Technology (MIT). O resultado do estudo demonstra um paradoxo da privacidade digital, uma vez que consumidores dizem se importar com a privacidade, entretanto, durante o processo, acabam por fazer escolhas que são inconsistentes com as preferências informadas. O estudo demonstrou que pequenos incentivos, custos ou falta de orientação podem levar as pessoas a salvaguardar menos os seus dados. Por um lado, isso pode levar os reguladores a questionarem o valor dos incentivos declarados na determinação dos regulamentos e legislações de privacidade. Por outro lado, isso pode indicar a necessidade de protecções de privacidade mais amplas, já que os indivíduos precisam ser protegidos por sua disposição de compartilhar seus dados em troca de incentivos.

Os regulamentos de privacidade dos Estados Unidos da América e da Organização para a Cooperação e Desenvolvimento Económico (OCDE) baseiam-se na ideia de que, com

[254] GRUPO DE TRABALHO DO ARTIGO 29.º Comissão Europeia. Direção-Geral de Justiça para a Proteção de Dados. **Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679**. 28 nov. 2017. p. 18.
[255] Ibidem. pp. 18-19.
[256] Ibidem. p. 19.

transparência e escolha suficientes, os consumidores tomarão decisões de privacidade mais informadas, o que de acordo com a pesquisa, pode não ser uma verdade absoluta.[257]

A regulamentação segue um modelo moderno e uma abordagem pragmática, uma vez que parte dos dados pode ser valiosa, e a avaliação automatizada da personalidade pode ser usada para muitos propósitos diferentes. O uso da publicidade comportamental direcionada e ajustada às necessidades dos clientes, com a possibilidade de personalizar produtos e serviços, permitindo que as empresas e organizações possam compreender atuais e potenciais clientes, prevendo inclusive o comportamento desses clientes. O perfil pode apoiar-se na identificação de fraudes, tal como prevenir a fraude de cartão de crédito. A suspeita de fraude pode ser o resultado de uma análise das compras anteriores do titular do cartão de crédito e, portanto, também pode ser elegível para uma avaliação dos titulares do cartão de crédito. Em diversos casos, detalhes sobre uma pessoa são suficientes para tirar conclusões informadas sobre sua personalidade.[258]

5.3 Direito à explicação

Segundo o Considerando 71 do RGPD, o titular dos dados deverá ter o direito de não ficar sujeito a uma decisão, que possa incluir uma medida, que avalie aspetos pessoais que lhe digam respeto, que se baseie exclusivamente no tratamento automatizado e que produza efeitos jurídicos a ele 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. Esse tratamento inclui a definição de perfis mediante qualquer forma de tratamento automatizado de dados pessoais para avaliar aspetos pessoais relativos a uma pessoa singular, em especial a análise e previsão de aspetos relacionados com o desempenho profissional, situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados, quando produz efeitos jurídicos que lhe digam respeto ou a afetem significativamente de forma similar.[259]

As garantias previstas no Considerando 71 são quase idênticas às previstas no Artigo 22.º, n.º 3, do RGPD, com a diferença essencial de que o Considerando 71 aborda ainda o

[257] ATHEY, Susan; CATALINI, Christian; TUCKER, Catherine. The Digital Privacy Paradox: Small Money, Small Costs, Small Talk. **National Bureau of Economic Research**. Cambridge, 2017. pp.17-18.
[258] WIEDEMANN, 2018. pp. 06-07.
[259] REGULAMENTO (UE), 2016.

direito de "obter uma explicação sobre a decisão tomada na sequência dessa avaliação". A omissão deliberada deste texto no Artigo 22.º, n.º 3, indica que os legisladores não pretendiam que os titulares de dados exercessem efetivamente o direito de obter as explicações acerca das decisões automatizadas.[260]

Importa trazer a análise o caso do Google, na Espanha, caso em que foi realizada discussão acerca dos direitos de proteção de dados de um indivíduo em relação ao que o Google exibia em seu mecanismo de busca, considerando que as informações estavam muito desatualizadas e não eram relevantes para as circunstâncias atuais do indivíduo. O Tribunal enfatizou que o mecanismo de busca poderia afetar significativamente os direitos fundamentais de privacidade e proteção de dados, observando que o processamento permite que qualquer usuário da Internet obtenha uma visão geral estruturada das informações a partir de uma lista de resultados, sendo as informações relacionadas a muitos aspetos da vida pessoal do indivíduo. Sem o mecanismo de pesquisa, seria muito difícil criar um perfil tão detalhado do interessado.[261]

A decisão concluiu que a possibilidade de permitir o processamento dependerá do exercício de equilíbrio no contexto do mecanismo de pesquisa da Google, de modo que os interesses comerciais de um mecanismo de pesquisa no processamento não podem superar o direito do titular à privacidade e proteção de dados. A decisão reconheceu que o equilíbrio pode depender, de acordo com uma análise do caso concreto, da natureza da informação em questão e de sua sensibilidade com a privacidade do titular e do interesse do público em ter acesso à referida informação.[262] O Tribunal de Justiça da União Europeia (TJUE) também reconheceu que o interesse público pode superar os direitos pessoais e as objeções à definição de perfis, por exemplo, dependendo da importância de uma pessoa como figura pública ou não.[263]

Importa referir que o titular dos dados tem direito a uma explicação acerca da decisão automatizada. Apesar da falta de apoio direto no texto do regulamento, mais do que um direito à informação, os titulares dos dados têm direito a uma explicação da decisão

[260] WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano - Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation**. International Data Privacy Law**, 2017. p. 06.
[261] PETKOVA; BOEHM, 2017. pp. 8-9.
[262] Ibidem.
[263] Ibidem. p. 10.

automatizada, esta explicação deve se relacionar com a lógica e funcionalidade do sistema e os critérios e ponderações usados na decisão específica.[264]

É necessário entender melhor o que seria a explicação acerca do processo automatizado de tomada de decisão. Duas formas de explicação podem estar em discussão:

> i) a função do sistema, ou seja, a lógica, a importância, as consequências esperadas e a função geral do sistema, podendo especificar os requisitos, árvores de decisão, modelos predefinidos, critérios e estruturas de classificação;
> ii) a justificativa e instâncias individuais de uma decisão automatizada específica, por exemplo, ponderação de recursos, identificação de regras de decisão para um caso específico, informações sobre referência ou grupo de perfis.[265]

O direito de explicação ou o simples direito de ser informado, por si só, é insuficiente e, dado que as soluções até agora pensadas já não são eficazes, o estado de coisas deve ser reajustado, reconsiderando que o algoritmo deve ser apresentado em contornos mais transparentes, no qual as decisões sejam mais compreensíveis e contestáveis. [266]

Entre a tomada de decisão totalmente automatizada em virtude da tomada de decisão totalmente humana, existem inúmeros níveis de automação que podem ser estabelecidos. Há situações em que o resultado de uma análise automatizada é apenas um dos diversos fatores que formam a base para uma decisão subsequente, sendo que nessa fase se utiliza de uma decisão impulsionada por humanos. Essa pessoa terá o poder de decidir como proceder, bem como todas as informações necessárias para tomada de decisão. Isso também pode incluir a possibilidade de o interessado ser contactado antes da tomada daquela decisão.

5.4 Uso de decisões automatizadas e discriminação

Importa referir que a definição de perfis e uso de decisões automatizadas podem gerar discriminação ou prejuízos em diversos casos, por exemplo, ao impedir o acesso de pessoas a oportunidades e ofertas de emprego, problemas na contratação de crédito ou seguros. O risco de discriminação associado ao uso de algoritmos é reconhecido, e tem sido discutido atualmente. O design de *softwares* discriminatórios, seja de forma intencional ou não intencional, que ao utilizar um conjunto de dados não representativos ou incompletos e

[264] LEAL, 2017. p. 128.
[265] WACHTER; MITTELSTADT; FLORIDI, 2017. p. 03.
[266] CALVÃO, 2019. p. 87.

mecanismos de aprendizado de máquina parcialmente controlados pode facilmente levar à discriminação.

Os modelos de aprendizado de máquina têm probabilidade de ajudar a tornar a alocação de recursos mais equitativa, os algoritmos podem utilizar as informações com mais eficiência do que os humanos e, portanto, poderão ser menos inclinadas do que os humanos a confiar em estereótipos. Algoritmos podem ser necessários para otimizar os objetivos, sob certas restrições e, portanto, pode ser mais fácil impor objetivos sociais em algoritmos do que nas decisões subjetivas de seres humanos. Os cientistas sociais percorrerão um longo caminho para definir formalmente esses tipos de problemas e preocupações. Com isso, pode-se ter implementações eficientes para pesquisas futuras.

A preocupação é que a inteligência artificial pode perpetuar outras desvantagens para grupos historicamente marginalizados. O preconceito também pode surgir se houver uma correlação, mesmo que sem nenhuma causa. Um algoritmo pode inferir que se um dos pais de um arguido foi para a prisão, o acusado tem maior probabilidade de ser enviado para a prisão. Embora essa correlação possa existir e mesmo que a inferência seja preditiva, parece injusto que tal acusado receba uma sentença mais severa, uma vez que não há relação causal. A parcialidade pode também surgir porque os decisores humanos confiam mais na precisão das recomendações de algoritmos do que deveriam e desconsideram outras informações.[267]

Os sistemas de IA que permitem a classificação social de indivíduos para uso por autoridades públicas ou em nome de autoridades públicas podem criar resultados discriminatórios e levar à exclusão de certos grupos, bem como violar o direito à dignidade e à não discriminação e aos valores de igualdade e justiça. Esses sistemas de inteligência artificial avaliam ou classificam a credibilidade dos indivíduos com base em seu comportamento social em uma variedade de contextos ou características conhecidas ou previsíveis, que levam a um tratamento prejudicial ou desfavorável de indivíduos ou grupos inteiros de indivíduos em contextos sociais alheios ao contexto em que os dados foram inicialmente gerados ou coletados.[268]

Credit scoring descreve o ato de calcular a qualidade de crédito dos consumidores e entidades privadas por meio de análise de dados, sendo amplamente utilizado por bancos e outras instituições financeiras e *fintechs*, em particular, no contexto de pedidos de empréstimos. O *credit scoring* se baseia na ideia de prever se haverá o cumprimento das

[267] COECKELBERGH, 2020. p. 130.
[268] COMISSÃO EUROPEIA, 2021.

obrigações decorrentes de um empréstimo, por meio da análise de dados. O ponto de atenção reside no facto de que uma classificação de crédito desfavorável pode levar à negativa da concessão de um empréstimo, o que, por sua vez, pode impedir o interessado de iniciar um negócio, construir uma casa, cursar uma faculdade, entre outras necessidades.

É de extrema importância que tanto os legisladores como a própria sociedade estejam cientes dos impactos legais e éticos acerca da utilização das decisões automatizadas, com base em definição de perfis. Neste caso, o Artigo 22.º do RGPD aponta que pode ser visto como uma tentativa de encontrar um equilíbrio entre a privacidade do titular dos dados em questão e a admissibilidade de modelos de negócios que usam os dados.[269] O uso de decisões automatizadas pode gerar oportunidade de negócios, redução de custos de conservação dos dados e a capacidade de tratar elevado volume de informação. É necessário que haja um equilíbrio entre os princípios da minimização de dados, limitação das finalidades e da limitação da conservação devido à utilização de decisões automatizadas.

5.5 Direito à portabilidade de dados e tratamento automatizado

A portabilidade de dados pessoais trata-se de uma facilitação aos usuários de migração entre serviços *on-line*, uma vez que esses dados são os meios de acesso e aquisição de produtos e serviços, a atividades económico-financeiras, entre outros usos, sendo, portanto, imprescindível disciplinar essa tramitação, e proteger os dados pessoais, assim como preservar e equilibrar os direitos e deveres e a relação de confiança entre as partes envolvidas.

A portabilidade ocorre por meio de transferência de dados pessoais em diferentes plataformas digitais, permitindo a interoperabilidade entre diferentes serviços. No RGPD, há o incentivo de desenvolver formatos interoperáveis entre suas próprias plataformas e as de terceiros. Na ausência de interoperabilidade, o usuário tem o direito de receber seus dados de forma estruturada e em formato acessível, a fim de transmiti-los a outra plataforma que possa fazer uso deles.

Os principais objetivos relacionados à implementação do direito à portabilidade de dados pessoais: a) Minorar o efeito *lock-in;* b) Reforçar o controlo e o reuso de dados pessoais por parte dos titulares; c) Equilibrar a relação entre os titulares dos dados pessoais

[269] WIEDEMANN, 2018. p. 22.

e as entidades que beneficiam com o tratamento dos mesmos; e d) Promover a criação de uma nova economia digital.[270]

O efeito de *lock-in* resulta em barreira à mudança de serviço pelo titular dos dados, sendo que a impossibilidade de obter ou transmitir dados pessoais cria, inevitavelmente, tal efeito, uma vez que impossibilita ou dificulta a alteração de prestador de serviço por parte do titular. O direito à portabilidade de dados pessoais visa diminuir este efeito, permitindo que os dados sejam portados, sendo que o interessado tem o direito de mudar de prestador de serviço, circunstância ainda mais facilitada pelo facto de a transferência, a pedido do interessado, poder ser efetuada diretamente entre os responsáveis pelo tratamento dos dados.

O direito à portabilidade de dados pessoais faz com que os prestadores de serviços concorram para fornecer um melhor serviço, garantindo, deste modo, a concorrência no mercado digital, uma vez que os prestadores de serviços terão de apresentar melhores produtos e serviços para fidelizar os utilizadores.

O Grupo do Artigo 29.º para a Proteção de Dados também faz uma interpretação sobre os dados fornecidos por titulares de maneira ampla:[271]

> Os dados fornecidos pelo titular devem igualmente incluir os dados pessoais que sejam observados a partir das atividades dos utilizadores, tais como os dados brutos tratados por um contador inteligente ou por outros tipos de objetos conectados, os registos das atividades e os históricos da utilização de um sítio Web ou das pesquisas realizadas.

Ainda de acordo com o Grupo do Artigo 29.º, esta interpretação tem relação com o Considerando 68, que acentua os objetos da portabilidade, além dos dados fornecidos pelo indivíduo também cabe proteção aos dados observados, ou seja, provenientes da interação estabelecida entre o usuário e a plataforma digital, a forma como usufrui dela, cujos registos se fixam em históricos de navegação, em suas buscas, nos dados de tráfego, em sua geolocalização entre outras registos deixadas pelo usuário no universo *on-line*.

Há uma carência na LGPD acerca de algumas questões que se referem à portabilidade dos dados pessoais, levando a legislação brasileira a recorrer à RGPD, dada a sua importância:

[270] FIDALGO, Vitor Palmela. O Direito à Portabilidade de Dados Pessoais. **Revista de Direito e Tecnologia**, 1(1) (2019). p. 96.
[271] Ibidem. p. 9

> Ao recorrer ao [RGPD], o diploma europeu dispões expressamente que apenas são portáveis os dados pessoais quando aquele tratamento tiver por base o consentimento ou um contrato firmado entre as partes. Além disso, o [RGPD] igualmente prevê, como anteriormente referenciado, que a portabilidade é restrita aos dados tratados em meio automatizado. Ambas as especificações presentes no [RGPD] não são dispostas na redação da LGPD.[272]

A possibilidade de exigir que os dados sejam transmitidos diretamente entre controladores é uma novidade do RGPD, indo além da ideia subjacente ao direito de acesso, uma vez que os dados pessoais podem ser transmitidos sem a intervenção direta do próprio titular, que apenas dará o seu consentimento para a transmissão.

[272] FIDALGO, 2019. p. 16

CONCLUSÃO

Por meio desta pesquisa realizou-se uma análise acerca da Proteção de Dados e seus desafios perante novas tecnologias. Em termos gerais, analisou-se o Regulamento Geral de Proteção de Dados, passando pela análise do conceito de dado pessoal, bem como dos princípios relativos ao tratamento de dado pessoal. Observou-se que o RGPD defende os direitos e as liberdades fundamentais das pessoas singulares e a proteção das pessoas singulares, relativamente ao tratamento de seus dados pessoais, como um direito fundamental.

O objetivo principal do RGPD é buscar um espaço de liberdade, segurança e justiça, visando ao progresso, utilizando-se de regras e procedimentos sólidos, permitindo a confiança na era digital. Todos os princípios relativos à proteção de dados devem ser aplicados a qualquer informação relativa a uma pessoa singular identificada ou identificável. Com relação a outro objetivo do RGPD, o de atribuir um sentido amplo ao conceito de dado pessoal, não há delimitação apenas no que se refere às informações sensíveis ou de ordem privada.

O entendimento do legislador se coloca no sentido de considerar dado pessoal como qualquer informação que diga respeto a uma determinada pessoa. E que ao cessar o fato gerador do tratamento de dados pessoais, o responsável pelo tratamento deverá proceder à sua anonimização de tal forma que o titular não seja mais ou não possa mais ser identificado. Analisamos ainda a pseudonimização, que corresponde a uma técnica de desidentificação e conduz à criação de dados que se situam entre dados pessoais e dados não pessoais, de modo que não possam mais ser atribuídos a um determinado titular dos dados sem recurso a informações adicionais.

Viu-se também que a Constituição da República Portuguesa, em seu Artigo 35.º, n.º 1, dispões sobre o direito de acesso do cidadão a seus respetivos dados informatizados, sendo conferido três direitos constitucionais: o direito de acesso do titular dos dados aos registos informáticos, bem como a sua retificação, atualização ou eliminação; o direito ao sigilo de dados; e o direito ao não tratamento de alguns tipos de dados pessoais.

Diante da análise realizada, é importante ponderar que o RGPD trouxe à discussão um tema de extrema relevância na atualidade e que deve ser ponderado por todos, buscando sempre um tratamento de dados realizado de forma lícita, leal e transparente. Referidos princípios, quais sejam, licitude, lealdade e transparência, devem ser vislumbrados por todos

aqueles que efetuam o tratamento de dados pessoais. Cumpre destacar que o respetivo responsável deverá zelar pelo cumprimento dos princípios relativos ao tratamento dos dados pessoais, pela confidencialidade dos dados pessoais, e ainda pela sua guarda de forma segura.

O tratamento de dados pessoais fundado em interesses legítimos exige uma avaliação cuidadosa, incluindo se o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados pessoais são recolhidos, que podem ser tratados para esse fim. Os interesses e os direitos fundamentais do titular dos dados podem, em particular, prevalecer sobre os interesses do responsável pelo tratamento, quando os dados pessoais são tratados em circunstâncias em que os titulares dos dados já não esperam um tratamento adicional. Poderá ser considerado interesse legítimo caso possa ser demonstrado que o tratamento une um direito fundamental, corresponde total ou parcialmente a um interesse público e se identifica com outros fundamentos de licitude que constam no Artigo 6.º, n.º 1 do RGPD ou no caso de haver o reconhecimento jurídico.

A Lei n.º 58, de 8 de agosto de 2019, assegura a execução, na ordem jurídica portuguesa, aplicando-se aos tratamentos de dados pessoais realizados no território português, independentemente da natureza pública ou privada do responsável pelo tratamento ou do subcontratante. Dispões também que o encarregado é designado com base nos requisitos previstos no RGPD, devendo exercer a sua função com autonomia técnica perante a entidade responsável pelo tratamento ou subcontratante, obrigando-se a manter sigilo sobre tudo o que se refirir às suas funções.

Analisou-se que o direito à portabilidade oferece ao titular a opção de de receber um conjunto de dados pessoais e a de transmitir esses dados entre controladores privados de dados, sem necessariamente seguir a sua transmissão imediata a outro titular, não apenas nas situações em que o titular pretenda transferir todos os seus dados para outro provedor, mas também os casos em que deseja garantir a interoperabilidade entre os sistemas que utiliza. O prazo de conservação de tais dados precisa estar fixado para a devida prossecução da sua natureza e finalidade, sendo lícita a conservação dos dados pessoais, desde que sejam adotadas medidas técnicas e organizativas adequadas a garantir os direitos do titular dos dados.

Analisou-se, ainda, o quanto disposto na Lei n.º 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais Brasileira, no que se refere aos princípios relativos ao tratamento dos dados pessoais, as bases legais para o tratamento dos dados pessoais

previstos, e por fim, as sanções e autoridade nacional de Proteção de Dados previstas na referida lei.

Tratou-se da adequação à regulamentação de Proteção de Dados, passando pela auditoria inicial, definição de medidas de adequação e implementação das medidas de adequação, para adequação à legislação de proteção de dados pessoais, a fim de conhecer todos os procedimos, métodos e detalhes da coleta e tratamento de dados. Demonstrou-se que as políticas internas e procedimentos da organização deverão ser constantemente atualizados conforme existirem novas atividades de tratamento e/ou caso haja alteração nas atividades de tratamento em vigor, devendo, ainda, ser implementados sistemas de gestão de segurança da informação com o objetivo de evitar violações de dados pessoais. O relatório final de implementação das medidas de adequação a legislação de proteção de dados corresponde ao principal instrumento para que a organização possa comprovar a conformidade à legislação. Avaliou-se a necessidade de adoção de medidas de segurança proporcionais à operação da organização, devendo-se ter em conta os riscos apresentados pelo tratamento.

Quanto aos aspetos do *compliance* e sua relação com as normas de proteção de dados, depreendeu-se que para estar em conformidade com a legislação, as organizações devem conhecer detalhadamente toda regulamentação e legislação aplicáveis, de forma a implementar com eficiência as políticas de coleta, uso, tratamento, proteção e segurança dos dados dos titulares.

A respeito do conceito de consentimento, de acordo com o RGPD deve ser vislumbrado 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 respeto sejam objeto de tratamento. Facto que o pedido de consentimento tem de ser apresentado de forma clara e objetiva, utilizando uma linguagem fácil de compreender, e de uma forma que o distinga de outras informações, como os termos e condições. O consentimento deve ser livre, específico, informado e explícito.

No decorrer da análise, observou-se que a legislação europeia não explicita a que se refere o interesse legítimo, entretanto aponta, por meio dos Considerandos 47 a 49, que pode haver interesse legítimo quando há uma relação relevante e apropriada entre o titular dos dados e o responsável pelo tratamento, em situações como quando o titular dos dados é um cliente ou está ao serviço do responsável pelo tratamento; e que a existência de um interesse legítimo exige uma avaliação cuidadosa, incluindo se o titular dos dados pode razoavelmente

prever, no momento e no contexto em que os dados pessoais são recolhidos, que podem ser tratados para esse fim.

Acerca das novas tecnologias relacionadas à Proteção de Dados, apresentou-se o *big data* e a caracterização dos seus 3Vs - volumetria, variedade e velocidade. Tendo-se, assim, um grande volume e variedade de dados coletados em alta velocidade, viabilizando oportunidades de desenvolvimento da atividade económica, permitindo a tomada de decisões de maneira mais acertada, por meio de atividades de tratamento de dados. A utilização do *big data* tem grande importância para o desenvolvimento da economia e da inovação, de maneira que, no cenário atual da sociedade, viabiliza o desenvolvimento e o crescimento económico, sendo necessário contribuir de forma que a coleta, o processamento e a análise desse grande volume e variedade de dados possa proporcionar ao detentor das informações uma maior eficiência e celeridade para as suas tomadas de decisões, pautadas sempre em questões éticas, de forma a evitar eventual prejuízo face a este processamento.

Mediante os princípios da finalidade, da adequação e da necessidade do *big data* identificou-se um impasse, por apresentar-se em oposição às práticas de tratamento de grandes volumes e variedade de dados pessoais. Inúmeras ferramentas utilizadas em *big data* são baseadas na reunião de dados que são coletados a partir das mais diferentes formas, origens, momentos, contextos e para finalidades diversas, muitas vezes sequer conhecidas no momento da coleta. Não raramente, a finalidade ou mesmo a utilidade dos dados são conhecidas apenas após o tratamento, tornando a observância a tais princípios uma tarefa difícil.

Os princípios asseguram ainda o livre acesso e a qualidade dos dados pessoais, o que garante ao seu titular o direito de solicitar correções, visando eliminar dados desatualizados ou incorretos. Assegura-se ainda o respeito aos direitos fundamentais do indivíduo, evidenciando que questões éticas devem também estar presentes nas atividades de tratamento de dados pessoais. Muito se discute acerca da criação de um regime especial para o processamento dos dados em termos de *big data*, regime este que desconsideraria a distinção entre dados pessoais e dados não pessoais.

Uma variedade de novas áreas de pesquisa pode ser iniciada contando-se com melhores medições, novos métodos diferenciais e questões essenciais. A futura força de trabalho terá de ser treinada com habilidades empíricas e de ciência de dados. Importante que a filosofia e a ciência sejam amplamente utilizadas para verificar e discutir as hipóteses de utilização e exploração da IA. O papel de verificar como a inteligência artificial será

utilizada, bem como a análise ética de sua utilização, deve assegurar que seja possível contribuir e participar da evolução tecnológica de forma positiva.

A economia, de modo geral, tende a ser profundamente transformada pela inteligência artificial e pela *machine learning*. Os modelos estatísticos podem ser otimizados, mais robustos e possuírem propriedades desejáveis de proteção devido à não manipulação, garantindo a equidade.

No que diz respeito às ferramentas de inteligência artificial, analisamos a consultoria robótica, cuja definição tem como premissas três pilares: consultoria automática e diretamente acedida pelos utilizadores, sem ou com mínima intervenção humana.

Vimos que está em curso uma proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece normas harmonizadas para IA (Regulamento de Inteligência Artificial). Por meio do uso de IA, é possível aprimorar as previsões, otimizar as operações e a alocação de recursos e personalizar a prestação de serviços, além de contribuir para resultados sociais e ambientais positivos e proporcionar vantagens competitivas para empresas e países europeus. Entretanto, os mesmos elementos e técnicas que produzem os benefícios socioeconómicos da IA também podem levar a novos riscos ou consequências negativas para os cidadãos e a sociedade. Nesse cenário, a União Europeia procura adotar uma abordagem equilibrada, de modo a preservar a sua liderança tecnológica e assegurar que as novas tecnologias são desenvolvidas e utilizadas de acordo com os valores, direitos e princípios fundamentais da União.

Outra tecnologia analisada neste estudo é a denominada *blockchain*, que são redes nas quais trafegam transações comerciais que computam dados pessoais de clientes e guardam qualquer tipo de dados (documentos, arte, negociações, registos entre outros dados). Sua funcionalidade destaca três momentos: o momento do registo das informações em bloco, que podem ser tangíveis (produtos) ou intangíveis (intelectual); a conexão interblocos, anteriores e posteriores, formando uma cadeia de dados segura, respeitando-se toda a movimentação das transações; e o bloqueio conjunto das transações de forma irreversível, tornando a *blockchain* um sistema seguro, inviolável e confiável como um todo. Entretanto, a indestrutibilidade e imutabilidade tornam qualquer modificação ou uma *erasure* (apagamento) tecnicamente impossível.

Como útimo recurso artificialmente inteligente é a Internet das Coisas (IoT) que está por toda parte, uma realidade global em relação à qual o Direito trabalha para estabelecer

garantias legais de que a sociedade não se torne refém de si mesma e nem a terceiros ao ter sua vida divulgada indevidamente.

Constatou-se que decisões tomadas exclusivamente com base em definição de perfis e uso de decisões automatizadas que dispensam a intervenção humana no processo de tomada de decisão apenas poderão ser utilizadas em caráter excepcional, respetadas algumas previsões tratadas pelo RGPD. Nestes casos, o responsável pelo tratamento dos dados pessoais deverá demonstrar a inexistência de métodos alternativos eficazes que possam ser utilizados no caso concreto, cabendo-lhe demonstrar que o tratamento automatizado é indispensável. Caso existam métodos alternativos eficazes e menos invasivos, esse tratamento não será considerado necessário.

Outra exceção refere-se ao tratamento automatizado e autorizado pelo direito da União Europeia ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e em qual estejam previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados.

A última exceção refere-se ao tratamento automatizado baseado no consentimento explícito do titular dos dados. O RGPD exige um consentimento explícito, uma vez que o tratamento automatizado pode acarretar prejuízos para o titular de dados, sendo importante garantir um elevado nível de controle sobre referidos dados pessoais. O direito de explicação é simplesmente o direito de ser informado sobre todas as necessidades para tomadas de decisões em relação aos seus dados, incluindo-se a possibilidade de o interessado ser contactado antes da tomada daquela decisão.

Importa referir que entre a tomada de decisão totalmente automatizada face a tomada de decisão totalmente humana, existem inúmeros níveis de automação que podem ser estabelecidos. Há situações em que o resultado de uma análise automatizada é apenas um dos diversos fatores que formam a base para uma decisão subsequente, sendo que nessa fase se utiliza de uma decisão impulsionada por humanos, que terão o poder de decidir como proceder, bem como todas as informações necessárias para tomada de decisão.

Direito à portabilidade de dados pesssoais e tratamento automatizado é uma facilitação aos usuários de migração entre serviços *on-line*, uma vez que esses dados são os meios de acesso e aquisição de produtos e serviços, a atividades económico-financeiras, entre outros usos, sendo, portanto, imprescindível disciplinar essa tramitação, e proteger os dados pessoais, assim como preservar e equilibrar os direitos e deveres e a relação de

confiança entre as partes envolvidas. O RGPD incentiva o desenvolvimento de formatos interoperáveis entre plataformas próprias e de terceiros.

Como tratado neste estudo, é necessário que os agentes envolvidos no tratamento de dados pessoais possam demonstrar tanto o cumprimento das normas jurídicas quanto à eficácia das medidas adotadas. A proteção à privacidade deve estar inserida em todas as atividades que envolvam o tratamento de dados pessoais, sendo de extrema importância que tanto os legisladores como a própria sociedade estejam cientes dos impactos legais e éticos acerca da utilização das novas tecnologias, bem como da tentativa de encontrar o equilíbrio entre a privacidade do titular dos dados em questão e a admissibilidade de modelos de negócios que usam os referidos dados.

O uso de novas tecnologias pode gerar oportunidades de negócios, redução de custos de conservação dos dados e a capacidade de tratar elevado volume de informação. A economia digital trará cada vez mais novos desafios ao mercado, que deve estar preparado a ultrapassá-los de maneira satisfatória. A regulamentação deve evoluir no sentido de que seja considerada uma aliada ao desenvolvimento tecnológico e desenvolvimento do mercado digital, nomeadamente no que se refere à busca pela proteção dos dados pessoais, de forma que a evolução esteja aliada à segurança, bem como à solidez e transparência.

BIBLIOGRAFIA

AGÊNCIA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA. Conselho da Europa - **Manual da Legislação Europeia sobre Proteção de Dados**. 2014.

AGNELLUTTI, Cody - **Big data: an exploration of opportunities, values, and privacy issues**. New York, USA: Nova Science Publishers, 2014.

ALVES, Lurdes Dias - **Regulamento geral de proteção de dados: principais dificuldades e dúvidas das organizações e dos titulares de dados pessoais na adaptação ao atual regime**. Cyberlaw. Lisboa, Portugal. 1(6) (2018).

ANTUNES, Luis - **Pôr em prática o RGPD.** Lisboa, Portugal: FCA, 2018.

ARENDT, Hanna - **Between Past and Future: Eight exercises in Political Thought**, Londres: Penguin Books, 1993.

ARISTÓTELES - **Ética a Nicômaco**. 4.ª ed. São Paulo: Nova Cultura, 1991.

ASSEMBLEIA DA REPÚBLICA. Lei n.º 147/2015. [Em linha]. **Diário da República** n.º 176/2015, Série I, 9 set. 2015, 7342-7500. [Consult. 16 jan. 2022]. Disponível em WWW:<URL:https://dre.pt/dre/detalhe/lei/147-2015-70237675>.

ASSI, Marcos - **Compliance: como implementar**. São Paulo: Trevisan, 2018.

ATHEY, Susan; CATALINI, Christian; TUCKER, Catherine - The Digital Privacy Paradox: Small Money, Small Costs, Small Talk. **National Bureau of Economic Research**. Cambridge, 2017.

ATHEY, Susan; CATALINI, Christian; TUCKER, Catherine - **The Impact of Machine Learning on Economics**. Stanford, 2018.

BAGNOLI, Vicente - **Direito econômico e concorrencial**. 7.ª ed. rev., atual e ampl. São Paulo: Revista dos Tribunais, 2017.

BLOK, Marcella - **Compliance e governança corporativa: atualizado de acordo com a Lei Anticorrupção Brasileira (Lei 12.846) e o decreto-lei 8.421/15**. Rio de Janeiro: Freitas Bastos, 2017.

BODDINGTON Paula - Artificial Intelligence: Foundations, Theory, and Algorithms, Towards a Code of Ethics for Artificial Intelligence. **Springer International Publishing**. Oxford, United Kingdom, 2017.

BRASIL - **Constituição da República Federativa do Brasil de 1988**. [Em linha]. 1988. [Consult. 10 fev. 2022]. Disponível em WWW:<URL:http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>.

BRITO, Beatriz Gontijo de; CAMPO, Aline França - Instituto Iberoamericano de Estudos Jurídico**.** [Em linha] **Revista Ibérica do Direito**. 1(2) (jul./dez., 2020). p. 99. [Consult. 15 jan. 2022]. Disponível em WWW:<URL:https://revistaibericadodireito.pt/index.php/capa/article/view/8/10>.

CALVÃO, Filipa - Comissão Nacional de Proteção de Dados. **Fórum de Proteção de Dados**. Lisboa. n.º 6, nov. 2019.

CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA. [Em linha]. **Jornal Oficial da União Europeia**. 7 jun. 2016. 2016/C 202/02. [Consult. 8 jan. 2022]. Disponível em WWW:<URL:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/ TXT&from=FR>.

COECKELBERGH Mark - **AI ethics**. Cambridge, MA: The MIT Press, 2020.

COIMBRA, Marcelo de Aguiar; MANZI, Vanessa Alessi - **Manual de compliance: preservando a boa governança e a integridade das organizações**. São Paulo: Atlas, 2010.

COMISSÃO EUROPEIA - **Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de Inteligência Artificial (Regulamento Inteligência artificial) e altera determinados atos legislativos da União**, Bruxelas, 21 abr. 2021.

COMO FUNCIONA A TECNOLOGIA BLOCKCHAIN. [Em linha]. **Exame Online**. Future of Money. 23 dez. 2021. [Consult. 10 fev. 2022]. Disponível em WWW:<URL:http://exame.com/future-of-money/como-funciona-a-tecnologia-blockchain/>.

COMPARATO, Fábio Konder - **A afirmação histórica dos direitos humanos**. 9.ª ed., rev. e atual. São Paulo: Saraiva, 2015.

CONSTITUIÇÃO DA REPÚBLICA PORTUGUESA - Sétima Revisão Constitucional. [Em linha]. **Diário da República**. n.º 155, I Série-A, 12 ago. 2005. [Consult. 12 jan. 2022]. Disponível em WWW:<URL:https://dre.pt/legislacao-consolidada/-/lc/34520775/view>.

CORDEIRO, A. Barreto Menezes - **Dados Pessoais: Conceito, Extensão e Limites**. Lisboa, Portugal: Centro de Investigação de Direito Privado. [Em linha]. 2018 (a). [Consult. 12 fev. 2022]. Disponível em WWW:<URL:https://blook.pt/publications/publication/e38a9928dbce/>.

CORDEIRO, A. Barreto Menezes - O tratamento de dados pessoais fundado em interesses legítimos. [Em linha]. **Revista de Direito e Tecnologia**. (1)1 (2019). [Consult. 13 fev. 2022]. Disponível em WWW:<URL:https://blook.pt/publications/ publication/29c85b840a65/>.

CORDEIRO, A. Barreto Menezes - **Direito da Proteção de Dados**. Coimbra: Almedina, 2020.

DIAS, Carlos André Ferreira. **A Privacidade na Era da Internet das Coisas**. Direito de Personalidade e Proteção de Dados. [Em linha]. Ciências Jurídico-Civilísticas. Faculdade de Direito. Universidade do Porto. out. 2019. Dissertação de Mestrado em Direito, p. 49. [Consult. 10 fev. 2020]. Disponível em WWW:<URL:https://repositorio-berto.up.pt/bitstream/10216/124801/2/370854.pdf>.

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

EDELWEISS, Nina - **Algoritmos e programação com exemplos em Pascal e C**. Porto Alegre, RS: Bookman, 2014.

ESPÍNDOLA, Maria Fernanda; TOMAZ, Roberto Epifanio - Compliance: o que é, objetivo, aplicação e benefícios. **Revista Síntese de Direito Empresarial**. São Paulo, 10(57) (jul./ago. 2017) 9-20.

FIDALGO, Vítor Palmela - **Inteligência Artificial e Direitos de Imagem**. [Em linha]. 2018. [Consult. 16 jan. 2022]. Disponível em WWW:<URL:https://blook.pt/publications/fulltext/c73d596c5b9b/>.

FIDALGO, Vitor Palmela. O Direito à Portabilidade de Dados Pessoais. **Revista de Direito e Tecnologia**, 1(1) (2019).

FLORÊNCIO FILHO, Marco Aurélio - Aspectos criminais do ECA na sociedade da informação. In ABRUSIO, Juliana. (Coord.) - **Educação digital**. São Paulo: Revista dos Tribunais, 2015.

GABARDO, Emerson; CASTELLA, Gabriel Morettini - A nova lei anticorrupção e a importância do compliance para as empresas que se relacionam com a Administração Pública. **A&C - Revista De Direito Administrativo & Constitucional**. Belo Horizonte: Fórum. 15(60) (abr./jun.2015).

GOODMAN, Bryce; FLAXMAN, Seth - **European Union regulations on algorithmic decision-making and a "right to explanation".** Oxford Internet Institute, United Kingdom, 2016.

GRUPO DE TRABALHO DO ARTIGO 29.º. Comissão Europeia. Direção-Geral de Justiça para a Proteção de Dados - **Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679**. 28 nov. 2017.

GRUPO DE TRABALHO DO ARTIGO 29.º. Comissão Europeia, Direção-Geral de Justiça para a Proteção de Dados - **Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679**. 6 fev. 2018.

HOFFMANN-RIEM, W - Artificial Intelligence as a Challenge for Law and Regulation. In WISHMEYER T; RADEMACHER R. (Eds) - **Regulating Artificial Intelligence.** [Online] Switzerland: Springer, 2020. pp 1-29. [Consult. 02 feb. 2022]. Available from WWW:<URL:https://doi.org/10.1007/978-3-030-32361-5>.

IBM - **O que é a tecnologia blockchain?** 2021. [Em linha]. [Consult. 02 fev. 2022]. Disponível em WWW:<URL:https://www.ibm.com/br-pt/topics/what-is-blockchain>.

INFOCURIA JURISPRUDÊNCIA. 25 jun. 2013. p. 4. [Em linha]. [Consult. 10 fev. 2022]. Disponível em WWW:<URL:https://curia.europa.eu/juris/document/document.jsf?docid=138782&doclang=PT>.

KALYVAS, James R.; OVERLY, Michael R - **Big data: a business and legal guide**. New York, 2015.

KLAR, Manuel; KÜHLING, Jürgen - **Anotação ao artigo 4.º do RGPD** em Kühling/Buchner, DatenschutzGrundverordnung, 2.ª ed. Beck, Munique, 2018, Rn.9.

LEAL, Ana Alves - Aspetos jurídicos da análise de dados na internet (*Big data analytics*) nos setores bancário e financeiro: proteção de dados pessoais e deveres de informação. In CORDEIRO, António Menezes; DUARTE, Diogo Pereira; OLIVEIRA, Ana Perestrelo de - **FinTech: desafios da tecnologia**. Coimbra: Almedina, 2017.

LEI Nº 13.709, de 14 de agosto de 2018, do Congresso Nacional. [Em linha]. **Diário Oficial da União.** 15 ago. 2018. [Consult. 8 jan. 2022]. Disponível em WWW:<URL:http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>.

LEI Nº 58/2019, de 8 de agosto, da Assembleia da República Portuguesa. [Em linha]. **Diário da República.** 1.ª série. n.º 151. 2019. [Consult. 8 jan. 2022]. Disponível em WWW:<URL:https://dre.pt/pesquisa/-/search/123815982/details/maximized>.

LIMA, Taisa Maria Macena de; SÁ, Maria de Fátima Freire de - Inteligência Artificial e Lei Geral de Proteção de Dados Pessoais. **Revista Brasileira de Direito Civil – RBDCivil,** Belo Horizonte, 26(4); (2020) 227-246.

MAGALHÃES, Filipa Matias; PEREIRA, Maria Leitão - **Regulamento Geral de Proteção de Dados - Manual Prático**. Porto: Vida Económica, 2018.

MAGALHÃES, Guilherme Martins (Coord.) - **Direito privado e internet – atualizado pela Lei nº 12.965/2014**. São Paulo: Atlas 2014.

MARQUES, Claudia Lima - **Contratos no código de defesa do consumidor: o novo regime das relações contratuais**. 7.ª ed. São Paulo: Revista dos Tribunais, 2014.

MASSENO, Manuel David; MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. A Segurança na Proteção de Dados – Entre o RGPD Europeu e a LGPD Brasileira. [Em linha]. **Rev. do Cejur: Prestação Jurisdicional**. Florianópolis, 8(1)e346, (jan./dez. 2020) 1-28. [Consult. 10 fev. 2022]. Disponível em WWW:<URL:https://revistadocejur.tjsc.jus.br/cejur/article/download/346/181/614>. ISSN Eletrônico 2319-0884.

MEDON, F. O direito à imagem na era das *deepfakes*. **Revista Brasileira de Direito Civil. RBDCivil.** Belo Horizonte. 27; (jan./mar., 2021) 251-277.

MENDES, Laura Shertel - **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014.

MENDOZA, Isak; BYGRAVE, Lee A - The Right not to be Subject to Automated Decisions based on Profiling. University of Oslo Faculty of Law Legal Studies. **Research Paper Series**. 2017.

MINISTÉRIO DAS FINANÇAS. Regime Geral das Instituições de Crédito e Sociedades Financeiras. Decreto-Lei n.º 298/92. [Em linha]. **Diário da República** n.º 301/1992, 6º Suplemento, Série I-A, 31 dez. 1992. [Consult. 16 jan. 2022]. Disponível em WWW:<URL:https://dre.pt/dre/legislacao-consolidada/decreto-lei/1992-70072322>.

MINISTÉRIO DAS FINANÇAS. Código dos Valores Mobiliários. Decreto-Lei n.º 486/99. [Em linha]. **Diário da República** n.º 265/1999, Série I-A, 13 nov. 1999. [Consult. 16 jan. 2022]. Disponível em WWW:<URL:https://dre.pt/dre/legislacao-consolidada/decreto-lei/1999-34575175>.

NEW LAW - **O blockchain**. [Em linha]. [Consult. 15 jan. 2022]. Disponível em WWW:<URL:https://newlaw.com.br/direito-ao-esquecimento/>.

PEREIRA COUTINHO, Francisco; CANTO MONIZ, Graça Pereira (Coords.) - **Anuário da Proteção de Dados - 2018**. Lisboa: CEDIS, 2018.

PEREIRA COUTINHO, Francisco; CANTO MONIZ, Graça Pereira (Coords.) - **Anuário de Proteção de Dados - 2019**. Lisboa: CEDIS, 2019.

PEREIRA, Caio Mario da Silva - **Instituições de direito civil**. Vol. III. atual. 19.ª ed. Rio de Janeiro: Forense, 2015.

PETKOVA, Bilyana; BOEHM, Franziska - Profiling and the Essence of the Right to Data Protection. **Forthcoming in Cambridge Handbook of Consumer Privacy**. 2017.

REBELO, M.P - Os desafios do RGPD perante as novas tecnologias blockchain. [Em linha]. **Rev Bio y Der**. 46 (2019) 117-131. p. 119. [Consult. 15 jan. 2022]. Disponível em WWW:<URL:https://scielo.isciii.es/pdf/bioetica/n46/1886-5887-bioetica-46-00117.pdf >. ISSN 1886-5887.

REGULAMENTO (UE) 2016/679 do Parlamento Europeu e do Conselho da União Europeia de 27 de abril de 2016. [Em linha]. **Jornal Oficial da União Europeia.** 4 maio 2016. [Consult. 8 jan. 2022]. Disponível em WWW:<URL:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>.

RINGE, Wolf-Georg; RUOF, Christopher - A Regulatory Sandbox for Robo Advice, ILE University of Hamburg, Institute of Law and Economics (ILE), Hamburg. **Working Paper Series**. (14) (2018) 04-05.

ROCHA F. R. - Responsável pelo tratamento e subcontratante. In CORDEIRO, A.B.M (Coord.) - **Comentário ao Regulamento Geral de Proteção de Dados e à Lei nº 12** Faculdade de Direito. Universidade de Lisboa. Almedina, 2021. pp. 232-287.

RODOTÀ, Stefano - **A vida na sociedade da vigilância: a privacidade hoje**. Maria Celina Bodin de Moraes (Org.). Danilo Doneda e Lucianda Cabral Doneda (Trad.). Rio de Janeiro: Renovar, 2008.

RODRIGUES, Silvio - **Direito civil. Dos contratos e das declarações unilaterais de vontade**. Vol. 3. 30.ª ed. São Paulo: Saraiva, 2004.

SALDANHA, Nuno - **Novo Regulamento Geral de Proteção de Dados**. Lisboa: FCA, 2018.

SALDANHA, Nuno - **RGPD - Guia para uma auditoria de conformidade – Dados, privacidade, implementação, controlo, compliance,** Lisboa: FCA, 2019.

SALO, Marika; HAAPIO, Helena - **Robo-Advisors And Investors: Enhancing Human-Robot Interaction Through Information Design. Associate Professor of Business Law**. University of Vaasa/International Contract Counsel, Lexpert. 2017. ISBN 978-3-903035-15-7.

SANTOS, Sofia Berberan; GABRIEL, João - **Regulamento Geral de Protecção de Dados, Legislação e Algumas Notas**. Lisboa: CPA Academy, 2017.

STATISTA. **Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions).** [Online]. 2016. [Consult. 10 feb. 2022]. Available from WWW:<URL:https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>.

TRATADO SOBRE O FUNCIONAMENTO DA UNIÃO EUROPEIA (versão consolidada). [Em linha]. **Jornal Oficial da União Europeia**. 7 jun. 2016. 2016/C 202/47. [Consult. 12 jan. 2022]. Disponível em WWW:<URL:https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF>.

TIBCO Software - **O que é a internet das coisas**. [Em linha]. 2020. [Consult. 12 fev. 2022]. Disponível em WWW:<URL:https://www.tibco.com/pt-br/reference-center/what-is-the-internet-of-things-iot>.

TRIBUNAL CONSTITUCIONAL - **Estudos em homenagem ao Conselheiro Presidente Joaquim de Sousa Ribeiro**. Coimbra: Almedina, 2019.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA - **A proteção de dados pessoais no âmbito das publicações relativas aos processos judiciais no Tribunal de Justiça**. [Em linha]. 2015. [Consult. 13 jan. 2022]. Disponível em WWW:<URL:https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-11/tra-doc-pt-div-c-0000-2015-201508723-05_00.pdf>.

UNIVERSIDADE DE COIMBRA - **Informação Administrativa e Proteção de Dados. Dados Pessoais**. [Em linha]. 2020 (a). [Consult. 2 fev. 2022]. Disponível em WWW:<URL:https://www.uc.pt/protecao-de-dados/protecao_dados_pessoais/conceitos_basicos_protecao_de_dados/dados_pessoais>.

UNIVERSIDADE DE COIMBRA - **Informação Administrativa e Proteção de Dados. Anonimização e Pseudonimização**. [Em linha]. 2020 (b). [Consult. 12 fev. 2022]. Disponível em WWW:<URL:https://www.uc.pt/protecao-de-dados/protecao_dados_pessoais/anonimizacao>.

VICENTE, Dario Moura; CASIMIRO, Sofia de Vasconcelos - Data Protection in the Internet, Ius Comparatum. **Global Studies in Comparative Law**. Vol. 38, Alemanha: Springer, 2020.

VOIGT, Paul; BUSSCHE, Axel von dem - **The UE general data protection regulation (GDPR): a practical guide.** Alemanha: Springer International Publishing, 2017.

WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano - Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. **International Data Privacy Law**, 2017.

WIEDEMANN, Klaus - Automated Processing of Personal Data for the Evaluation of Personality Traits: Legal and Ethical Issues. [Online]. **Max Planck Institute for Innovation & Competition Research Paper** 18(04) (jan. 16, 2018). [Consult. 12 fev. 2022]. Available from WWW:<URL:https://ssrn.com/abstract=3102933> or <http://dx.doi.org/10.2139/ssrn.3102933>.