UNIVERSIDADE
PORTUCALENSE

REGINALDO DE JESUS CORDEIRO JUNIOR

O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS:

um estudo comparado entre o RGPD e a LGPD no contexto da interoperabilidade administrativa e do uso da tecnologia *Blockchain*

Curso de Mestrado em Ciências Jurídicas e Políticas

Orientadora: Joana Covelo de Abreu

Porto, setembro de 2020

REGINALDO DE JESUS CORDEIRO JUNIOR

O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS:

um estudo comparado entre o RGPD e a LGPD no contexto da interoperabilidade administrativa e do uso da tecnologia *Blockchain*

Dissertação apresentada à Universidade Portucalense Infante D. Henrique para obtenção do grau de Mestre em Direito

Orientadora: Joana Covelo de Abreu

Porto, setembro de 2020.

UNIVERSIDADE PORTUCALENSE

Aos meus pais, Reginaldo e Maria Celeste, pelo carinho recebido ao longo dos anos.

A minha esposa Martha Regina, a minha filha Rafaela e a minha enteada Yasmim, pelo incentivo e compreensão, em razão dos momentos em família que deixei de compartilhar, na busca desse tão sonhado objetivo.

AGRADECIMENTOS

Agradeço a todos aqueles que, direta ou indiretamente, contribuíram para a elaboração desta dissertação e, de modo especial, à Prof. Dra. Joana Covelo de Abreu, pela segura orientação, ao Prof. Dr. Carlos Henrique Rodrigues Vieira, pelo auxílio, e a minha tia Prof. Msc Lusimar Silva Ferreira, pela colaboração na normalização desta obra.

“Proteção de dados é uma expressão de liberdade e dignidade pessoais e, como tal, não se deve tolerar que um dado seja usado de modo a transformar um indivíduo em objeto sob vigilância constante.”

Stefano Rodotà

O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS:

um estudo comparado entre o RGPD e a LGPD no contexto da interoperabilidade administrativa e do uso da tecnologia *Blockchain*

RESUMO

A presente dissertação corresponde ao estudo sobre a proteção de dados pessoais no RGPD e na LGPD, em um ambiente de interoperabilidade administrativa e visa aferir a compatibilidade das normas de proteção de dados com a tecnologia *Blockchain.* Apresenta o direito à proteção de dados pessoais, sua consolidação como um direito fundamental e o tratamento distinto desse direito, uma vez que, enquanto no ordenamento jurídico europeu ele é tratado como um direito autónomo, distinto do direito à intimidade da vida privada e familiar, no ordenamento jurídico brasileiro ele é visualizado como uma extensão do direito à intimidade da vida privada e familiar. Este esforço científico tenta ainda expor a influência do RGPD na LGPD, seguido da análise do âmbito de aplicação, dos direitos dos titulares dos dados pessoais, da regulação sectorial pelas autoridades de controlo e do regime sancionatório e jurisdicional, de ambas as normas. Versa sobre os desafios para a proteção dos dados pessoais, diante da digitalização e da interoperabilidade administrativa, assim como a importância desta para o Mercado Único Digital. Trata sobre o nível de proteção adequado assegurado pelos RGPD e Regulamento n.° 2018/1725, na União Europeia, e pela LGPD, no Brasil, no contexto da interoperabilidade. Por fim, apresenta o surgimento, o conceito e a estrutura da tecnologia *Blockchain*, assim como a dificuldade de compatibilidade desta com alguns direitos do RGPD e LGPD, embora conceba que não deixa de ser uma alternativa viável para o adensamento do caminho ínsito à interoperabilidade administrativa visando a consolidação Administração Pública em Linha e das cidadanias nacional e supranacional.

Palavras-chave: Proteção de dados pessoais – RGPD e LGPD. Interoperabilidade administrativa. Mercado Único Digital. *Blockchain.*

THE FUNDAMENTAL RIGHT TO THE PROTECTION OF PERSONAL DATA:

a comparative study between GDPR and LGPD in the context of administrative interoperability and the use of Blockchain technology

ABSTRACT

This dissertation corresponds to the study about protection of personal data in the GDPR and LGPD, in an environment of administrative interoperability and it aims to measure the compatibility of data protection standards with Blockchain technology. It presents the right to the protection of personal data, its consolidation as a fundamental right and the different treatment of that right, as while in the European legal system it is treated as an independent law, distinct from the right to privacy, in Brazilian legal system it is seen as an extension of the right to privacy. This scientific effort also tries to expose the influence of the GDPR on the LGPD, followed by the analysis of the scope, rights of the holders of personal data, the sectorial regulation by the supervisory authorities and the sanction and jurisdictional regime of both legal rules. It verses about challenges for the protection of personal data, in the context of digitization and administrative interoperability, as well as its importance for the Digital Single Market. It addresses the adequate level of protection provided by the GDPR and Regulation n.° 2018/1725, in the European Union, and by the LGPD, in Brazil, in the context of interoperability. Finally, it presents the emergence, the concept and the structure of Blockchain technology, as well as the difficulty of compatibility with some rights of the GDPR and LGPD, but that it is still a viable alternative for the densification of the inherent way to administrative interoperability, aiming at the the consolidation of e-Government, and national and supranational citizenships.

Keywords: Personal data protection – GDPR and LGPD. Administrative interoperability. Digital Single Market. Blockchain.

LISTA DE ABREVIATURAS E SIGLAS

AMA - Agência para a Modernização Administrativa

ANPD - Autoridade Nacional de Proteção de Dados

AEPD - Autoridade Europeia para Proteção de Dados

APDs - Autoridades de Proteção de dados

API - Application Programming Interface

art. - artigo

arts. - artigos

CCb - Código Civil brasileiro

CDCb - Código de Defesa do Consumidor brasileiro

CDFUE - Carta dos Direitos Fundamentais da União Europeia

CE - Conselho da Europa

CEDH - Convenção Europeia dos Direitos do Homem

CEPD - Comité Europeu de Proteção de Dados

CFb - Constituição Federal brasileira

CIA - Agência Central de Inteligência do Estados Unidos da América

CNPDPP - Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

CPCb - Código de Processo Civil brasileiro

CPF - Cadastro de Pessoas Físicas

DeB - Double-entry Bookkeping

EDPB - European Data Protection Board

DLT - Distributed Ledger Technology

GDPR - General Data Protection Regulation

GT29 - Grupo de proteção das pessoas no que diz respeito a tratamento de dados pessoais

HTTP - Hypertext Transfer Protocol

ICP - Infraestrutura de Chave Pública

IDES - Índice de Digitabilidade da Economia e da Sociedade

IoT - Internet of Things

IP - Internet Protocol

IPA - Interface de Programação de Aplicativos

LGPD - Lei Geral de Proteção de Dados brasileira

n.° - número

n.^{os} - números

NoSQL - Not only Structured Query Language

OCDE - Organização para a Cooperação e Desenvolvimento Económico

OECD - Organisation for Economic Co-operation and Development

P2P - Peer-to-Peer

PKI - Public Key Infrastructure

RGPD - Regulamento Geral de Proteção de Dados da União Europeia

RIPDT - Relatório de Impacto à Proteção de Dados Pessoais

SQL - Structured Query Language

STF - Supremo Tribunal Federal

TEDH - Tribunal Europeu dos Direitos do Homem

TFUE - Tratado sobre o Funcionamento da União Europeia

TUE - Tratado da União Europeia

TJUE - Tribunal de Justiça da União Europeia

TICs - Tecnologias da Informação e da Comunicação

UE - UNIÃO EUROPEIA

URL - Uniform Resource Locator

WP29 - Working Party Article 29

WWW - Word Wide Web

SUMÁRIO

1. INTRODUÇÃO.....12

2. DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS.....16

2.1 Da consagração expressa e implícita do direito fundamental à proteção de dados pessoais – reflexão.....20

2.2 Da solução jurídico-constitucional brasileira e europeia.....35

2.2.1 A solução constitucional brasileira – da interpretação extensiva do direito fundamental à intimidade da vida privada e familiar.....35

2.2.2 A solução jusfundamental europeia – o artigo 8º da Carta dos Direitos Fundamentais da União Europeia (CDFUE) como forma de independentização do direito fundamental à proteção de dados pessoais.....47

3. A CONCRETIZAÇÃO LEGISLATIVA DAS DINÂMICAS JUSFUNDAMENTAIS.....53

3.1 O Regulamento Geral sobre a Proteção de Dados na União Europeia e a sua influência no ordenamento jurídico.....56

3.1.1 Âmbito de aplicação.....64

3.1.2 Direitos dos titulares dos dados pessoais.....72

3.1.3 A regulação sectorial pelas autoridades de controlo e o regime sancionatório e jurisdicional.....90

3.2 A Lei Geral de Proteção de Dados brasileira e a sua adequação jurídico-constitucional.....108

3.2.1 Âmbito de aplicação.....117

3.2.2 Direitos dos titulares dos dados pessoais.....127

3.2.3 A regulação sectorial pela autoridade de controlo e o regime sancionatório e jurisdicional.....137

4. OS DESAFIOS DA DIGITALIZAÇÃO E DA INTEROPERABILIDADE ADMINISTRATIVA PARA A PROTEÇÃO DE DADOS PESSOAIS EM FACE DA DATIFICAÇÃO DA VIDA.....155

4.1 A interoperabilidade administrativa no contexto do Mercado Único Digital.....162

4.2 O nível de proteção adequado assegurado pelos RGPD e Regulamento n.° 2018/1725, na União, e pela LGPD, no Brasil, em um contexto de interoperabilidade.....175

4.3 As novas tecnologias – a *Blockchain* –, o RGPD e a LGPD. Uma solução para a interoperabilidade?.....180

4.3.1 A tecnologia *Blockchain* – seu surgimento e a mudança de um paradigma.....183

4.3.2 Conceito e estrutura da tecnologia *Blockchain*.....186

4.3.3 A tecnologia *Blockchain* e a incidência do RGPD e da LGPD.....193

4.3.4 A dificuldade de compatibilização da *Blockchain* com alguns direitos do RGPD e da LGPD.....196

4.3.5 A *Blockchain* e sua aplicação na Administração Pública – a consolidação da cidadania nacional e supranacional.....202

5. CONCLUSÃO.....210

REFERÊNCIAS.....218

1. INTRODUÇÃO

No decorrer dos séculos a sociedade sofreu mutações no que tange à sua organização social, sendo que, em cada momento histórico, sempre houve um elemento primordial para o seu desenvolvimento económico e social.

Na sociedade agrícola o elemento essencial foi a terra e seus produtos; na sociedade industrial, as máquinas e a eletricidade; na pós-industrial o setor de serviço, como bancário, securitário, jurídico e educacional e, por fim, na atual sociedade informacional, a informação.

Tal informação, que organiza e move a sociedade, é impulsionada pela tecnologia na seara eletrónica, a qual possibilita processamento e a transmissão dessa informação com uma enorme amplitude, tanto quantitativa, *em pen drives, compact disc,* computadores, plataformas ou nuvem, quanto qualitativa, de uma forma organizada, permitindo o seu acesso de forma facilitada.

O direito à informação, fundamental para a efetivação da democracia, é composto por um tripé: o de informar, o de se informar e o de ser informado. Mas na sociedade da informação, os dados pessoais e a informação tornam-se uma moeda de troca, sendo fonte de poder, tanto para fins económicos, como para fins políticos. Daí porque a importância do estudo do direito à proteção dos dados pessoais somente pode ser compreendida quando vislumbrado o grau de relevância que tais dados adquiriam na sociedade informacional.

Nesse contexto, como elemento nuclear da informação encontram-se os dados pessoais, sendo que, a todo momento, somos compelidos a fornecê-los, inclusive de cunho íntimo, como forma de participar da sociedade, interagir uns com os outros, celebrar negócios jurídicos, postular e exercer direitos ou até mesmo efetuar pesquisas. Redes sociais, *sites*, *blogs* ou e-mails são locais onde os dados pessoais são objeto de recolha.

Nesses termos, os dados pessoais tornam-se objetos de cobiça, tanto pelo setor público, quanto pelo setor privado, surgindo o que se denomina de sociedade de vigilância, esta realizada especialmente por parte dos governos e das empresas.

E, a partir desse poder, é possível produzir e propagar mais informações, direcionadas a interesses específicos.

Ademais, a sociedade da informação é uma sociedade de rede, ou seja, é organizada por meios de comunicação e de redes sociais que promovem a conexão a nível grupal, organizacional, público e privado. Nesse cenário, de "estar em rede", a interoperabilidade entre os sistemas, nos setores público e privado, se torna também um alvo, como forma de promover o desenvolvimento económico, a melhor prestação de serviços e a comunicação.

O surgimento da tecnologia *Blockchain* emerge nesse contexto de ampla conexão e interoperabilidade, quando utilizadores buscam praticidade e celeridade na solução de suas demandas, com melhor prestação de serviços, conjugando com a tentativa de preservação da segurança e da integridade dos dados.

Por outro lado, com o tratamento maciço de dados pessoais, direitos fundamentais mais diversos são expostos a riscos, como o de liberdade, de privacidade, de igualdade e de não discriminação. Aliás, a própria democracia também está ameaçada.

Casos concretos como o da Cambridge Analytica*,* envolvendo Facebook, o qual pode ter comprometido o resultado das eleições nos Estados Unidos da América, e o do ex-técnico da CIA, Edward Snowden, o qual revelou que programas de espionagem norte-americanos utilizam servidores de empresas como a Google, a Apple e o Facebook, expõem o aspecto negativo da internet, da rede, e o quão importante é o combate ao tratamento indevido dos dados pessoais.

Em um ambiente no qual os dados pessoais e a informação assumem papel relevante na dinâmica social, a ciência do direito, como reguladora das relações sociais, através das normas de proteção de dados pessoais, não pode se eximir de mais um desafio que lhe é imposto, tutelar direitos fundamentais, de forma efetiva, e, ao mesmo tempo, promover o desenvolvimento económico, a estabilidade e segurança nas relações negociais originadas ou aprimoradas através das tecnologias da informação e da comunicação.

Mas até que ponto o direito à proteção de dados pessoais constitui-se como um direito fundamental? E se fundamental, seria um direito autónomo ou uma mera extensão do direito à intimidade da vida privada e familiar?

A caracterização desse direito como um direito fundamental, ou não, deve ser fixada, posto que isto definirá as características daquele direito, em um regime jurídico que é próprio da jusfundamentalidade. O reconhecimento da sua autonomia possibilitará o regramento legítimo de situações fáticas, de forma efetiva, que não estejam abarcadas, especificamente, por outros direitos ou que estes não sejam suficientes para atender às expectativas.

Entretanto, o reconhecimento da fundamentalidade de um direito, através de normas constitucionais estatais, de regra, não é suficiente para o resguardo amplo desse direito, posto que se exige a concretização legislativa da demanda jusfundamental através de uma normatização específica. Em termos de concretização surgem, como expoentes, o RGPD europeu e a LGPD brasileira.

Não é uma novidade que RGPD serviu de inspiração e de base para a LGPD, mas é essencial o estudo comparado de ambos os textos normativos, a fim de se mapear as convergências, e responder à indagação principal: tais legislações são capazes de assegurar a "proteção adequada" dos dados pessoais e com nível de equivalência, em contexto de interoperabilidade administrativa, constituindo-se utilização da tecnologia *Blockchain* uma alternativa viável de interoperabilidade e a proteção dos dados pessoais?

Tendo por pressuposto tais proposições e indagações, far-se-á, inicialmente, uma explanação sobre o que é dado pessoal, informação e tratamento, bem como se a conceituação do direito à proteção dos dados pessoais.

Posteriormente, versar-se-á sobre o direito à proteção de dados como um direito fundamental, seguindo-se a distinção entre duas soluções jurídico-constitucionais: a brasileira, que adota a interpretação extensiva do direito fundamental à intimidade da vida privada e familiar; e a europeia, que visualiza o direito à proteção de dados como um direito independente.

Não se poderia tratar sobre a concretização legislativa das demandas jusfundamentais, sem que estejam assentes os alicerces históricos e teóricos da fundamentalidade do direito à proteção de dados pessoais.

Logo em seguida, passar-se-á ao estudo comparativo das duas normas expoentes na tutela desse direito fundamental, o Regulamento Geral sobre a Proteção de Dados da União Europeia e a Lei Geral de Proteção de Dados Pessoais, discorrendo-se sobre a

influência daquele no ordenamento jurídico brasileiro, assim como, em relação a ambas as normas, sobre o âmbito de aplicação, os direitos específicos dos titulares, a regulação sectorial pelas autoridades de controlo e o regime sancionatório e jurisdicional.

Por conseguinte, passar-se-ão aos desafios impostos para a proteção dos dados pessoais, em razão da relevância alcançada por estes na sociedade informacional e o seu tratamento, em larga escala, assim como a necessidade de busca pela interoperabilidade, em específico, a administrativa, no contexto do Mercado Único Digital, e o nível de proteção adequado assegurado pelos RGPD e Regulamento n.° 2018/1725, na União, e pela LGPD, no Brasil, em um contexto de interoperabilidade.

E nesse capítulo abordar-se-á, também, o surgimento, a estrutura e o conceito da tecnologia *Blockchain*, vislumbrada como a mudança de um paradigma e um dos caminhos para a interoperabilidade.

Igualmente, de fundamental importância será o estudo sob a submissão da tecnologia *Blockchain* ao RGPD e à LGPD e a dificuldade de compatibilização de alguns direitos dispostos naquelas normas com a *Blockchain.*

Analisar-se-á, ainda, o uso da *Blockchain* na Administração Pública, como um dos vetores para a consolidação da cidadania nacional e supranacional.

Por fim, apresentar-se-ão algumas conclusões e encerra-se a dissertação com as referências.

2. DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS

Os termos "dado" e "informação" têm sido utilizados, muitas vezes, de forma indiscriminada, embora cada um possua certa peculiaridade. Enquanto o "dado" seria aquela informação no seu estado mais primitivo, de forma fragmentada, a "informação" já é algo além do que se encontra contido no "dado", ao cognitivo do que ali consta. Conforme leciona Doneda: "[...] o dado estaria associado a uma espécie de 'pré-informação', anterior à interpretação e ao processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição".[1] Mas a utilização indiscriminada se justifica em razão da tutela legal ser homogénea.

Nesse contexto, o que nos interessa não é o dado ou a informação sob qualquer espécie, mas somente a informação ou dado pessoal. A característica da pessoalidade corresponde a um vínculo objetivo com uma pessoa, algo sobre ela. Esse algo pode corresponder a características ou atos por ela praticados como: o nome, o estado civil, a idade, o domicílio, as convicções, os comportamentos, as opiniões externadas. Logo se observa que se apartam desse vínculo objetivo as informações que não são propriamente de natureza pessoal, ainda que a ela se refiram, como as opiniões de terceiro e a sua produção intelectual considerada em si mesma.

Nesse sentido se manifestou o Conselho da Europa (CE), através da Convenção n.° 108, adotada em Estrasburgo, em 1981, segundo a qual informação pessoal é qualquer informação relativa a uma pessoa singular identificada ou suscetível de identificação.[2]

O Regulamento Geral de Proteção de Dados da União Europeia (RGPD), ao conceituar "dados", dispõe, no art. 4º, n.° 1, que:

> 1) "Dados pessoais", [visam referir-se à] informação relativa a uma pessoa singular identificada ou identificável ("titular dos dados"); é considerada identificável uma pessoa singular que possa ser identificada, direta ou

[1] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Revista Espaço Jurídico.* Joaçaba, jul./dez. 2011*,* v. 12, n. 2, [consultado 8 janeiro 2020], p. 91-108, cit. p. 94. Disponível na internet: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315/658>. ISSN 2179-7943.

[2] CONSELHO DA EUROPA. Convenção n.° 108. Estrasburgo, 28 de janeiro de 1981. [Consultado 26 março 2020]. Disponível na internet: <https://www.cnpd.pt/home/legis/internacional/Convencao108.htm>."Artigo 2º - Definições. Para os fins da presente Convenção: a) 'Dados de carácter pessoal' significa qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação ('titular dos dados');"

> 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;[3]

Da mesma forma, dispõe a Lei n.° 13.709/2018, ou seja, a Lei Geral de Proteção de Dados brasileira (LGPD): "Art. 5º. Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;"[4]

Como se vê, trata-se de conceito bastante amplo, e conforme leciona Gediel e Corrêa:

> [n]isso incluem-se, é claro, o nome, o endereço, o telefone, os números dos documentos de identificação, mas também currículos escolares, dados profissionais, fiscais e bancários, dívidas e créditos, meios de pagamento, o endereço eletrônico, o IP (Internet Protocol – que permite a identificação do usuário de computador), imagens recolhidas por câmeras de segurança, fotografias disponibilizadas na Internet, e, ainda, hábitos de consumo, dados de saúde e biométricos.[5]

Nesse mesmo sentido, Silveira e Froufe teorizam que dados pessoais não são somente aqueles que, de forma direta, possibilitam a identificação de uma pessoa, mas também aqueles que permitem que se chegue a esta identificação, através de conceitos e conteúdos, mesmo sem referência direta.[6]

Trata-se de um conceito expansionista, que se refere a qualquer tipo de informação que permita a identificação do titular, presente ou futura, ou seja, ainda que o vínculo não seja estabelecido de imediato, mas de maneira indireta ou mediata.[7]

Além da noção de dados pessoais, a legislação ainda conceitua e confere maior

---

[3] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). *"J.O.U.E."* (04-05-2016). [Consultado 12 janeiro 2020]. Disponível na internet: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=pt>.

[4] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). *"D.O.U."* (15-08-2018). [Consultado 15 janeiro 2020]. Disponível na internet: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>.

[5] GEDIEL, José Antônio Peres; CORRÊA, Adriana Espíndola. Proteção jurídica de dados pessoais: a intimidade sitiada entre o estado e o mercado. *Revista da Faculdade de Direito Universidade Federal do Paraná,* Curitiba, jun. 2008, n. 47, [consultado 15 fevereiro 2019], p. 141-153, cit. p. 144. Disponível na internet: <https://revistas.ufpr.br/direito/article/view/15738>. ISSN 2236-7284.

[6] SILVEIRA, Alessandra; FROUFE, Pedro. Do mercado interno à cidadania de direitos: a proteção de dados pessoais como a questão jusfundamental identitária dos nossos tempos*. UNIO – EU Law Journal.* Braga, jul. 2018, v. 4, n. 2, [consultado 18 fev. 2020], p. 4-20, cit. p. 5. Disponível na internet: <https://revistas.uminho.pt/index.php/unio/article/view/16/48>. ISSN 2183-3435.

[7] MACHADO, Diego Carvalho et al. *GDPR e suas repercussões no direito brasileiro*: primeiras impressões de análise comparativa. Instituto de Referência em Internet e Sociedade: Belo Horizonte, 2018. [Consultado 19 março 2020]. p. 8. Disponível na internet: <https://irisbh.com.br/wp-content/uploads/2018/06/GDPR-e-suas-repercussões-no-direito-brasileiro-IRIS-1.pdf>.

proteção à figura que denomina de dados sensíveis. Esses dados são aqueles que possuem maior potencialidade de lesão a direitos e garantias fundamentais, especialmente lesões com potencialidades discriminatórias, conforme pode-se constatar do disposto no art. 5º, inciso II da LGPD[8]. Tal previsão também é estabelecida no Considerando 51 do RGPD, no seu artigo 4º, n. 13, 14 e 15, referentes aos dados genéticos, dados biométricos e dados relativos à saúde, e no seu artigo 9º, sob a epígrafe de "Tratamento de categorias especiais de dados pessoais" [9]. Segundo Bioni, assim como um dado anónimo pode se converter em um dado pessoal, a partir de um dado "trivial" pode, em face da mineração e tecnologia como *Big Data*, prever comportamentos e acontecimentos, inclusive individualidades sensíveis, como estado de saúde, orientação sexual, raça.[10] Em relação a esses dados, especialmente sensíveis, a regra é a proibição de tratamento, salvo nos casos em que se adotem medidas de segurança devidamente estabelecidas, ora havendo autorização expressa do titular ou através da menção expressa a tal tratamento na legislação aplicável, conforme o disposto no art. 9º, n.° 2 do RGPD[11] e art. 11, incisos I e II da LGPD[12].

A noção do que seja o tratamento dos dados pessoais é de suma importância, uma vez que é através dele que se expõe o titular dos dados a riscos, dotando-se aqueles dados de valor económico e político. Afinal, tal tratamento assume hoje diversas formas e naturezas, nomeadamente pelo impacto das tecnologias de informação ao serviço do tratamento de dados. E é em razão dessa relevância que se tem a amplitude do que seria

---

[8] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 13.709... op. cit. "Art. 5º Para os fins desta Lei, considera-se: II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;"

[9] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit. "(51) Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. Deverão incluir-se neste caso os dados pessoais que revelem a origem racial ou étnica, não implicando o uso do termo 'origem racial' no presente regulamento que a União aceite teorias que procuram determinar a existência de diferentes raças humanas... Artigo 4º Definições [...]13) 'Dados genéticos', os dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa; 14) 'Dados biométricos', dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos; 15) 'Dados relativos à saúde', dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde; Artigo 9º Tratamento de categorias especiais de dados pessoais 1. É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa. 2. O disposto no n.° 1 não se aplica se se verificar um dos seguintes casos: [...]"

[10] BIONI, Bruno Ricardo. *Proteção de dados pessoais:* a função e os limites do consentimento. 2ª ed. rev., atual. e refor. Rio de Janeiro: Forense, 2020. p. 84. ISBN 978853098862-3.

[11] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit.

[12] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 13.709… op. cit.

o tratamento dos dados pessoais, tanto na LGPD[13], quanto no RGPD[14]. Na realidade, visou-se tratar de todo o "percurso" atinente aos dados pessoais: desde a sua colheita ao seu apagamento / anonimização.

Assentes tais premissas, pode-se afirmar que o direito à proteção de dados pessoais é aquele conferido ao seu titular a fim de poder controlar e acompanhar o tratamento dos seus dados pessoais de forma ampla, assegurando a legítima fruição da vida social, combatendo o seu uso indevido. Ou seja, visa permitir ao titular controlar todo o fluxo de informações pessoais expostas e não apenas de fazer cessar utilizações ou invasões ilegais à intimidade.

Segundo Bolesina, é o direito que permite a uma pessoa gerir seus dados pessoais, com o fim de ingerir-se ou opor-se às práticas ilegais ou não de coleta, análise, armazenamento e uso desses dados, pela negação, retificação, atualização, redirecionamento e/ou o apagamento dos mesmos.[15]

Já Rodotà assim o define como "[o] direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular."[16]

Esse direito, se por um lado tutela os dados pessoais pelo titular, por outro assegura a possibilidade de utilização por terceiros, seguindo os ditames constitucionais, em respeito à dignidade da pessoa humana, à boa-fé, à segurança e à transparência.

Pode-se asseverar ainda que esse direito se configura como o poder de se definir e de se defender quanto a sua identidade perante a sociedade, com a abertura ou fechamento das oportunidades. A posição do indivíduo na sociedade é determinada em muito por esse direito que o indivíduo possui de controlo das suas informações pessoais.

---

[13] Ibid. "Art. 5º Para os fins desta Lei, considera-se: X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;"

[14] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit. "Para efeitos do presente regulamento, entende-se por: 2) «Tratamento», uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;"

[15] BOLESINA, Iuri. *O direito à extimidade:* as inter-relações entre identidade, ciberespaço e privacidade. Florianópolis: Empório do Direito, 2017. p. 153. ISBN 978859477084-4.

[16] RODOTÀ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: renovar, 2008. p. 15. ISBN 978857147688-2.

Conforme leciona Schreiber "[o] destino da pessoa humana acaba decidido não com base na sua real personalidade, mas com base na representação virtual que é construída a partir dos dados pessoais coletados de modo mais ou menos aleatório."[17]

E cabe ao titular pleitear as diversas formas de controlo e não apenas a interrupção ou abstenção que a privacidade clássica lhe asseguraria.

2.1 Da consagração expressa e implícita do direito fundamental à proteção de dados pessoais – reflexão

O direito à proteção de dados pessoais configura-se como um direito fundamental e da personalidade.

A consagração do direito à proteção de dados como um direito fundamental decorre da evolução nas relações sociais e económicas, uma vez que a evolução dos direitos está ligada à evolução da sociedade, com raízes no ser humano e no reconhecimento de que este é titular de direitos.

O direito à proteção dos dados pessoais não deixa de ser uma evolução alcançada oriundo do desenvolvimento do direito da privacidade.

Antes do século XIX, a privacidade já fazia parte do quotidiano da vida das pessoas, atrelada a outras esferas, como a política, a religião, a família. Cots e Oliveira citam exemplos bíblicos de indivíduos que se isolaram para maior contato com a divindade, como João Batista e Jesus, ou ainda que foram encaminhados ao deserto como Elias e Moisés para o aperfeiçoamento. Maomé também costumava, desde jovem, a se recolher em uma gruta, longe de Meca.[18]

A limpidez da distinção entre o público e o privado, existente na antiguidade grega e romana, com a supremacia do público, tende a se ofuscar na era moderna, com a noção da sociabilidade, o qual se aplicaria tanto ao âmbito público, quanto ao âmbito privado. No mundo moderno a economia passa a ser social, o trabalho realizado em público, com

[17] SCHREIBER, Anderson. *Direitos da personalidade.* 3ª ed. rev., atual. São Paulo: Atlas, 2014. p. 140. ISBN 978852249343-2.
[18] COTS, Márcio; OLIVEIRA, Ricardo. *Lei geral de proteção de dados pessoais comentada*. 3ª ed. São Paulo: Thomson Reuteres Brasil, 2019. p. 50. ISBN 978855321959-9.

redução do âmbito familiar. A antiga dicotomia evolui para duas: a primeira, sociedade e Estado, e a segunda, sociedade e indivíduo. Tais dicotomias modernas estão na base dos direitos humanos, passado a existir os campos do social-público (político) e do social-privado (económico, mercado).[19]

E aquilo que era privado, em razão da introdução no social, passa a exigir o interesse público, interesse comum, como a garantia da propriedade privada, a livre concorrência, a defesa dos direitos do consumidor, não se confundido com o social-público, mas havendo uma relação de dependência um para com o outro.

Daí a árdua tarefa de se estabelecer o que é o espaço público e o espaço privado, especialmente em uma sociedade complexa, quando interesses individuais se chocam com interesses que as pessoas possuem em comum com outras, que se situam no mundo público, superiores aos horizontes da vida de uma pessoa considerada na sua individualidade.[20]

Entrementes, não se pode negar a diversidade humana, a individualidade, sendo que o ser humano deve ser tratado com exclusividade. É fundamental o respeito pelas diferenças e particularidades de cada ser humano.

Assim, é compreensível o porquê da tutela do direito à privacidade/intimidade ter suas origens na era moderna, diante da necessidade da proteção da individualidade da pessoa.

Nesse contexto emerge a privacidade/intimidade, opondo-se ao social, razão pela qual Ferraz Junior proclama: "[o] direito à privacidade, portanto, é uma figura moderna, construída a partir da esfera privada e nela delineada, em contraposição ao social e, por extensão, ao político."[21]

Dotti enfatiza que a elaboração da autonomia do direito à intimidade/privacidade em relação aos demais direitos da personalidade teve início no final do século XIX,

---

[19] FERRAZ JÚNIOR, Tércio Sampaio. *Direito constitucional*: liberdade de fumar, privacidade, estado direitos humanos e outros temas. Barueri, SP: Manole, 2007. p. 173. ISBN 978852042451-3.

[20] GAMIZ, Mario Sergio de Freitas. *Privacidade e intimidade*: doutrina e jurisprudência. Curitiba: Juruá, 2012. p. 61. ISBN 978853623785-5.

[21] FERRAZ JÚNIOR, op. cit., p. 173.

ganhando corpo em face da revolução tecnológica do ocidente.[22]

A proteção da intimidade, no Direito Moderno, mais especificamente no século XIX, foi pensada e surgida como um direito individual que visava garantir um espaço reservado ao indivíduo, defendendo-o da intromissão de terceiros e dos meios de comunicação. Uma resistência às ingerências de uma sociedade massificada. Daí porque pensava-se a privacidade/intimidade como algo vinculado à inviolabilidade de domicílio, de comunicação, de correspondência e outros.

Thomas Cooley, juiz norte-americano, definiu a privacidade como o "direito de ser deixado só" em sua obra "*A Treatise on the Law of Torts*"[23].

O primeiro trabalho desenvolvido e importante marco no estudo do direito da privacidade/intimidade foi a publicação do artigo *The Right to Privacy,* de autoria de Warren e Brandeis, em 15 dezembro de 1890, o qual deu uma nova conotação ao direito de estar só. Tal obra, seja pelo pioneirismo no tratamento académico, seja pela influência que exerceu e ainda exerce, sustenta a necessidade de proteção do indivíduo contra o uso indiscriminado das fotografias e a invasão da vida privada pela imprensa jornalística, pregando que o indivíduo tem liberdade de fixar até que ponto os seus sentimentos, emoções e pensamentos devem ser revelados, considerando a existência de danos imateriais, sofrimentos, distintos dos materiais ou económicos, proclamando que o direito à privacidade englobava todas as manifestações do modo de ser de um indivíduo, as quais mereceriam proteção contra os meios de comunicação social. E tais danos existiriam independentemente da malícia da editora ou da verdade dos fatos. Inclusive versou o artigo sobre as situações em que não haveria violação ao direito à privacidade, como, por exemplo, nas hipóteses do interesse público ou quando o próprio indivíduo publica os fatos ou autoriza a divulgação, sugerindo a responsabilidade criminal do violador, além de uma compensação substancial em razão do dano aos sentimentos.[24]

Sob a visão dessa época, na ideia de privacidade, ou seja, segundo a teoria da *Privacy* norte-americana, é possível se vislumbrar dois elementos: a liberdade de negar,

---

[22] DOTTI, René Ariel. *Proteção da vida privada e liberdade de informação*: possibilidades e limites. São Paulo: Revista dos Tribunais, 1980. p. 27. ISBN 852030036-7.

[23] COTS, op. cit., p. 51.

[24] WARREN, Samuel D. e BRANDEIS, Louis D. The rigth of privacy. *Harvard Law Review,* Boston, dez. 1890, v. 4, n. 5, [consultado 11 março 2020], p. 193-220. Disponível na internet: <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>.

verdadeira inviolabilidade, com respeito à autonomia e a proteção da integridade psicofísica do indivíduo.

Na Alemanha, a noção de privacidade tem suas origens segundo Miranda, Rodrigues Jr. e Fruet, na jurisprudência alemã do século XIX, que envolvera a proteção da imagem do ex-chanceler Otto Von Bismarck. Tendo esse falecido em 1898, dois jornalistas conseguiram entrar em seu quarto, após terem subornado empregados e fotografaram seu cadáver, com o objetivo de vender as imagens. Os herdeiros de Bismarck processaram os fotógrafos, tendo o Tribunal do Reich (*Reichgerichtshof*) proferido decisão em 28.12.1899, impedindo a divulgação das imagens, além da apreensão das chapas, dos negativos e das impressões. Porém, o fundamento foi a entrada ilegal dos jornalistas na propriedade particular do ex-chanceler.[25]

Como se observa, ainda que Warren e Brandeis demonstrem preocupação com os elementos imateriais, a construção é baseada, assim como no caso do ex-chanceler, em uma visão negativa do direito e de natureza patrimonialista. Segundo Rodotà é o modelo burguês, individualista, solitário e patrimonial.[26]

Sob a ótica individualista, a tutela da intimidade e da vida privada constitui-se na proibição de acesso a determinados dados e informações que se insiram na esfera privada da pessoa, como questões religiosas, familiares, sexuais, sigilo de dados, telefónico, epistolar, de domicílio. Algo ainda vinculado à noção de propriedade.

No século XX, tem-se o desenvolvimento dos estudos dos direitos da personalidade na Europa continental.

A personalidade é vista como conjunto de caracteres próprios da pessoa, é o primeiro bem da pessoa, que lhe pertence. A proteção do ser humano não deve se operar somente sob o ponto de vista patrimonial, material, mas também a sua essência. Tais direitos da personalidade tutelam a esfera extrapatrimonial do indivíduo, em que uma série de valores indeterminados, não redutíveis à pecúnia, existem e devem ser observados e respeitados. Eles são o núcleo dos direitos da pessoa humana com

[25] MIRANDA, Jorge; RODRIGUES JUNIOR, Otavio Luiz; FRUET Gustavo Bonato. Principais problemas dos direitos da personalidade e estado da arte da matéria no direito comparado. In: MIRANDA, Jorge; RODRIGUES JUNIOR, Otavio Luiz; FRUET Gustavo Bonato (Coord.). *Direitos da Personalidade*. São Paulo: Atlas, 2012. p. 15. ISBN 978852247134-8.

[26] RODOTÀ, op. cit., p. 25.

existência constitucional e, como tal, designados como direitos fundamentais. Indispensáveis à existência digna, ao desenrolar saudável e pleno das virtudes psicofísicas da pessoa, razão pela qual não são passíveis de taxação exauriente e certa. Resguardam a dignidade da pessoa humana, encontrando nela o seu núcleo essencial.

Gagliano e Pamplona Filho afirmam que "[c]onceituam-se os direitos da personalidade como aqueles que tem por objeto os atributos físicos, psíquicos e morais da pessoa em si e em suas projeções sociais."[27] Nessa mesma linha de entendimento, Gomes enfatiza que esses direitos não têm objeto a própria personalidade, mas certas qualidades, atributos, expressões ou projeções da personalidade.[28]

A essencialidade de tais direitos reflete-se tanto ao mínimo necessário à proteção da personalidade, quanto à perda de interesse do indivíduo por demais direitos subjetivos, caso eles não existissem. Sabia a lição de Cupis.[29]

Exercendo a função de sujeito de direitos subjetivos, o indivíduo converte em objeto alguns dos seus atributos ou bens que lhe são próprios, razão pela qual o objeto dos direitos da personalidade não é o ser humano em sua totalidade, mas as realidades antropológicas (a vida, saúde) ou de ordem moral (nome, honra, liberdade).[30] Caracteres corpóreos e incorpóreos que correspondem à projeção da pessoa. Protege-se o que é próprio de cada pessoa, como o direito à vida, o direito à integridade física e psíquica, o direito à integridade intelectual, o direito ao próprio corpo, o direito à privacidade, incluindo a intimidade, o direito à liberdade, o direito à honra, o direito à imagem, o direito ao nome, à proteção dos dados e outros. São os bens jurídicos mais fundamentais, uma vez que são expressões da pessoa humana considerada em si mesma.

Tais estudos do direito da personalidade enfatizam o direito à intimidade e à vida privada, como um direito extrapatrimonial, que tem por finalidade a proteção da pessoa

---

[27] GAGLIANO, Pablo Stolze; Pamplona FILHO, Rodolfo. *Novo curso de direito civil:* parte geral. 8ª ed. rev., atual. e reform. São Paulo: Saraiva, 2007. v. 1. p. 135. ISBN 850205748-0.

[28] GOMES, Orlando. *Introdução ao direito civil.* 19ª ed. Rio de Janeiro: Forense, 2007. p. 136. ISBN 978853092582-6.

[29] CUPIZ, Adriano de. Os direitos da personalidade*.* Tradução: Adriano Vera Jardim e Antônio Miguel Caeiro. Lisboa: Morais, 1961. p. 17. apud LEONARDI, Marcel. *Tutela e privacidade na internet.* São Paulo: Saraiva, 2011. p. 91. ISBN 978850200000-0. "Os direitos da personalidade são aqueles direitos subjetivos cuja função, relativamente a personalidade, e especial, constituindo o *minimum* necessário e imprescindível ao seu conteúdo, sem os quais a personalidade restaria uma susceptibilidade completamente irrealizada, privada de todo o valor concreto: direitos sem os quais todos os outros direitos subjetivos perderiam o interesse para o indivíduo – o que vale dizer que, se eles não existissem, a pessoa não existiria como tal."

[30] MATTIA, Fábio Maria de. Direitos da personalidade: aspectos gerais. Revista de direito civil, São Paulo, RT, v.3, 1978. p. 40 apud JABUR, Gilberto Haddad. *Liberdade de pensamento e direito à vida privada:* conflito entre direitos da personalidade. São Paulo: Revista dos Tribunais, 2000. p. 85. ISBN 852031928-9.

e a maneira de ser do indivíduo. A privacidade, em geral, em todos os estudos é vista com um direito de proteção da liberdade do indivíduo, delimitando um espaço de autonomia, necessário à existência do ser humano, evitando a intromissão da sociedade ou do Estado.

O foco da privacidade transfere-se do ambiente para a conduta ou atividade e tal alteração foi reconhecida a partir do julgado do Tribunal Europeu de Direitos Humanos do caso *Von Hannover* (Princesa Caroline de Mónaco) vs. Alemanha, onde frisou-se que a tutela da vida privada não é condicionada à pessoa, que pode ser celebridade ou comum, tampouco ao ambiente, que pode ser público ou privado, mas a essência da atividade desempenhada pela pessoa, em face da perceção objetiva dos fatos "legítima expectativa objetiva à vida privada".[31]

Nas sociedades contemporâneas, a sociedade da informação, da evolução tecnológica e da globalização, têm-se um crescente aumento na troca de dados pessoais, com sua utilização cada vez maior para as mais diversas finalidades, que vão desde a identificação e classificação, com uso até para fins comerciais.

Tal modificação e complexidade nas relações sociais exigiu uma nova concepção do que seja intimidade/privacidade e como deve se operar a sua tutela. Nesse sentido Gediel e Corrêa afirmam:

> [d]e um lado, relativiza-se a intimidade, ampliando-se a possibilidade de acesso a dados e informações de natureza pessoal; de outro, busca-se fortalecer a proteção da pessoa inserindo nos poderes do titular desse direito de personalidade o controle não só sobre o acesso, mas também no que se refere ao seu tratamento, à sua utilização e à sua circulação.[32]

Ou seja, a noção da espera privada e sua tutela ultrapassa a garantia do segredo dos dados pessoais e adentra na possibilidade de o indivíduo controlar o acesso e o uso dos seus dados que compõem sua identidade pessoal e possibilitam o desenvolvimento de sua personalidade.

Em sua obra *Privacy and freedom,* Westin, em 1967, sustenta uma nova noção da privacidade, rompendo com a noção da privacidade clássica, de abstenção de não

[31] BOLESINA, op. cit., p. 147.
[32] GEDIEL, op. cit., p. 143.

intromissão, introduzindo a nova dimensão liberdade informativa.[33]

E mais, de uma noção de privacidade vinculada à propriedade, com uma conotação individualista do que pertence ao indivíduo, a privacidade agora deve tutelar a igualdade de tratamento dos indivíduos na sua participação na sociedade de uma forma democrática, ou seja, uma conotação não individualista.

Isto não significa o abandono na concepção clássica de privacidade, posto que tais problemas ainda seguem presentes, havendo a coexistência de dois influxos: um que é direcionado para as invasões ilegais à intimidade e outro voltado para fruição informacional dos dados pessoais, sejam eles íntimos ou não.[34]

Partindo-se dessas premissas, passa-se a compreender o elo entre informação pessoal e privacidade, em uma correlação simplória que seria no sentido de quanto maior a divulgação da informação pessoal menor o grau de privacidade do titular. Embora a problemática da proteção de dados pessoais não se esgote unicamente nessa relação, serve ela para demonstrar como e porque os ordenamentos jurídicos passaram a tutelar a proteção dos dados pessoais, sendo visto com um desdobramento da proteção do direito à privacidade. Com a ascensão cada vez maior da importância da informação a noção de privacidade passa a girar em torno dos dados pessoais. Assim, a disciplina da proteção de dados pessoais passa a ser vista como verdadeira herdeira da disciplina da privacidade.

Porém, a proteção de dados pessoais não deve ser vista unicamente no interesse da privacidade, uma vez que outros interesses devem ser considerados, de maneira a abranger as formas de controlo que são possíveis com a manipulação de dados. E esses interesses devem ser considerados pelo que representam, não apenas sob a ótica de violação da privacidade.

Nesses termos, um dado que se refere a uma pessoa é a extensão ou projeção do seu titular, devendo ser visto como um novo tipo de identidade, que distingue uma pessoa de outra. Eis ai o direito à proteção de dados pessoais como um direito da personalidade.

Diante do fato da proteção de dados atingir um local de destaque, autores

[33] BOLESINA, op. cit., p. 159.
[34] Ibid., p. 150.

divergem. Enquanto Doneda sustenta que ela representa a continuação da privacidade por outros meios[35], Zanon prega a autonomia e o caráter inédito da proteção dos dados pessoais em relação à privacidade.[36] A tutela dos dados pessoais que, inicialmente, parecia apenas realizar alterações específicas e pontuais no ordenamento jurídico, com fins de adequar o uso dos meios tecnológicos da informação, acabou por dar origem às bases do que se poderia chamar de direito fundamental à proteção de dados pessoais.

O reconhecimento do direito à proteção de dados pessoais como um direito fundamental perpassa por uma noção de direito fundamental.

O caráter fundamental de um direito deve ser visto sob uma dupla perspectiva. É ele fundamental por ser essencial ao ser humano, à sua existência, e para de fins de sobrevivência, de desenvolvimento, de interação e convivência com os outros. Mas também é fundamental pelo fato do Estado o ter eleito como algo que serve de base de legitimação da atuação Estatal, seja restringindo ou impedindo a atuação deste, como condicionante negativa, seja exigindo uma atuação positiva, de implementação e concretização. Sob esse segundo prisma é que Nunes Júnior proclama que a existência de um estado de direito perpassa pela existência de tais direitos.[37]

Nesse contexto, é de particular relevância o papel das Constituições na efetiva proteção dos direitos fundamentais, uma vez que ainda que disposto em uma declaração da ONU, a mesma é apenas uma recomendação feita a seus membros, não possuindo força vinculante, posto que dependerá da adoção de cada Estado a sua fundamentalidade.

Segundo Pérez Luño, os direitos fundamentais são

> [...] un conjunto de facultades e instituciones que, en cada momento histórico, concretan las exigências de la dignidade, la libertad y la igualdad humanas, las cuales deben ser reconocidas positivamente por los ordenamientos jurídicos a nivel nacional e internacional.[38]

---

[35] DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais:* elementos da formação da lei geral de proteção de dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019. p. 47. ISBN 978855321957-5.

[36] ZANON, João Carlos. *Direito à proteção dos dados pessoais.* São Paulo: Revista dos Tribunais, 2013. p. 67,146. ISBN 978852034905-2.

[37] NUNES JUNIOR, Vital Serrano. *A proteção constitucional da informação e o direito à crítica jornalística.* São Paulo: Editora FTD, 1997. p. 15. ISBN 853223758-4.

[38] PÉREZ LUÑO, Antônio Henrique. *Derechos Humanos, Estado de Derecho y Constitutión.* 7ª ed. Madrid: Tecnos, 2001. p.48. ISBN 843093723-4.

Tais direitos, em regra, dentre eles a proteção de dados pessoais, concretizariam o princípio da dignidade da pessoa humana em dois sentidos: sob uma visão subjetiva conferem às pessoas posições jurídicas favoráveis que devem ser respeitadas por terceiro e pelo Estado; já sob uma visão objetiva regram a atuação Estatal de forma racional, fixando a sua organização e um modelo de Estado, verdadeiro ditame da soberania popular sobre o poder constituído.

Segundo Mendes e Branco "[...] é esse princípio que inspira os típicos direitos fundamentais, atendendo à exigência do respeito à vida, à liberdade, à integridade física e íntima de cada ser humano, ao postulado da igualdade em dignidade de todos os homens e segurança."[39]

Nesse diapasão é que Sanchís proclama que tais direitos têm relação com a vida, a dignidade, a liberdade, a igualdade e a participação política, sendo que somente se tal direito ou instituição estiver servindo a algum desses valores, é que se poderia caracterizá-lo como fundamental, privilegiando uma concepção histórica desses direitos.[40] É bem verdade que adoção de tal critério de vincular um direito fundamental ao princípio da dignidade da pessoa humana, onde aquele concretizaria este, conforme o que foi exposto, é criticada por Canotilho, já que excluiria do âmbito dos direitos fundamentais aqueles que não tenham um radical subjetivo, ou seja, que não tenham por pressuposto a ideia do princípio da dignidade da pessoa humana.[41] Tal afirmação do autor português encontraria guarida em razão da existência de direitos fundamentais assegurados às pessoas coletivas e outros. E para tanto podemos citar os estabelecidos no art. 5º, incisos XXI, XXV e XXVIII da Constituição Federal brasileira (CFb).[42]

E nesse ponto, assiste razão ao renomado autor. Pode-se declamar que direitos que

---

[39] MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de direito constitucional.* 13ª ed. rev. e atual. São Paulo: Saraiva, 2018. p. 140. ISBN 978854722974-0.

[40] SANCHÍS, Luís Pietro. *Estudios sobre derechos fundamentales.* Madrid: Debate, 1990. p. 88. ISBN 978847444443-8.

[41] CANOTILHO, José Joaquim Gomes. *Direito constitucional e teoria da constituição.* 7ª ed. Coimbra: Almedina, 2003. p. 407. ISBN 978972402106-5.

[42] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Constituição da República Federativa do Brasil. "*D.O.U.*" (05-10-1988). [Consultado 20 março 2020]. Disponível na internet: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. "Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: XXI - as entidades associativas, quando expressamente autorizadas, têm legitimidade para representar seus filiados judicial ou extrajudicialmente; XXV - no caso de iminente perigo público, a autoridade competente poderá usar de propriedade particular, assegurada ao proprietário indenização ulterior, se houver dano; XXVIII - são assegurados, nos termos da lei: a) a proteção às participações individuais em obras coletivas e à reprodução da imagem e voz humanas, inclusive nas atividades desportivas; b) o direito de fiscalização do aproveitamento econômico das obras que criarem ou de que participarem aos criadores, aos intérpretes e às respectivas representações sindicais e associativas."

se assentam na dignidade da pessoa humana são direitos fundamentais materialmente. Mas eles não se limitam a esse fundamento. Tratam-se de direitos que se assentam valores no tempo e no espaço e que correspondem a uma determinada cultura, uma vez que a própria Constituição encana valores, que não ficam ao bel prazer da capacidade ou vontade do constituinte. Existe aí um traço marcante da moral. São direitos que refletem a ideia de Direito, do sentimento jurídico coletivo, de uma concepção de Constituição dominante.[43]

Nesse diapasão, o direito à vida privada, à intimidade e à proteção de dados se caracterizariam, não apenas como direitos fundamentais formais, devido à sua previsão no art. 5º inciso X da Constituição Federal brasileira (CFb), art. 26º, n.° 1 e 35º da Constituição portuguesa[44] e art. 18, n.° 1 da Constituição espanhola[45], mas também como um direito fundamental material, por ter em sua essência a dignidade e a liberdade.

Viktor Mayer-Schönberger[46] visualiza quatro diferentes gerações de leis na tutela dos dados pessoais, que vão desde um enfoque mais técnico e restrito, até a técnicas mais amplas e compatíveis com a profundidade da tecnologia adotada para o tratamento desses dados, com seu enquadramento na seara dos direitos fundamentais.

A primeira geração era composta por leis que miravam o controlo nos grandes centros elaboradores de dados, pelo que havia uma preocupação com a concessão de autorizações para a criação desses bancos de dados e com o seu controlo pelos órgãos públicos. Focavam ainda no controlo do uso de informações pessoais pelo Estado,

---

[43] MIRANDA, Jorge. *Manual de direito constitucional*. 4ª ed. Coimbra: Coimbra Editora, 2008. t. 4. p. 12. ISBN 978972321613-4.

[44] PORTUGAL. ASSEMBLEIA CONSTITUINTE – Constituição da República Portuguesa. *"D.R."* (10-04-1976). [Consultado 20 março 2020]. Disponível na internet: <https://dre.pt/legislacao-consolidada/-/lc/34520775/view>. "Artigo 26º (Outros direitos pessoais) 1. A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à protecção legal contra quaisquer formas de discriminação. [...]Artigo 35.º *(Utilização da informática)* 1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei. 2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente. 3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis. 4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei. 5. É proibida a atribuição de um número nacional único aos cidadãos. 6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional. 7. Os dados pessoais constantes de ficheiros manuais gozam de protecção idêntica à prevista nos números anteriores, nos termos da lei."

[45] ESPANHA. ASSEMBLEIA CONSTITUINTE – Constitución Española. *"B.O.E"* (29-12-1978). [Consultado 20 março 2020]. Disponível na internet: <http://www.lamoncloa.gob.es/documents/constitucion_es1.pdf>. "Artículo 18 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen."

[46] MAYER-SCHÖNBERGER, Viktor. General development of data protection in Europe. In: AGRE, Phillip; ROTENBERG, Marc (Org.). *Technology and privacy*: The new landscape. Cambridge: MIT Press, 1997. p. 219-242. ISBN 978026201162-4.

destinatário principal dessas normas. Havia um receio no uso indiscriminado dessa tecnologia e dos computadores, vistos como uma ameaça. Em tais leis os bancos de dados eram tratados como algo tecnocrático e não como uma possível violação à privacidade, sem prever uma participação do cidadão neste processo.[47]

A segunda geração de leis, surgida na segunda metade da década de 70, abandona o foco do centro dos grandes bancos de dados, devido a sua proliferação, o que tornava impossível o controlo por autorizações, e se baseiam na privacidade, sendo a proteção de dados pessoais visto como uma liberdade negativa, a qual é exercida pelo próprio titular, independente de terceiros ou fiscais. Como exemplo pode-se citar: a Lei Federal da República Federativa da Alemanha sobre proteção de dados pessoais de 1977 – *Bundesdatenschutzgesetz* – e a Lei Francesa de Proteção de Dados Pessoais de 1978 – *Informatique et Libertées*.

Na década de 1980 surge uma terceira geração de leis de proteção de dados, as quais, apesar o foco no indivíduo titular, a proteção é visualizada de como um processo mais complexo, levando em consideração o contexto, posto que o fornecimento dos dados pessoais torna-se o requisito para a participação da vida em sociedade, passando o fornecimento dos dados pessoais a ser uma regra. Procura-se, assim, não apenas prever a liberdade do indivíduo de fornecer ou não os seus dados, mas assegurar a efetividade desse direito, no tratamento e utilização, o efetivo exercício da autodeterminação informativa, combatendo situações em que a liberdade de decidir livremente seja suprimida no todo ou em parte. O tratamento dos dados pessoais passa a ser visto como um processo, desde a inclusão até utilização pelo banco ou por terceiros, além do direito à informação.

Por fim, emerge uma quarta geração de leis que procura suprir o caráter exclusivista da autodeterminação informativa, a qual correspondia apenas a uma minoria a qual arcava com os custos económicos e sociais. A tutela dos dados pessoais, além do foco individual, passa a ter um enfoque coletivo, reconhecendo um desequilíbrio na relação entre o titular do direito e os entes que coletam e processam, especialmente em face da diminuição do seu poder de escolha para autorização do processamento de

[47] Ibid., p. 223-224.

dados. Há ainda uma redução no papel da decisão individual em determinadas modalidades de tratamento de dados pessoais, como certa utilização de dados sensíveis, que necessitam da mais alta proteção. Acrescente-se ainda o surgimento de autoridades independentes para fazer valer a legislação e de normas conexas específicas para alguns setores de processamento de dados, como crédito ao consumo, saúde e bancário.

A crescente evolução da legislação mundial, com mudança de perfil e foco ao longo dos anos em diversos países, não embaraça a visualização de objetivos e de uma atuação legislativa embasada em alguns princípios comuns básicos, vinculados à proteção da pessoa e aos direitos fundamentais e que também são o alicerce da sua autonomia, os quais serão dispostos em momento oportuno.

Nessa seara, a Convenção de Estrasburgo n.° 108, de 28 de janeiro de 1981, foi um divisor de águas, ao tratar o direito à proteção de dados pessoais sob a ótica de um direito fundamental. No seu preâmbulo, ela prima pelo respeito aos direitos do homem e às liberdades fundamentais, almejando ainda "[...] alargar a protecção dos direitos e das liberdades fundamentais de todas as pessoas, nomeadamente o direito ao respeito pela vida privada, tendo em consideração o fluxo crescente, através das fronteiras, de dados de carácter pessoal susceptíveis de tratamento automatizado."[48] Mais adiante, o art. 1º, que dispõe sobre os objetivos e as finalidades, menciona "[...] o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito ("protecção dos dados")." Tal Convenção enaltece o disposto no art. 8º da Convenção Europeia dos Direitos do Homem (CEDH), celebrada em Roma, 1950.[49]

Cite-se também o Tratado sobre o Funcionamento da União Europeia (TFUE), que versa sobre o assunto no art. 16º:

> Artigo 16º (ex-artigo 286º TCE) 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. O Parlamento Europeu e o

[48] CONSELHO DA EUROPA. Convenção n.° 108, op. cit.

[49] Id. Convenção Europeia dos Direitos do Homem. Estrasburgo, 2 de outubro de 2013. [Consultado 30 março 2020]. Disponível na internet: <https://www.echr.coe.int/Documents/Convention_POR.pdf >. "ARTIGO 8° Direito ao respeito pela vida privada e familiar - 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem - estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros."

> Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes. As normas adotadas com base no presente artigo não prejudicam as normas específicas previstas no artigo 39º do Tratado da União Europeia.[50]

De forma expressa dispôs a Diretiva 95/46/CE de 24 de outubro de 1995, incluindo a proteção de dados como um direito fundamental de respeito à vida privada, no art. 1º.[51]

Mais adiante, tem-se a Carta dos Direitos Fundamentais da União Europeia (CDFUE), de 7 de dezembro de 2000, a qual já trata o direito à proteção dos dados pessoais em artigo distinto do direito ao respeito pela vida privada e familiar, ou seja, no art. 8º, enquanto este segundo está disposto no art. 7º.[52] Esta Carta dos Direitos Fundamentais assumiu caráter juridicamente vinculativo com o tratado de Lisboa, tal como resulta do artigo 6º, n.° 1 do Tratado da União Europeia, passando a ter o mesmo valor jurídico dos Tratados.

E, por fim, o RGPD que dispõe expressamente no Considerando 1: "[a] proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental."[53]

Ora, este veio revogar a prévia Diretiva e atualizar a proteção de dados no contexto europeu, através de um ato jurídico – o Regulamento – que é diretamente aplicável na

---

[50] UNIÃO EUROPEIA – Tratado sobre o funcionamento da união europeia (versão consolidada). "*J.O.U.E.*" (07-6-2016).[Consultado 30 março 2020]. Disponível na internet: <https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF>.

[51] PARLAMENTO EUROPEU; CONSELHO – Directiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995 relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. "*J.O.C.E.*" (23-11-1995). [Consultado 30 março 2020]. Disponível na internet: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT>. "Artigo 1 Objecto da directiva 1 . Os Estados-membros assegurarão, em conformidade com a presente directiva, a protecção das liberdades e dos direitos, fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais."

[52] Id. – Carta dos direitos fundamentais da união europeia. "*J.O.U.E.*" (07-06-2016). [Consultado 30 março 2020]. Disponível na internet: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR>. "Artigo 7º. Respeito pela vida privada e familiar. Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações. Artigo 8º Proteção de dados pessoais. 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses 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 respeito e de obter a respetiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente."

[53] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit.

ordem jurídica dos seus Estados-Membros, promovendo uma uniformização do direito aplicável.

Mas além de fundamental é um direito da personalidade, conforme mencionado na classificação citada. Bolesina ressalta que a proteção de dados pessoais é essencial, pois o tratamento deles afeta direta e indiretamente a vida de cada pessoa, influenciando nas oportunidades que recebe ou não, inclusive no desenvolvimento da personalidade.[54]

Tal direito confere deferência às escolhas existenciais, com resguardo da liberdade e do desenvolvimento da personalidade, combatendo formas de discriminação institucionais e sociais. Assim Zanon elucida:

> [a] proteção dos dados pessoais resguarda a pessoa de não ser discriminada pelas suas crenças religiosas, suas opiniões políticas e filosóficas, por sua etnia, condições de saúde ou orientação sexual; proteger os dados pessoais significa, também, evitar o indivíduo seja impedido de acessar bens e serviços, a princípio só oferecidos àqueles com bons credenciais; conferir proteção aos dados pessoais implica, ainda, livrar-se de etiquetas e chancelas. Portanto, com a proteção dos dados pessoais, busca-se sobretudo, a não discriminação, a não exclusão e a promoção da liberdade.[55]

Esse direito é comprometido com o desenvolvimento da personalidade e com as práticas democráticas.

Independentemente de como se visualize o direito à proteção de dados, como um direito autónomo ou como prolongamento, uma decorrência do direito à privacidade, configura-se ele como um direito fundamental da personalidade.

Direitos tidos por fundamentais ou humanos tem, em regra, uma matriz principiológica. E, assim sendo, a sua característica de universalidade assenta-se no reconhecimento, mas não na sua interpretação e tutela. Bolesina ressalta que Westin já vislumbrava tal situação em relação à privacidade no mundo ocidental desde a década de 60.[56] Portanto, a proteção de dados pessoais pode variar de acordo com a cultura de cada povo.

Partindo-se dessa premissa, visualiza-se, hodiernamente, dois modelos jurídicos de tutela dos dados pessoais, como forma de evitar a coleta e uso indevido: o modelo norte-americano e o europeu. O modelo norte-americano tem o seu foco principal na

[54] BOLESINA, op. cit., p. 158.
[55] ZANON, op. cit., p. 151.
[56] BOLESINA, loc. cit.

valorização da escolha individual, a liberdade, enquanto que o europeu tem por fundamento a dignidade da pessoa humana, com forte regulação, ainda que não despreze o consentimento. Nesse sentido é que Rodotà afirma que o ocidente conta com dois modelos mais populares em torno da privacidade e da proteção de dados pessoais: o norte-americano, assentado na ideia de liberdade, e o europeu, calcado na dignidade da pessoa humana.[57]

O sistema europeu, seguido pelo Brasil, regulando de forma minuciosa, reflete a preocupação em se equilibrar a proteção da pessoa, com os interesses da coletividade e do Estado, permitindo o tratamento dos dados pessoais nas diversas situações dispostas no art. 6º do RGPD[58] e art. 7º da LGPD[59], não limitando a licitude do tratamento apenas ao consentimento do seu titular, mas colocando a tónica num esclarecimento cabal do titular aquando o tratamento permitindo.

Afinal, a tutela jurídica dos dados pessoais não deve permanecer centrada exclusivamente no consentimento do titular do direito, na sua autonomia e confidencialidade. Primeiro, porque na presente sociedade as pessoas acabam por abrir mão de seus direitos como forma de obter mais segurança e de participar da vida tecnológica social, com a prevalência dos interesses do mercado e do Estado que, sendo fatores de pressão, acabam por incidir, apesar de serem desconsiderados; segundo, porque tais dados podem ser excepcionados do controlo individual, não apenas por

[57] RODOTÀ, op. cit., p. 120.

[58] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit. "Artigo 6º Licitude do tratamento 1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações: a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas; b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados; c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; f) O tratamento 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."

[59] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 13.709… op. cit. "Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei n.° 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente."

razões de interesse público, mas nas diversas hipóteses descritas no art. 6º do RGPD e art. 7º da LGPD, já citados.

Mas, independentemente do modelo de tutela adotado, o americano ou o europeu, visa-se assegurar a autonomia do indivíduo, sua liberdade, sua privacidade, atendando-se para o combate à discriminação.

Nesse diapasão é que diversos ordenamentos jurídicos elevam a categoria do direito à proteção de dados como um direito fundamental e que serve, também, ao direito à privacidade.

2.2 Da solução jurídico-constitucional brasileira e europeia

Uma das principais discussões em torno do direito de proteção dos dados pessoais é a questão da autonomia dele em relação ao direito à intimidade da vida privada e familiar.

Têm-se aí duas posições: a proteção de dados pessoais é um direito novo e autónomo ou a proteção de dados está inserida no direito à vida privada e familiar, em face da ampliação, contextualização e atualização desse derradeiro direito.

Mas independentemente da posição adotada, a fundamentalidade do direito à proteção de dados pessoais está resguardada.

2.2.1 A solução constitucional brasileira – da interpretação extensiva do direito fundamental à intimidade da vida privada e familiar

A Constituição Federal brasileira (CFb) não prevê, de forma expressa, o direito à proteção de dados pessoais como um direito autónomo e, muito menos, como um direito fundamental formal taxativo.

É passível de se compreender a não inserção no texto constitucional, em razão de que o tema, proteção de dados pessoais, somente há alguns poucos anos é que passou a

ser objeto distinto da agenda política brasileira, diferentemente do que ocorre na Europa, que se ocupa há mais de cinco décadas, e os Estados Unidos, há cerca de duas décadas.

Assim, face a ausência de uma previsão expressa, tem-se a extensão do direito à proteção à intimidade e à vida privada, ou seja, a privacidade como um todo.

A expansão da privacidade pode ser verificada, tanto no direito norte-americano, quanto no direito germânico, tendo por fundamento o livre desenvolvimento da personalidade. Doneda assim nominou de "força expansiva" da privacidade em face das necessidades atuais.[60]

A noção de direito à privacidade hodierna não corresponde à do século pretérito ou do início deste. Tal noção do direito é estabelecida por circunstâncias externas e internas. Circunstâncias externas seriam aspectos materiais ou não como: condições de residência, a divisão do trabalho, o grau de interação, a densidade da população e demais relações sociais. Já a circunstância interna corresponde à atuação do próprio indivíduo, que estabelece o seu âmbito íntimo, ou seja, a dimensão de sua intimidade. Ademais, novas tecnologias conduzem à uma necessária adaptação a uma nova noção do direito à privacidade, diferentemente da concepção clássica.

Também não existe uma previsão da extensão do direito à privacidade em sede legal e constitucional, havendo uma enorme variedade de circunstâncias que podem surgir, de acordo com o contexto social e político.

Importante observar que o problema de conceituação do conteúdo da privacidade não se limita à dicotomia que existe entre o modelo da *Civil Law* e o da *Common Law*. É bem verdade que existem diferenças entre o modelo de privacidade/intimidade romano-germânico, cujo fundamento principal é a dignidade e o modelo de privacidade/intimidade anglo-saxão, o qual tem a liberdade como fundamento principal. Mas mesmo entre os países do mesmo modelo, com a existência de diretivas que fixam padrões mínimos, as diferenças culturais influenciam nesses padrões mínimos quando transpostos para o direito interno. O mesmo se diga na adoção de padrões mundiais. Daí a dificuldade, diante das variáveis, de se estabelecer um conceito sobre tal direito, com um enorme dinamismo.

[60] DONEDA, Danilo. *Da privacidade …* op. cit. p. 43.

Rodotà ressalta que o direito à privacidade estrutura-se atualmente como "pessoa-informação-circulação-controle", e não mais como "pessoa-informação-segredo".[61]

E com base nessa estrutura Ferraz Junior prega novos conceitos de proteção da esfera privada, sendo que o foco principal deve ser dado à comunicação, e não ao conteúdo da decisão informativa. Seria a liberdade por meio da comunicação e não a liberdade de comunicação, uma vez que a liberdade em rede informatizada se manifesta sempre em reciprocidade: a informação posta individualmente em rede e, simultaneamente, para os outros.[62]

Por sua vez Rodotà enfatiza que seria "[...] o direito de manter o controlo sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada."[63]

Superadas estariam aquelas conceituações do direito à intimidade e à vida privada (privacidade) de forma unitária, como o de "estar só" ou de não sofre interferências alheias ou de decidir sobre a divulgação ou não destes aspectos privados. A definição isolada de cada um deles é insuficiente para a tutela da intimidade e da vida privada. A busca por conceitos unitários como forma de definir esse direito fundamental, passível de ser aplicado a qualquer situação confronta-se com a multiplicidade de tal direito. De acordo com cada doutrinador, encontram-se conceitos mais ou menos abrangentes. Esse seria o principal problema desse método de conceituação unitário, uma vez que acaba por produzir conceitos ora excessivamente restritivos, ora excessivamente abrangentes.[64]

Acrescente-se ainda que a procura por um núcleo comum que possa ser encontrado a todas as situações fáticas, dificulta a identificação do que faz parte do âmbito de proteção desse direito, e, consequentemente, do sopesamento no caso de choque com outros direitos.

E mais, o fato dele não ser encontrado em todas as situações, conduz ao surgimento das teorias reducionistas, que não vislumbram a autonomia do direito da

---

[61] RODOTÀ, Stefano. *Tecnologie e diritti*. Bologna: Mulino, 1995. p. 102. ISBN 978881504855-4.
[62] FERRAZ JUNIOR, Tércio Sampaio. A liberdade como autonomia recíproca de acesso a informação. In: GRECO, Marco Aurélio; MARTINS, Ives Gandra da Silva (Coord.). *Direito e Internet:* relações jurídicas na sociedade informatizada. São Paulo: Revista dos Tribunais, 2001. p. 244. ISBN 852032034-1.
[63] RODOTÀ, Stefano. *Tecnologie …* op. cit. p. 122.
[64] LEONARDI, op. cit. p. 51.

privacidade, mas apenas como algo incluído no direito geral de liberdade, ou derivado de outros direitos, ou ainda representando uma forma menos precisa de abordar valores específicos, tais como liberdades de expressão, de associação e de crença.[65] Porém, tais conceitos esquecem a complexidade multifacetária, reduzindo apenas a um dos aspectos.

Doneda enfatiza que a privacidade relaciona-se com uma série de diversos interesses distintos, modificando o seu perfil tradicional.[66]

Portanto, sob o modelo brasileiro, há necessidade de uma visão plural, ou seja, expansiva do direito à intimidade e da vida privada.

Os mais diversos interesses distintos existentes no direito à privacidade são reconhecidos inclusive pela Carta dos Direitos Fundamentais da União Europeia (CDFUE) tutelando a vida privada e familiar no art. 7º, sob uma ótica individualista de vedação a intromissão de terceiros, e no art. 8º a tutela dos dados pessoais de natureza dinâmica.[67]

O mesmo ocorre com a Constituição Federal brasileira (CFb) e o direito infraconstitucional que fixam diversas normas destinadas à tutela da privacidade em sentido amplo que abarcam todos os conceitos tratados.

Nesse diapasão a corrente pluralista procura conceituar a privacidade partindo de situações que configurariam afronta a esse direito.

Segundo Pereira, o primeiro autor a valer-se dessa maneira para conceituar o direito à intimidade foi Prosser, em 1960, sendo que elas seriam: intrusões em seu isolamento, em sua solidão ou em seus assuntos privados; divulgação ao público de fatos considerados privados; publicação de fatos que representem o indivíduo sob uma falsa aparência não difamatória e apropriação por parte de terceiros de certos elementos da personalidade do indivíduo com ânimo de lucro. [68]

Fariñas Matoni acrescenta que é o mais correto seria adotar o método taxonómico,

---

[65] Ibid., p. 79.

[66] DONEDA, Danilo. *Da privacidade*… op. cit., p. 41.

[67] PARLAMENTO EUROPEU; CONSELHO – Carta dos direitos fundamentais da união europeia. op. cit. "Artigo 7º. Respeito pela vida privada e familiar - Todas as pessoas tem direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações. Artigo 8º. Protecção de dados pessoais 1. Todas as pessoas têm direito à protecção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objecto 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 respeito e de obter a respectiva rectificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente."

[68] PROSSER, W. L. Privacy, California Law Review, n. 48, 1960 apud PEREIRA, Marcelo Cardoso. *Direito à intimidade na internet.* Curitiba: Juruá, 2011. p. 111. ISBN 853620516-4.

ou seja, com a enumeração dos conteúdos possíveis, diante da complexidade de tal direito e da sua praticidade.[69]

Da Conferência Nórdica sobre o Direito à Intimidade, realizada em maio de 1967, resultou o documento de Estocolmo, que seguindo a doutrina pluralista elencou cinco ofensas ao direito à intimidade e à vida privada. Cunha Júnior[70] os descreve: penetração no âmbito de solidão da pessoa, que inclui a perseguição, a espionagem e o chamamento constante ao telefone; a gravação de conversas e de cenas fotográficas ou cinematográficas do indivíduo em seu círculo privado ou em circunstâncias íntimas ou situações danosas a sua moral; audição de conversas por interferência mecânica de telefone, microfilmes dissimulados; exploração de nome, identidade ou semelhança da pessoa sem o seu consentimento, utilização de declarações falsas, crítica a vida das pessoas e revelação de fatos íntimos; utilização em meios de informação de fotografias ou gravações obtidas sub-repticiamente nas formas anteriores.

Moraes adota esse mesmo entendimento, fixando as hipóteses de como forma de conceituá-lo, estabelecendo o âmbito de proteção de tal direito.[71]

Mas, ainda que se adote a corrente pluralista para fins de conceituação, devido a volatividade e a evolução do que seria privacidade, as situações de ofensa devem ser visualizadas como *numerus apertus*, sob pena de em um curto espaço de tempo entrarem em descompasso com a realidade.

Considerando as novas formas de ameaça à privacidade, diante da evolução tecnológica, e necessidade de um conceito plural, passou a doutrina norte-americana a visualizá-la como um conjunto de proteções contra diversos problemas distintos, mas que se relacionam. Nesse diapasão é a proposta de Solove, o qual defende um conceito pluralístico, social e pragmático, com foco nos problemas que precisam de resolução e na utilidade social da tutela. Para tanto, afasta-se da busca por um núcleo que seria comum a todas as situações daquele direito e fundando-se no conceito de semelhanças de família de Ludwig Wittgenstein, tem-se que certas coisas parecem estar ligadas por alguma característica essencial comum, mas que na verdade se conectam por uma série de

[69] FARIÑAS MATONI, Luis Maria. *El derecho a la intimidad*. Madrid: Trivium, 1983, p. 309. ISBN 848614408-6.
[70] CUNHA JÚNIOR, Dirley da. *Curso de direito constitucional*. 12ª ed. rev., ampl. e atual. Salvador: JUSPODIVM, 2018, p. 626. ISBN 978854421926-3.
[71] MORAES, Alexandre de. *Direito Constitucional.* 24ª ed. São Paulo: Atlas, 2009. p. 53. ISBN 978852245401-3.

semelhanças relacionadas, inexistindo a característica comum. Assim o direito à intimidade e vida privada seria o conjunto de proteções contra uma pluralidade de problemas distintos, relacionados entre si.[72] Para tanto, seguindo também a taxonomia para quem os problemas da privacidade poderiam ser divididos em quatro géneros e dezesseis espécies: a) coleta de informações: vigilância e interrogação; b) processamento de informações: agregação; identificação; insegurança; uso secundário e exclusão; c) disseminação de informações: quebra de confidencialidade; revelação; exposição; aumento da acessibilidade; chantagem; apropriação e distorção; d) invasão: intrusão e interferência em decisões.[73]

Não se pode negar que tal forma de conceituar está direcionada a resolução de problemas em categorias, aproxima-se à práxis do direito romano, não havendo uma certa preocupação com a construção de uma ciência do direito e de um sistema normativo.

Mas tal conceito plural da privacidade seguido as semelhanças de família revela a importância de tal direito ser visto de forma ampla, pelo que taxonomia auxilia a identificar os casos que ameaçam a privacidade na atualidade, especialmente mediante o uso da Internet, situações que nem sempre conseguem ser tuteladas com a adoção de conceitos unitários.

Assim, chega-se a afirmar que

> [...] a expressão privacidade provou ser um poderoso grito de batalha retórico, em uma gama de contextos não relacionados e, assim como a emotiva palavra *liberdade*, ela significa tantas coisas diferentes para tantas pessoas distintas que perdeu qualquer conotação legal precisa que um dia poderia ter tido. [74]

Mas além da ampliação da ideia do que seja a intimidade e a vida privada (privacidade) para enquadramento do direito à proteção dos dados pessoais, é necessária uma ampliação dos elementos que compõem a esfera privada. Essa esfera não é mais um espaço de solidão, de individualidade, constituindo-se de novas situações e interesses que podem se apresentar em um ambiente de sociabilidade, como opiniões, preferências,

---

[72] SOLOVE, Daniel J. *Understanding privacy*. Cambridge: Harvard University Press, 2008. p. 171-172. ISBN 978067403507-2.
[73] Ibid., p. 104-105.
[74] Cf. MCCARTHY, J. Thomas. *The rights of publicity and privacy*. 2. ed. Saint Paul: West Group, 2000, § 5.7, apud LEONARDI, op. cit., p. 48-49.

comportamentos, ideias, que se pretende manter o controlo e o seu acesso.

E um terceiro ponto ainda merece ressalva. É que como forma de abarcar a proteção de dados no seio da intimidade e da vida privada, desloca-se o eixo central do privado para o pessoal, mas sem abandono do privado, em atenção aos elementos informacionais inerentes ao pessoal, que podem ser secretos, ou não.

Em um sistema jurídico aberto, um direito ou alguma outra figura jurídica, como ocorre com a privacidade, pode, mantendo a mesma nomenclatura, sofrer alterações no seu sentido, podendo exercer as mais diversas funções, de acordo com o contexto cultural, histórico e social, onde se encontram.[75]

O Brasil firmou em 15 de novembro de 2003 a XIII Cumbre Ibero-Americana de Chefes de Estado e de Governo – Declaração de Santa Cruz de La Sierra –, a qual reconhece no item 45 o direito à proteção de dados como um direito fundamental:

> Estamos também conscientes de que a protecção de dados pessoais é um direito fundamental das pessoas e destacamos a importância das iniciativas reguladoras ibero-americanas para proteger a privacidade dos cidadãos, contidas na Declaração de Antigua, pela qual se cria a Rede Ibero-Americana de Protecção de Dados, aberta a todos os países da nossa Comunidade.[76]

No que tange ao complexo conjunto de previsões constitucionais, por assim dizer indiretas, o art. 5º, inciso X da CFb dispõe que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, sendo assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;".[77] Tal dispositivo apresenta a intimidade e a vida privada como valores eminentemente individual, ao assegurar àquele indivíduo que teve tal direito vilipendiado o direito à indenização.

Mais adiante tem-se o regramento da interceptação de comunicações telefônicas, telegráficas ou de dados no art. 5º, inciso XII.[78]

---

[75] MONTEIRO FILHO, Carlos Edison do Rêgo; CASTRO, Diana Paiva de. Potencialidades do direito de acesso na nova lei geral de proteção de dados (Lei 13.709/2018). In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.) *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 323-345. cit. p. 325. ISBN 978855321663-5.

[76] DÉCIMO TERCEIRO CUMBRE IBERO-AMERICANA DE CHEFES DE ESTADO E DE GOVERNO. *Declaração de Santa Cruz de La Sierra.* Bolívia, 14 e 15 de novembro de 2003. [Consultado 18 fevereiro 2020]. Disponível na internet: <https://www.segib.org/wp-content/uploads/DECLARASAO-STA-CRUZ-SIERRA.pdf>.

[77] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Constituição… op. cit.

[78] Ibid."XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;"

A CFb também prevê um instrumento de proteção, ação constitucional de *habeas data*, prevista no art. 5º, inciso LXXII, que basicamente estabelece uma modalidade de direito de acesso e retificação dos dados pessoais. [79]

Some-se a tais dispositivos o sopesamento que deve operar entre o direito à proteção dos dados pessoais, como decorrência do direito à intimidade com a garantia de liberdade de expressão – art. 5º, inciso IX –, o direito à informação – art. 5º, inciso XIV–, sendo que esse direito inclui o direito ao recebimento de informações de interesse coletivo ou particular dos órgãos públicos – art. 5º, inciso XXXIII –, bem como o direito à obtenção de certidões de repartições públicas – art. 5º, inciso XXXIV –.[80]

Diante dos dispositivos constitucionais citados, assenta-se uma crítica ao constituinte brasileiro. Ao que indica, tal constituinte entendeu que seria possível tratar de forma adequada e suficiente o problema da proteção dos dados pessoais mediante categorias abstratas e genéricas. Ou seja, exemplificando, bastaria se verificar se a informação é essencialmente pública ou privada, se a comunicação é sigilosa ou não. Seria uma avaliação genérica se algo é proibido ou permitido. Daí porque Doneda afirma que se trata de "[...] um sistema baseado em etiquetas, permissões ou proibições para o uso de informações específicas, sem considerar os riscos objetivos potencializados pelo tratamento informatizado das informações pessoais."[81]

Ademais, esse sistema ao mesmo tempo que considera a privacidade como um direito fundamental – no inciso art. 5º, X –, se refere à inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas – no art. 5º, XII –, dando a entender que a proteção seria somente na hipótese de comunicação.[82] Daí porque Ferraz Junior sustenta que a Constituição tutelaria apenas

[79] Ibid. "LXXII - conceder-se-á *habeas data:* a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;"

[80] Ibid. "IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença; XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional; XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado; XXXIV - são a todos assegurados, independentemente do pagamento de taxas: a) o direito de petição aos Poderes Públicos em defesa de direitos ou contra ilegalidade ou abuso de poder; b) a obtenção de certidões em repartições públicas, para defesa de direitos e esclarecimento de situações de interesse pessoal;"

[81] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. op. cit. p. 104.

[82] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Constituição… op. cit.

a comunicação de dados e não os dados em si mesmo, na modalidade de garantia do sigilo.[83] E seguindo esse raciocínio, inexistiria uma garantia de natureza constitucional de inviolabilidade sobre dados armazenados em computador.

O tratamento do tema da informação pessoal de uma maneira dualista, algo permissivo e proibido, e de garantias constitucionais para os dados somente sob a ótica da comunicação, acaba por não refletir a complexidade da matéria, posto que a interceptação ou escuta é apenas parte do problema. Ademais, tal tratamento, leva à interpretação de que o constituinte foi extremamente permissivo com a utilização dos dados pessoais.

Porém, há situações em que o indivíduo é ofendido em sua privacidade de uma maneira indireta, com utilização abusiva de suas informações pessoais existentes em bancos de dados. Sem falar na questão de que hoje somos muitas vezes mais reconhecidos e identificados, verdadeira representação da personalidade, pelos nossos dados pessoais, demonstrando a relação direta entre dados pessoais e personalidade.

Daí porque, sob o ponto de vista constitucional brasileiro, necessária se faz interpretação dos incisos X e XII do art. 5º da CFb, de uma forma mais extensiva e adequada à Sociedade da Informação atual, através da correlação dos direitos relacionados à privacidade e à comunicação de dados, como forma se tutelar a personalidade do indivíduo de uma forma ampla e adequada.

Ressalta-se que tramita no Congresso Nacional brasileiro o Projeto de Emenda Constitucional (PEC 17/2019), já aprovado no Senado Federal, que prevê a inclusão do inciso XII-A no art. 5º da CFb, como um direito fundamental, de forma taxativa, nos seguintes termos: "É assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais."[84]

Assim, diante de tamanha generalidade e abstração no trato da proteção dos dados

[83] FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito da Universidade de São Paulo*, São Paulo, 1993, v. 88, [consultado 14 fevereiro 2020], p. 439-459. cit. p. 447. Disponível na internet: <http://www.revistas.usp.br/rfdusp/article/view/67231/69841>. ISSN 0303-9838. "A distinção é decisiva: o objeto protegido no direito à inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida (liberdade de negação). A troca de informações (comunicação) privativa é que não pode ser violada por sujeito estranho à comunicação."

[84] BRASIL. SENADO FEDERAL – *Proposta de emenda à constituição n.° 17, de 2019.* Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. [Consultado 12 março 2020]. Disponível na internet: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1571776979155&disposition=inline>.

pessoais, fez com que o Código de Defesa do Consumidor – Lei n.° 8.078/90, editado cerca de dois anos depois da CFb – fosse visto como o marco normativo dos princípios de proteção de dados pessoais no direito brasileiro, ao estabelecer no art. 43[85] uma série de direitos e garantias para o consumidor em relação às suas informações pessoais presentes nos bancos de dados e cadastros, adotando uma sistemática fundada nos *Fair Information Principles* em matéria consumerista. Tal texto legislativo trata de forma geral a relação entre consumidor e fornecedor, independentemente do meio que ocorram as relações comerciais, fixando normas sobre responsabilidade civil referente a danos causados ao consumidor por vícios e fato do produto ou serviço, sobre práticas comerciais abusivas e sobre cláusulas contratuais.

Da mesma forma, a Lei Complementar n.° 105/2001, que versa sobre o sigilo das operações, veda o acesso aos dados bancários sem consentimento do titular, salvo hipóteses expressas na lei.[86] Entretanto, tais leis infraconstitucionais constituem apenas dois regimes setoriais de tutela.

---

[85] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. *"D.O.U."* (12-09-1990). [Consultado 20 janeiro 2020]. Disponível na internet: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. "SECÇÃO VI - Dos Bancos de Dados e Cadastros de Consumidores - Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público. § 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores. § 6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor. Art. 44. Os órgãos públicos de defesa do consumidor manterão cadastros atualizados de reclamações fundamentadas contra fornecedores de produtos e serviços, devendo divulgá-lo pública e anualmente. A divulgação indicará se a reclamação foi atendida ou não pelo fornecedor. § 1° É facultado o acesso às informações lá constantes para orientação e consulta por qualquer interessado. § 2° Aplicam-se a este artigo, no que couber, as mesmas regras enunciadas no artigo anterior e as do parágrafo único do art. 22 deste código."

[86] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei Complementar n.° 105, de 10 de janeiro de 2001. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. *"D.O.U."* (11-01-2001). [Consultado 20 janeiro 2020]. Disponível na internet: <http://www.planalto.gov.br/ccivil_03/LEIS/LCP/Lcp105.htm>. "Art. 1º As instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados. § 3º Não constitui violação do dever de sigilo: I – a troca de informações entre instituições financeiras, para fins cadastrais, inclusive por intermédio de centrais de risco, observadas as normas baixadas pelo Conselho Monetário Nacional e pelo Banco Central do Brasil; II - o fornecimento de informações constantes de cadastro de emitentes de cheques sem provisão de fundos e de devedores inadimplentes, a entidades de proteção ao crédito, observadas as normas baixadas pelo Conselho Monetário Nacional e pelo Banco Central do Brasil; III – o fornecimento das informações de que trata o § 2º do art. 11 da Lei nº 9.311, de 24 de outubro de 1996; IV – a comunicação, às autoridades competentes, da prática de ilícitos penais ou administrativos, abrangendo o fornecimento de informações sobre operações que envolvam recursos provenientes de qualquer prática criminosa; V – a revelação de informações sigilosas com o consentimento expresso dos interessados; VI – a prestação de informações nos termos e condições estabelecidos nos artigos 2º, 3º, 4º, 5º, 6º, 7º e 9 desta Lei Complementar. VII - o fornecimento de dados financeiros e de pagamentos, relativos a operações de crédito e obrigações de pagamento adimplidas ou em andamento de pessoas naturais ou jurídicas, a gestores de bancos de dados, para formação de histórico de crédito, nos termos de lei específica."

De grande valia foi o Decreto Federal n.º 7.962/2013[87], que regulamentou o Código de Defesa do Consumidor, no que se refere às contratações no comércio eletrónico, introduzindo disposições jurídicas específicas. Esse Decreto, ressalta no art. 1º, que, no comércio eletrónico, as informações devem ser claras a respeito do produto, serviço e do fornecedor, o atendimento deve ser facilitado ao consumidor, bem como assegurado o direito de arrependimento. E mais adiante no art. 4º, inciso VII é estabelecido que para garantir o atendimento facilitado ao consumidor no comércio eletrónico, o fornecedor deverá utilizar mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor. O não cumprimento de tais obrigações resultará na possibilidade imposição das sanções administrativas, previstas no art. 56 do Código de Defesa do Consumidor, com possibilidade de ajuizamento de ações individuais ou coletivas *(class actions*) de responsabilidade por danos sofridos no âmbito de relações de consumo. Nesse sentido é que Veronese e Cunha afirmam, antes da vigência da LGPD:

> Verifica-se, assim, que o sistema jurídico brasileiro prevê a possibilidade de reparação de danos em relações de consumo decorrentes do incumprimento, pelo fornecedor, do dever de salvaguarda dos dados pessoais e bancários dos consumidores, bem como de aplicação de sanção administrativa por esse facto.[88]

O Marco Civil da Internet, Lei n.° 12.965/2014[89], estabelece a proteção da privacidade (art. 3º, inciso II) e a proteção dos dados pessoais (art. 3º, inciso III), dentre outros, como princípios a serem seguidos. Vários direitos e garantias são estabelecidos no art. 7º aos utilizadores da Internet no Brasil: a inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação (inciso I); a inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei (inciso II); a inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial (inciso III); o não

[87] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Decreto n.° 7.962, de 15 de março de 2013. Regulamenta a Lei n.° 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. *"D.O.U."* (15-03-2013). [Consultado 20 janeiro 2020]. Disponível na internet: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D7962.htm>.

[88] VERONESE, Alexandre; CUNHA, Marcele. Desafios do comércio eletrónico no Brasil: integração vertical entre fornecedores e meios de pagamentos, proteção de dados pessoais e cooperação regulatória internacional*. UNIO – EU Law Journal,* Braga, jul. 2018, v. 4, n. 2, [consultado 18 fevereiro 2020], p. 73-89, cit. p. 84. Disponível na internet: <https://revistas.uminho.pt/index.php/unio/article/view/23/53>. ISSN 2183-3435.

[89] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 12.965, de 23 de abril de 2014. Estabelece princípios garantias, direitos e deveres para o uso da internet no Brasil. *"D.O.U."* (24-04-2014). [Consultado 20 fevereiro 2020]. Disponível na internet: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>.

fornecimento a terceiros de seus dados pessoais, inclusive registo de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei (inciso VII); informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que (inciso VIII): a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais (inciso IX); exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registos previstas nesta Lei (inciso X). O art. 10 relata que a guarda e a disponibilização dos registos de conexão e de acesso a aplicações de internet, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas, sendo que medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais. O art. 11 ressalta que deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registos em qualquer operação de coleta, armazenamento, guarda e tratamento de registos, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional. Haverá ainda aplicação do *caput* do art. 11, se os dados foram coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil (§ 1º) e mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo económico possua estabelecimento no Brasil (§2º). O art. 12 ainda prevê quatro sanções administrativas, aplicadas de forma isolada ou cumulativamente, sem prejuízo das demais

sanções cíveis, criminais ou administrativas. Dessa forma, há possibilidade de cumulação com as penalidades estabelecidas no Código de Defesa do Consumidor.

Porém, Veronese e Cunha afirmavam: "Não obstante, parece claro que as leis citadas não são suficientes para gerar um conjunto normativo pleno e que o Brasil ainda requer uma legislação específica para a proteção dos dados pessoais, em padrões similares àqueles existentes na Europa [...]".[90]

Apenas recentemente, em 2018, foi editada a Lei n.° 13.709 (LGPD brasileira), fixando normas gerais para a proteção de dados, entrando em vigor somente no segundo semestre do corrente ano, no que tange aos dispositivos mais relevantes.

2.2.2 A solução jusfundamental europeia – o artigo 8.º da Carta dos Direitos Fundamentais da União Europeia (CDFUE) como forma de independentização do direito fundamental à proteção de dados pessoais

Na Europa o direito à proteção de dados pessoais já recebe tratamento destacado há cerca de quatro décadas, surgindo nos anos 70. Para tanto, cite-se a Constituição da República Portuguesa, na sua versão original de 1976, dispondo sobre a reserva da intimidade da vida privada e familiar no art. 33º, enquanto a proteção de dados pessoais era elencada no art. 35º.[91] Para tanto, as tradições constitucionais comuns aos diversos Estados-Membros conduziram ao avanço e à solução hoje acolhida CDFUE, esta dotada de força vinculativa em razão do Tratado de Lisboa.

Ressalte-se que fenómeno diverso ocorreu no Brasil, em que a preocupação com o direito à proteção de dados pessoais é incipiente.

A legislação da União Europeia (UE), atualmente, trata o direito de proteção aos dados pessoais como um direito independente, autónomo, do direito à privacidade e fundamental.

Se por um lado a Convenção de Estrasburgo, n.° 108 de 1981, conforme

[90] VERONESE, Alexandre; CUNHA, Marcele. Desafios… op. cit., p. 87.
[91] PORTUGAL. ASSEMBLEIA CONSTITUINTE – Constituição da República Portuguesa. *"D.R."* (10-04-1976) (Versão Original). [Consultado 12 março 2020]. Disponível na internet: <http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=4&tabela=lei_velhas&nversao=1&so_miolo= >.

mencionado no item 2.1., foi um divisor de águas, ao tratar o direito à proteção de dados pessoais como um direito fundamental, por outro, a Carta dos Direitos Fundamentais da União Europeia (CDFUE) foi pioneira em realizar a distinção entre o direito à privacidade à proteção de dados pessoais. Para tanto chegou a tratar cada um dos direitos em artigos distintos. O direito ao respeito pela vida privada e familiar, ou seja, à privacidade, no art. 7°, e o direito à proteção dos dados pessoais no art. 8º.

Dispõem os arts. 7º e 8º, respectivamente:

> Respeito pela vida privada e familiar.
> Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.
>
> Proteção de dados pessoais
> 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
> 2. Esses 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 respeito e de obter a respetiva retificação.
> 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.[92]

Bolesina proclama que o direito à privacidade apareceria no art. 7º, em uma conotação individual, passiva e defensiva, sendo uma forma de evitar intromissões não-desejadas na vida privada e familiar, enquanto que o direito à proteção de dados pessoais, previsto o art. 8º, teria a conotação coletiva, propositiva, dinâmica e ativa, tendo em vista a tutela do processamento de dados pessoais, não apenas de modo individual e direto, quando de maneira coletiva e através das autoridades competentes.[93]

Ou seja, antes mesmo da edição do RGPD, e diferentemente do ordenamento jurídico constitucional brasileiro, já existia previsão legislativa direcionada a vislumbrar o direito à proteção de dados pessoais como um direito autónomo.

Na seara jurisdicional, o Tribunal Constitucional alemão possui julgado paradigmático, quando declarou a inconstitucionalidade parcial da Lei do Censo alemã de 1993, de 25 de março de 1982, ao afirmar que o compartilhamento dos dados pessoais obtidos deveria se destinar exclusivamente para a finalidade de recenseamento,

[92] PARLAMENTO EUROPEU; CONSELHO – Carta dos direitos fundamentais da união europeia. Op. cit.
[93] BOLESINA, op. cit., p. 160.

estatística, não podendo os dados serem cruzados com outros registos públicos para uma finalidade genérica de execução administrativa, como ditava a lei. Nesse julgado o direito à proteção de dados é visualizado como um direito autónomo da personalidade, não recorrendo à dicotomia do público e privado.[94]

Segundo Abreu, para a consagração do direito à proteção de dados com um direito autónomo, inserido como está na CDFUE, no capítulo das liberdades, houve uma tripla influência: as tradições constitucionais comuns aos Estados-membros, os instrumentos de proteção dos direitos humanos de caráter internacional (Tratados e Convenções) e o exercício da atividade jurisprudencial relacionada a eles. Em relação a esta última, mesmo não tendo a Convenção Europeia dos Direitos do Homem (CEDH) feito referência expressa sobre tal direito, o Tribunal Europeu dos Direitos do Homem (TEDH), fez-lo extrair do art. 8º em alguns julgados como: Leander vs. Swiden de 26 de março de 1987 (Processo n.° 9.248/1981), Amann vs. Swizerland de 16 de fevereiro de 2000 (Processo n.° 27.798/95) e Rotaru vs. Romania de 4 de maio de 2000 (Proc. n.° 28.341/1995).[95]

O trato do direito à proteção de dados como um direito autónomo tem sua razão de ser, uma vez que o direito à privacidade não possui o mesmo alcance daquele. Isso pode ser constado porque, além de tutelar a privacidade, ele também ampara direitos como a igualdade, a liberdade (especialmente de escolha) e à não discriminação.

Para o direito da UE, todos os dados pessoais devem ser protegidos, sejam eles passíveis ou não de causar dano à privacidade. Não precisam eles ser íntimos ou privados. A sua construção possui por baliza o conceito de dado pessoal.

Segundo Silveira e Froufe, a autonomia que é conferida à proteção dos dados pessoais relativamente à privacidade é justificada em razão de nem todos os dados possuírem a mesma natureza, tratando-se de um avanço civilizatório densificado pelo RGPD.[96]

Considerar que o direito à proteção de dados é uma mera evolução do direito à

---

[94] BIONI, Bruno Ricardo. *Proteção de dados pessoais...* op. cit., p. 97-99.

[95] ABREU, Joana Covelo de. O mercado único digital e a interoperabilidade administrativa: a proteção dos dados pessoais na articulação entre administrações públicas nacionais e as instituições e órgãos da União Europeia – reflexões prospectivas. In: GOMES, Carla Amado et al. (Coord.) *O direto administrativo nos 30 anos da constituição brasileira de 1988*: um diálogo luso-brasileiro. Lisboa: ICJP/CIDP, 2019. [Consultado 8 maio 2020]. p. 206-242. cit. p. 230. Disponível na internet: <https://www.icjp.pt/sites/default/files/publicacoes/files/ebook_da30anoscb_icjp15mar2019.pdf>. ISBN 978989872236-2.

[96] SILVEIRA, op. cit., p. 20.

privacidade é uma construção dogmática errónea, uma vez que o direito à privacidade funciona sob a lógica da dicotomia entre o público e o privado, enquanto que o direito à proteção de dados não se situa naquela dicotomia, bastando que a informação esteja vinculada a uma pessoa, seja um dado pessoal, para que ser objeto de tutela.[97]

Ademais, o direito à proteção de dados pessoais origina-se posteriormente ao direito à privacidade, e assume particular atualidade nos tempos que correm pois também pode ser intuído como resultado da sociedade da informação. Afinal, este é uma decorrência visível do fenómeno da era digital, em especial a capacidade de coleta, armazenamento e tratamento em massa dos dados pessoais.

Segundo Zanon, enquanto a privacidade estaria voltada para questões em torno da intimidade e da vida privada, em uma lógica passivo-defensiva, conferindo poderes ao titular para obstar ou fazer cessar as intromissões ilegais, a proteção de dados teria por foco os elementos informacionais, em uma lógica ativa-propositiva, atribuindo ao titular poderes de controlar e determinar o grau de uso dos dados pessoais por terceiros.[98]

E nesse ponto, como alicerce da jusfundamentalidade do direito à proteção de dados pessoais e, principalmente, a sua autonomia frente ao direito à privacidade, que se desenvolveram diversos direitos assegurados ao titular e alguns princípios gerais de direito.

Tais princípios comuns têm sua vertente em documento emanado por uma comissão de especialistas reunidos, um Comité Consultivo de Sistemas Automatizado de Dados Pessoais *(Advisory Committee on Automated Personal Data Systems)*, na primeira metade da década de 70, no âmbito do Departamento de Saúde, Educação e Bem-Estar (*Department of Health, Education and Welfare)*, Estados Unidos da América, especificamente na área da saúde, designados pelo Secretário desse órgão, a qual chegou à conclusão da relação direta existente entre a privacidade e os tratamentos de dados pessoais, sendo necessário o estabelecimento de regras de controlo sobre tais informações pessoais.[99]

---

[97] BIONI, Bruno Ricardo. *Proteção de dados pessoais...* op. cit., p. 95.
[98] ZANON, op. cit., p. 67, 147-149.
[99] UNITED STATES OF AMERICA. Records, Computers and The Rights of Citizens – *Report of the Secretary's Advisory Committee on Aumomated Personal Data Systems*. 1973. [Cited 15 march 2020]. Available from internet: <https://aspe.hhs.gov/report/records-computers-and-rights-citizens>. "Under current law, a person's privacy is poorly protected against arbitrary or abusive record-

Essas regras de caráter procedimental fixaram um conjunto de medidas que podia ser visualizado em diversas normativas de proteção de dados pessoais, tornando-se um núcleo comum, denominado *Fair Information Practice Principles.* Esse núcleo comum ganhou expressão como um conjunto de princípios a serem aplicados na proteção de dados pessoais, principalmente com a Convenção 108 de Estrasburgo e as *Guidelines* da Organização para a Cooperação e Desenvolvimento Económico (OCDE), ambas no início dos anos 1980. Rodotà elabora uma síntese destes princípios[100]:

a) Princípio da publicidade ou transparência, uma vez que todo banco de dados deve ser de conhecimento público, seja através da autorização para funcionar, ou envio de relatórios periódicos ou comunicação a uma autoridade;

b) Princípio da exatidão, uma vez que o banco de dados deve corresponder à verdade, possuindo mecanismos de correção e atualização periódica;

c) Princípio da finalidade, segundo o qual todo banco de dados pessoais deve atender à finalidade para qual solicitou a autorização do titular do dado pessoal, como forma de evitar o uso abusivo ou ilegal dos dados;

d) Princípio do livre acesso, segundo o qual o titular tem todo o direito de ter conhecimento dos seus dados constantes no banco, podendo controlá-los, corrigi-los e atualizá-los;

e) Princípio da proteção física e lógica, posto que os dados armazenados devem ser protegidos contra alteração, utilização, acesso e destruição não autorizada.

---

keeping practices. For this reason, as well as because of the need to establish standards of record-keeping practice appropriate to the computer age, the report recommends the enactment of a Federal 'Code of Fair Information Practice' for all automated personal data systems. The Code rests on five basic principles that would be given legal effect as 'safeguard requirements' for automated personal data systems. - There must be no personal data record keeping systems whose very existence is secret. - There must be a way for an individual to find out what information about him is in a record and how it is used. - There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent. - There must be a way for an individual to correct or amend a record of identifiable information about him. - Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data". "De acordo com as leis atuais, a privacidade de uma pessoa é mal protegida contra práticas arbitrárias ou abusivas de manutenção de registos. Por esse motivo, é necessário se estabelecer padrões de práticas de manutenção de registos apropriados à era da computação, sendo que o relatório recomenda a promulgação de um 'Código de práticas justas de informações' Federal para todos os sistemas automatizados de dados pessoais. O Código baseia-se em cinco princípios básicos que teriam efeito legal como 'requisitos de salvaguarda' para sistemas automatizados de dados pessoais. - Não deve haver sistemas de manutenção de registos de dados pessoais cuja existência seja secreta.- Deve haver uma maneira de um indivíduo descobrir quais informações sobre ele estão em um registo e como são usadas.- Deve haver uma maneira de um indivíduo impedir que informações sobre ele, obtidas para um propósito, sejam usadas ou disponibilizadas para outros fins sem o seu consentimento.- Deve haver uma maneira de um indivíduo corrigir ou alterar um registo de informações identificáveis sobre ele. - Qualquer organização que crie, mantenha, use ou divulgue registos de dados pessoais identificáveis deve garantir a confiabilidade dos dados para o uso pretendido e deve tomar precauções para evitar o uso indevido dos dados". (tradução nossa).

[100] RODOTÀ, Stefano. *Repertorio di fine secolo*. Bari: Laterza, 1999. p. 62. ISBN 978884205859-5.

Nesse mesmo período, década de 70, na Grã-Bretanha, o Comité da Privacidade, sob a coordenação de Kenneth Younger, emitiu um relatório com dez princípios em prol da proteção da privacidade, semelhantes aos citados, tendo em vista o risco de tratamento de dados de forma automatizada realizada por empresas privadas. O mesmo ocorreu na Alemanha, quando em 1975 foi publicada a Lei do Estado de Hesse, a primeira lei de proteção de dados pessoais no mundo, com princípios também semelhantes.[101]

Tais princípios, de uma forma fragmentada ou condensada são a coluna vertebral das normas nacionais e internacionais e até de ajustes privados, na tutela direito à proteção dos dados pessoais. É em torno deles que gravita as questões que o próprio ordenamento se depara e deve dar uma resposta satisfatória, solucionando a problemática emergida.

Assim, o surgimento de tais princípios comuns reforça uma inclinação não apenas à autonomia da proteção dos dados pessoais, como também à sua qualificação como um direito fundamental.

[101] BIONI, BRUNO Ricardo; MENDES, Laura Schertel. Regulamento europeu de proteção de dados pessoais e a lei geral brasileira de proteção de dados: mapeando divergências na direção de um nível de equivalência. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.) *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 797-819. cit. p. 807-808. ISBN 978855321663-5.

3. A CONCRETIZAÇÃO LEGISLATIVA DAS DINÂMICAS JUSFUNDAMENTAIS

O direito à proteção de dados pessoais, por ser um direito fundamental, apresenta algumas características:

a) a universalidade, uma vez que todas as pessoas naturais são titulares do direito fundamental à proteção de dados pessoais. A qualidade de ser humano é uma condição bastante para a titularidade dele. Essa universalidade se faz presente, não apenas no polo ativo, mas no polo passivo, uma vez que a obrigatoriedade de respeito a esse direito é direcionada, não apenas ao poder público, mas também aos particulares;

b) a inalienabilidade/indisponibilidade, uma vez que o titular do direito à proteção de dados não pode excluir a possibilidade de o exercer, tanto física, quanto juridicamente, como ocorre com a renúncia ou a transferência a título gratuito ou oneroso. Em decorrência da indisponibilidade, não pode o titular abrir mão dele irrevogavelmente. A doutrina[102] sustenta que a indisponibilidade dos direitos fundamentais se assenta no princípio/valor da dignidade da pessoa humana. A dignidade tem por fundamento a potencialidade de o homem se autodeterminar e de ser livre. Dessa forma, considerando que o indivíduo não pode abrir mão da qualidade humana, também não poderia ser livre para abrir mão de sua dignidade e, consequentemente, do direito nela fundado. Mas isto não implica que não possa o mesmo sofrer limitações, de natureza voluntária ou legal, especialmente quando em confronto com outros direitos ou interesses de igual ou maior estrutura jurídico-valorativa;

c) a historicidade, uma vez que não se tem como compreender o direito à proteção de dados e seu alcance dissociado do contexto histórico. Mendes e Branco ressaltam que "[...] não podem pretender valia unívoca de conteúdo a todo tempo e em todo lugar."[103] Na historicidade assenta-se a sua natureza evolutiva. Em razão desse caráter evolutivo, um mesmo direito pode ter aplicação distinta, de acordo com o momento;

[102] MENDES, op. cit., p. 145.
[103] Ibid., p. 144.

d) a força vinculativa, tendo em vista que as normas de direito infraconstitucional devem ter um caráter conformador ou concretizador do direito fundamental à proteção de dados. Segundo Marineli, seria o que se denomina de vinculação dos poderes públicos, Legislativo, Executivo e Judiciário, e dos particulares nas relações intersubjetivas;[104]

e) de aplicabilidade imediata. Tal característica é encontrada, expressamente, no art. 5º, §1º da CFb[105], art. 18º, n.° 1 da Constituição portuguesa[106] [107] e art. 1º, n.° 3 da Constituição alemã[108]. Em face dessa característica, fica superada a concepção do Estado de Direito formal, quando os direitos fundamentais, dentre eles o direito à proteção de dados, somente ganham expressão quando regulados por lei infraconstitucional, na dependência absoluta de uma intermediação legislativa a fim de produzir efeitos. Até mesmo porque a Constituição é obra do constituinte originário, acima dos poderes constituídos, expressão da soberania popular, onde a dependência à atuação do legislador e à impossibilidade de defesa judicial direta conduziu à degeneração da Constituição democrática de Weimar, abrindo brecha para a implantação do nazismo. Segundo Mendes e Branco "O significado essencial dessa cláusula é ressalvar que as normas que definem direitos fundamentais são normas de caráter preceptivo e não meramente programático."[109] Canotilho assevera que os direitos fundamentais não são meras normas para produção de outras normas, mas sim normas que diretamente regulam de relações jurídicas, ou seja, *norma normata* e não *norma normarum*.[110] Porém, não se pode olvidar, como afirma esse derradeiro autor, que tal aplicabilidade direta é uma

---

[104] MARINELI, Marcelo Rumão. *Privacidade e redes sociais virtuais:* sob a égide da Lei n.° 12.965/2014 - Marco civil da internet. Rio de Janeiro: Lumen Juris, 2017. p. 38. ISBN 978855190053-6.

[105] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Constituição da República Federativa do Brasil. Op. cit.

[106] PORTUGAL. ASSEMBLEIA CONSTITUINTE – Constituição da República Portuguesa. Op. cit. "Artigo 18.º (Força jurídica) 1. Os preceitos constitucionais respeitantes aos direitos, liberdades e garantias são directamente aplicáveis e vinculam as entidades públicas e privadas."

[107] Na República Portuguesa, apenas os direitos, liberdades e garantias e os direitos económicos, sociais e culturais, de natureza análoga aos primeiros, gozam de aplicabilidade direta e automática, o que ocorre com o direito à proteção de dados pessoais, que se encontra dentre os direitos, liberdades e garantias.

[108] ALEMANHA. PARLAMENTO FEDERAL ALEMÃO – Lei Fundamental da República Federal da Alemanha. Tradução: Assis Mendonça. Promulgada (23-05-1949). [Consultado 12 março 2020]. Disponível na internet: <https://www.btg-bestellservice.de/pdf/80208000.pdf>."Artigo 1 [Dignidade da pessoa humana – Direitos humanos – Vinculação jurídica dos direitos fundamentais] (3) Os direitos fundamentais, discriminados a seguir, constituem direitos diretamente aplicáveis e vinculam os poderes legislativo, executivo e judiciário."

[109] MENDES, op. cit., p. 154.

[110] CANOTILHO, op. cit., p. 438.

> normatividade qualificada. Isto quer dizer que determinadas normas de direitos fundamentais exigem, para produzir efeitos plenos e até mesmo adquirir sentido, certa atuação legislativa, devido uma densidade normativa baixa, ou seja, nem sempre de forma automática direitos e garantias previstos nas normas constitucionais transmutam-se em direitos subjetivos e concretos. Nessa senda, Vieira de Andrade vislumbra a aplicabilidade imediata como uma norma princípio, a qual estabelece uma ordem de otimização, com maior eficácia, desde que possível, aos direitos fundamentais.[111]

Portanto, ainda que o direito à proteção de dados pessoais seja dotado de aplicabilidade imediata, capaz de gerar direitos subjetivos, não fica afastada a importância do Poder Legislativo e a regulamentação específica da matéria, a fim de se estabelecerem requisitos e pressupostos para o exercício do direito à proteção de dados. Conforme Marmelstein, trata-se de densificar a norma constitucional, conferindo maior segurança jurídica.[112]

Ademais, sendo o direito à proteção de dados um direito fundamental, é ele dotado da função de proteção perante terceiros, pelo que cabem ao Estado os deveres de regular e de fiscalizar o exercício, assegurando, ainda, a função de liberdade no plano jurídico-subjetivo, ou seja, de o titular poder exercê-lo positivamente (liberdade positiva) e de exigir omissões dos poderes públicos, de forma a evitar agressões lesivas por parte dos mesmos (liberdade negativa).

A elaboração de normas que regulem a matéria pode se dar, ainda que de forma específica, a nível geral ou setorial.

Na União Europeia (UE), a proteção de dados pessoais é regida, de forma geral, pelo Regulamento Geral de Proteção de Dados (RGPD) ou *General Data Protection Regulation* (GDPR).

Já no Brasil, a regulação geral da proteção dos dados pessoais é ditada pela Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n.° 13.709, de 14 de agosto de 2018, além de normas setoriais.

---

[111] ANDRADE, José Carlos Vieira de. *Os direitos fundamentais na constituição portuguesa de 1976*. 5ª ed. reimpressão. Coimbra: Almedina, 2017. p. 256. ISBN 978972404669-3.

[112] MARMELSTEIN, George. *Curso de direitos fundamentais.* 5ª ed. São Paulo: Atlas, 2014, p. 308. ISBN 978852248805-6.

3.1 O Regulamento Geral sobre a Proteção de Dados na União Europeia e a sua influência no ordenamento jurídico brasileiro

Anteriormente ao RGPD, a proteção de dados pessoais, na UE, era regida pela Diretiva 95/46/CE.

As Diretivas vinculam o Estado-Membro destinatário quanto ao resultado a alcançar, deixando, no entanto, às instâncias nacionais a competência quanto à forma e aos meios, conforme o art. 288º do Tratado sobre o Funcionamento da União Europeia (TFUE)[113]. A Diretiva assenta na dinâmica de ter de ser transposta para o direito interno dos diversos Estados-Membros, determinando que seja a legislação nacional a aplicável aos casos concretos. Tal determina que o efeito dela decorrente seja o de uma harmonização do direito aplicável – os Estados vinculam-se quanto aos fins a atingir, que terão de ser iguais; mas têm liberdade quanto aos meios para os atingir.

No dizer de Bioni e Schertel Mendes: "[a] diretiva consistia em orientações de como os países membros da União Europeia deveriam formular suas respectivas leis nacionais, havendo, por conseguinte, bastante espaço para variação jurídica por cada um dos países membros."[114]

Porém, com o surgimento de novos riscos, tornou-se necessária a elaboração de uma nova norma, a fim de promover a segurança jurídica, o desenvolvimento económico, assegurando aos titulares dos dados pessoais o efetivo controlo destes.

Segundo Moniz, a Diretiva teria sido atingida pelo "desafio de conexão regulatória", "problema de ritmo" ou "dilema de Collingridge".[115]

Essa legislação deve ser capaz de enfrentar as novas questões levantadas pela economia digital e a propagação das tecnologias da informação e da comunicação de uma maneira isonômica entre os diferentes Estados-Membros da União.[116]

Quanto ao seu objetivo, o Considerando 2 do RGPD menciona que este visa "[...]

---

[113] UNIÃO EUROPEIA – Tratado sobre o funcionamento da união europeia. Op. cit.

[114] BIONI, BRUNO R.; MENDES, Laura Schertel. Regulamento europeu… op. cit., p. 804.

[115] MONIZ, Graça Canto. Finalmente: coerência no âmbito de aplicação do regime da União Europeia de proteção de dados pessoais! O fim do enigma linguístico do artigo 3.º, n.º 2 do RGPD. *UNIO – EU Law Journal*, Braga, jul. 2018, v. 4, n. 2, [consultado 18 fevereiro 2020], p. 119-131, cit. p. 125. Disponível na internet: <https://revistas.uminho.pt/index.php/unio/article/view/25/57>. ISSN 2183-3435. (tradução nossa). No original: *"challenge of regulatory connection", "pacing problem", "Collingridge dilemma").*

[116] MACHADO, op. cit., p. 7.

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."[117]

Assim, o RGPD nasce como peça fundamental para as políticas públicas de promoção de um Mercado Único Digital, ou seja, o qual tem em vista garantir a livre circulação de pessoas, serviços e bens no mundo digital, resguardando a concorrência leal e a proteção dos consumidores e dos seus dados pessoais, assegurando, ainda, a Europa como líder mundial na economia digital.[118] Nesse sentido, o Mercado Único Digital passa a ser visto como interesse público primário.[119]

É patente, dentre os objetivos, a preocupação de o Regulamento compatibilizar a proteção daquele direito fundamental com o progresso económico e social, possibilitando a consolidação e a convergência das economias internas, conforme o Considerando 2.[120] E isto é essencial, uma vez que, na sociedade tecnológica, a cada dia, surgem desafios às figuras jurídicas como a Inteligência Artificial, a *Blockchain* ou as Criptomoedas. Sem falar do aumento estratosférico do fluxo de dados, não apenas entre indivíduos e empresas, mas também entre países.

A existência de uma norma regulando a questão confere segurança jurídica a todas as relações económicas, entre os atores sociais, pessoas físicas ou jurídicas, posto que deixa claro o que é permitido, o que é proibido, a responsabilidades, os danos e as sanções, proporcionando o surgimento e o desenvolvimento de tais relações.

Tal preocupação com a segurança vai ao encontro à crítica de que uma regulamentação da matéria comprometeria os negócios que dependem dos dados pessoais.

---

[117] PARLAMENTO EUROPEU; CONSELHO. Regulamento (EU) 2016/679 … op. cit.

[118] LOPES, Tereza Vale. Responsabilidade e governação das empresas no âmbito do novo regulamento sobre a proteção de dados. *Anuário da Proteção de dados 2018.* Lisboa: CEDIS, 2018. [Consultado 20 março 2020]. p. 45-69. cit. p. 46. Disponível na internet: <http://cedis.fd.unl.pt/wp-content/uploads/2018/04/ANUARIO-2018-Eletronico.pdf>. ISBN 978972993995-2.

[119] ABREU, Joana Covelo. O mercado único digital como o novo mundo para a união europeia: repercussões na estrutura regulatória social e institucional – a redefinição do serviço universal e do organismo de reguladores europeus das comunicações eletrónicas (ORECE). *UNIO – EU Law Journal,* Braga, jul. 2018, v. 4, n. 2, [consultado 18 fevereiro 2020], p. 59-72, cit. p. 60. Disponível na internet: <https://revistas.uminho.pt/index.php/unio/article/view/20/52>. ISSN 2183-3435.

[120] PARLAMENTO EUROPEU; CONSELHO. Regulamento (EU) 2016/679… op. cit. "Considerando o seguinte: [...] (2) Os princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente o direito à proteção dos dados pessoais. O presente regulamento tem como objetivo 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."

Conforme leciona Lima:

> [e] é exatamente nesse sentido que tem seguido o GDPR, que apresenta como objeto a proteção de dados pessoais em geral, propiciando aos titulares integral controle e entendimento sobre o que está sendo realizado com seus dados pessoais (em todo ciclo da vida, que se inicia com a coleta, passa pelo uso, compartilhamento e armazenamento, encerrando-se com a exclusão), sem que isso impacte negativamente os novos modelos de negócios.[121]

Dessa forma, a UE adotou o RGPD, de 27 de abril de 2016, publicado em 4 de maio do mesmo ano e aplicável desde 25 de maio de 2018.

Segundo Silveira e Froufe:

> [o] RGPD não introduz, portanto, uma ilusão. O silêncio e a inatividade deixam (mesmo) de ser considerados consentimentos válidos, sendo necessária uma ação afirmativa clara para manifestar o consentimento ao tratamento dos dados. Como vivemos em sociedades democráticas, cumpre ao titular dos dados atribuir a esse consentimento a relevância (ou, ao contrário, a ligeireza) que considere compatível com o exercício dos seus direitos – recorde-se, fundamentais.[122]

Pelo fato de o referido texto normativo possuir a natureza jurídica de Regulamento, detém caráter geral e obrigatório em todos os seus elementos e é aplicável diretamente em todos os Estados-Membros, conforme o mesmo art. 288º do TFUE[123]. É geral por não individualizar destinatários; obrigatório por impor as suas disposições a todos, indivíduos, União Europeia e suas instituições e Estados-Membros e suas entidades públicas; e aplicável diretamente, posto que naquelas situações em que o regulamento é um ato legislativo completo e perfeito, em que não há necessidade de intervenção dos Estados-Membros para efetivar a sua transposição, os seus efeitos jurídicos fazem-se sentir direta e automaticamente. É dispensável qualquer ato de recepção nacional do regulamento no ordenamento jurídico dos Estados-Membros e, não está dependente, em princípio, de medidas complementares de execução. Portanto, um Regulamento tem aplicabilidade direta e, em regra, aplicabilidade imediata. Na data da sua entrada em vigor, o regulamento é automaticamente incorporado no direito interno, enquanto Regulamento.[124]

---

[121] LIMA, Caio César Carvalho. Objeto, Aplicação material e Aplicação territorial. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords.) *Comentários ao GDPR:* Regulamento Geral de Proteção de Dados da União Europeia. São Paulo: Thomson Reuters Brasil, 2018. p. 23-36. cit. p. 25-26. ISBN 978855321230-9.

[122] SILVEIRA, op. cit., p. 19.

[123] UNIÃO EUROPEIA – Tratado sobre o funcionamento da união europeia. Op. cit.

[124] CAMPOS, João Mota de; CAMPOS, João Luís Mota de; PEREIRA; António Pinto. Manual de Direito Europeu. Coimbra: Coimbra Editora, 214. p. 313 e ss. apud FREITAS, Pedro Miguel. Regulamento geral de proteção de dados: uma visão portuguesa sobre o

O aperfeiçoamento da legislação Europeia sobre a proteção de dados pessoais gerou impactos em todo o mundo. Tal impacto deve-se ao fato de que o Regulamento não se aplicar somente às empresas europeias, mas a todas que tratam dados pessoais de pessoas naturais que se encontrem no território europeu no instante da coleta ou ainda que ofereçam serviços a tais pessoas.

Conforme leciona Cots e Oliveira, nesse cenário tem-se uma situação de marginalização na qual o Brasil se encontraria, com a diminuição da competitividade das empresas brasileiras no cenário internacional, verdadeiro isolamento jurídico, caso não fossem tomadas as medidas necessárias a fim de se tornar um país mais confiável, em termos de segurança jurídica.[125]

Não se pode negar que casos concretos como o da Cambridge Analytica*,* que pode ter mudado o resultado das eleições nos Estados Unidos da América diante do tratamento indevido de dados pessoais, também contribuíram para a aprovação da LGPD brasileira, mas nenhum deles se compara com a edição do Regulamento europeu.

Assim, projetos de lei, que se arrastavam, sofreram verdadeira alavancagem até a edição da LGPD. A génese das leis gerais de produção de dados se confunde com a agenda de padronização das normas, como forma de se obter textos normativos nacionais e transnacionais que sejam convergentes e não restrinjam o fluxo de informações entre países, assegurando a proteção dos dados.

Embora a questão aparentemente tenha um foco económico, a regulação do setor serve à proteção da privacidade, liberdade, igualdade das pessoas, em uma época de crescente processamento de dados, compartilhamento de informações, inteligência artificial, com surgimento de redes sociais, bancos de dados e digitalização de dados que se encontravam em papel.

Tendo em vista a inegável influência do RGPD sobre LGPD, o que conduziu a semelhanças em diversos pontos, há também diferenças entre os regimes jurídicos, sendo uma das mais relevantes a técnica legislativa utilizada.

---

regime sancionatório*. UNIO – EU Law Journal,* Braga, jul. 2018, v. 4, n. 2, [consultado 18 fevereiro 2020], p. 113-118, cit. p. 114. Disponível na internet: <https://revistas.uminho.pt/index.php/unio/article/view/24/56 >. ISSN 2183-3435.

[125] COTS, op. cit., p. 25-26.

Em termos quantitativos, o RGPD é um texto normativo mais consolidado, fruto de uma longa trajetória europeia na busca da proteção dos dados pessoais, com 173 considerandos interpretativos e 99 artigos, enquanto a LGPD possui apenas 65 artigos, sem nenhum considerando interpretativo.

A verificação da convergência entre os dois textos normativos somente pode ser alcançada, não sob uma visão quantitativa, mas qualitativa, incidente sobre a racionalidade regulatória que orienta cada um deles.

Sob esse prisma, a convergência se faz presente em três pontos: os princípios enumerados, onde se incluem práticas justas e direitos dos titulares; no modelo de proteção anterior *ex ante;* o papel central da *accountability*.[126] Acrescenta-se ainda o sistema de *enforcement,* ainda que forma mais genérica.

Os princípios descritos na lei brasileira são fruto de um reconhecimento transfronteiriço sobre os princípios que ditam a matéria, além, é claro, do RGPD. No art. 6º da LGPD[127] constam diversos princípios, os quais visam estabelecer marcos para os dispositivos legais, diversos deles abertos, sendo que a interpretação somente será efetivada aquando da aplicação. Além de todos os princípios do RGPD (licitude, lealdade, transparência, limitação da finalidade, minimização dos dados, limitação da conservação, exatidão, integridade, confidencialidade e responsabilidade), a LGPD ainda prevê mais três nos incisos: prevenção, segurança e não discriminação, o que demonstra a preocupação da Lei com aspectos de natureza contemporânea e novas demandas sociais, em razão de possibilidade discriminatória decorrente de decisões automatizadas.[128] Em

[126] BIONI, BRUNO R.; MENDES, Laura Schertel. Regulamento europeu…, op. cit., p. 805.

[127] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 13.709… op. cit. "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - qualidade dos dados: 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; VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - segurança: 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; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: 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."

[128] BIONI, BRUNO R.; MENDES, Laura Schertel. Regulamento europeu… op. cit., p. 808.

destaque, ainda, o princípio da boa-fé no *caput* do citado artigo, seguindo a tradição do direto civil germânico de controlo de situações partindo de parâmetros objetivos.

No que tange aos direitos dos titulares, existe também uma forte convergência, fruto da influência, como em relação aos direitos de acesso, de notificação, de retificação, de cancelamento e de portabilidade, este último uma novidade em ambos os sistemas. A coincidência ocorre até no número do capítulo em que tais direitos são regulados. Em ambas as normas é o capítulo III. Mas não se pode negar que o direito de oposição é mais amplo no RGPD, por assegurar a possibilidade de oposição à comercialização direta dos dados pessoais nos termos do art. 21, n.^{os} 2 e 3[129]. Já em relação às decisões automatizadas, ambas as normas asseguram o direito de explicação e de auditoria, quando a decisão afetar os interesses do titular. Porém, a possibilidade de revisão humana da decisão, presente no art. 23, n.° 3 do RGPD, não é mais assegurada na LGPD, tendo em vista a exclusão da expressão "por pessoa natural" no art. 20, alteração prevista pela Lei n.° 13.853/2019[130]. Da mesma forma, outra divergência, em relações às decisões automatizadas, seria a de que, na LGPD, os dados pessoais referentes ao exercício de um direito não podem ser utilizados em seu prejuízo, conforme o art. 21, dispositivo que não consta, expressamente, no RGPD. A possível existência de um direito ao esquecimento é previsto, ao menos em nomenclatura, expressamente, no art. 17 do RGPD[131], não constando de forma expressa na LGPD. Assim, as diferenças não são marcantes.

O modelo *ex ante* de proteção dos dados pessoais é seguido por ambas as normas, uma inovação do RGPD, adotada pela LGPD, tendo por fundamento que não existem mais dados pessoais irrelevantes, diante da potencial violação aos direitos fundamentais. Dessa forma, dados pessoais somente podem ser tratados desde que haja uma causa jurídica legal, as quais, para o RGPD, estão dispostas no art. 6º[132], em um número total de

---

[129] PARLAMENTO EUROPEU; CONSELHO. Regulamento (EU) 2016/679… op. cit.

[130] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 13.853, de 08 de julho de 2019. Altera a Lei n.° 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. *"D.O.U."* (20-12-2019). [Consultado 20 fevereiro 2020]. Disponível na internet: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm>.

[131] PARLAMENTO EUROPEU; CONSELHO. Regulamento (EU) 2016/679… op. cit.

[132] PARLAMENTO EUROPEU; CONSELHO. Regulamento (EU) 2016/679… op. cit. "Artigo 6º Licitude do tratamento. 1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações: a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas; b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados; c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que

seis, enquanto na LGPD elas totalizam dez, previstas no art. 7º[133] (a que acrescem as bases de licitude de tratamento de dados especialmente sensíveis, constantes no art. 9º, n.° 2 do RGPD e art. 11, incisos I e II da LGPD). Quanto à base legal conferida à administração pública, tem-se uma distinção das normas, uma vez que o art. 7º, inciso III da LGPD autoriza apenas para fins de políticas públicas, mas que pode ter sua base jurídica alargada pelo disposto no art. 23[134].

Em relação à *accountability,* prestação de contas, que se faz presente no RGPD europeu e na LGPD brasileira, Bioni e Mendes afirmam: "[n]a linha da GDPR, a lei brasileira previu o princípio da *accountability,* ao lado dos relatórios de impacto à proteção de dados pessoais, selos e códigos de boas condutas."[135] Tal assertiva pode ser constatada, respectivamente, nos art. 6º, inciso X, art. 5º, inciso XVII, art. 33, inciso II, "d" e art. 50, todos da LGPD[136]. Em ambos dos sistemas não é necessária a comunicação de todas e quaisquer atividades de tratamento às autoridades responsáveis pela fiscalização. Um dos mecanismos criados é o Relatório de Impacto à Proteção de Dados Pessoais (RIPDP), que o controlador deve obrigatoriamente efetuar quando houver alto risco,

está investido o responsável pelo tratamento; f) O tratamento 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."

133 BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 13.709… op. cit. "Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei n.° 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente."

134 Ibid. "Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei n.° 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que: [...]"

135 BIONI, BRUNO R.; MENDES, Laura Schertel. Regulamento europeu… op. cit., p. 814.

136 BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 13.709… op. cit. "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] X - responsabilização e prestação de contas: 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. [...] Art. 5º Para os fins desta Lei, considera-se: [...] XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco; [...] Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos: [...] II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de: [...] d) selos, certificados e códigos de conduta regularmente emitidos; [...] Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais."

sendo que o RGPD somente exige a comunicação à autoridade quando a atividade implicar em risco elevado para os titulares dos dados, que não pode ser mitigado pela tecnologia disponível e pelos custos da implementação, devendo aguardar o responsável a autorização da autoridade para prosseguir ao processamento.[137] Ademais, o RGPD estabelece quando o relatório é obrigatório e em que momento deve haver comunicação com a autoridade fiscalizadora. Nesse ponto, Silveira e Froufe são enfáticos no sentido de que o RGPD

> [...] introduz uma obrigação de notificação à autoridade de controlo, o mais tardar no prazo de 72 horas, quando a violação de dados for suscetível de implicar um risco para os direitos e liberdades individuais, obrigando a que se informe o titular dos dados acerca da violação. Este aspeto reforça muitíssimo a proteção comparativamente com o regime anterior, já que só os prestadores de serviços de comunicações eletrónicas, os operadores de serviços essenciais e os prestadores de serviços digitais é que estavam obrigados a notificar violações de dados ao abrigo das diretivas em vigor.[138]

A LGPD, apesar de prever o relatório de impacto à proteção de dados pessoais, no art. 5º, inciso XVII[139], não o torna obrigatório, previamente, para atividades de alto risco, como exige o RGPD, podendo apenas ser exigido, posteriormente, pela autoridade nacional de proteção. Ademais, o texto normativo brasileiro não fixa quais os casos ele deve ser exigido e quais seriam as atividades de alto risco, sendo necessária uma regulamentação futura. Mas apesar de algumas diferenças na operacionalização, percebe-se a semelhança estrutural e a influência do RGPD na Lei brasileira.

Em relação ao sistema de *enforcement,* o RGPD baseia-se em uma autoridade de controlo independente, que deverá manter padrões de aplicação do texto, com funções fiscalizatória, consultiva, decisória e sancionatória. A independência da citada autoridade é consagrada nos Considerandos 121, 123, 125 e 129. A LGPD brasileira, seguindo postura semelhante, criou a Autoridade Nacional de Proteção de Dados (ANPD) que, após veto

---

[137] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit. "Considerando o seguinte: [...] (84) A fim de promover o cumprimento do presente regulamento nos casos em que as operações de tratamento de dados sejam suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo seu tratamento deverá encarregar-se da realização de uma avaliação de impacto da proteção de dados para determinação, nomeadamente, da origem, natureza, particularidade e gravidade desse risco. Os resultados dessa avaliação deverão ser tidos em conta na determinação das medidas que deverão ser tomadas a fim de comprovar que o tratamento de dados pessoais está em conformidade com o presente regulamento. Sempre que a avaliação de impacto sobre a proteção de dados indicar que o tratamento apresenta um elevado risco que o responsável pelo tratamento não poderá atenuar através de medidas adequadas, atendendo à tecnologia disponível e aos custos de aplicação, será necessário consultar a autoridade de controlo antes de se proceder ao tratamento de dados pessoais."

[138] SILVEIRA, op. cit., p. 19.

[139] BRASIL. PRESIDÊNCIA DA REPÚBLICA– Lei n.° 13.709... op. cit.

por vício de iniciativa e recriação pela Medida Provisória 869/2018, foi finalmente estabelecida pela Lei n.° 13.853/2019[140], através dos arts. 55-A a 55-L, como órgão da administração pública federal integrante da Presidência da República, mas em caráter transitório, podendo ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial vinculada à Presidência da República. Ou seja, a natureza jurídica do órgão ainda não está definida, havendo um certo comprometimento na sua independência, ainda que resguardada a sua autonomia técnica e decisória.

Destarte, o RGPD incentivou e norteou a criação desse novo regime de proteção nacional brasileiro, descrito na LGPD, legislação essa essencial para permitir a interoperabilidade entre os sistemas, possibilitando o reconhecimento de país "adequado", fundamental à proteção de dados em âmbito nacional e transnacional e ao livre fluxo de dados entre o Brasil e os Estados-Membros da União Europeia.

3.1.1 Âmbito de aplicação

O RGPD tem por objeto a proteção dos dados pessoais de uma maneira geral em todas as fazes de tratamento, que vão desde a coleta, o armazenamento, o uso, compartilhamento até a exclusão desses dados, assim como outros direitos fundamentais do indivíduo, *v.g.,* a privacidade, a liberdade, a autodeterminação informativa e a igualdade.

Essa tutela compreende todas as pessoas individuais que se localizem no espaço da União, não importando a nacionalidade ou local de residência, conforme constata-se dos Considerandos 2 e 14, em uma perspectiva jusfundamental. E não poderia ser diferente, pois a proteção de dados tem que ocorrer de forma universal, uma vez que o mundo digital não respeita as fronteiras entre países.

Nesse sentido a lição de Silveira e Froufe que

[140] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 13.853… op. cit.

> [c]umpre, antes de mais, recordar (eis o objetivo deste texto) que o RGPD concretiza as dimensões essenciais de um direito fundamental previsto no art. 8.º da CDFUE que se aplica universalmente a quem estiver no espaço da União. Somente nesta perspetiva jusfundamental é que o RGPD pode ser completamente percecionado: 'todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhe digam respeito'.[141]

No que tange ao polo passivo da relação obrigacional, comparando-se com a Diretiva vigente anteriormente, ampliaram-se os destinatários, a fim de abarcar, além do responsável, o subcontratante. O subcontratante, operador ou *processor* é um terceiro que realiza a atividade de tratamento de dados pessoais em nome de um responsável, sendo que este delega contratualmente, parte ou a totalidade das operações de tratamento, como o que ocorre no fornecimento de serviço de computação em nuvem.[142] Portanto, vislumbra-se dois requisitos para o reconhecimento da qualidade de subcontratante: ser pessoa física ou jurídica distinta e com autonomia em relação ao responsável pelo tratamento dos dados pessoais e realizar o tratamento dos dados em nome do responsável.

No que tange ao âmbito material do Regulamento, está sujeito a ele qualquer tratamento de dados pessoais, em todas as suas fases, total ou parcialmente automatizado, bem como aquele realizado por meio não automatizado contido em ficheiros ou destinado a esses, conforme o art. 2º, n.° 1[143]. Portanto, não importa se é usada ou não a tecnologia da informática ou digital. Por ser o RGPD uma norma geral, ele aplica-se a tratamento de dados relacionados a criança ou adolescente, a relação consumerista, a relação empregatícia, a relação com a internet e demais.

O RGPD, a fim de evitar dúvidas interpretativas, dispõe, no art. 2º, n.° 2[144], a que tratamentos ele não é aplicável:

a) efetuados no exercício de atividades não sujeitas à aplicação do direito da União, como a assuntos referentes à defesa e segurança nacional;

b) efetuados pelos Estados-Membros no exercício de atividades abrangidas pelo

[141] SILVEIRA, op. cit., p. 18.
[142] MACHADO, op. cit., p. 14-15.
[143] PARLAMENTO EUROPEU; CONSELHO. Regulamento (EU) 2016/679 … op. cit.
[144] Ibid. "Artigo 2º (2).O presente regulamento não se aplica ao tratamento de dados pessoais: a) Efetuado no exercício de atividades não sujeitas à aplicação do direito da União: b) Efetuado pelos Estados-Membros no exercício de atividades abrangidas pelo âmbito de aplicação do título V, capítulo 2, do TUE; c) Efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas; d) Efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública."

âmbito de aplicação do título V, capítulo 2, do Tratado da União Europeia, ou seja, segurança e política externa, envolvendo controlo de fronteiras, asilo e emigração.

Essas duas hipóteses devem ser analisadas em conjunto com o Considerando 16[145], uma vez que este avança que fica excluída da aplicação do Regulamento a matéria não sujeita à aplicação do direito da União, como a referente à segurança nacional e a realizada pelos Estados-Membros no exercício de atividades relacionadas com a política externa e de segurança comum da União.

c) realizados por pessoa física no exercício das atividades pessoais ou domésticas, ou seja, o tratamento efetuado para fins pessoais, como listas de contatos, trocas de correspondência, atividades de rede sociais, incidindo, portanto, sobre aqueles com fins profissionais ou comerciais. Mas se o serviço for promovido por terceiros, a esses terceiros, controladores e processadores, se aplicará o Regulamento. O Considerando 18[146] dispõe sobre tal situação de exclusão. Frise-se que, tratando-se de exceção, deve ela ser interpretada de forma restritiva. Assim, o Tribunal de Justiça da União Europeia (TJUE), sob a vigência da Diretiva 95/46/CE, que continha dispositivo semelhante, se manifestou no sentido de que, não se enquadraria na exceção, um circuito interno de TV residencial cuja câmera captava imagens da calçada pública, o que seria diferente em relação a um livro de endereços[147];

d) realizados pelas autoridades com fins de prevenção, investigação, deteção e

[145] Ibid. "Considerando o seguinte: [...] (16) O presente regulamento não se aplica às questões de defesa dos direitos e das liberdades fundamentais ou da livre circulação de dados pessoais relacionados com atividades que se encontrem fora do âmbito de aplicação do direito da União, como as que se prendem com a segurança nacional. O presente regulamento não se aplica ao tratamento de dados pessoais pelos Estados-Membros no exercício de atividades relacionadas com a política externa e de segurança comum da União."

[146] Ibid. "Considerando o seguinte: [...] (18) O presente regulamento não se aplica ao tratamento de dados pessoais efetuado por pessoas singulares no exercício de atividades exclusivamente pessoais ou domésticas e, portanto, sem qualquer ligação com uma atividade profissional ou comercial. As atividades pessoais ou domésticas poderão incluir a troca de correspondência e a conservação de listas de endereços ou a atividade das redes sociais e do ambiente eletrónico no âmbito dessas atividades. Todavia, o presente regulamento é aplicável aos responsáveis pelo tratamento e aos subcontratantes que forneçam os meios para o tratamento dos dados pessoais dessas atividades pessoais ou domésticas."

[147] UNIÃO EUROPEIA. TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA (TJUE). Pedido de decisão prejudicial no processo C - 212/13. 4ª Secção. Data do acórdão: 11.12.2014. [Consultado 20 março 2020]. Disponível na internet: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=160561&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=143990>."35 Por conseguinte, há que responder à questão submetida que o artigo 3.°, n.° 2, segundo travessão, da Diretiva 95/46 deve ser interpretado no sentido de que a exploração de um sistema de câmara que dá lugar a uma gravação vídeo de pessoas, guardada num dispositivo de gravação contínua, como um disco rígido, sistema esse instalado por uma pessoa singular na sua casa de família, para proteger os bens, a saúde e a vida dos proprietários dessa casa, e que vigia igualmente o espaço público, não constitui um tratamento de dados efetuado no exercício de atividades exclusivamente pessoais ou domésticas, na acepção desta disposição."

> repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, que são regulados pela Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, que versa sobre a Proteção dos Dados Destinados às Autoridades Policiais e Judiciais. Esses termos resultam do Considerando 19[148].

Por sua vez, passa-se à análise do âmbito de aplicação territorial e extraterritorial do Regulamento.

O RGPD é aplicável a todos os Estados-Membros da União Europeia e a três países integrantes do Espaço Económico Europeu, Liechtenstein, Noruega e Islândia.

O art. 3º do RGPD[149] tem por pressuposto que o responsável pelo tratamento ou subcontratante tenha alguma ligação com a União Europeia. Essa ligação pode ser decorrente de ali possuir um estabelecimento ou por tratar dados pessoais de titulares aí localizados, sendo as suas atividades direcionadas para os mesmos, para o mercado da União Europeia.

Antes da edição do RGPD, ainda sob a vigência da Diretiva 95/46/CE, o TJUE, ao analisar o caso *Google Spain,* interpretando teleologicamente o artigo 4.º, n.° 1, alínea a) da citada Diretiva, se pronunciou sobre a aplicabilidade das regras da UE em matéria de proteção de dados pessoais, em relação a um responsável pelo tratamento com estabelecimento principal num terceiro país. A Google Inc., empresa-mãe do grupo Google, com sede nos Estados Unidos, foi considerada o responsável pelo tratamento, enquanto a subsidiária, a Google Spain, o estabelecimento daquela empresa-mãe.[150]

De forma mais explícita, segundo o art. 3º, n.° 1 do RGPD, se o estabelecimento, seja do responsável – controlador – ou de um subcontratante – processador – se situar no território da União Europeia, a ele se aplica o Regulamento, independentemente de onde venha a ocorrer o tratamento dos dados pessoais, se dentro ou fora da União

---

[148] PARLAMENTO EUROPEU; CONSELHO. Regulamento (EU) 2016/679 … op. cit. "Considerando o seguinte: [...] (19) A proteção das pessoas singulares em matéria de tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, e de livre circulação desses dados, é objeto de um ato jurídico da União específico. O presente regulamento não deverá, por isso, ser aplicável às atividades de tratamento para esses efeitos. Todavia, os dados pessoais tratados pelas autoridades competentes ao abrigo do presente regulamento deverão ser regulados, quando forem usados para os efeitos referidos, por um ato jurídico da União mais específico, a saber, a Diretiva (EU) 2016/680 do Parlamento Europeu e do Conselho [...]

[149] Ibid.

[150] MONIZ, Graça Canto. Finalmente… op. cit., p. 122.

Europeia, desde que o tratamento seja realizado no contexto das atividades. Neste sentido Silveira e Froufe discorrem:

> [o] âmbito de aplicação territorial do RGPD está, antes de mais, relacionado com a localização do estabelecimento do responsável pelo tratamento de dados ou subcontratante – caso se encontre na União, o tratamento está sujeito ao RGPD independentemente de o tratamento ocorrer dentro ou fora da União.[151]

Em relação ao subcontratante, estes estão vinculados diretamente ao RGPD e às obrigações aí previstas, como: registo das atividades de tratamento, cooperação com a autoridade de controlo, segurança do tratamento, notificação de violação de dados pessoais, designação do encarregado de proteção de dados e transferência de dados pessoais para países terceiros ou organizações internacionais descritas no art. 30.º, n. º 2, art. 31.º, art. 32.º, art. 33.º, n.º 2, art. 37.º e do art. 44.º, todos do RGPD, respectivamente.[152]

Quanto ao que se possa entender por situar-se o estabelecimento no território da União, o Considerando 22 relata que é necessária uma instalação estável, mas é irrelevante tratar-se de uma sucursal ou filial: "[o] estabelecimento pressupõe o exercício efetivo e real de uma atividade com base numa instalação estável. A forma jurídica de tal estabelecimento, quer se trate de uma sucursal quer de uma filial com personalidade jurídica, não é fator determinante nesse contexto."[153]

Portanto, se o responsável ou subcontratante estiverem localizados na União Europeia, mesmo que os dados não estejam armazenados no território da União, aplica-se o RGPD, posto que é uma decorrência lógica que fará tratamento de dados pessoais de titulares localizados na União.

Além do critério da territorialidade, o RGPD prevê a possibilidade de sua aplicação para as hipóteses de extraterritorialidade, ou seja, sua aplicação a empresas que não se localizem no território da União Europeia, prevista no art. 2º, n.^{os} 2 e 3. Aqui o RGPD leva em consideração, como fator de conexão, os destinatários da atividade dos responsáveis pelo tratamento.

---

[151] SILVEIRA, op. cit., p. 18.
[152] MONIZ, Graça Canto. Finalmente… op. cit., p. 126.
[153] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit.

Frise-se, desde já, que é irrelevante que o titular dos dados seja ou não um cidadão europeu, ou que tenha ou não residência na União Europeia, bastando que na União se encontre fisicamente.

Machado ressalta que muito contribui o TJUE para uma interpretação extensiva de aplicação da norma europeia, citando, *v.g.,* o caso Weltimmo.[154]

Nas versões originais, em português e em espanhol do RGPD, constava erro de tradução no art. 3º, n.° 2, posto que dispunha "[...] titulares residentes no território da União [...]", exigência que não existia na versão oficial em inglês, francesa e italiana. Tal exigência conflitava com os Considerandos 2 e 14. Porém, tais erros de tradução foram objeto de retificação, procedendo-se às alterações ao artigo 3º, n.° 2 das versões oficiais portuguesa[155] e espanhola[156], sendo abolida a questão da residência do titular de dados pessoais. Superadas tais divergências, são adotados três critérios:

a) *primus,* que haja oferecimento de serviços ou produtos a titulares dos dados que se encontram na União Europeia, independente do pagamento. A empresa mantém a vinculação indissociável com o território. Porém, é indispensável, nessa hipótese, que haja a intenção, o dolo, de oferecer tal serviço para esses titulares, caso contrário o regulamento incidiria sobre qualquer site comercial estrangeiro que pudesse ser acessado por titular localizado na União Europeia. A fim de se apurar a intenção de oferecimento por parte do estabelecimento na

[154] MACHADO, op. cit., p. 14-15. "No caso Weltimmo, a Corte esclareceu que o conceito de estabelecimento se 'estende a toda atividade real e efetiva — ainda que mínima — exercida mediante uma instalação estável'. Construiu-se aí uma concepção flexível — não formalista — do conceito, válida 'especialmente para as empresas que se dedicam a oferecer serviços exclusivamente pela Internet' [...]No caso descrito, a atividade exercida pela sociedade empresária eslovaca Weltimmo envolvia a exploração de websites de anúncios de imóveis situados na Hungria. Após o período de um mês de fornecimento gratuito de publicidade em torno dos imóveis transacionados por terceiros, a empresa passava então a faturar o serviço e cobrar pagamentos dos anunciantes húngaros, mesmo após requerimento para a exclusão do anúncio e apagamento dos dados pessoais, formulado dentro do mencionado prazo de gratuidade. Além dessas circunstâncias, foram considerados relevantes no exame feito pela CJUE o fato de a empresa haver constituído representante na Hungria e o seu sítio eletrônico utilizar o idioma húngaro para operação das atividades. Ao final, a CJUE decidiu que a empresa responsável pelo tratamento de dados pessoais (e provedora de aplicação de internet) se dedicava a uma atividade real e efetiva no território húngaro."

[155] CONSELHO DA UNIÃO EUROPEIA. Documento n.° 8088/2018, 19 de abril de 2018. *"J.O.U.E."* (23-05-2018), L127/2. [Consultado 25 março 2020]. p. 278. Disponível na internet: <http://data.consilium.europa.eu/doc/document/ST-8088-2018-INIT/en/pdf>. "Na página 33, artigo 3.º, n.º 2 Onde se lê: '2. O presente regulamento aplica-se ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com:', leia-se: '2. O presente regulamento aplica-se ao tratamento de dados pessoais de titulares que se encontrem no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com:'"

[156] Ibid, p. 13. "4) En la página 33, artículo 3, apartado 2: donde dice: '2. El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:', debe decir: '2. El presente Reglamento se aplica al tratamiento de datos personales de interesados que se encuentren en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:'"

hipótese versada, não deve ser considerado apenas um fator, mas a conjugação deles. O Considerando 23[157] revela alguns desses fatores: o oferecimento de produtos ou serviços ou possibilidade de solicitação em língua de um dos Estados-Membros da União; o uso de moeda corrente de um ou mais Estados que fazem parte da União ou até mesmo a referência a utilizadores que se localizem na União. Lima afirma que:

> [...] inclui-se nessa situação o oferecimento de número de telefone com código internacional de um dos países da União, ou a utilização de um dos CCTLD (*Country Code Top Level Domain*) próprios de países europeus (tais como .pt, .fr, .it, .de, entre outros).[158]

Inúmeras situações podem ser pensadas, de acordo com essa primeira hipótese, tanto pela aplicação, como pela exclusão do Regulamento. Pela aplicação tem-se: empresa que, mesmo não estado situada no território da União, adquire anuncio patrocinado a ser apresentado a titular localizado na União; aquisição de um estrangeiro, não residente na União, ao qual lhe é oferecido um plano temporário pela sua operadora natal após já se encontrar em território da União Europeia. Pela não aplicação: cidadão residente na União Europeia que se dirige a empresa estabelecida fisicamente em outro país que não pertence à União, fornecendo os seus dados, com o objetivo de usufruir de algum serviço; contrato com provedor de conexão de internet móvel celebrado entre estrangeiro e empresa sediada no país daquele e que posteriormente o titular estrangeiro viaja para a União Europeia, sendo que essa situação equipara-se a gozo e não a oferta de serviços ou bens; empresa situada fora da União que contrata empresa situada fisicamente na União com fim desta atuar somente como provedor de hospedagem, armazenado dados, ainda que essa atividade esteja ocorrendo na União, posto que entendimento oposto violaria a *ratio* da lei.

b) *secundus,* que exista o controlo do comportamento do titular do dado que esteja na União Europeia. Esse controlo do comportamento corresponde ao

[157] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit. "Considerando o seguinte: [...] (23) O mero facto de estar disponível na União um sítio *web* do responsável pelo tratamento ou subcontratante ou de um intermediário, um endereço eletrónico ou outro tipo de contacto, ou de ser utilizada uma língua de uso corrente no país terceiro em que o referido responsável está estabelecido, não é suficiente para determinar a intenção acima referida, mas há fatores, como a utilização de uma língua ou de uma moeda de uso corrente num ou mais Estados-Membros, com a possibilidade de encomendar bens ou serviços nessa outra língua, ou a referência a clientes ou utilizadores que se encontrem na União, que podem ser reveladores de que o responsável pelo tratamento tem a intenção de oferecer bens ou serviços a titulares de dados na União."

[158] LIMA, op. cit., p. 32.

monitoramento do comportamento pela internet, capaz de realizar o perfil da pessoa, analisando e prevendo as preferências, desempenho profissional, comportamento, saúde, localização e seus atos em geral. Empresas de publicidade digital e de comércio eletrónico estariam incluídas. Nesse sentido, o Considerando 24[159] versa sobre o tema. Para essa hipótese, não basta a mera coleta de dados de titulares localizados na União por *sites* ou aplicativos. Necessário que se estabeleça o *profiling*, cujo conceito é estabelecido no art. 4º, n.° 4 do Regulamento[160]. Machado leciona que

> [a] regra tem ampla aplicação para empresas provedoras de serviços de internet, tais como aplicativos de redes sociais, correio eletrónico e motores de busca, enfim, serviços que de alguma maneira monitoram a atividade online de seus usuários, especialmente para fins publicitários É o caso da publicidade comportamental, na qual são utilizados principalmente cookies.[161]

c) *tertius,* quando o responsável pelo tratamento, embora não presente na União Europeia, esteja em local que se aplica a legislação de um Estado-Membro por força do direito internacional público. O Considerando 25 cita duas hipóteses: missão diplomática e posto consular de Estado-Membro.

Moniz cita dois exemplos, em relação às hipóteses elencadas:

> (1) um nacional de um dos Estados-Membros transmite dados pessoais durante as férias nos EUA a um responsável pelo tratamento estabelecido nesse país – este titular dos dados não está protegido pelo RGPD uma vez que não se encontra no território da UE; (2) um turista chinês, durante as suas férias em Portugal, transmite os seus dados pessoais a um responsável pelo tratamento estabelecido num país terceiro que, através de seu sítio online vende e entrega os seus produtos na UE – este titular dos dados está protegido pelo RGPD desde que sua localização seja no território de um Estado-Membro quando efetua a compra de um produto.[162]

No elo estabelecido entre o responsável ou controlador e o subcontratante ou processador, podem ainda surgir situações que suscitem dúvidas quanto à aplicação do RGPD. Quando responsável e subcontratante possuem estabelecimento na União, é

---

[159] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit. "Considerando o seguinte: [...] (24) [...] A fim de determinar se uma atividade de tratamento pode ser considerada 'controlo do comportamento' de titulares de dados, deverá determinar-se se essas pessoas são seguidas na Internet e a potencial utilização subsequente de técnicas de tratamento de dados pessoais que consistem em definir o perfil de uma pessoa singular, especialmente para tomar decisões relativas a essa pessoa ou analisar ou prever as suas preferências, o seu comportamento e as suas atitudes."

[160] Ibid. "Artigo 4º Definições. Para efeitos do presente regulamento, entende-se por: [...] 4) 'Definição de perfis', qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações;"

[161] MACHADO, op. cit., p. 19.

[162] MONIZ, Graça Canto. Finalmente… op. cit., p. 128.

cristalina a aplicação do regulamento. Mas pode um subcontratante, situado fora da União, ser contratado por responsável com estabelecimento situado na União ou o subcontratante possuir estabelecimento na União, enquanto o responsável está localizado em país que não faz parte da União Europeia.

Na situação em que um subcontrate, situado fora da União, é contratado por responsável com estabelecimento situado na União, a aplicação do RGPD se dará, diretamente, a ele, nas hipóteses do art. 3º, n.° 2 (tratamento realizado em nome do responsável seja relativo a informações de natureza pessoal de residentes na UE para o fornecimento de bens e serviços ou o monitoramento do comportamento dos titulares dos dados) ou indiretamente, diante da vinculação ao responsável em razão da obrigatoriedade do contrato, ou outro ato normativo, pois as regras são aplicáveis à sua atividade, em face o art. 28, n.° 3 do RGPD.[163]

Já quando o subcontratante possui estabelecimento na União, enquanto o responsável está localizado em país que não faz parte da União Europeia, não se fazendo presente, em relação ao responsável, as situações do art. 3º, n.[os] 1 e 2 do RGPD, E. J. Kindt sustenta que aplicação do RGPD a esse responsável não deve se dar em sua totalidade, mas apenas nos limites das normas jurídicas celebradas com o subcontratante, caso contrário, haveria uma sujeição às normas europeias de qualquer empresa responsável no mundo que decida contratar um operador com base na Europa.[164] Nessa seara, acrescenta-se que o sistema internacional é estruturado na não interferência, exigindo instrumentos jurídicos de pactuação entres os Estados, como forma de se obter uma normatização global.

3.1.2 Direitos dos titulares dos dados pessoais

O RGPD, no afã de concretizar o direito fundamental à proteção de dados, direito esse que teve sua autonomia consagrada no art. 8º da CDFUE e art. 16º do TFUE, estabelece diversos direitos específicos aos titulares de dados pessoais. Moniz afirma:

---

[163] MACHADO, op. cit., p. 16.

[164] KINDT, E. J. Why research may no longer be the same: About the territorial scope of the New Data Protection Regulation. *Computer Law and Security Review*, v. 32, n. 5, p. 737, 2016 apud Ibid., p. 16.

> [...] certo é que o direito à proteção de dados é concretizado, em legislação secundária, por uma cartilha de direitos específicos, previstos no RGPD, que outorgam ao titular dos dados as faculdades necessárias para participar e decidir sobre o destino dos seus dados pessoais.[165]

Acolhendo o Regulamento o princípio da autonomia deliberativa, põe-se em destaque a vontade individual, tendo, como consequências, a participação do titular dos dados, com possibilidade de influenciar no tratamento, e a previsão de um rol de direitos, mesmo quando o tratamento não tem por fundamento o consentimento daquele titular.

Assim, o RGPD, além de garantir um grau de uniformização e de segurança bem com maior que a Diretiva 95/46/CE, pela sua própria natureza jurídica, concentrou esforços transparência das operações do tratamento, assegurando aos titulares o amplo conhecimento e exercício dos direitos previstos.

Os direitos dos titulares dos dados estão dispostos no capítulo III do RGPD[166], sendo esse dividido em cinco secções. A primeira secção é composta pelo art. 12º e dispõe sobre "Transparência e regras para o exercício dos direitos dos titulares dos dados". A segunda secção, composta pelos arts. 13º, 14º e 15º, é intitulada de "Informação e acesso aos dados pessoais". A terceira secção é formada pelos arts. 16º a 20º e denominada de "Retificação e apagamento". A quarta secção, composta pelos arts. 21º e 22º, trata do "Direito de oposição e decisões individuais automatizadas". Por fim, a derradeira secção do capítulo III, a quinta, refere-se às "Limitações", que estão dispostas no art. 23º.

Nesse capítulo III, além dos direitos dos titulares, constam também conceitos, regras e princípios.

Pode-se elencar, conforme disposto no Regulamento, oito direitos: de informação; de acesso; de retificação; de apagamento de dados; de limitação de tratamento; de portabilidade; de oposição e, por fim, de objeção quanto a decisões individuais automatizadas.

Antes da análise de cada direito, deve-se discorrer algo sobre a transparência, devido ao elo permanente existente com os direitos que serão expostos.

---

[165] MONIZ, Graça Canto. Direitos do titular dos dados pessoais: o direito à portabilidade. *Anuário da Proteção de dados 2018*, Lisboa: CEDIS, 2018. [Consultado 20 março 2020]. p. 11-34. cit. p. 12-13. Disponível na internet: <http://cedis.fd.unl.pt/wp-content/uploads/2018/04/ANUARIO-2018-Eletronico.pdf>. ISBN 978972993995-2.

[166] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit.

A secção I, do capítulo III do RGPD, versa sobre a transparência e as regras para o exercício dos direitos em geral pelo titular. A transparência, não é propriamente um direito do titular, mas um princípio que se encontra elencado no art. 5º, n.° 1, alínea a), ao dispor que: "1. Os dados pessoais são: a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados ('licitude, lealdade e transparência');"[167] Ou seja, encontra-se o princípio da transparência ao lado dos princípios da licitude e da lealdade, tornando-se aquele aspecto essencial desses dois últimos, ainda que atrelado ao direito da informação.

Segundo Maldonado, "[a] transparência, em uma forma simples de ser compreendida, diz respeito à atuação clara, aberta e honesta sobre quem é responsável pelo tratamento, assim como de que forma e por qual razão serão utilizados os dados pessoais de um determinado titular."[168]

Especificamente, sobre o princípio da transparência vigoram as *Guidelines on Transparency under Relugation 2016/679*[169], editadas pelo antigo "Grupo de proteção das pessoas no que diz respeito a tratamento de dados pessoais" (GT29) ou *Working Party Article 29 (WP29)*, criado pela Diretiva 95/46/CE, a qual foi ratificada pelo atual, Comité Europeu para a Proteção de Dados (CEPD) ou *European Data Protection Board (EDPB),* na primeira reunião, desde que tais *guidelines* não contrariassem o Regulamento. Tais *guidelines* enfatizaram que, embora a transparência não esteja conceituada no RGPD, seus elementos são devidamente mencionados, ressaltando que a informação/comunicação deve ser concisa, inteligível e facilmente acessível. Tais *guidelines* estabelecem como a transparência deve se operar em três faixas, com função interpretativa e de orientação prática: na informação ao titular dos dados; na comunicação realizada entre o responsável pelo tratamento e o titular dos dados; e quanto às regras para que o titular possa exercer os direitos como um todo de maneira facilitada. Seria a transparência uma expressão do princípio da equidade na seara do

[167] Ibid.

[168] MALDONADO, Viviane Nóbrega. Direitos dos titulares dos dados. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords.) *Comentários ao GDPR:* Regulamento Geral de Proteção de Dados da União Europeia. São Paulo: Thomson Reuters Brasil, 2018. p. 85-109. ISBN 978855321230-9.

[169] GRUPO DE PROTEÇÃO DAS PESSOAS NO QUE DIZ RESPEITO A TRATAMENTO DE DADOS PESSOAIS (GT29). *Guidelines on Transparency under Relugation 2016/679.* [Consultado 10 fevereiro 2020]. Disponível na internet: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227>.

processamento dos dados pessoais, prevista no art. 8º da CDFUE[170]. Assim, percebe-se que a transparência visa assegurar ao titular a compreensão de todo o processo, gerando uma confiança no sistema que afetam os cidadãos em geral, possibilitando, a eles, a defesa e proteção dos seus dados.

Como decorrência desse princípio, em relação às informações prestadas e à comunicação realizada entre o responsável pelo tratamento e o titular dos dados, devem estas, segundo o art. 12º, n.° 1 do RGPD[171], serem realizadas de forma concisa, transparente, inteligível e de fácil acesso, com uma linguagem clara e simples, especialmente quando informações forem direcionadas a crianças. Tal informação pode ser por escrito, meio eletrónico, ou mesmo oralmente, esta última se solicitada pelo titular, após comprovada a sua identidade. Quando um titular solicitar uma informação, o responsável pelo tratamento não pode se recusar, exceto não se estiver em condições de fazer a identificação do titular (art. 12º, n.° 2 do RGPD) ou de confirmar a titularidade do postulante, sendo que, nessa derradeira hipótese, pode solicitar que lhe sejam fornecidas as informações adicionais que forem necessárias para confirmar a identidade do titular dos dados (art. 12º, n.° 6 do RGPD)[172].

O responsável tem obrigação de fornecer as informações sem demora, observado o prazo máximo de um mês, podendo prorrogar-se por até dois meses, devendo, porém, nessa última hipótese, comunicar ao postulante o motivo demora, ainda no prazo do primeiro mês (art. 12º, n.° 3 do RGPD). O descumprimento implicará na possibilidade de representação perante um órgão de controlo ou ação judicial.[173]

Em regra, as informações, comunicações e medidas pleiteadas são gratuitas, salvo se os pleitos forem manifestamente infundados ou excessivos, estes pelo fato de serem repetitivos (art. 12º, n.° 5 do RGPD). Pode, contudo, o responsável, ao invés de cobrar pelo serviço, denegar o atendimento ao pleito.[174]

Na segunda Secção do capítulo III do RGPD[175], composta pelos arts. 13º a 15º, têm-

[170] PARLAMENTO EUROPEU; CONSELHO – Carta dos direitos fundamentais da união europeia. Op. cit.
[171] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit.
[172] Ibid.
[173] Ibid.
[174] Ibid.
[175] Ibid.

se os direitos à informação e de acesso. Para tanto, essa segunda secção divide-se em três partes: o art. 13º regulando as informações a serem concedidas quando os dados foram obtidos perante o titular; o art. 14º regrando às informações quando os dados não foram obtidos com o titular; e o art. 15º regulando o direito de acesso do titular aos seus dados.

Quando os dados forem obtidos perante o titular, o n.° 1, do art. 13º do RGPD[176] trata sobre a necessidade de informação: da identidade e dos contatos do responsável pelo tratamento e do encarregado de proteção; das finalidades do tratamento; dos destinatários ou a categoria de destinatários; das garantias apropriadas ou adequadas e aos meios de obter cópia ou onde foram disponibilizadas, nas hipóteses de transferências internacionais (para terceiro país ou organizações internacionais). Já o n.° 2 versa sobre as informações adicionais, em atenção à transparência, como as referentes: ao prazo de conservação dos dados pessoais; à existência do direito de acesso aos dados pessoais que lhe digam respeito; à sua retificação ou ao seu apagamento; à limitação do tratamento ou de se opor ao tratamento; à portabilidade dos dados; à retirada do consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado; à apresentação de reclamação a uma autoridade de controlo; à comunicação de que os dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados; à existência de decisões automatizadas, inclusive a definição de perfis. Por fim, o n.° 3 dispõe sobre a obrigatoriedade prévia da informação ao titular quando responsável pelo tratamento tiver a intenção de proceder ao tratamento posterior dos dados pessoais, para fins diversos daquele para o qual os dados tenham sido recolhidos, enquanto que o n.° 4 do art. 13º do RGPD dispensa a informação quando o titular já tiver conhecimento.

Quando os dados não forem obtidos perante o titular, o art. 14º da LGPD[177] exige, além das informações dispostas no art. 13º, citadas no parágrafo anterior, a informação da origem dos dados pessoais e se eles provêm de fontes acessíveis ao público. Para tanto, o item 3 do art. 14º estabelece qual o prazo que o responsável pelo tratamento

[176] Ibid.
[177] Ibid.

dispõe para comunicação dessas informações, já que os dados não foram obtidos diretamente perante o titular. Será no prazo razoável a contar da obtenção, não superior a um mês ou momento da primeira comunicação ao titular dos dados, quando a obtenção tiver essa finalidade de comunicação, ou até a primeira divulgação desses dados, quando estiver prevista a divulgação dos dados a terceiro. Semelhante ao que ocorre com relação aos dados obtidos perante o titular, que não se aplica a regra da obrigatoriedade no fornecimento das informações, quando o titular dos dados já tiver conhecimento, o art. 14º, n.° 5 do RGPD, além dessa hipótese, prevê a dispensa da informação quando: reste comprovada a impossibilidade de disponibilizar a informação; o esforço envolvido seja desproporcionado; a obtenção ou divulgação dos dados esteja prevista no direito da União ou do Estado-Membro; ou os dados pessoais devam permanecer confidenciais em virtude de uma obrigação de sigilo profissional regulamentada pelo direito da União ou de um Estado-Membro, inclusive uma obrigação legal de confidencialidade.[178]

Segundo Maldonado, o Regulamento busca prestar as informações necessárias ao titular dos dados, independente de requerimento, logo no início do tratamento, que se dá quando do recolhimento, sendo ele obtido diretamente com titular ou através de terceiro.[179]

A tutela efetiva do direito ao controlo dos dados pessoais pelo titular está em uma relação diretamente proporcional como a efetividade do direito de acesso.

Os direitos de informação e de acesso constituem o núcleo da proteção de dados pessoais, uma vez que são indispensáveis para que o titular possa exercer os demais direitos, permitindo a identificação dos dados conhecidos por terceiros, os usos, a licitude do tratamento, a veracidade e a qualidade daqueles dados.[180]

Mas para que esse direito de acesso se efetive, obstáculos devem ser transpostos pelo legislador. Rodotà elenca as causas predominantes do parco exercício desse direito de acesso: sob o aspecto do procedimento ter-se-ia os custos financeiros e o tempo despendido, a carência de alfabetização, a falta de informação e o desnível financeiro e técnico entre os titulares e os responsáveis pelo tratamento; sob o aspecto do

[178] Ibid.
[179] MALDONADO, Viviane Nóbrega. Direitos dos titulares… op. cit., p. 97.
[180] MONIZ, Graça Canto. Direitos do titular dos dados pessoais… op. cit., p. 16.

funcionamento do acesso, corresponde à pouca utilidade das informações, quando se desconhece o sistema de tratamento; sob o aspecto do âmbito de incidência do acesso, correspondente ao excesso de vedações ao acesso de acordo com a categoria das informações.[181]

O direito de acesso aos dados pessoais é esmiuçado, no art. 15º do RGPD, e visando superar tais obstáculos, assegura ao titular dos dados o direito de obter do responsável pelo tratamento a informação de que os seus dados pessoais são ou não objeto de tratamento e, em caso positivo, de ter acesso a eles e a diversas informações, como a origem dos dados, finalidades do tratamento, as categorias dos dados pessoais tratados, os destinatários ou categorias de destinatários, o prazo de conservação dos dados pessoais, a existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação ou oposição ao tratamento, o direito de apresentar reclamação a uma autoridade de controlo, dentre outros. [182]

Quando os dados transpõem as fronteiras da União Europeia, há uma maior possibilidade de o titular não conseguir exercer seus direitos, daí a relevância do direito à informação, previsto no art. 15.º, no n.º 2 do RGPD.[183]

Ao responsável pelo tratamento caberá, em razão do direito de acesso, fornecer uma cópia sobre os dados tratados, de forma gratuita e, quando solicitada por meio eletrónico, por este meio será fornecida a informação, salvo se solicitada por outro meio, conforme o art. 15º, n.° 3º do RGPD.

Em seguida, têm-se os direitos de retificação, de apagamento, de limitação de tratamento e de portabilidade, todos regulados na secção 3, do capítulo III do RGPD[184], contendo o título denominação aquém do que é regulado, dificultando a compreensão.

O direito de retificação dos dados pessoais está previsto no art. 16º do RGPD[185]. Após o acesso e verificação por parte do titular da qualidade dos dados, possui ele o direito de retificação, caso ateste alguma inexatidão ou incompletude. A importância da retificação se justifica diante dos riscos correspondentes à identificação das pessoas, com

[181] RODOTÀ, Stefano. *A vida na sociedade de vigilância…* op. cit. p. 68.
[182] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit.
[183] MONIZ, Graça Canto. Direitos do titular dos dados pessoais… loc. cit.
[184] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit.
[185] Ibid.

reflexos na formação do perfil dos titulares, devendo as empresas dispor de meios para correção das informações erróneas ou desatualizadas, bem como para o seu complemento. Tal previsão se compatibiliza com o princípio da qualidade dos dados (*data accuracy),* previsto em diversas *guidelines da* Organização para a Cooperação e Desenvolvimento Económico (OCDE) ou *Organisation for Economic Co-operation and Development* (OECD)[186], que visam proteger a privacidade nos fluxos de dados pessoais transnacionais, e com o princípio da exatidão do art. 5º, n.° 1, alínea d) do RGPD.

O direito de apagamento dos dados pessoais, tratado no art. 17º do RGPD, não se constitui em uma novidade trazida pelo Regulamento, uma vez que a norma anterior, a Diretiva 95/46/CE, já dispunha expressamente sobre tal direito. Entretanto, o título do citado artigo assim é disposto "Direito ao apagamento dos dados ('direito a ser esquecido')". O RGPD, em tal título, utiliza os termos como sinónimos. Resta saber se agiu com propriedade tal norma.

A era digital modificou consideravelmente a forma como o ser humano lidava com as suas lembranças. Segundo Mayer-Schönberger, na era digital houve a inversão entre o lembrar e o esquecer. Ambos são importantes, pois lembrar permite comparar, aprender e adquirir experiência para mudar; já o esquecer possibilita vivermos o presente, nos libertando dos grilhões do passado. Se anteriormente esquecer era a regra e o ser humano tinha que escolher o que lembrar, face a dificuldade e o custo, nessa nova era esquecer é a exceção, diante do grande número de informações encaminhados para memória digital.[187]

Nesse contexto, ganha expressão o direito ao esquecimento. Para os italianos é o *dirrito all'oblio*. Já para os norte-americanos *right to be forgotten.* Na França, *droit a l'oubli.* A relevância de tal direito é revelada por François Ost, para quem, pessoa pública ou não, lançados fomos diante da cena e colocados sobre os projetores da atualidade, razão pela qual temos o direito, depois de certo tempo de sermos deixado em paz, recaindo no esquecimento e no anonimato, do qual não queríamos ter deixado.[188] A sua

[186] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* [Cited 28 march 2020]. Available from internet: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>.

[187] MAYER-SCHÖNBERGER, Viktor. *Delete:* the virtue of forgetting in the digital age. New Jersey: Princeton University, 2009. p. 196. ISBN 978069113861-9.

[188] OST, François. *O tempo do direito.* Tradução: Élcio Fernandes. Bauru: Edusc, 2005. p. 160. ISBN 978857460127-4.

origem, no direito continental europeu, está vinculada a casos de pessoas que foram condenadas, após o cumprimento de pena, algo semelhante a uma reabilitação criminal, expandindo-se posteriormente a discussão para a seara cível.

O direito ao esquecimento, pode ser definido, como aquele que qualquer pessoa humana possui de se opor a uma recordação opressiva de fatos perante a sociedade, impedindo o desenvolvimento da sua identidade pessoal, a conferir a terceiros que características de sua personalidade que não mais correspondem à realidade.[189]

Não se trata de um direito atrelado à vontade individual de não ser lembrado contra a sua vontade, em uma conotação privada de um indivíduo proprietário, mas um direito vinculado à identidade pessoal. Nas lições de Choeri, o direito à identidade pessoal é aquele

> [...] de toda pessoa expressar sua verdade pessoal, 'quem de fato é', em suas realidades física, moral e intelectual. A tutela da identidade impede que se falseie a 'verdade' da pessoa, de forma a permanecerem intactos os elementos que revelam sua singularidade como unidade existencial no todo social.[190]

Partindo dessa noção do direito ao esquecimento, constata-se que não há uma correspondência do fundamento entre aquele direito e o direito ao apagamento, a defesa da identidade pessoal. Segundo Schreiber, "[...] as hipóteses de apagamento de dados constantes no regulamento europeu não condizem um mecanismo de tutela da identidade da pessoa em face de recordações opressivas, mas sim remédio associado à dinâmica específica da proteção de dados pessoais."[191]

O Regulamento, no art. 17º, n.° 1[192], elenca seis hipóteses em que resta configurado o direito do titular dos dados de ver eles apagados, a saber: os dados não são mais necessários para os fins que levou ao tratamento; há retirada do consentimento, não havendo outro fundamento legal; há oposição ao tratamento e não há interesses legítimos prevalentes que justifiquem o tratamento; os dados foram tratados ilicitamente

---

[189] SCHREIBER, Anderson. Direito ao esquecimento. In: SALOMÃO, Luís Felipe; TARTUCE, Flávio.(Coord.). *Direito Civil:* diálogos entre a doutrina e jurisprudência. São Paulo: Atlas, 2018. p. 70. ISBN 978859701465-5.

[190] CHOERI, Raul Cleber da Silva. *O direito à identidade na perspectiva civil-constitucional.* Rio de Janeiro: Renovar, 2010. p. 244. ISBN 978857147789-6.

[191] SCHREIBER, Anderson. Direito ao esquecimento e proteção de dados pessoais na Lei n.° 13.709/2018: distinções e potenciais convergências. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.) *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 367-384. cit. p. 377-378. ISBN 978855321663-5.

[192] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit.

na sua origem; o apagamento atende a uma obrigação jurídica de direito da União Europeia ou de Estado-Membro a que o responsável está sujeito e os dados pessoais foram recolhidos na oferta de serviços da sociedade de informação com relação às crianças.

Ou seja, os dados podem ser objeto de apagamento nessas hipóteses, mesmo que não correspondam a informações do passado do titular, que afetem a sua identidade pessoal, reputação ou o desenvolvimento da sua personalidade.

Com relação à hipótese de apagamento, em que o titular dos dados se opõe ao tratamento e não há "interesses legítimos prevalentes" que o justifiquem (art. 17º, n.° 1, alínea c) do RGPD)[193], tem-se na citada expressão um conceito jurídico indeterminado, cabendo ao magistrado sopesar valores quando da apreciação do caso concreto. Nesse sentido Machado: "[...] devem os tribunais sopesar se existe interesse do próprio responsável pelo tratamento ou de terceiros, que seja preponderante em relação a direitos e liberdades fundamentais do titular dos dados protegidos pela lei."[194] Os Considerandos 47 a 49 auxiliam na interpretação da expressão.[195]

---

[193] Ibid. "Artigo 17º Direito ao apagamento dos dados («direito a ser esquecido») 1. O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos: [...] c) O titular opõe-se ao tratamento nos termos do artigo 21º, n.° 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21º, n.° 2;"

[194] MACHADO, op. cit., p. 12.

[195] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit. "Considerando o seguinte: [...] (47) Os interesses legítimos dos responsáveis pelo tratamento, incluindo os dos responsáveis a quem os dados pessoais possam ser comunicados, ou de terceiros, podem constituir um fundamento jurídico para o tratamento, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais do titular, tomando em conta as expectativas razoáveis dos titulares dos dados baseadas na relação com o responsável. Poderá haver um interesse legítimo, por exemplo, quando existir uma relação relevante e apropriada entre o titular dos dados e o responsável pelo tratamento, em situações como aquela em que o titular dos dados é cliente ou está ao serviço do responsável pelo tratamento. De qualquer modo, a existência de um interesse legítimo requer uma avaliação cuidada, nomeadamente da questão de saber se o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados pessoais são recolhidos, que esses poderão vir a ser tratados com essa finalidade. Os interesses e os direitos fundamentais do titular dos dados podem, em particular, sobrepor-se ao interesse do responsável pelo tratamento, quando que os dados pessoais sejam tratados em circunstâncias em que os seus titulares já não esperam um tratamento adicional. Dado que incumbe ao legislador prever por lei o fundamento jurídico para autorizar as autoridades a procederem ao tratamento de dados pessoais, esse fundamento jurídico não deverá ser aplicável aos tratamentos efetuados pelas autoridades públicas na prossecução das suas atribuições. O tratamento de dados pessoais estritamente necessário aos objetivos de prevenção e controlo da fraude constitui igualmente um interesse legítimo do responsável pelo seu tratamento. Poderá considerar-se de interesse legítimo o tratamento de dados pessoais efetuado para efeitos de comercialização direta. (48) Os responsáveis pelo tratamento que façam parte de um grupo empresarial ou de uma instituição associada a um organismo central poderão ter um interesse legítimo em transmitir dados pessoais no âmbito do grupo de empresas para fins administrativos internos, incluindo o tratamento de dados pessoais de clientes ou funcionários. Os princípios gerais que regem a transmissão de dados pessoais, no âmbito de um grupo empresarial, para uma empresa localizada num país terceiro mantêm-se inalterados. (49) O tratamento de dados pessoais, na medida estritamente necessária e proporcionada para assegurar a segurança da rede e das informações, ou seja, a capacidade de uma rede ou de um sistema informático de resistir, com um dado nível de confiança, a eventos acidentais ou a ações maliciosas ou ilícitas que comprometam a disponibilidade, a autenticidade, a integridade e a confidencialidade dos dados pessoais conservados ou transmitidos, bem como a segurança dos serviços conexos oferecidos ou acessíveis através destas redes e sistemas, pelas autoridades públicas, equipas de intervenção em caso de emergências informáticas (CERT), equipas de resposta a incidentes no domínio da segurança informática (CSIRT), fornecedores ou redes de serviços de comunicações eletrónicas e por fornecedores de tecnologias e serviços de segurança, constitui um interesse legítimo do responsável pelo tratamento. Pode ser esse o caso quando

Entretanto, tal direito, ainda que exista uma das situações do parágrafo anterior, não subsiste quando presentes uma das hipóteses do art. 17º, n.°3 do RGPD: ao exercício da liberdade de informação ou de expressão; ao tratamento realizado em razão de cumprimento de obrigação legal do direito da União ou do Estado-Membro, ao exercício de funções de interesse público ou de autoridade pública de que está investido o responsável pelo tratamento; por motivos de interesse público relacionado à saúde pública; para fins de arquivo de interesse público, de investigação científica ou histórica ou estatísticos e para efeitos de declaração, exercício ou defesa de um direito num processo judicial.[196] O Considerando 65[197] também dispõe em sentido semelhante ao que é disposto no art. 17º, n.[os] 1 e 3 do RGPD[198].

Mas quando se fala em apagamento, este deve ocorrer de forma ampla, dos arquivos e sistemas, não bastando que ocorra a mera ocultação. Até mesmo a permanência de *backups* somente é admitida de forma justificada, devidamente comunicada ao titular.[199]

A análise dos requisitos legais para o apagamento deve ser efetuada pelo responsável pelo tratamento, após o requerimento do titular dos dados, atendendo o pleito no prazo de um mês, comunicando o postulante. Se quem recebe o pleito de apagamento não é o responsável pelo tratamento, o receptor deve comunicar imediatamente aquele para efetuar a análise do pedido. Para atendimento do pleito deve o processador adotar todas as medidas que forem razoáveis, considerando a tecnologia e os custos, inclusive de natureza técnica, até para comprovar que o pleito foi atendido, o

---

o tratamento vise, por exemplo, impedir o acesso não autorizado a redes de comunicações eletrónicas e a distribuição de códigos maliciosos e pôr termo a ataques de «negação de serviço» e a danos causados aos sistemas de comunicações informáticas e eletrónicas."

[196] Ibid.

[197] Ibid. "Considerando o seguinte: [...] (65) Os titulares dos dados deverão ter direito a que os dados que lhes digam respeito sejam retificados e o «direito a serem esquecidos» quando a conservação desses dados violar o presente regulamento ou o direito da União ou dos Estados-Membros aplicável ao responsável pelo tratamento. Em especial, os titulares de dados deverão ter direito a que os seus dados pessoais sejam apagados e deixem de ser objeto de tratamento se deixarem de ser necessários para a finalidade para a qual foram recolhidos ou tratados, se os titulares dos dados retirarem o seu consentimento ou se opuserem ao tratamento de dados pessoais que lhes digam respeito ou se o tratamento dos seus dados pessoais não respeitar o disposto no presente regulamento. Esse direito assume particular importância quando o titular dos dados tiver dado o seu consentimento quando era criança e não estava totalmente ciente dos riscos inerentes ao tratamento, e mais tarde deseje suprimir esses dados pessoais, especialmente na Internet. O titular dos dados deverá ter a possibilidade de exercer esse direito independentemente do facto de já ser adulto. No entanto, o prolongamento da conservação dos dados pessoais deverá ser efetuado de forma lícita quando tal se revele necessário para o exercício do direito de liberdade de expressão e informação, para o 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, por razões de interesse público no domínio da saúde pública, para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial."

[198] Ibid.

[199] MALDONADO, Viviane Nóbrega. Direitos dos titulares… op. cit., p. 102.

que é, em regra, realizado por meio de *logs.*

Caso o responsável pelo tratamento entenda pela existência de uma das hipóteses que o apagamento é vedado, deverá comunicar o titular postulante, indicando o dispositivo legal.

Não se pode negar certa dificuldade que é imposta ao responsável pelo tratamento de avaliar tais pleitos de remoção de dados em situações concretas, tanto que foram editadas *guidelines*[200]*,* a fim de auxiliar a análise dos pedidos de exclusão de dados pessoais.

Já o direito de limitação ao tratamento está previsto no art. 18º do RGPD[201]. São situações específicas em que o titular dos dados possui tal direito de restrição. Segundo Maldonado, tal direito não se confunde com o apagamento, quando há completa eliminação dos dados em face do requerimento do titular e inexista base legal para a subsistência do tratamento.[202]

A limitação ao tratamento pode ser exercida, nos termos do art. 18º do RGPD[203], quando: houver contestação da exatidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão; o tratamento é ilícito e o titular dos dados, ao invés do apagamento, solicita a limitação da sua utilização; o responsável pelo tratamento não precisa dos dados pessoais, mas esses dados são solicitados pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial; se tiver oposição ao tratamento nos termos do artigo 21º, n.° 1, até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados.

Segundo Moniz, esse direito "[...] poderá assumir uma natureza cautelar bastante útil enquanto o titular dos dados pondera uma estratégia de defesa judicial."[204]

A restrição pode ser temporal ou qualitativa, mas, em regra, elas são temporárias, sendo que o cancelamento da restrição deve ser comunicada previamente ao titular.

---

[200] COMISSÃO EUROPEIA. *Do we always have to delete personal data if a person asks?* [Consultado 19 março 2020]. Disponível na internet: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/do-we-always-have-delete-personal-data-if-person-asks_en>.

[201] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit.

[202] MALDONADO, Viviane Nóbrega. Direitos dos titulares… op. cit., p. 103.

[203] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit.

[204] MONIZ, Graça Canto. Direitos do titular dos dados pessoais… op. cit., p. 18.

Durante a restrição, exceto a conservação nas suas bases, os dados somente poderão ser objeto de tratamento se houver o consentimento do titular, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial, de defesa dos direitos de outra pessoa singular ou coletiva, ou por motivos de interesse público da União ou de um Estado-Membro, segundo o art. 18º, n.° 2 do RGPD.[205] Ou seja, o exercício do direito de limitação afeta todas as operações de tratamento, excetuando-se o direito de conservação. O Considerando 67[206] cita as maneiras de se operacionalizar o exercício desse direito.

O direito à portabilidade dos dados consiste em duas faculdades: o de receber os seus dados pessoais em um dispositivo e o de transmitir esses dados a outro responsável pelo tratamento. Esse direito seria a expansão da manifestação do consentimento e de sua revogação para fins de tratamento, pelo que não pode estar sujeito a cobrança de taxas, conforme a expressão "sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir", descrita no art. 20º, n.°1 do RGPD[207]. Trata-se de algo complementar ao direito de acesso. Não implica necessariamente em uma transmissão imediata a um novo responsável, permitindo ao titular administrar e reutilizar os seus dados, de acordo com os seus interesses. Pode, contudo, o titular visar, não a transmissão total, mas a interoperabilidade, ou seja, o trabalho em conjunto de sistemas, como várias "nuvens". Possui tal direito duas dimensões: uma individual e uma económica. A individual seria conferir ao titular um poder de autogestão dos seus dados, controlando o trâmite e o destinatário, conforme os seus interesses daquele, resultando confiabilidade no serviço. Trata-se do exercício do direito à autodeterminação informacional. A dimensão económica seria facilitar a circulação dos dados, aumentando a confiança na economia digital e a competitividade entre os prestadores de serviços. Ademais, favorece a inovação e o surgimento de novos negócios, considerando que os dados possuem, em nossa sociedade, valor económico, posto que permite à empresas prestar um serviço mais adequado e de melhor qualidade. Por fim, promove-se a redução ou eliminação dos

[205] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit.

[206] Ibid. "Considerando o seguinte: [...] (67) Para restringir o tratamento de dados pessoais pode recorrer-se a métodos como a transferência temporária de determinados dados para outro sistema de tratamento, a indisponibilização do acesso a determinados dados pessoais por parte dos utilizadores, ou a retirada temporária de um sítio *web* dos dados aí publicados. Nos ficheiros automatizados, as restrições ao tratamento deverão, em princípio, ser impostas por meios técnicos de modo a que os dados pessoais não sejam sujeitos a outras operações de tratamento e não possam ser alterados. Deverá indicar-se de forma bem clara no sistema que o tratamento dos dados pessoais se encontra sujeito a restrições."

[207] Ibid.

custos de troca *(switching costs),* combatendo o aprisionamento tecnológico (*vendor lock-in),* em que o titular dos dados permanece vinculado a um responsável.

O GT29 sustentou que o direito à portabilidade pertence ao regramento da proteção dos dados e não da concorrência, uma vez que sua aplicação não está restrita à permuta de fornecedor.[208] Porém, pensa-se como Cravo, que a portabilidade possuiria uma natureza jurídica especial, sendo uma intersecção entre a proteção de dados, a concorrência e a defesa do consumidor.[209]

Para tanto, o responsável pelo tratamento deve manter os dados em formato portável, possibilitando a exportação direta para outro responsável ou a entrega ao titular para que esse assim repasse. Mas quando se tratar de transmissão direta para o novo responsável pelo tratamento, faz-se necessário a existência da possibilidade técnica, não sendo incondicional, conforme art. 20º, n.° 2 do RGPD.

Formato portável é aquele estruturado, de uso corrente e de leitura automática. Esses seriam os requisitos mínimos para a interoperabilidade, ressaltando-se o Considerando 68.[210] *Guidelines* foram estabelecidas pelo GT29, em dezembro de 2016, e revisadas em abril de 2017[211], as quais estabelecem quais dos dados que podem ser portados, quais as medidas técnicas e os formatos admissíveis, sugerindo a adoção de uma Interface de Programação de Aplicativos (IPA) ou *Application Programming Interface (API),* facilitando o atendimento de postulações.

Não existe, porém, um direito geral à portabilidade. Segundo Moniz, "[...] de acordo com o art. 20º, o seu âmbito material de aplicação depende de um conjunto de condições cumulativas relacionadas com o tipo de dados, com o fundamento jurídico que enquadra

---

[208] GRUPO DE PROTEÇÃO DAS PESSOAS NO QUE DIZ RESPEITO A TRATAMENTO DE DADOS PESSOAIS (GT29). *Guidelines on the right to data portability.* [Consultado 18 fevereiro 2020]. Disponível na internet: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233>.

[209] CRAVO, Daniela Copetti. O direito à portabilidade na lei de proteção de dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.) *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.* São Paulo: Thomson Reuters Brasil, 2019. p. 347-365. cit. p. 350. ISBN 978855321663-5.

[210] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit. "Considerando o seguinte: [...] (68) Para reforçar o controlo sobre os seus próprios dados, sempre que o tratamento de dados pessoais for automatizado, o titular dos dados deverá ser autorizado a receber os dados pessoais que lhe digam respeito, que tenha fornecido a um responsável pelo tratamento num formato estruturado, de uso corrente, de leitura automática e interoperável, e a transmiti-los a outro responsável. Os responsáveis pelo tratamento de dados deverão ser encorajados a desenvolver formatos interoperáveis que permitam a portabilidade dos dados,[...]"

[211] GRUPO DE PROTEÇÃO DAS PESSOAS NO QUE DIZ RESPEITO A TRATAMENTO DE DADOS PESSOAIS (GT29). *Guidelines on the right to data portability.* Op. cit.

o tratamento e com o tipo de tratamento."[212]

Analisa-se, assim, o âmbito material do direito à portabilidade. Em relação ao tipo de dados, o art. 20º, n.° 1 do RGPD afirma "[...] que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento[...]".[213] Em relação à expressão "que lhe diga respeito", a interpretação deve ser ampla, incluindo os dados pseudonimizados e a informação sobre terceiros, mas desde que haja uma correlação com os dados do titular como, *v.g.,* os registos de chamadas telefônicas recebidas. Por sua vez, quanto à expressão "que tenha fornecido a um responsável pelo tratamento", incluem-se duas situações: aqueles dados fornecidos pelo titular de forma consciente e ativamente, como um telefone, endereço de e-mail; e aqueles obtidos através da observação, pelo fato do titular ter utilizado uma plataforma ou serviço, como os de navegação e os de deslocamento. Não abarca os dados inferidos, ou seja, aqueles obtidos da análise dos fornecidos.

Já em relação aos fundamentos jurídicos para a portabilidade, é necessário que o tratamento tenha se baseado no consentimento dado, nos termos do artigo 6º, n.° 1, alínea a), ou do artigo 9º, n.° 2, alínea a), ou num contrato referido no artigo 6º, n.° 1, alínea b), *v.g.,* objetos comprados em uma loja *on-line*, e que seja ele realizado por meios automatizados. Exclui-se o direito quando o tratamento é realizado por meio manual, bem como ele, o tratamento, seja necessário para o exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento, conforme art. 20º, n.^{os} 1 e 3 do RGPD.[214] O fundamento baseado no consentimento justifica-se, pois o direito à portabilidade por ser a expansão da manifestação da expansão do consentimento, segundo já afirmado.

Segundo o n.° 4 do art. 20º, não pode a portabilidade afetar direitos de terceiros, como direitos autorais, segredo comercial e propriedade intelectual que protegem o software e a empresa do responsável pelo tratamento, pelo que deve esse utilizar instrumentos para excluir dos dados aquelas informações danosas, mantendo só as do

[212] MONIZ, Graça Canto. Direitos do titular dos dados pessoais… op. cit., p. 26.
[213] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit.
[214] Ibid.

titular.[215]

Por fim, tem-se os direitos de oposição e de objeção em relação às decisões individuais automatizadas, inclusive às relacionadas a *profiling.*

O direito de oposição, segundo o art. 21º do RGPD, é aquele que possui o titular de se opor ao tratamento dos dados pessoais nas seguintes hipóteses: fins de comercialização; necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; por interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros; para fins de investigação científica ou histórica ou estatísticos.[216] Segundo Veronese, "[o] RGPD expandiu sobremaneira o direito de oposição ao tratamento de dados, em comparação com a Diretiva. Ele não se restringiu apenas a um tipo de tratamento de dados como os automatizados."[217]

Quando os dados pessoais são tratados para fins de comerciais, incluindo formação de perfis, o direito de oposição do titular não pode ser rebatido pelo responsável, sendo um direito absoluto, seguindo os ditames do art. 21º, n.° 2 do RGPD. Mas quando os dados são tratados nas hipóteses do n.° 1 do mesmo artigo (necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; por interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros; para fins de investigação científica ou histórica ou estatísticos), o direito de oposição do titular tem por pressuposto que ele possua razões legítimas e preponderantes à relação àquelas que fundamentam o tratamento, relacionadas com a sua situação particular. Segundo Moniz,

> [s]endo um reconhecimento do direito à autodeterminação, por um lado, o seu exercício não é absoluto – com a exceção dos tratamentos para efeitos de comercialização direta – e, por outro, a sua aplicação não é geral. Desde logo, depende do juízo de ponderação entre as 'razões imperiosas e legítimas' para o tratamento, invocadas pelo responsável, e os 'interesses, direitos e liberdades do titular dos dados'.[218]

[215] MONIZ, Graça Canto. Direitos do titular dos dados pessoais… op. cit., p. 32-33.
[216] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit.
[217] VERONESE, Alexandre. Os direitos de explicação e de oposição frente às decisões totalmente automatizadas: comparando o RGPD da União Europeia com LGPD brasileira. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.) *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 385-415. cit. p. 404. ISBN 978855321663-5.
[218] MONIZ, Graça Canto. Direitos do titular dos dados pessoais… op. cit., p. 19.

A análise do responsável pelo tratamento consiste em verificar quais as razões de tal tratamento, demonstrando de forma límpida que há razões para o tratamento, se negar o pleito. O certo é que todo pleito deve ser recebido e analisado, informando o postulante de todas as decisões. Frise-se que pode o titular buscar a tutela desse direito, tanto perante as autoridades administrativas, quanto perante as autoridades judiciais.

O direito de objeção consiste naquele que o titular detém de não se sujeitar à decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis.

O art. 2º, n.° 1 do RGPD menciona a sua aplicação ao tratamento de dados realizados por meios automatizados, total ou parcialmente. O Considerando 105 do RGPD estabelece que os Estados-Membros devem se submeter à "Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, de 28 de janeiro de 1981, e ao seu Protocolo Adicional". Em vigor, atualmente, a Convenção n.° 108+ em seu art. 9º, n.° 1, alínea a) ressalta, como direito, a não sujeição a uma decisão que lhe afete significativamente e que tenha por base o processamento automatizado de dados, sem que suas opiniões sejam levadas em consideração.[219]

As decisões individuais exclusivamente automatizadas são aquelas decisões adotadas sobre si por meios exclusivamente tecnológicos, ou seja, sem a participação humana, ressaltando-se que elas podem ser realizadas com ou sem a definição de perfis, quando se utilizam algoritmos e *machine learning*.

Segundo Machado, "[d]ecisões automáticas e sem qualquer intervenção humana parecem ir contra a noção de autonomia e personalidade no Regulamento Europeu."[220]

O RGPD não proíbe a prática de criação de perfis, mas procura prevenir riscos oriundos de uma decisão obtida sem a intervenção humana. Pensa-se que o problema não é propriamente a definição de perfis em si, mas a falta de informação sobre a lógica

[219] CONSELHO DA EUROPA. Convenção n.° 108+. Estrasburgo, 18 de maio de 2018. [Consultado 31 março 2020]. Disponível na internet: <https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf>. (tradução nossa). "Article 9 – Rights of the data subject 1. Every individual shall have a right: a. not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration;" (no original)

[220] MACHADO, op. cit., p. 12.

dos algorítmicos que lhes dão origem.

A decisão que importa para fins do regulamento é aquela que produz efeitos jurídicos, ou seja, afete um direito ou significativamente a pessoa, as suas circunstâncias, comportamentos ou escolhas. Cite-se, respectivamente, como a afetação ao direito de voto ou de obtenção de um crédito.

Entretanto, não pode o titular se valer, segundo o art. 22º, n.° 2 do RGPD[221], de tal direito se a decisão for: decorrente de consentimento expresso do titular dos dados; for necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento; ou se for autorizada pelo direito da União Europeia ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, estando previstas medidas adequadas para tutela dos direitos, liberdades e interesses do titular[222]. Diversamente do que ocorria com a Diretiva 95/46/CE, que não previa o consentimento explícito do titular no art. 15º, o RGPD o inclui no art. 22º, n.°2, alínea c).

Ou seja, assim como ocorre com outros direitos, este não é um direito geral e absoluto, uma vez que o seu campo de aplicação depende do fundamento jurídico que alicerça o tratamento dos dados.[223] Porém, quando se tratar de consentimento expresso do titular ou necessária à celebração ou execução de um contrato, a empresa de tratamento deve aplicar as medidas adequadas para proteção dos direitos, liberdades e interesses do titular dos dados, pelo menos o de obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão. São as garantias.

As decisões baseadas em algoritmos não podem utilizar categorias especiais de dados, a menos que a pessoa tenha dado o seu consentimento expresso, não vedado pelo direito, ou o tratamento seja de interesse público permitido pelo direito da União Europeia ou de Estado-Membro, segundo o art. 22º, n.° 4 do RGPD.[224]

Guidelines[225] foram fixadas pelo GT29 em relação às decisões automatizadas e *profiling*, fixando as hipóteses que justificariam o tratamento dos dados pessoais dessa

---

[221] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit.
[222] Ibid.
[223] MONIZ, Graça Canto. Direitos do titular dos dados pessoais… op. cit., p. 20.
[224] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit.
[225] GRUPO DE PROTEÇÃO DAS PESSOAS NO QUE DIZ RESPEITO A TRATAMENTO DE DADOS PESSOAIS (GT29). *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.* [Consultado 18 fevereiro 2020]. Disponível na internet: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053>.

maneira, bem como os direitos assegurados.

Mas como observa Moniz, em relação aos direitos dispostos no RGPD, o direito da União ou dos Estados-Membros pode fixar restrições a princípios específicos e a direitos do titular, a fim de resguardar interesses gerais, como a segurança do Estado, mas que devem respeitar a CDFUE e a CEDH.[226]

3.1.3 A regulação sectorial pelas autoridades de controlo e o regime sancionatório e jurisdicional

Como forma de assegurar a efetividade de aplicação de suas normas, o RGPD regula o setor de maneira a assegurar a harmonia na interpretação e na aplicação da legislação. Tal assunto encontra-se disposto nos Capítulos VI (Autoridades de controlo independentes), VII (Cooperação e Coerência) e VIII (Recursos, responsabilidade e penalidades).

Nessa seara destaca-se a atuação do Comité Europeu para a Proteção de Dados (CEPD), que é responsável pela edição de guias que auxiliam na interpretação dos textos legais. Tal órgão substituiu o extinto GT29, órgão consultivo europeu independente criado pela Diretiva 95/46/CE que existiu até 25 de maio de 2018. O CEPD ficou responsável pelas funções da GT29, as quais estão descritas no art. 30º da citada diretiva[227] combinado com art. 15º da Diretiva 2002/58/CE[228].

O Capítulo VI versa sobre as autoridades de controlo. A independência de tais entidades é regulada pela Secção 1. A fiscalização e a aplicação do RGPD é de responsabilidade imediata das autoridades públicas independentes, as Autoridades de Controlo ou Autoridades de Proteção de dados (APDs), a fim de defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e facilitar a

---

[226] MONIZ, Graça Canto. Direitos do titular dos dados pessoais… op. cit., p. 14.

[227] PARLAMENTO EUROPEU; CONSELHO – Directiva 95/46/CE… op. cit.

[228] PARLAMENTO EUROPEU; CONSELHO – Directiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002 relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas). *"J.O.C.E."* (31-07-2002). [Consultado 31 março 2020]. Disponível na internet:<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0058&from=EN>. "Artigo 15.º Aplicação de determinadas disposições da Directiva 95/46/CE [...] 3. O Grupo de Protecção das Pessoas no que respeita ao Tratamento de Dados Pessoais, instituído nos termos do artigo 29.º da Directiva 95/46/CE, realizará também as tarefas previstas no artigo 30.º da mesma directiva no que respeita às matérias abrangidas pela presente directiva, nomeadamente a protecção dos direitos e liberdades fundamentais e dos interesses legítimos no sector das comunicações electrónicas."

livre circulação desses dados na União. A criação da APD é de responsabilidade de cada Estado Membro, podendo este criar apenas uma ou mais. Na hipótese de existir mais de uma Autoridade no Estado-Membro, deve este indicar qual representará o Estado, perante a CEPD. *Verbi gratia*, em Portugal a APD denomina-se Comissão Nacional de Proteção de Dados[229], enquanto que na Espanha tem-se a *Agencia Española de Protección de Datos*[230], criadas, respectivamente, em 1994 e 1993. Cada APD possui um âmbito nacional e sua jurisdição está restrita ao território do Estado.

A independência das APDs e dos seus membros é sufragada no art. 52º do RGPD. Elas devem dispor de recursos humanos, técnicos e financeiros, instalações e infraestruturas necessárias, sendo que o controlo financeiro da ADP não pode afetar a sua independência e o seu orçamento anual deve ser separado e público, podendo estar integrado no orçamento geral do Estado ou nacional. Por sua vez, a fim de resguardar a independência dos membros da APDs, não podem esses, durante o mandato, desempenhar nenhuma atividade, remunerada ou não, que com elas seja incompatível, nem praticar qualquer ato incompatível com as suas funções.[231] Exige-se, portanto, reputação ilibada. Ademais, detém os membros estabilidade funcional, somente sendo exonerados na hipótese de falta grave ou não cumprimento das condições exigidas para o exercício das suas funções.[232] Segundo Blum e Arantes, tal estabilidade é outro ponto relevante para "[...] assegurar o melhor desempenho dos funcionários das DPAs, na hipótese de eventuais pressões externas (*v.g.* sociais e/ou políticas) e internas (*v.g.* posicionamento divergente dentro da autoridade)."[233]

Os membros devem deter habilitação, conhecimento técnico e experiência no que tange à proteção de dados pessoais, sendo essencial, no procedimento de escolha e de nomeação, a observância do princípio da transparência.

---

[229] Informação disponível na internet: <https://www.cnpd.pt/>. [Consultado 18 março 2020].

[230] Informação disponível na internet: <https://www.aepd.es/es>. [Consultado 18 março 2020].

[231] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit. "Artigo 52º Independência [...] 2. Os membros das autoridades de controlo não estão sujeitos a influências externas, diretas ou indiretas no desempenho das suas funções e no exercício dos seus poderes nos termos do presente regulamento, e não solicitam nem recebem instruções de outrem. 3. Os membros da autoridade de controlo abstêm-se de qualquer ato incompatível com as suas funções e, durante o seu mandato, não podem desempenhar nenhuma atividade, remunerada ou não, que com elas seja incompatível."

[232] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit. "Artigo 52º Independência [...] 4. Os membros da autoridade de controlo só são exonerados se tiverem cometido uma falta grave ou se tiverem deixado de cumprir as condições exigidas para o exercício das suas funções."

[233] BLUM, Renato Opice; ARANTES, Camila Rioja. Autoridades de controle, atribuições e sanções. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords.) *Comentários ao GDPR:* Regulamento Geral de Proteção de Dados da União Europeia. São Paulo: Thomson Reuters Brasil, 2018. p. 227-252. p. 234. ISBN 978855321230-9.

Os Estados-Membros possuem ampla autonomia, segundo o art. 54º, n.° 1, do RGPD[234] para fixar as regras de constituição das suas APDs, ou seja, dispor sobre: a constituição, as qualificações e as condições de elegibilidade, a regra e o procedimento de nomeação dos membros, a duração dos mandados, a possibilidade de renomeação, as ações, as funções e os benefícios que com elas são incompatíveis, durante o mandato e após o seu termo, regras que regem a cessação da relação de trabalho e demais disposições.

A obrigação de sigilo profissional é exigida aos membros e ao pessoal das APDs sobre quaisquer informações confidenciais que tenham obtido em razão do exercício de suas funções, durante e após o mandato, inclusive comunicações com pessoas singulares sobre violações ao RGPD.

A Secção II, do Capítulo VI, versa sobre a competência, atribuições e poderes das autoridades de controlo. A competência das APDs está cingida ao território do Estado-Membro e não incide sobre operações de tratamento efetuadas por tribunais no exercício da sua função jurisdicional, ou seja, não se sobrepõe à competência judicial.

O RGPD estabeleceu, no art. 56, a competência da *lead* APD, também denominada de APD principal, com função precípua de tratamento dos dados transfronteiriços. Trata-se de uma inovação do RGPD denominada *one-stop-shop,* centralizando o controlo em apenas uma autoridade, com o objetivo de harmonizar a fiscalização e a aplicação das leis de proteção de dados, mecanismo não previsto na Diretiva 95/46/CE.

A dificuldade da implantação na prática da *one-stop-shop* fez com que o GT29 fixasse *guidelines*[235], em 13 de dezembro de 2016, atualizadas em 5 de abril de 2017, dispondo, inclusive, sobre o conceito de processamento transnacional de dados.

É a localização do estabelecimento único ou principal daquele que trata ou é subcontratado para tratar os dados que determina qual será a APD principal, o local onde as decisões relevantes são tomadas, onde ocorre o exercício efetivo das atividades de gestão correspondente ao tratamento de dados. Blum e Arantes esclarecem que se o

---

[234] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit.

[235] GRUPO DE PROTEÇÃO DAS PESSOAS NO QUE DIZ RESPEITO A TRATAMENTO DE DADOS PESSOAIS (GT29). *Guidelines on the Lead Supervisory Authority (wp244rev.01).* [Consultado 2 março 2020]. Disponível na internet: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235>.

tratamento é realizado por um grupo de empresas com sede na União Europeia, a competência será determinada pela empresa *holding*.[236] Na verdade, a identificação de estabelecimento principal é feito pelo responsável pelo tratamento. Mas essa identificação pode ser questionada pela APD. A competência de uma APD pode ser preservada, ainda que não se configure como APD principal, nas hipóteses do art. 56º, n.° 2 do RGPD, ou seja, quando as reclamações que lhe sejam apresentadas ou a eventuais violações do presente regulamento corresponderem a matéria relacionada apenas com um estabelecimento no seu Estado-Membro ou se afetar substancialmente titulares de dados apenas no seu Estado-Membro[237]. Nessas hipóteses, deve a APD interessada notificar a DPA principal com a maior brevidade possível, tendo essa o prazo de três semanas para decidir sobre sua competência para o caso. Mas ainda que a APD principal se julgue competente, poderá a APD que informou apresentar um projeto da decisão, o qual será levado em conta quando da decisão da APD principal.

As APDs possuem suas atribuições descritas no art. 57º, n.° 1 do RGPD, que incluem, não apenas a fiscalização e aplicação do RGPD, mas também: a conscientização da população e empresas das regras, obrigações e direitos previstos no regulamento; a investigação de ilícitos; o aconselhamento do Governo, instituições e organismos a respeito das medidas legislativas e administrativas referentes à defesa dos direitos e liberdades das pessoas singulares relacionadas ao tratamento de dados; o tratamento de reclamações; a elaboração e conservação de lista associada à exigência de realizar uma avaliação do impacto sobre a proteção de dados; o fornecimento de orientações sobre o tratamento; o incentivo, tanto na elaboração de códigos de conduta, dando parecer sobre eles, aprovando os que preveem garantias suficientes, quanto no estabelecimento de procedimentos de certificação de proteção de dados, de selos e marcas de proteção de dados, aprovando os critérios de certificação. Ressalte-se ainda a cooperação com as demais autoridades de controlo e a contribuição para as atividades do Comité.[238]

No cumprimento de suas atribuições, as APDs devem adotar medidas para facilitar, aos titulares dos dados pessoais, o exercício do direito de reclamação, inclusive formulários eletrónicos, sendo o exercício de tal direito realizado de forma gratuita, salvo

[236] BLUM, op. cit., p. 235-236.
[237] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit.
[238] Ibid.

quando o pedido for infundado ou manifestamente excessivo, em que é permitida a cobrada taxa pelos custos administrativos, devidamente justificado pela autoridade de controlo. Tais determinações de acesso dos titulares estão previstas nos n.os 2, 3 e 4 do art. 57 do RGPD.[239]

No que tange aos poderes conferidos às APDs, estes podem ser divididos em três categorias, descritos no art. 58º do RGPD[240]: investigativos, corretivos e consultivos.

Os poderes de investigação estão descritos no n.° 1, do art. 58º do RGPD, citando-se a realização de investigação sob a forma de auditorias, a revisão de certificações, a requisição de informações, documentos e acesso a instalações.

Os poderes corretivos são previstos no n.° 2, do mesmo artigo, do RGPD e incluem: a possibilidade de advertências, repreensões, imposições aos responsáveis pelo tratamento de satisfação do exercício dos direitos do titular e de comunicação ao titular dos dados de violação de dados pessoais; a imposição de limitação temporária ou definitiva, a retificação ou apagamento dos dados pessoais; a retirada de uma certificação ou a determinação para que o organismo responsável retire a certificação emitida, ou não a conceda; a imposição de pena pecuniária e a suspensão do envio de dados para organizações internacionais ou destinatários situados em países terceiros, com forte impacto no âmbito internacional. Portanto, as APDs podem impor sanções, bem como fiscalizar o cumprimento.

Já os poderes de consultivos, descritos no art. 58º, n.° 3 do RGPD visam à conscientização sobre o RGPD para as empresas, entidades governamentais e sociedade em geral, como: emissão de pareceres; emissão de conselhos em procedimentos de consulta prévia; autorização de tratamento previsto no artigo 36º, n.° 5, se a lei do Estado-Membro exigir tal autorização prévia; emissão de pareceres e aprovação de projetos de códigos de conduta; acreditar organismos de certificação; emitir certificações e aprovar os critérios de certificação; adotar as cláusulas-tipo de proteção de dados previstas no artigo 28º, n.° 8, e no artigo 46º, n.° 2, alínea d); autorizar as cláusulas contratuais e acordos administrativos, previstos no artigo 46º, n.° 3, alíneas a) e b),

[239] Ibid.
[240] Ibid.

respectivamente, e aprovar as regras vinculativas aplicáveis às empresas, nos termos do artigo 47º.[241]

Ademais, a fim de aplicar as disposições do RGPD, podem as APDs, levar ao conhecimento do Poder Judiciário as violações da norma, ajuizando ações ou intervindo em processos visando o cumprimento da legislação, nos termos do art. 58º, n.° 5 do RGPD. Ressalte-se que, os Estados-Membros podem estabelecer por lei outros poderes às APDs, não podendo prejudicar a cooperação e a coerência.

Devem tais autoridades de controlo elaborar, por fim, o Relatório Anual de Atividades, conforme o art. 59º do RGPD, com a descrição das violações e das medidas adotadas, e que será apresentado ao Parlamento Nacional, ao Governo e às outras autoridades designadas no direito do Estado-Membro, com acesso ao público, à Comissão e ao Comité.[242]

Como forma de assegurar o funcionamento adequado e uniforme do sistema de regulatório, o RGPD dispõe no Capítulo VII sobre a cooperação e a coerência, a primeiro na Secção 1, a segunda na Secção 2. A harmonização é algo indispensável para que se efetive o controlo sobre o processamento dos dados e a aplicação da legislação. Nos termos de Blum e Arantes, "[a] tônica do capítulo é estabelecer mecanismos de consenso entre a DPA principal e as demais DPAs interessadas, ressaltando a necessidade da troca de informação e apoio entre essas."[243]

Quando da vigência da Diretiva 95/96/CE, havia uma atuação individualizada de cada uma das APDs, em relação à proteção de dados, com predomínio da burocracia, insegurança jurídica e dispêndio desnecessário de recursos.

A cooperação visa alcançar um consenso nas decisões, tanto que, nos termos do art. 60º, n.° 2, a autoridade de controlo principal pode, a qualquer momento, solicitar às outras autoridades de controlo interessadas a assistência mútua do art. 61º e a realização de operações conjuntas do art. 62º, para fins de investigações e de monitoramento da execução de medidas relativas a responsáveis pelo tratamento ou subcontratantes

[241] Ibid.
[242] Ibid.
[243] BLUM, op. cit., p. 243.

estabelecidos noutros Estados-Membros.[244]

No que tange à cooperação em matéria de decisões pela autoridade de controlo principal, com procedimento previsto no art. 60º, as APDs interessadas emitem parecer sobre o projeto de decisão apresentado pela autoridade de controlo principal, podendo aquelas apresentar objeção no prazo de quatro semanas a contar da cientificação. A não objeção ao projeto de decisão implica em concordância e vinculação. Se a autoridade de controlo principal não der seguimento à objeção ou caso entenda que esta não é pertinente ou fundamentada, deve remeter a questão para o procedimento de controlo da coerência, disposto no art. 63º. A cooperação é verificada até mesmo em termos de notificação da decisão. Sendo favorável a reclamação, a autoridade de controlo principal notifica o estabelecimento principal ou o estabelecimento único do responsável pelo tratamento ou do subcontratante, consoante o caso, e informa as outras autoridades de controlo interessadas e o Comité da decisão em causa, incluindo um sumário dos fatos e dos motivos pertinentes, ficando a cargo da autoridade de controlo, à qual tenha sido apresentada a reclamação, informar o autor da reclamação. Já se for recusada ou rejeitada uma reclamação, a autoridade de controlo à qual a reclamação tiver sido apresentada adota a decisão, notifica o autor da reclamação e informa desse fato o responsável pelo tratamento. Por sua vez, se a autoridade de controlo principal e as autoridades de controlo interessadas concordarem em recusar ou rejeitar determinadas partes de uma reclamação e tomar medidas relativamente a outras partes da mesma reclamação, é adotada uma decisão separada para cada uma dessas partes da matéria. Enquanto que a autoridade de controlo principal adota a decisão na parte das medidas relativas ao responsável pelo tratamento e informa desse fato o estabelecimento principal ou o estabelecimento único do responsável pelo tratamento ou do subcontratante no território do seu Estado-Membro, comunicando ainda o autor da reclamação, a autoridade de controlo do autor da reclamação adota a decisão na parte relativa à recusa ou à rejeição da referida reclamação e notifica o autor da reclamação, informando o responsável pelo tratamento ou o subcontratante.

Acrescente-se, ainda, no campo da cooperação a assistência mútua. A assistência

[244] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit.

mútua inclui os pedidos de informação e as medidas de controlo, ou seja, os pedidos de autorização prévia e de consulta prévia, de inspeção e de investigação, conforme o art. 61º do RGPD. Em regra, as medidas tomadas em razão de assistência mútua são gratuitas, mas, em circunstâncias excepcionais, podem as autoridades de controlo acordar regras de indenização recíproca. O prazo para a prestação de informações é um mês a contar da recepção do pedido apresentado por outra autoridade de controlo, sendo que, na hipótese de descumprimento, a autoridade de controlo requerente pode adotar uma medida provisória no território do respetivo Estado-Membro. Diante do dever de assistência mútua, uma autoridade de controlo não pode indeferir um pedido de informação formulado por outra autoridade de controlo, salvo se não for a competente ou o pleito violar o RGPD, o direito da União Europeia ou do Estado-Membro, conforme o art. 61º, n.° 4 do RGPD. [245]

Por fim, ainda na seara da cooperação, tem-se a possibilidade de operações conjuntas, tanto de investigações, quanto de execução de medidas. Na hipótese de um número significativo de titulares substancialmente afetados localizarem-se em mais de um Estado-Membro ou o responsável pelo tratamento ou o subcontratante possuir estabelecimento em diversos Estados-Membros, todas as APDs podem participar da operação. Pode ainda haver outorga de poderes de investigação e de prática de atos entre as APDs nas operações conjuntas.[246]

No que tange à coerência, esta tem por objetivo assegurar uma aplicação uniforme do RGPD em todos os Estados-Membros.

Nessa seara tem-se o CEPD, criado pelo RGPD, dotado de personalidade jurídica

---

[245] Ibid.

[246] Ibid. "Artigo 62º Operações conjuntas das autoridades de controlo 1. As autoridades de controlo conduzem, sempre que conveniente, operações conjuntas, incluindo investigações e medidas de execução conjuntas nas quais participem membros ou pessoal das autoridades de controlo de outros Estados-Membros. 2. Nos casos em que o responsável pelo tratamento ou o subcontratante tenha estabelecimentos em vários Estados-Membros ou nos casos em que haja um número significativo de titulares de dados em mais do que um Estado-Membro que sejam suscetíveis de ser substancialmente afetados pelas operações de tratamento, uma autoridade de controlo de cada um desses Estados-Membros tem direito a participar nas operações conjuntas. A autoridade de controlo competente nos termos do artigo 56º, n.° 1 ou n.° 4, convida a autoridade de controlo de cada um desses Estados-Membros a participar nas operações conjuntas e responde sem demora ao pedido de uma autoridade de controlo para participar. 3. As autoridades de controlo podem, nos termos do direito do seu Estado-Membro, e com a autorização da autoridade de controlo de origem, conferir poderes, nomeadamente poderes de investigação, aos membros ou ao pessoal da autoridade de controlo de origem implicados nas operações conjuntas ou, na medida em que o direito do Estado-Membro da autoridade de controlo de acolhimento o permita, autorizar os membros ou o pessoal da autoridade de controlo de origem a exercer os seus poderes de investigação nos termos do direito do Estado-Membro da autoridade de controlo de origem. Esses poderes de investigação podem ser exercidos apenas sob a orientação e na presença de membros ou pessoal da autoridade de controlo de acolhimento. Os membros ou pessoal da autoridade de controlo de origem estão sujeitos ao direito do Estado-Membro da autoridade de controlo de acolhimento."

própria e de independência, conforme arts. 68º, n.° 1 e 69º. Segundo Blum e Arantes, é responsável pela coerência das decisões aplicadas pelas APDs.[247]

O Comité é composto por um diretor da autoridade de controlo de cada Estado-Membro e da Autoridade Europeia para a Proteção de Dados (AEPD), ou pelos respetivos representantes, sendo que se um Estado-Membro possuir mais de uma autoridade de controlo, haverá apenas um representante comum, nomeado nos termos do direito desse Estado-Membro. A Comissão pode participar nas atividades e reuniões do Comité, mas não tem direito de voto. A AEPD tem direito de voto apenas nas decisões que digam respeito a princípios e normas aplicáveis às instituições, órgãos, organismos e agências da União que correspondam, em substância, às do presente regulamento. Tais regras constam no art. 68º do RGPD[248]. As decisões do Comité, segundo o art. 72º do RGPD, são tomadas por maioria simples dos seus membros, salvo disposição em contrária no RGPD, como, *verbi gratia*, o seu regulamento interno que é aprovado por maioria de dois terços dos seus membros.[249]

É determinado que as ADPs submetam ao Comité as decisões que afetem os titulares dos dados de outros Estados-Membros. Cabe ao Comité, tanto a apresentação de pareceres, quanto a tomada de decisões com efeito vinculante.

A emissão de pareceres ocorre, nos termos do art. 64º, mediante o envio da decisão pelas autoridades de controlo, nas hipóteses de: situações sujeitas à exigência de avaliação do impacto; aprovação da edição ou alteração de um código de conduta; aprovação de critérios de certificação; aferição de conteúdo de cláusulas-tipo de proteção de dados, autorizações *ad hoc* e regras vinculativas às empresas.

Já as decisões vinculativas são tomadas na hipótese de divergências das ADPs, especialmente em matéria transnacional de dados, conforme o art. 65º do RGPD. O RGPD também previu, no art. 66º, o procedimento de urgência, quando este se fizer necessário para defender os direitos e liberdades dos titulares dos dados. Podem as autoridades de controlo adotar medidas urgentes provisórias, aplicadas unicamente no seu território por período não superior a três meses, quando do procedimento de controlo da coerência

[247] BLUM, op. cit., p. 247.
[248] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit.
[249] Ibid.

dos arts. 63º, 64º e 65º ou do procedimento do art. 60º, ou postular um parecer ou decisão vinculativa definitiva do Comité, quando estiver adotado a medida provisória, mas se fizer necessária a definitiva. Ao invés da autoridade de controlo adotar a medida urgente, pode ela solicitar o parecer ou a decisão urgente ao Comité, para defender os direitos e liberdades dos titulares dos dados, devendo expressar os motivos. O RGPD ainda prevê diversas atribuições ao Comité no art. 70º[250]. Em que pese o princípio da transparência nortear o RGPD, os debates do Comité são confidenciais quando tal órgão considerar necessário, seguindo o seu regulamento interno (art. 76º, n.°1).

Por fim, adentra-se à análise do Capítulo VIII do RGPD, que é nominado de "Vias de recurso, responsabilidade e sanções", aplicável nas situações de violação aos dispositivos do Regulamento.

O RGPD garante aos titulares dos dados pessoais, quando houver alguma violação ao Regulamento, o direito de: reclamação a uma autoridade de controlo, ação judicial contra a autoridade de controlo e contra o responsável pelo tratamento ou o subcontratante.

O direito de reclamação é o de acesso a uma autoridade de controlo, podendo esta ser do domicílio ou do local de trabalho do titular dos dados ou, ainda, do local onde foi praticada a infração. Porém, a autoridade de controlo que recebeu a reclamação poderá não ser aquela que apreciará o caso, diante do princípio *one-stop-shop*. O autor da reclamação também possui o direito de informação sobre o andamento e a uma decisão, a cargo da autoridade de controlo, conforme o art. 77º.

O RGPD também assegurou ao titular dos dados ou pessoa coletiva a via judicial, contra as APDs ou em face de um responsável pelo tratamento ou um subcontratante, conforme art. 78º e 79º[251]. Em relação às APDs, pode o titular ajuizar a ação em face das decisões vinculativas das autoridades de controlo ou quando a autoridade de controlo for inerte, ou seja, não tratar a reclamação ou não informar o titular dos dados, no prazo de três meses, sobre o andamento ou o resultado. Já em relação ao responsável pelo tratamento ou um subcontratante, esta é cabível quando tiverem seus direitos violados

[250] Ibid.
[251] Ibid.

em face de um tratamento contrário ao Regulamento. Mas o direito ação judicial não exclui um possível recurso administrativo ou uma via extrajudicial.

Seguindo o art. 80º do RGPD[252], pode o titular, tanto na reclamação, quanto na via judicial, atuar diretamente ou ser representado por uma organização, organismo ou associação sem fins lucrativos, de interesse público devidamente constituído no Estado, que atue na defesa dos direitos e liberdades relacionada à proteção de dados. Tal entidade será uma mandatária, podendo estar autorizada até a receber indenização do responsável pelo tratamento ou subcontratante, se previsto na legislação do Estado-Membro essa derradeira hipótese.

Visando conferir maior segurança jurídica e uniformização nas decisões judiciais dos Estados-Membros da União, o art. 81º prevê a possibilidade de suspensão do processo, *ex officio,* da ação mais nova ou a declinação da competência, essa a pedido da parte, quando tramitarem em Tribunais de Estados-Membros distintos ações relativas ao mesmo assunto no que se refere às atividades de tratamento do mesmo responsável pelo tratamento ou subcontratante. Para que haja a declinação de competência, deve a primeira ação encontrar-se na primeira instância, ser esse primeiro Tribunal acionado competente para conhecer dos pedidos e a lei autorize que seja apensada a segunda ação.

O agente que causa danos materiais ou imateriais, por violação à legislação, deve reparar o lesado, conforme o disposto no art. 82º do RGPD. Trata-se, assim, da responsabilidade civil, o dever de indenização do responsável pelo tratamento e/ou do subcontratante. Para a configuração da responsabilidade civil, três elementos se apresentam como pressupostos: a ilicitude, o nexo causal e o dano.

a) em relação à ilicitude, o disposto no art. 82º, n.° 1 é bastante amplo e alcança toda e qualquer "violação do presente regulamento", interpretação extensiva que deve prevalecer, apesar do disposto no n.° 2 aparente restringir a responsabilidade apenas aos danos decorrentes do tratamento dos dados. Daí porque pode a responsabilidade decorrer de tratamentos ilegais, afronta a direitos, obrigações ou vedações legais que estejam indiretamente relacionadas

[252] Ibid.

com as atividades dos agentes de tratamento.[253] Mas não apenas a violação ao RGPD enseja indenização. O Considerando 146 também a assegura por danos provocados "pela violação de outras regras do direito da União ou dos Estados-Membros e os que violem os atos delegados e de execução adotados nos termos do presente regulamento e o direito dos Estados-Membros que dê execução a regras do presente regulamento."[254]

b) em relação ao dano, este não é definido no RGPD, pelo que caberá ao direito interno dos Estados-Membros ou ao TJUE determinar o que seria o dano. Além dessa questão, outras duas podem ser acrescidas: a quantificação do dano que será efetuada por cada sistema jurídico e a competência dos Tribunais dos Estados-Membros para apreciar tais litígios reparatórios, conforme o art. 82º, n.° 6 do RGPD. Como forma de assegurar certa uniformidade, na interpretação pelos Tribunais locais, o Considerando 146 estabelece que "[o] conceito de dano deverá ser interpretado em sentido lato à luz da jurisprudência do Tribunal de Justiça, de uma forma que reflita plenamente os objetivos do presente regulamento", assim como que "[o]s titulares dos dados deverão ser integral e efetivamente indenizados pelos danos que tenham sofrido."[255] Segundo o art. 82º, n.° 1, o dano pode ser material (patrimonial) ou imaterial (a discriminação, a exposição pública, a ansiedade e outros). O TJUE[256], no que tange à responsabilidade civil, determina a observância, por parte dos Tribunais locais, de dois princípios, o da equivalência e o da efetividade[257]. Seguindo o entendimento do TJUE, ao apreciar a causa, os Tribunais devem atentar para que o efeito da decisão desestimule a reiteração da conduta[258], mas sem a

---

[253] CORDEIRO, A. Barreto Menezes. Repercussões do RGPD sobre a responsabilidade civil. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.) *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 777-795. cit. p. 780. ISBN 978855321663-5.

[254] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit.

[255] Ibid.

[256] UNIÃO EUROPEIA. TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA (TJUE). Pedido de decisão prejudicial no processo C - 494/16: Tribunal de Trapani - Itália- Espanha. 1ª Secção. Data do acórdão: 7.3.2018. [Consultado 26 março 2020]. Disponível na internet: < http://curia.europa.eu/juris/document/document.jsf?text=&docid=200013&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=911006>.

[257] O princípio da equivalência assegura que os lesados não podem ser postos, quando da aplicação do Direito da União, em uma situação inferior quando se aplique um dispositivo de lei interna análoga. Já o princípio da efetividade assegura que não sejam postos obstáculos ao exercício dos direitos reconhecidos pelo Direito da União.

[258] UNIÃO EUROPEIA. TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA (TJUE). Pedido de decisão prejudicial no processo C - 180/95: Pedido de decisão prejudicial: Arbeitsgericht Hamburg - Alemanha. Data do acórdão: 22.4.1997. [Consultado 26 março 2020]. Disponível na internet:

função punitiva, salvo se o Direito local estabelecer essa sanção para casos similares[259].

c) o nexo causal é o elo entre a violação e o dano, conforme as expressões "devido a" do art. 82º, n.° 1 ou "causados por" do art. 82º, n.° 2, ambos do RGPD. Também, em sede de nexo causal, devem os Tribunais locais interpretar tal nexo de acordo com a jurisprudência do TJUE, seguindo os princípios da equivalência e da efetividade. Frise-se que o TJUE não exige o nexo causal direto entre ato infrator e o dano. [260]

No que tange aos sujeitos lesados, para fins de reparação civil, amparados com fulcro no art. 82º do RGPD, surge a indagação se seria qualquer pessoa singular ou somente os titulares dos dados. Em prol de qualquer pessoa singular, têm-se os seguintes argumentos: o art. 82º, n.° 1 utiliza a expressão "qualquer pessoa"; o Considerando 146, faz uso, no primeiro parágrafo, da expressão "danos de que alguém possa ser vítima"; um dos objetivos é a proteção dos direitos e liberdades fundamentais das pessoas singulares, não somente a proteção de dados, assim como a livre circulação dos dados na União, nos termos do art. 1º, n.° 2 e 3 do RGPD; o art. 82º, n.° 2 do RGPD não exclui os danos causados a terceiros; o RGPD fixa deveres genéricos aos agentes de tratamento, além dos deveres para com os titulares dos dados. Já a favor de que o art. 82º apenas beneficiaria os titulares dos dados, têm-se: o Considerando 146, faz referência no sexto parágrafo apenas aos titulares dos dados; o RGPD tem como designo proteger os direitos dos titulares dos dados pessoais; poderia ter sido utilizado o termo pessoas singulares ou coletivas, mas assim não o fez; o art. 82º, n.° 2 do RGPD faz referência à expressão tratamento dos dados, o que pressupõe a relação entre os dados e o titular; as obrigações impostas aos agentes de tratamento visam proteger os interesses dos titulares dos dados e não de terceiros.[261] Cordeiro cita como defensores da primeira teoria Matthias Bergt,

---

<http://curia.europa.eu/juris/showPdf.jsf?text=&docid=100350&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=914963>.

[259] Id. Pedido de decisão prejudicial no processo C - 295/04: Pedido de decisão prejudicial: Giudice di pace di Bitonto - Itália. 3ª Secção. Data do acórdão: 13.7.2006. [Consultado 26 março 2020]. Disponível na internet: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=56474&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=916296>.

[260] Id. Pedido de decisão prejudicial no processo C - 557/12: Pedido de decisão prejudicial: Oberster Gerichtshof (Áustria). 5ª Secção. Data do acórdão: 5.6.2014. [Consultado 26 março 2020]. Disponível na internet: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=153312&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=920778>.

[261] CORDEIRO, op. cit., p. 785-786.

Sabine Quaas e Philip Laue, Judith Nink e Sascha Kremer; e da segunda, mais restritiva, Peter Gola, Carlo Plitz, Bernhard Krebe, Eike Michael Frenzel, Thomas Becker, Jürgen Hartung e Lisa Büttgen.[262] Adota-se o entendimento de que o artigo ampara qualquer pessoa singular lesada e não apenas os titulares dos dados, diante dos fundamentos expostos, especialmente por pretender o RGPD a tutela dos direitos e garantias fundamentais de forma ampla, incluindo a proteção de dados pessoais.

Quanto aos responsáveis pela reparação do dano, com fulcro no art. 82º do RGPD, existem duas categorias de sujeitos: os responsáveis pelo tratamento e os subcontratantes. Os responsáveis têm sua definição estabelecida no art. 4º, n.° 7 do RGPD, pessoa singular ou coletiva, privada ou pública, que determina as finalidades e os meios de tratamento de dados pessoais. Já o subcontratante, com definição no art. 4º, n.° 8 do RGPD, é uma pessoa singular ou coletiva, pública ou privada, que trate os dados pessoais por conta do responsável pelo tratamento. Este é um mandatário. Como forma de distinguir as duas figuras, Voigt e Bussche citam características dos responsáveis: liberdade de utilização dos dados pessoais; conjugação de dados recebidos com os já detidos anteriormente; a possibilidade de utilização para outros fins distintos dos fixados inicialmente; recolha dos dados diretamente com os titulares; assunção de responsabilidades autônomas pelo tratamento.[263]

Caso o lesado deseje interpor ação contra outro que não seja um dos agentes citados, não pode ele se utilizar do art. 82º do RGPD, podendo se valer, no caso do ordenamento jurídico português, do art. 483º do Código Civil.[264]

O responsável pelo tratamento é responsável civilmente desde que esteja envolvido no tratamento que viole o regulamento. Já o subcontratante somente poderá ser responsabilizado por violações às suas obrigações que lhe sejam específicas ou por não cumprir as instruções lícitas do responsável. (art. 82º, n.° 2 do RGPD). Obrigações específicas ao subcontratante situam-se nos arts. 28º, 29º, 32º, 37º e 38 do RGPD. Deve o

[262] Ibid., p. 784-785.

[263] VOIGT, Paul; BUSSCHE, Axel von dem. The EU General Data Protection Regulation (RGPD) apud Ibid., p. 788.

[264] PORTUGAL – Código Civil - Decreto-Lei n.º 47344. *"D.G."* (25-11-1966). [Consultado 26 março 2020]. Disponível na internet: < https://dre.pt/web/guest/legislacao-consolidada/-/lc/123928118/202003261339/diploma?did=34509075&_LegislacaoConsolidada_WAR_drefrontofficeportlet_rp=indice>. "SECÇÃO V Responsabilidade civil SUBSECÇÃO I Responsabilidade por factos ilícitos ARTIGO 483º (Princípio geral) 1. Aquele que, com dolo ou mera culpa, violar ilicitamente o direito de outrem ou qualquer disposição legal destinada a proteger interesses alheios fica obrigado a indemnizar o lesado pelos danos resultantes da violação. 2. Só existe obrigação de indemnizar independentemente de culpa nos casos especificados na lei."

subcontratante, mesmo como mandatário, respeitar as normas do RGPD e os direitos dos titulares, ainda que tenha que contrariar as instruções recebidas, razão pela qual somente será responsável se descumprir instruções lícitas, sendo que as ilícitas, além de não as cumprir, deve as informar ao responsável, conforme o art. 28, n.°3 do RGPD. Mas conforme leciona Cordeiro, se o subcontratante, ao seguir as instruções do responsável viole o RGPD ou legislação extravagante, poderá ele ser responsabilizado, caso haja a violação de uma obrigação específica.[265]

O responsável pelo tratamento e o subcontratante somente poderão se eximir da responsabilidade se provarem que, "de modo algum", são responsáveis pelo dano. Nesse ponto deve-se compreender esse art. 82º, n.° 3 que cabem a eles a prova de que não existe a ilicitude e culpa de seus atos (exclusão da ilicitude e culpa), ou não terem contribuído de forma alguma para o dado de qualquer relação (exclusão do nexo causal) com o dano, para fins de rechaçar a responsabilidade.

Como forma de assegurar a reparação integral dos danos ao titular dos dados lesado, caso haja mais de um responsável pelo dano, o RGPD prevê a responsabilidade solidária e conjunta de todos os envolvidos no tratamento, responsável pelo tratamento e subcontratante. Em que pese o Considerando 146[266] estabelecer uma exceção à regra da solidariedade, a sua aplicação é duvidosa, posto que não consta da parte normativa, não havendo justificativa alguma.

É assegurando, entretanto, o direito de regresso daquele que indenizou na totalidade, uma vez que qualquer responsável pelo tratamento que esteja envolvido é responsável pelos danos causados em face de um tratamento que afronte o regulamento, mas subcontratante somente é responsável caso não tenha cumprido as obrigações específicas aos subcontratantes ou se não tiver atendido às instruções lícitas do responsável pelo tratamento (art. 82º).[267]

No que tange às sanções, passíveis de serem aplicadas aos infratores da legislação,

[265] CORDEIRO, op. cit., p. 790.

[266] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit. "Considerando o seguinte: [...] (146) [...] Porém, se os processos forem associados a um mesmo processo judicial, em conformidade com o direito dos Estados-Membros, a indemnização poderá ser repartida em função da responsabilidade que caiba a cada responsável pelo tratamento ou subcontratante pelos danos causados em virtude do tratamento efetuado, na condição de ficar assegurada a indemnização integral e efetiva do titular dos dados pelos danos que tenha sofrido."

[267] Ibid.

a análise deve ocorrer da combinação dos arts. 83º e 84º, com os Considerandos 148, 149 e 152.

O art. 83º do RGPD estabelece as coimas. O n.° 2[268] do citado artigo elenca as condições que devem ser levadas em consideração na dosimetria das coimas, sendo que elas devem ser individualizadas, efetivas, proporcionais e dissuasivas.

O RGPD usa, como sinónimos, na versão em português, as expressões "sanções administrativas" e "coimas", em que pese no direito português as coimas localizem-se no "Direito de Mera Ordenação Social", âmbito distinto do Direito Penal e do Direito Administrativo.

Dessa forma, ainda que apenas o art. 84º do RGPD seja intitulado de sanções, elas não se esgotam nesse artigo, uma vez que existe previsão das coimas no art. 83º. Aliás, o art. 84 do RGPD fixa que os Estados-Membros podem estabelecer outras sanções, e que tais sanções devem ser também, efetivas, proporcionadas e dissuasivas. Aliás, esse artigo não deixa claro quanto à possibilidade de estabelecimento de sanções de natureza penal e quais outras sanções poderiam ser aplicadas e em que medida. Se por um lado isso atende ao respeito à peculiaridade de cada ordenamento jurídico nacional, por outro pode conduzir a tratamentos distintos em situações jurídicas idênticas, quando ocorridas em países diversos, mas pertencentes à União Europeia.

Da análise conjunta com os Considerandos 148, 149 e 152, não resta dúvida quanto à possibilidade do estabelecimento de sanções penais pelos Estados-Membros, para a hipótese de descumprimento do RGPD.[269]

---

[268] Ibid. "2. Consoante as circunstâncias de cada caso, as coimas são aplicadas para além ou em vez das medidas referidas no artigo 58º, n.° 2, alíneas a) a h) e j). Ao decidir sobre a aplicação de uma coima e sobre o montante da coima em cada caso individual, é tido em devida consideração o seguinte: a) A natureza, a gravidade e a duração da infração tendo em conta a natureza, o âmbito ou o objetivo do tratamento de dados em causa, bem como o número de titulares de dados afetados e o nível de danos por eles sofridos; b) O caráter intencional ou negligente da infração; c) A iniciativa tomada pelo responsável pelo tratamento ou pelo subcontratante para atenuar os danos sofridos pelos titulares; d) O grau de responsabilidade do responsável pelo tratamento ou do subcontratante tendo em conta as medidas técnicas ou organizativas por eles implementadas nos termos dos artigos 25º e 32º; e) Quaisquer infrações pertinentes anteriormente cometidas pelo responsável pelo tratamento ou pelo subcontratante; f) O grau de cooperação com a autoridade de controlo, a fim de sanar a infração e atenuar os seus eventuais efeitos negativos; g) As categorias específicas de dados pessoais afetadas pela infração; h) A forma como a autoridade de controlo tomou conhecimento da infração, em especial se o responsável pelo tratamento ou o subcontratante a notificaram, e em caso afirmativo, em que medida o fizeram; i) O cumprimento das medidas a que se refere o artigo 58º, n.° 2, caso as mesmas tenham sido previamente impostas ao responsável pelo tratamento ou ao subcontratante em causa relativamente à mesma matéria; j) O cumprimento de códigos de conduta aprovados nos termos do artigo 40º ou de procedimento de certificação aprovados nos termos do artigo 42º; e k) Qualquer outro fator agravante ou atenuante aplicável às circunstâncias do caso, como os benefícios financeiros obtidos ou as perdas evitadas, direta ou indiretamente, por intermédio da infração."

[269] Ibid. "Considerando o seguinte: [...] (148) A fim de reforçar a execução das regras do presente regulamento, deverão ser impostas sanções, incluindo coimas, por violação do presente regulamento, para além, ou em substituição, das medidas adequadas que

Conforme leciona Freitas

> [d]eixando de lado a confusão terminológica entre 'sanções administrativas' e 'coimas' – que ocorre ao longo do Regulamento e cuja explicação pode ser encontrada nas idiossincrasias jurídicas dos Estados-Membros, por vezes emprestando-lhe um caráter administrativo, outras vezes reconhecendo-lhe autonomia diante de outros ramos jurídicos –, verifica-se que os Estados-Membros têm, pelo menos segundo a sua tradição jurídica, a possibilidade de punir as infrações ao RGPD com coimas (ou sanções administrativas noutros ordenamentos) ou sanções penais.[270]

Dois patamares de coima são estabelecidos. Para infrações mais leves, o teto é de EUR 10 milhões ou, no caso de empresa, 2% do faturamento bruto anual do exercício fiscal anterior à instauração do processo, o que forma maior, da empresa ou do conglomerado.[271] Segundo Machado,

> [n]esse caso, diversas são as situações previstas no GDPR, como por exemplo, violação de princípios como "privacy by design", não cumprimento das obrigações relacionadas ao processamento ou a não designação de um Responsável pela Proteção de Dados. As multas para esses casos buscam remediar a efetiva ou potencial violação dos direitos estabelecidos nos artigos 8º, 11, 25, 39, 42 e 43 do Regulamento.[272][273]

Já para infrações mais graves, o teto da coima é de EUR 20 milhões ou, no caso de empresa, a 4% do faturamento bruto anual, o que for maior.[274] Blum e Arantes esclarecem que

---

venham a ser impostas pela autoridade de controlo nos termos do presente regulamento. Em caso de infração menor, ou se o montante da coima suscetível de ser imposta constituir um encargo desproporcionado para uma pessoa singular, pode ser feita uma repreensão em vez de ser aplicada uma coima. Importa, porém, ter em devida conta a natureza, gravidade e duração da infração, o seu caráter doloso, as medidas tomadas para atenuar os danos sofridos, o grau de responsabilidade ou eventuais infrações anteriores, a via pela qual a infração chegou ao conhecimento da autoridade de controlo, o cumprimento das medidas ordenadas contra o responsável pelo tratamento ou subcontratante, o cumprimento de um código de conduta ou quaisquer outros fatores agravantes ou atenuantes. A imposição de sanções, incluindo coimas, deverá estar sujeita às garantias processuais adequadas em conformidade com os princípios gerais do direito da União e a Carta, incluindo a proteção jurídica eficaz e um processo equitativo. (149) Os Estados-Membros deverão poder definir as normas relativas às sanções penais aplicáveis por violação do presente regulamento, inclusive por violação das normas nacionais adotadas em conformidade com o presente regulamento, e dentro dos seus limites. Essas sanções penais podem igualmente prever a privação dos lucros auferidos em virtude da violação do presente regulamento. Contudo, a imposição de sanções penais por infração às referidas normas nacionais, bem como de sanções administrativas, não deverá implicar a violação do princípio non bis in idem, conforme é interpretado pelo Tribunal de Justiça. [...] (152) Sempre que o presente regulamento não harmonize sanções administrativas, ou se necessário noutros casos, por exemplo, em caso de infrações graves às disposições do presente regulamento, os Estados-Membros deverão criar um sistema que preveja sanções efetivas, proporcionadas e dissuasivas. A natureza das sanções, penal ou administrativa, deverá ser determinada pelo direito do Estado-Membro."

[270] FREITAS, op. cit., p. 116.

[271] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit. "Artigo 83º Condições gerais para a aplicação de coimas [...] 4. A violação das disposições a seguir enumeradas está sujeita, em conformidade com o n.° 2, a coimas até 10 000 000 EUR ou, no caso de uma empresa, até 2 % do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado: a) As obrigações do responsável pelo tratamento e do subcontratante nos termos dos artigos 8º, 11º, 25º a 39º e 42º e 43º; b) As obrigações do organismo de certificação nos termos dos artigos 42º e 43º; c) As obrigações do organismo de supervisão nos termos do artigo 41º, n.° 4;"

[272] MACHADO, op. cit., p. 13.

[273] *"Privacy by design"* é a "Privacidade desde a concepção". (tradução nossa). Princípio segundo o qual qualquer projeto que envolva tratamento de dados pessoais deve ser realizado mantendo a proteção e a privacidade desses dados em todas as suas fases, desde a concepção.

[274] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit. "Artigo 83º Condições gerais para a aplicação de coimas [...] 5. A violação das disposições a seguir enumeradas está sujeita, em conformidade com o n.° 2, a coimas até 20 000 000

> [...] ainda que a legislação do Estado Membro não preveja a aplicação de sanções pecuniárias pelas DPAs no caso de violações no tratamento de dados pessoais, as multas poderão ser sugeridas pelas DPAs e impostas pelo judiciário – desde que preservado o caráter proporcional e dissuasório das sanções.[275]

Caso ocorra, em uma mesma operação de tratamento, violação a diversas disposições do RGPD, o valor máximo da coima será até o montante previsto para a infração mais grave.

Conforme se observa, o teto das coimas diverge, não apenas em face da espécie da infração, mas também quando o infrator é empresa ou não.

A noção de empresa deve ser obtida, não apenas do art. 4º, n.° 18 do RGPD[276], mas através do Considerando 150, segundo o qual "[s]empre que forem impostas coimas a empresas, estas deverão ser entendidas como empresas nos termos dos artigos 101º e 102º do TFUE para esse efeito."[277] Ou seja, a noção de empresa, para fins de aplicação de coimas estende-se a grupo empresarial, que por sua vez é definido no art. 4º, n.° 19 do RGPD[278]. O TJUE já se manifestou nesse sentido.[279]

O RGPD não fixou um valor mínimo para as coimas, estabelecendo apenas critérios para a sua fixação com alto nível de discricionariedade, afastando-se de um modelo

---

EUR ou, no caso de uma empresa, até 4 % do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado: a) Os princípios básicos do tratamento, incluindo as condições de consentimento, nos termos dos artigos 5º, 6º, 7º e 9º; b) Os direitos dos titulares dos dados nos termos dos artigos 12º a 22º; c) As transferências de dados pessoais para um destinatário num país terceiro ou uma organização internacional nos termos dos artigos 44º a 49º; d) As obrigações nos termos do direito do Estado-Membro adotado ao abrigo do capítulo IX; e) O incumprimento de uma ordem de limitação, temporária ou definitiva, relativa ao tratamento ou à suspensão de fluxos de dados, emitida pela autoridade de controlo nos termos do artigo 58º, n.° 2, ou o facto de não facultar acesso, em violação do artigo 58º, n.° 1. 6. O incumprimento de uma ordem emitida pela autoridade de controlo a que se refere o artigo 58º, n.° 2, está sujeito, em conformidade com o n.° 2 do presente artigo, a coimas até 20 000 000 EUR ou, no caso de uma empresa, até 4 % do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante mais elevado."

[275] BLUM, op. cit., p. 251.

[276] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit. "Artigo 4º Definições Para efeitos do presente regulamento, entende-se por: [...]18) 'Empresa', uma pessoa singular ou coletiva que, independentemente da sua forma jurídica, exerce uma atividade económica, incluindo as sociedades ou associações que exercem regularmente uma atividade económica;"

[277] Ibid.

[278] Ibid. "Artigo 4º Definições Para efeitos do presente regulamento, entende-se por: [...]19) 'Grupo empresarial', um grupo composto pela empresa que exerce o controlo e pelas empresas controladas;"

[279] UNIÃO EUROPEIA. TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA (TJUE). Pedido de decisão prejudicial no processo C - 217/05: Tribunal Supremo - Espanha. 3ª Secção. Data do acórdão: 14.12.2006. [Consultado 20 março 2020]. Disponível na internet: < http://curia.europa.eu/juris/showPdf.jsf?text=&docid=66539&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=139883>. "39. Ora, é de jurisprudência constante que, no contexto do direito comunitário da concorrência, o conceito de empresa abrange qualquer entidade que exerça uma actividade económica, independentemente do estatuto jurídico dessa entidade e do seu modo de financiamento (acórdãos de 23 de Abril de 1991, Höfner e Elser, C-41/90, Colect., p. I-1979, n.º 21, e de 11 de Julho de 2006, FENIN/Comissão, C-205/03 P, ainda não publicado na Colectânea, n.º 25). 40 O Tribunal de Justiça precisou igualmente que o conceito de empresa, inserido no mesmo contexto do direito da concorrência, deve ser entendido como designando uma unidade económica do ponto de vista do objecto do acordo em causa, mesmo que, do ponto de vista jurídico, essa unidade económica seja constituída por várias pessoas singulares ou colectivas (acórdão de 12 de Julho de 1984, Hydrotherm, 170/83, Recueil, p. 2999, n.º 11)."

numérico e delimitado, o que seria mais adequado, como forma de resguardar a segurança jurídica, evitando-se discrepâncias. Segundo Freitas,

> [...] este modelo de determinação da medida da coima levanta sérias dúvidas quanto à sua compatibilidade com os princípios fundamentais encontrados nos textos constitucionais dos Estados-Membros e nos instrumentos jurídicos supranacionais no domínio da proteção de direitos humanos, nomeadamente o princípio da legalidade e da certeza.[280]

3.2 A Lei Geral de Proteção de Dados brasileira e a sua adequação jurídico-constitucional

A Lei Geral de Proteção de Dados (LGPD) é o primeiro texto normativo brasileiro a tratar sobre a proteção de dados pessoais de forma específica, suprindo uma lacuna no marco regulatório.

Antes do citado texto legal, existiam textos normativos esparsos, como: Lei do Cadastro Positivo (Lei n.° 12.414/2011), o Código de Defesa do Consumidor (Lei n.° 8.078/1990), a Lei de Acesso à Informação (Lei n.° 12.527/2011) e o Marco Civil da Internet (Lei n.° 12.965/2014).

A LGPD não é uma mera continuação dessa legislação anterior, posto que traz uma nova regulamentação e abordagem sobre a proteção e uso dos dados pessoais, reconhecendo a importância desde na sociedade da informação. E nenhum dos instrumentos jurídicos anteriores é capaz de alcançar os objetivos desse novo texto normativo. Tal norma fixou regras objetivas de tratamento dos dados pessoais. Cots e Oliveira sustentam "[...] torna-se possível responder a perguntas básicas sobre se um tratamento de dados pessoais é lícito ou não sem que se adentre considerações subjetivas a respeito de violação da privacidade ou de outros direitos de natureza subjetiva."[281]

Devido à importância dessa nova lei para a sociedade atual, aplicável nas mais diversas situações de tratamento de dados e a introdução através dela de novos elementos jurídicos, o legislador brasileiro foi levado a fazer constar no texto, de forma

[280] FREITAS, op. cit., p. 118.
[281] COTS, op. cit., p. 8.

expressa, conceitos, princípios e um período *de vacatio legis* longo, se comparados com demais normas (24 meses, conforme o art. 65, inciso II).

A fim de compreender como a LGPD se adequa ao sistema constitucional brasileiro, deve-se elucidar e diferenciar alguns termos trazidos por ela, a correspondência e a compatibilidade deles com a Constituição Federal brasileira (CFb).

A LGPD prevê objetivos e fundamentos, figuras distintas tratadas de forma harmoniosa, conferindo coerência e efetividade na sua aplicação. A definição de cada uma delas é essencial para o enquadramento da LGPD na seara constitucional e sua convergência com os dispositivos constitucionais.

Objetivos são as direções, as intenções delineadas, delimitadas, que visam um fim específico. É algo que se pretende alcançar, o propósito.

Fundamento, do latim *fundamentum*, é o alicerce onde se apoia e se desenvolve algo. Segundo Cots e Oliveira, "[...] o suporte sobre o qual se sustenta alguma coisa."[282] A base sobre a qual é construído um argumento, ou, no caso, a lei.

O art. 1º, parte final, da LGPD dispõe que o objetivo texto legislativo é "[...] proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural."[283]

A utilização do verbo "proteger" no artigo demonstra que o legislador vislumbrou o titular de dados em uma posição de vulnerabilidade perante àquele que realiza do tratamento. Ou seja, trata-se de uma relação que se desenvolve de uma maneira desigual, sendo que a lei viria para equilibrar as relações jurídicas. Semelhante postura é encontrada no Código de Defesa do Consumidor brasileiro, conforme disposto nos arts. 1º e 4º, inciso I[284].

O direito de liberdade, como objetivo da lei, de uma forma genérica, está disposto no art. 5º, *caput* da CFb. Tarefa das mais árduas é definir tal direito, em face das suas

[282] Ibid., p. 46.
[283] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 13.709... op. cit.
[284] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 8.078... op. cit. "Art. 1° O presente código estabelece normas de proteção e defesa do consumidor, de ordem pública e interesse social, nos termos dos arts. 5°, inciso XXXII, 170, inciso V, da Constituição Federal e art. 48 de suas Disposições Transitórias. Art. 4º A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios: I - reconhecimento da vulnerabilidade do consumidor no mercado de consumo;"

mais diversas vertentes, como a liberdade de ação, locomoção, opinião ou pensamento, expressão, crença, reunião, informação, dentre outros. Mas de uma forma geral, pode-se dizer que ele é o direito fundamental que assegura à pessoa humana o poder de escolha e de atuação, com fim de satisfação pessoal. Segundo Cunha Júnior, é uma prerrogativa fundamental que confere o ser humano do poder de autodeterminação ou de determinar-se de acordo com a sua consciência.[285]

A privacidade, a qual englobaria a intimidade e vida privada do art. 5º, inciso X da CFb, e o desenvolvimento da personalidade, sem o qual não se teria como atender a um dos fundamentos da república, a dignidade da pessoa humana do art. 1º, inciso III da *lex mater*[286]*,* são os dois outros objetivos*.*

A privacidade mantém um elo indissociável com a liberdade. Exercer o direito à privacidade é exercer o direito à liberdade, liberdade de se expor ou não de não se expor, em que medida deve ser essa exposição, de revelar seus dados ou não e o controlo dos revelados.

Por óbvio, não se tem como se promover o desenvolvimento da personalidade sem a tutela dos dados pessoais, por ser este um direito da personalidade, conforme já exposto. Esses dois objetivos também foram descritos como fundamentos.

O objetivo legal expresso de "livre desenvolvimento da personalidade" denota a amplitude dos objetivos, não se restringindo à tutela da privacidade, o que inclui a própria autonomia e individualidade. Daí porque Frazão afirma que "[...] o objetivo central da LGPD é resgatar a dignidade dos titulares de dados e seus direitos básicos relacionados à autodeterminação informativa."[287] Tenciona uma ampla proteção ao cidadão em seus direitos fundamentais, inclusive a cidadania e a dignidade, uma vez que, conforme afirma Pasquale, aqueles que controlam os dados inovaram em um sistema em que a maximização do lucro e a inovação estariam acima de qualquer outro valor, não para tratar os titulares dos dados decentemente.[288]

---

[285] CUNHA JÚNIOR, op. cit. p. 604.

[286] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Constituição da República Federativa do Brasil. Op. cit.

[287] FRAZÃO, Ana. Objetivos e alcance da lei geral de proteção de dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.) *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 99-129. cit. p. 100. ISBN 978855321663-5.

[288] PASQUALE, Franck. *The black box society*: The secret algorithms that control money and information. Cambridge: Harvard University Press, 2015. p. 146. ISBN 978067436827-9.

Como fundamentos, têm-se no art. 2º: a autodeterminação informativa (inciso II); a liberdade de expressão, de informação, de comunicação e de opinião (inciso III); a inviolabilidade da intimidade, da honra e da imagem (inciso IV); o desenvolvimento económico e tecnológico e a inovação (inciso V); a livre iniciativa, a livre concorrência e a defesa do consumidor (inciso VI); os direitos humanos, a dignidade e o exercício da cidadania pelas pessoas naturais (inciso VII).[289]

A autodeterminação informativa, que serve de base para o direito à proteção dos dados, consiste naquele que o titular desfruta de controlar os seus dados com liberdade associada à informação. Segundo Cots e Oliveira "Ao titular não incumbe presumir o que será feito com seus dados, sendo obrigação do controlador prestar quantas informações forem necessárias para que a tomada de decisão do titular se dê da melhor maneira possível"[290] Segundo Menezes e Colaço é "[...] a faculdade de o indivíduo decidir, por si só, sobre a exibição e o uso de seus dados pessoais."[291] Esse direito de controlar os seus dados e informações, expressa-se através do consentimento. Mas não em qualquer consentimento. Somente naquele consentimento baseado em uma comunicação eficiente, um consentimento informado, livre e consciente e delimitado para quem e em certas condições. Nesse sentido Tepedino e Teffé advogam que "[...] o vocábulo informado significa que o titular do bem tem de ter ao seu dispor as informações necessárias e suficientes para avaliar corretamente a situação e forma como os seus dados serão tratados."[292] Há, no caso, uma conjugação do dever do controlador de informar o titular sobre os dados deste objeto de tratamento, com a possibilidade de manifestação da vontade do titular dos dados que não poderá ser tolhida por terceiros. E frise-se, a utilização o tratamento das informações sem as hipóteses legais ou para fins diversos daqueles que foram autorizados caracteriza-se como desvio do direito. Nesse sentido Cardoso sustenta que "[...] o abuso do direito se dá através do exercício 'em

[289] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 13.709... op. cit.
[290] COTS, op. cit., p. 52.
[291] MENEZES, Joyceane Bezerra de; COLAÇO, Hian Silva. Quando a lei geral de proteção de dados não se aplica? In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.) *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 157-197. cit. p. 169. ISBN 978855321663-5.
[292] TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.) *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 287-322. cit. p. 301. ISBN 978855321663-5.

direção contrária ou disforme com a função e o espírito' do direito."[293] E esse abuso configura-se com uma violação ao princípio da dignidade humana, uma vez que afeta direitos da personalidade do indivíduo.

A dignidade da pessoa humana é o epicentro dos direitos fundamentais e um dos fundamentos do Estado Democrático de Direito, nos termos do art. 1º, inciso III da CFb.[294] Igualdade e liberdade são essenciais a esse princípio. Esse Estado justifica-se como um meio para assegurar essas liberdades e a igualdade, não compactuando que tais direitos sejam meramente formais. Em outra perspectiva, proteger e incentivar as liberdades equivale a proteger e incentivar a participação política dos indivíduos.

A liberdade de expressão, de informação, de comunicação e de opinião, como fundamentos da LGPD, demonstra que deve haver uma coexistência harmónica entre a privacidade, a proteção de dados e tais liberdades. Essas liberdades têm por pressuposto que o homem busca a sua realização pessoal, cabendo a ele decidir por qual caminho seguir. A liberdade de expressão, de opinião e de informação encontram-se previstas nos artigos 5º incisos IV, IX e XIV da CFb[295].

O direito à informação, em seu tripé de informar, de se informar e de ser informado também se configura como um direito fundamental. Canotilho e Moreira, em relação à abrangência direito à informação, sobre tais facetas, lecionam:

> [o] primeiro consiste, desde logo, na liberdade de transmitir ou comunicar informações a outrem, de as difundir sem impedimentos, mas pode também revestir de forma positiva, enquanto direito a informar, ou seja, direitos a meio para informar. O direito de se informar consiste designadamente na liberdade de escolha da informação, de procura de fontes de informação, isto é, no direito de não ser impedido de se informar. Finalmente, o direito de ser informado é a versão positiva do direito de se informar, consistindo num direito a ser mantido adequadamente e verdadeiramente informado, desde logo, pelos meios de comunicação[...] e pelos poderes públicos [...][296]

Em relação à distinção entre os direitos de opinião e de expressão, Cunha Junior proclama que o direito de opinião é a liberdade de manifestação do pensamento,

---

[293] CARDOSO, Vladimir Mucury. O abuso do direito na perspectiva Civil-Constitucional. In: MORAES, Maria Celina Bodin de (Coord.). *Princípios do direito civil contemporâneo*. Rio de Janeiro: Renovar, 2006. p. 61-110. cit. p. 73. ISBN 857147575-X

[294] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Constituição da República Federativa do Brasil. Op. cit.

[295] Ibid.

[296] CANOTILHO, José Joaquim Gomes; MOREIRA, Vital. *Constituição da república portuguesa anotada.* 3ª ed. Coimbra: Coimbra, 1993. p. 189. ISBN 972320592-0.

expondo juízos, conceitos, convicções e conclusões sobre alguma coisa; já o direito de expressão é o de manifestar as sensações, os sentimentos ou a criatividade do indivíduo, pela pintura, música, teatro, fotografia e outros.[297]

Já Mendes e Branco amplia o conceito de liberdade de expressão, discorrendo que ela tutela, pelo menos quando não houver colisão com outros direitos fundamentais ou valores constitucionalmente estabelecidos, toda opinião, convicção, comentário, avaliação ou julgamento sobre qualquer assunto ou sobre qualquer pessoa, envolvendo tema de interesse público, ou não, de importância e de valor, ou não.[298]

A relatividade dos direitos fundamentais é essencial à coexistência de todos eles. Pois conforme afirmam Matos e Ruzyk:

> Como integrante da liberdade individual, a autodeterminação informativa não poderia, por evidente, ser pensada de modo a aniquilar outras dimensões do mesmo princípio da liberdade, que tem a liberdade de expressão como pilar essencial tanto à compreensão da dimensão privada do princípio como, sobretudo, à própria democracia.[299]

Já a liberdade de comunicação assenta na característica humana da sociabilidade, essencial para a sua a integridade psicossocial.

Ou seja, tais direitos ou liberdades, assim como a tutela dos dados pessoais, visam proporcionar o desenvolvimento da personalidade, sendo necessário de que o indivíduo detenha meios de conhecer a realidade e suas interpretações, para que possa participar de um debate livre e conscientemente tome suas próprias decisões. E esse debate depende de busca da verdade. Coderch cita argumentos em prol da liberdade de expressão: o humanista, quando a liberdade de expressão é vista como um encadeamento dedutivo da dignidade humana; o democrático, uma vez que ela assegura o pluralismo de opiniões, essencial para uma formação da vontade livre, a base de um sistema democrático; o "cético", de criticar o governo, essencial para o controlo da atividade política, por ser esta egoística e interesseira.[300]

---

[297] CUNHA JÚNIOR, op. cit., p. 607.

[298] MENDES, op. cit., p. 268.

[299] MATOS, Ana Carla Harmatiuk; RUZYK, Carlos Eduardo Pianovski. Diálogos entre a lei geral de proteção de dados e a lei de acesso à informação. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.) *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 199-218. cit. p. 204. ISBN 978855321663-5.

[300] CODERCH, Pablo Salvador. *El derecho de la libertad.* Madrid: Centro de Estudios Constitucionales, 1993. p. 40. ISBN 978842590947-4.

A lei também tem por fundamento a inviolabilidade da intimidade, da honra e da imagem. A utilização do termo intimidade decorre da antiga doutrina da existência dos círculos concêntricos, de origem alemã, já superada, onde a intimidade era vista como o círculo mais interior, enquanto a vida privada ou privacidade seria o círculo maior que abarcaria a intimidade.[301] Essa distinção foi acolhida no art. 5º, inciso X da CFb, onde contam os termos "intimidade" e "vida privada". Conclui-se que o constituinte foi zeloso a fim evitar dúvidas interpretativas, optando por incluir os dois termos, assegurando a tutela constitucional de ampla.

A honra e a imagem como fundamentos são também direitos da personalidade previstos no mesmo inciso constitucional. No que tange ao direito à honra, este também é um bem imaterial relativo à personalidade humana, sendo esse patrimônio moral digno de proteção. Também está previsto no art. 5º, inciso X da Constituição Federal brasileira (CFb), como direito distinto da imagem. Seria a honra o conjunto de atributos físicos, morais ou intelectuais correspondentes a uma pessoa. Segundo Noronha a honra seria "[...] o complexo ou conjunto de predicados ou condições da pessoa que lhe conferem consideração social e estima própria."[302] Possui duas aceções, a honra subjetiva e a honra objetiva. A honra subjetiva diz respeito a ele próprio, a opinião que o sujeito tem dos seus atributos físicos, morais e intelectuais. Segundo Mirabete ela "[...] se traduz no apreço próprio, na estima a si mesmo, o juízo que cada um faz de si, que pensa de si, em suma, o auto-respeito, [...]".[303] Independe ela da opinião ou da visão de terceiros. Já a honra objetiva está ligada à visão que do indivíduo no meio social, a sua reputação. É a opinião de terceiros em relação aos atributos físicos, morais e intelectuais do titular do direito. Daí porque "[q]uando falamos que determinada pessoa tem boa ou má reputação no seio

---

[301] Uribe assenta a superação da presente Teoria pelo citado Tribunal Constitucional, pois não é possível realizar-se uma divisão estática em tema tão melindroso como este: "La doctrina alemana ha elaborado la teoría de las esferas, hoy superada por el Tribunal Constitucional Federal, con el reconocimiento del derecho a la autodeterminación informativa. En virtud de dicha teoría, se distinguen diferentes compartimentos o esferas concéntricas en los derechos de la personalidad con distinta intensidad de protección. Así un círculo de protección sería la llamada esfera individual que comprende todo lo relativo a la singularidad individual como la integridad corporal, el honor o el nombre y su protección en la sociedad. Una segunda esfera que abrazaría todo lo privado o íntimo y una tercera que englobaría todo lo secreto que se viola cuando es revelado o conocido por otros. Lo secreto hace referencia a las noticias que deben quedar ocultas, lo íntimo al ámbito de vida familiar y personal y lo individual a la peculiaridad de la persona. Esta teoría fue acogida en Europa y EEUU, si bien criticada por la imposibilidad de mantener dichas esferas en compartimento estancos, sin interrelaciones. Hoy se ha superado y la intimidad no es solo reserva, secreto, aislamiento, sino también control y poder de exclusión respecto a nuestra vida privada." URIBE, Carlos Enrique Serra. *Derecho a la intimidad y videovigilancia policial*. Madrid: Laberinto, 2006, p. 30. ISBN 978848483221-8.

[302] NORONHA, Edgard Magalhães. *Direito Penal:* dos crimes contra a pessoa; dos crimes contra o patrimônio. 33ª ed. São Paulo: Saraiva, 2003. v. 2. p. 110. ISBN 850204313-7.

[303] MIRABETE, Julio Fabbrini. *Manual de direito penal.* 24ª ed. São Paulo: Atlas, 2006. v. 2. p.127. ISBN 852244316-5.

social, estamos nos referindo à honra objetiva [...]".[304] O processamento de dados de forma indevida pode levar a lesões à honra objetiva e subjetiva, em face de divulgação e até a realização de atos discriminatórios.

A imagem é toda forma de representação, de identificação do indivíduo, que podem envolver aspectos físicos, plásticos ou fisionómicos. Está prevista nos incisos V, X e XXVIII, alínea a) do art. 5º da CFb[305]. O direito à imagem é aquele que a pessoa tem em relação à sua forma e os componentes que o distinguem dos demais, individualizando-o. Corresponde à proteção da projeção da personalidade física no mundo externo, como o corpo – face, perfil, olhos, nariz, busto, voz-, atitudes, sorrisos, gestos, vestimentas, expressões faciais e outras e, dessa forma, é possível de ser capturada através de imagens, através dos mais diversos meios, sejam estáticos, como fotografia, escultura, pintura, sejam dinâmicos, como as filmagens e gravações. No dizer de Bittar: "[...] é o vínculo que une a pessoa à sua expressão externa, tomada no conjunto ou em partes significativas (como a boca, os olhos, as pernas, enquanto individualizadoras da pessoa)."[306] Assim a configuração da imagem do indivíduo resta caracterizada não apenas pelo aspecto global físico, mas de partes do corpo ou características que permitam a identificação desse indivíduo. A imagem, como um direito da personalidade, é um dado pessoal. Isto porque ela é capaz de identificar uma pessoa, razão pela qual o seu processamento somente pode ser realizado observando-se os princípios e regras da lei geral de proteção de dados.

Como fundamentos da LGPD também são descritos o desenvolvimento económico, tecnológico e a inovação. Em um país com a economia de mercado, tais fundamentos emergem como valores constitucionais. Nesse sentido, a CFb, no seu art. 218[307] trata

[304] CAPEZ, Fernando. *Curso de direito penal:* parte especial. 15ª ed. São Paulo: Saraiva, 2015. v.2. p. 270. ISBN 978850261905-0.
[305] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Constituição da República Federativa do Brasil. Op. cit.
[306] BITTAR, Carlos Alberto. *Os direitos da personalidade.* 5ª ed. Rio de Janeiro: Forense Universitária, 2001, p. 90. ISBN 852180285-4.
[307] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Constituição da República Federativa do Brasil. Op. cit. "Art. 218. O Estado promoverá e incentivará o desenvolvimento científico, a pesquisa, a capacitação científica e tecnológica e a inovação. § 1º A pesquisa científica básica e tecnológica receberá tratamento prioritário do Estado, tendo em vista o bem público e o progresso da ciência, tecnologia e inovação. § 2º A pesquisa tecnológica voltar-se-á preponderantemente para a solução dos problemas brasileiros e para o desenvolvimento do sistema produtivo nacional e regional. § 3º O Estado apoiará a formação de recursos humanos nas áreas de ciência, pesquisa, tecnologia e inovação, inclusive por meio do apoio às atividades de extensão tecnológica, e concederá aos que delas se ocupem meios e condições especiais de trabalho. § 4º A lei apoiará e estimulará as empresas que invistam em pesquisa, criação de tecnologia adequada ao País, formação e aperfeiçoamento de seus recursos humanos e que pratiquem sistemas de remuneração que assegurem ao empregado, desvinculada do salário, participação nos ganhos econômicos resultantes da produtividade de seu trabalho. § 5º É facultado aos Estados e ao Distrito Federal vincular parcela de sua receita orçamentária a entidades públicas de fomento ao ensino e à pesquisa científica e tecnológica. § 6º O Estado, na execução das atividades previstas no caput, estimulará a articulação entre entes, tanto públicos quanto privados, nas diversas esferas de governo. § 7º O Estado

sobre o desenvolvimento científico, a pesquisa e a capacitação científica e tecnológica e a inovação, fundamentais para o desenvolvimento económico, proporcionando a geração de emprego e renda.

Tais deveres impostos são um dos objetivos fundamentais da República, previsto no art. 3º, inciso III, ou seja, garantir o desenvolvimento nacional. "Assim, por força da Carta Magna, a pesquisa científica básica e tecnológica receberá tratamento prioritário do Estado, tendo em vista o bem público e o progresso da ciência, tecnologia e inovação."[308]

Assim, a LGPD, além da tutela dos dados de forma individual, tem por outro lado que compatibilizar o desenvolvimento económico e tecnológico, não sendo um empecilho a estes.

São também fundamentos da LGPD a livre-iniciativa, a livre concorrência e a defesa do consumidor. A livre iniciativa é também um dos fundamentos da república e da ordem económica, prevista, respectivamente, no art. 1º, inciso IV e art. 170 da CFb. Ela é o direito de todo cidadão de lançar-se em uma atividade económica, de produção de bens e serviços. Essa liberdade de empreender, entretanto, pode ser mitigada quando em conflito com outro princípio ou fundamento constitucional. Por sinal, a ordem económica tem por fim a existência digna e os ditames da justiça social.

A livre concorrência e a defesa do consumidor também estão previstas no art. 170, incisos IV e V, respectivamente, da CFb, como princípios da ordem económica. A livre concorrência é um dos desdobramentos da livre iniciativa. Mas ainda que exista os princípios da livre iniciativa e da livre concorrência, a CFb assegurou um modelo de Estado intervencionista na modalidade direta (art. 173), indireta (art. 174) e através de monopólios (art. 177), quando necessário a atingir os seus fins, prevendo ainda o art. 173, §4º que a lei[309] reprimirá o abuso do poder económico que vise à dominação dos mercados, à eliminação da concorrência e ao aumento arbitrário dos lucros. Por sua vez, a defesa do consumidor, não apenas como um dos princípios da ordem económica, mas

promoverá e incentivará a atuação no exterior das instituições públicas de ciência, tecnologia e inovação, com vistas à execução das atividades previstas no caput."

[308] CUNHA JÚNIOR, op. cit., p. 1237.

[309] Cf. BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 12.529, de 30 de novembro de 2011. Estrutura o Sistema Brasileiro de Defesa da Concorrência; dispõe sobre a prevenção e repressão às infrações contra a ordem econômica...; *"D.O.U."* (01-11-2011). [Consultado 20 março 2020].Disponível na internet: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12529.htm>.

também como um direito fundamental, previsto no art. 5º, inciso XXXII da CFb, denota a devoção ao princípio da vulnerabilidade daquele.[310]

Portanto, em que pese a Constituição Federal brasileira (CFb) tenha firmado uma economia de livre mercado, com viés capitalista, uma vez que encontra-se assente na livre iniciativa económica privada e na apropriação privada dos meios de produção, o processo económico é condicionado ao bem-estar social ou melhoria da qualidade de vida.[311] Pode-se dizer que a CFb proclama uma economia social de mercado.

A LGPD assegura a livre concorrência entre as empresas, fixando regras e impedindo o lucro indiscriminado, bem como tutela o titular dos dados, consumidor ou não.

Por fim, tem-se por fundamentos da LGPD os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. Quanto aos três primeiros, já se frisou que o direito à proteção de dados pessoais é um direito fundamental, que tutela a personalidade, assentado na liberdade e dignidade da pessoa humana. Quanto ao exercício da cidadania das pessoas naturais deve-se fazer uma ressalva. A LGPD implanta uma cultura de cidadania de direitos, através da tutela da privacidade e do controlo dos dados pessoais como um todo, assegurando por outro lado o desenvolvimento da economia digital. Tem-se, assim, o cidadão, o indivíduo com sua dignidade e seus direitos fundamentais no centro nevrálgico do texto normativo.

Como leciona Frazão, "[...] o eixo valorativo da LGPD é a proteção da pessoa humana e de suas situações existenciais relevantes, o que deve ser levado em consideração para a interpretação de todas as suas disposições."[312]

3.2.1 Âmbito de aplicação

[310] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Constituição da República Federativa do Brasil. Op. cit.
[311] CUNHA JÚNIOR, op. cit., p. 1204.
[312] FRAZÃO, op. cit., p. 104.

A LGPD, assim como o RGPD, possui objetivo que explica o seu âmbito de aplicação alargado.

O modelo de tratamento dos dados pessoais disposto na LGPD é dotado de três características básicas: ampliação do conceito de dado pessoal; o respeito a uma base legal; e o interesse legítimo como hipótese que autorizaria a necessidade de realização de um balanceamento de interesses.[313]

Quanto ao âmbito material, segundo o art. 1º, a lei incidiria sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado.

O legislador apresentou, a fim de espancar dúvidas, um conceito legal de dados pessoais, assim dispondo: "Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;"[314]

Segundo Cots e Oliveira, trata-se de um critério expansionista, posto que os dados pessoais seriam não apenas aqueles que identifiquem a pessoa natural de forma imediata, como nome, imagem, CPF, mas também aqueles que tornam a pessoa identificável de fora indireta.[315]

É o oposto do critério reducionista que protegeria apenas os dados passiveis de identificar a pessoa natural imediatamente. Assim, ainda que um dado isoladamente não identifique o indivíduo, caso existam outros que conjugados, acabam por permitir a identificação, devem eles ser considerados como pessoais. Assim se o controlador não consegue identificar o indivíduo com base nos dados que dispõe, não se deve considerá-los como pessoais, até que o controlador disponha de outros que permitam a identificação.

Por sua vez, a *lex* conceitua o que seria o tratamento dos dados pessoais no art. 5º, inciso X.[316] O rol as atividades desenvolvidas como tratamento é meramente exemplificativa, diante da expressão utilizada de "toda operação", sendo que a prática de

[313] MENEZES, op. cit., 163.
[314] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 13.709... op. cit.
[315] COTS, op. cit., p. 74.
[316] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 13.709... op. cit. "Art. 5º Para os fins desta Lei, considera-se: X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;"

apenas uma delas é suficiente para a caracterização do tratamento, não existindo, portanto, a necessidade de cumulação.

A LGPD alcança o tratamento de dados *on-line* e *off-line,* posto que o art. 3º, *caput* utiliza a expressão "qualquer operação de tratamento".

E, nesse ponto, deve-se fazer um apontamento. A LGPD não revogou o Marco Civil da Internet, tanto que aquela alterou dois artigos deste. Ademais, o Marco Civil da internet trata de outros temas, estabelecendo diretrizes governamentais, fundamentos, objetivos e princípios da internet. Se por um lado a LGPD é mais específica quanto à proteção de dados pessoais em relação ao Marco Civil da Internet, por outro lado aquela é mais ampla quanto à proteção de dados, por alcançar os dados tratados fora da rede mundial de computadores. E nesse ponto tem-se a aplicação do art. 2º, §2º do Decreto-Lei n 4.657/42 (Lei de Introdução às normas do Direito Brasileiro) quando afirma: "§ 2º A lei nova, que estabeleça disposições gerais ou especiais a par das já existentes, não revoga nem modifica a lei anterior."[317] Portanto, conclui-se que a LGPD e o Marco Civil da Internet são normas complementares, quando o tratamento dos dados pessoais é realizado por meio da internet.[318] Daí ser compreensível o disposto no art. 64 da LGPD quando estabelece que os direitos e princípios nela previstos não excluem outros entabulados no ordenamento jurídico pátrio ou em tratados de que o Brasil seja parte.[319]

Entretanto, a LGPD fixou limites à sua aplicação quanto ao âmbito material, as quais estão previstas no art. 4º, a saber:[320]

a) tratamento realizado por pessoa natural para fins particulares e não

---

[317] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Decreto-Lei n.° 4.657, de 4 de setembro de 1942. Lei de Introdução às normas do Direito Brasileiro. *"D.O.U."* (09-09-1942). [Consultado 28 março 2020]. Disponível na internet: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del4657compilado.htm>.

[318] Nesse ponto Menezes e Colaço "Não obstante a LGPD ter passado a regular mais amiúde a matéria sobre o tratamento das informações, instituindo até uma base legal para o tratamento, o MCI continua vigente e aplicável quando esse tratamento ocorrer na internet. O diálogo de fontes, entre as legislações incidentes (LAI, CDC, MCI e LGPD), deverá ser utilizado de forma a garantir ampla tutela dos titulares de dados submetidos a processamento no meio virtual." MENEZES, op. cit., p. 192.

[319] BRASIL. PRESIDÊNCIA DA REPÚBLICA– Lei n.° 13.709... op. cit.

[320] Ibid. "Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II - realizado para fins exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) 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 nesta Lei."

económicos. Considerando a amplitude do conceito de tratamento de dados, dentre eles, coleta, recepção, armazenamento, eliminação, comunicação, transferência, extração, constata-se que a pessoa natural realiza diariamente tal tratamento com os dados de seus interlocutores, uma decorrência da comunicação humana. Em regra, são dados pessoais obtidos como fruto de uma vida comum, que permitem a identificação de indivíduos, como nome, endereço, e-mail, telefone, opiniões políticas, orientação sexual, religiosa. Dados pessoais podem constar em cartas, bilhetes, mensagens sms, conversas gravadas de *whatsapp* ou e-mail nunca apagados pelos interlocutores, em agenda telefónica de um celular ou de caderno de anotações, álbuns físicos ou virtuais, com fotos e vídeos, em redes sociais alimentadas com informações sobre si e pessoas próximas. Qualquer dado pessoal do interlocutor pode ser colecionado por aquele que o recepciona, intencionalmente ou não. Mas nessas hipóteses, para que incida a exclusão da LGPD, não deve haver os fins de obtenção de uma vantagem económica. A razão da exclusão se justifica pelo fato que, nessas hipóteses, a interação entre o titular dos dados e o responsável pelo tratamento ocorrem em pé de igualdade, no mesmo patamar. Segundo Menezes e Colaço,

> [a]inda que seja possível a violação da privacidade nesses casos, não haverá a necessidade de aplicação de uma lei cujo fim primordial é o de tutelar a privacidade da pessoa natural em relações profundamente díspares, como aquelas que se estabelecem no Âmbito da sociedade das redes, na qual o poder informacional é dominado pelos agentes econômicos e/ou pelo próprio Estado, organizados como pessoas jurídicas de direito público ou privado.[321]

Mas ainda que não haja a incidência da LGPD nessa hipótese, não pode o interlocutor usar para tais dados de forma que cause dano moral ao titular, podendo resultar em um ilícito civil ou penal. Diversamente, conforme afirma Cots e Oliveira, haverá incidência da norma na hipótese de dados armazenados em um celular corporativo de um representante comercial;[322]

b) tratamento realizado para fins exclusivamente jornalísticos, previsto no art. 4º,

[321] MENEZES, op. cit., p. 175.
[322] COTS, op. cit., p. 65.

inciso II, alínea a) da LGPD. O Supremo Tribunal Federal (STF)[323] reconheceu que a atividade jornalística não pode estar reservada apenas às pessoas dotadas de curso superior específico, uma vez que qualquer controlo nesse sentido caracterizaria censura prévia das liberdades de expressão e de informação, as quais são vedadas no art. 5º, inciso IX da CFb.[324] Assim se justificaria a presente exclusão em face da atividade jornalística, posto que a aplicação seria regulação prévia de interesses da personalidade, como a liberdade de informação jornalística, enquanto que os ditames constitucionais fixam um controlo posterior como a vedação do anonimato (art. 5º inciso IV), direito de resposta (art. 5º inciso V), indenização por dano material ou moral (art. 5º inciso X). O problema é como se reconhecer uma atividade exclusivamente jornalística. Se antes mesmo do incremento tecnológico e da decisão citada, que assegura a liberdade da atividade jornalística, a difusão de ideias e informações acobertadas sob a denominação de atividade jornalística já servia aos mais variados interesses, religiosos, económicos, políticos, dentre outros, o que dificultava caracterizar a atividade como exclusivamente jornalística, quanto mais agora, diante daqueles dois fatores que colaboraram para uma enorme quantidade de informação constante nos meios digitais, como *sites, blogs* e redes sociais. Deve-se atentar para a função social e o interesse público da atividade jornalística, excluindo-se a mera liberdade de expressão pessoal ou comercial. Para tanto, Menezes e Colaço entendem que é aquela desenvolvida por profissional de jornalismo e dos órgãos de comunicação na divulgação das notícias.[325] A fim de determinar se uma atividade desempenhada se enquadraria na exclusão legal, Cots e Oliveira citam alguns critérios: a empresa tem como objeto social ou atividade preponderante o jornalismo; a notícia possui interesse público ou relevância social; as informações são baseadas em fatos objetivos ou possuem fundamentação teórica plausível; há indicação de fontes

[323] BRASIL. Supremo Tribunal Federal. Recurso Extraordinário n.° 511.961-SP. Relator: Min. Gilmar Mendes. Brasília, DF, 17 de junho de 2009. [Consultado 31 março 2020]. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=605643>.

[324] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Constituição da República Federativa do Brasil. Op. cit.

[325] MENEZES, op. cit., p. 178.

confiáveis, e outras.[326] Por fim, ressalte-se que se o grupo económico desenvolve outras atividades, além da jornalística, a única hipótese de se excluir a aplicação da LGPD é se o grupo possuir divisão no banco de dados, caso contrário todo o banco estará sujeito à presente norma;

c) tratamento de dados para fins exclusivamente artísticos, previsto no mesmo art. 4º, inciso II, alínea a) da LGPD. Visou a norma ampliar a liberdade de expressão, reconhecendo ainda a importância da arte no desenvolvimento do ser humano. A dificuldade encontrada nessa hipótese é definir o que seria artístico. Para tanto, pode-se valer do art. 7º da Lei n.° 9.610/1998[327], *lex* que versa sobre os direitos autorais, ao tratar da proteção das obras do "espírito humano", dentre as quais as artísticas, como: desenho, pintura, música, dança, cinema, coreografia, teatro, escultura, ilustrações. Segundo Menezes e Colaço, "[...] entende-se por obra artística ou de fins artísticos aquela que se fez como fruto da capacidade criativa que também constitui uma expressão do direito da personalidade.";[328]

d) tratamento de dados pessoais para fins académicos, estampado no art. 4º, inciso II, alínea b) da LGPD[329]. A finalidade académica está relacionada com objetivos científicos, artísticos ou literários.

> Disso se infere que o trabalho académico está correlacionado às atividades voltadas para o desenvolvimento do conhecimento e da pesquisa científicos realizados, primordialmente, no âmbito das universidades, cuja autonomia é constitucionalmente assegurada.[330]

Mas embora excluídos da aplicação da LGPD, as pessoas titulares desses dados não estão desprotegidas. A Lei n.° 8.080/1990[331] e a Lei n.° 8.142/1990[332]

---

[326] COTS, op. cit., p. 67.

[327] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 9.610, de 19 de fevereiro de 2018. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. *"D.O.U."* (20-02-1998). [Consultado 31 março 2020]. Disponível na internet: < http://www.planalto.gov.br/ccivil_03/leis/l9610.htm>.

[328] MENEZES, op. cit., p. 183.

[329] BRASIL. PRESIDÊNCIA DA REPÚBLICA– Lei n.° 13.709... op. cit. "Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: [...] II - realizado para fins exclusivamente: [...] b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;"

[330] MENEZES, op. cit., loc. cit.

[331] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 8.080/1990, de 19 de setembro de 1990. Dispõe sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes e dá outras

trazem dispositivos constando limites éticos na pesquisa da área da saúde. O dispositivo legal da LGPD foi mal redigido e trata-se de uma hipótese de aplicação mitigada e não de exclusão. Isto pode ser constatado pela redação do dispositivo, que faz referência aos arts. 7º e 11 da mesma *lex,* onde têm-se as hipóteses em que é admissível o tratamento dos dados comuns e dados sensíveis. E até mesmo uma alegação de legítimo interesse está regulada no art. 10. Na verdade existe sim aplicação da lei aos fins exclusivamente académicos, sendo que a intenção do legislador foi evitar que o responsável pelo tratamento realizasse esse, valendo-se da alegação académica, com fins comerciais;

e) tratamento realizado para fins de um interesse público determinado, tendo por fundamento a segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão a infrações penais, nos termos do art. 4º, inciso III da LGPD. Em relação aos demais tratamentos de dados pelo Poder Público, LGPD se aplicará, como ocorre no âmbito fiscal, sendo que a partir do momento em que se identificar um crime, o tratamento para fins de investigação não será mais tutelado pela LGPD. Restrições a esse tratamento foram previstas nos parágrafos do mesmo artigo.[333] É necessária lei específica para o tratamento de dados pessoais por fundamento no interesse público, mas que deve observar os princípios gerais de proteção, o devido processo legal e os direitos dos titulares constantes na LGPD. Frise-se que o tratamento dos dados pessoais, nessa hipótese, pode até ser realizado por entidade privada, estando sempre sob tutela do Poder Público, não podendo

providências. *"D.O.U."* (20-09-1990). [Consultado 31 março 2020]. Disponível na internet: <http://www.planalto.gov.br/ccivil_03/leis/l8080.htm>.

[332] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 8.142/1990, de 28 de dezembro de 1990. Dispõe sobre a participação da comunidade na gestão do Sistema Único de Saúde (SUS) e sobre as transferências intergovernamentais de recursos financeiros na área da saúde e dá outras providências. *"D.O.U."* (31-12-1990). [Consultado 31 março 2020]. Disponível na internet: <http://www.planalto.gov.br/ccivil_03/leis/L8142.htm>.

[333] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 13.709... op. cit. "[...] § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei. § 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo. § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais. § 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público.

corresponder à totalidade dos dados, exceto se constituída a entidade privada de capital exclusivamente público. Segundo Cots e Oliveira, com a proibição de tratamento da totalidade de dados por ente privado, evita-se o risco de vazamentos, até mesmo de eliminação ou perda completa.[334] Em termos gerais, não se pode negar que tal regramento se justifica diante do considerável valor económico do banco de dados do setor público, sendo que as tentativas de corrupção por partes de agentes públicos devem ser combatidas. Nesse ponto, frise-se a autorização da criação, no Ministério da Justiça e Segurança Pública, do Banco Nacional Multibiométrico e de Impressões Digitais pela Lei n.° 13.964/2019 (Conhecida por lei Anticrime) que acrescentou o art. 7º-C à Lei n.° 12.037/2009, sendo que devem ser observados os direitos dos titulares dos dados e os princípios da LGPD, ainda que o tratamento seja para fins de segurança pública e de investigação criminal, proteção da pessoa em face do Estado de Vigilância. Menezes e Colaço ressaltam que já é comum a contratação de empresas especializadas pela administração pública para a realização de atividades conectas a serviços estratégicos, como a contratação de empresas privadas para: atuação no monitoramento de veículos visando a fiscalização de pagamento de imposto (IPVA); controlo de tráfego com a instalação de semáforos inteligentes; desenvolvimento de sistemas inteligentes de gerenciamento de processos judiciais, com possibilidade de identificação de demandas repetitivas.[335] Mas, nesse ponto, surge a indagação de qual autoridade será responsável pelo controlo, já que não se aplica ao LGPD e, por consequência, a ANPD não atuaria nessa seara. Pelo que se depreende, ficaria a cargo apenas da pessoa jurídica de direito público a fiscalização. Haveria, assim, uma fragilidade no controlo desses dados e no exercício do direito por parte dos titulares;

f) tratamento realizado sobre dados originários do exterior e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com

[334] COTS, op. cit., p. 71.
[335] MENEZES, op. cit., p. 190.

> 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 brasileira (art. 4º, inciso IV da LGPD)[336]. Tal norma pode beneficiar empresas brasileiras operadoras, que tratem dados oriundos do exterior e de titulares lá localizados, sem compartilhamento no território brasileiro. Mas é essencial que o país de onde os dados são originários assegure a proteção adequada, caso contrário, haverá a incidência da LGPD, adotando critério semelhante ao RGPD europeu. A avaliação do nível adequado de proteção do país de proveniência é realizada pela ANPD, seguindo o disposto no art. 33 e art. 34 da LGPD. Daí é que Cots e Oliveira citam quatro situações em relação ao inciso IV do art. 4º: empresa brasileira que é contratada por empresa alemã para tratar de dados de seus conterrâneos, com retorno à própria empresa alemã, não se aplica a LGPD; se a empresa alemã contrata a empresa brasileira para tratar de dados de pessoas localizadas no Brasil, independentemente do destino do tratamento, ou se a empresa brasileira foi contratada para tratar de dados pessoais de residentes na Alemanha, com compartilhamento com empresa brasileira, haverá a incidência da LGPD; também haverá a aplicação da mesma lei se a empresa brasileira tiver sido contratada por empresa norte-americana para tratar de dados de indivíduos residentes naquele país, com retorno para a empresa contratante, diante do baixo nível de proteção dos dados pessoais naquele país.[337]

No que tange ao âmbito territorial de aplicação da LGPD, o art. 3º é que disciplina a matéria. A aplicação da lei independe do meio, do país da sede da pessoa jurídica ou natural que realiza o tratamento ou do país onde estejam localizados os dados. O que é fundamental é que se verifique uma das hipóteses dos incisos do art. 3º, que por sinal são independentes e não cumulativas, saber:

a) tratamento dos dados pessoais realizado no território nacional (art. 3º, inciso I da LGPD). Como a lei não especificou, não há distinção se está sendo o

[336] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 13.709... op. cit.
[337] COTS, op. cit., p. 71-72.

tratamento realizado pelo operador ou diretamente pelo *controller.* Com arrimo nesse inciso, a aplicação da LGPD incidirá se o tratamento estiver sendo realizado do Brasil, ainda que os dados sejam de pessoas localizadas em outro país ou de um estrangeiro. Menezes e Colaço ressaltam

> [...] um estrangeiro não residente no país, mas em trânsito ou em simples conexão, por exemplo, em aeroporto brasileiro, será tutelado pela legislação brasileira no que tange ao tratamento de dados que eventualmente forneceu para utilizar dos serviços de *wi-fi* da concessionária do aeroporto, por exemplo.[338]

A LGPD adota critério distinto do RGPD europeu, uma vez que para este último o requisito é que a empresa, responsável pelo tratamento, esteja situada na União Europeia e não o local do tratamento dos dados, mas por outro lado se assemelham por tutelar dados daqueles que se situam nos respectivos territórios, independente da nacionalidade ou residência, como se verá em seguida;

b) tratamento dos dados pessoais tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional (art. 3º, inciso II da LGPD). É irrelevante a nacionalidade do titular dos dados, ainda que estrangeiro, desde que esteja definitivamente ou provisoriamente no Brasil e ainda que a empresa seja estrangeira, como a Amazon ou a Dell. A lei não esclarece como poderia restar configurada a situação de oferta de bens ou serviços a indivíduos localizados no território nacional. E aqui pode-se utilizar o mesmo critério adotado pelo RGPD da União Europeia: o oferecimento de produtos ou serviços ou possibilidade de solicitação em língua portuguesa, o uso do Real como moeda corrente ou até mesmo a referência a utilizadores que se localizem no Brasil;
c) dados tenham sido coletados no território brasileiro (art. 3º, inciso III da LGPD). Trata-se de previsão leal desnecessária, posto que já incluída no inciso I do art. 3º da LGPD, uma vez que a coleta é uma das atividades de tratamento, conforme o art. 5º, inciso X da LGPD.

[338] MENEZES, op. cit., p. 193.

3.2.2 Direitos dos titulares dos dados pessoais

O Capítulo III da LGPD tem como título "Dos direitos do titular". Diferentemente do RGPD que divide o capítulo III, correspondente aos direitos do titular, em secções, tratando de forma minuciosa cada um deles, a LGPD assim não procede, mantendo em um único tópico, sendo bem mais sucinto, pecando pelo trato genérico e ausência de sistemática.

Ademais, o rol de direitos tratados no Capítulo III é apenas exemplificativo, uma vez que diversos direitos estão dispostos em outros capítulos, como a autodeterminação informativa, liberdade de expressão, inviolabilidade da privacidade, defesa do consumidor, desenvolvimento da personalidade, no art. 2º.

Adentrando na análise dos direitos específicos do capítulo III, inicialmente, fim de espancar dúvidas de qual seria o sujeito ativo de proteção da norma, o art. 17 menciona o termo "Toda pessoa natural". Descreve, ainda, o mesmo artigo, os direitos fundamentais de liberdade, de intimidade e de privacidade. Descrição essa desnecessária, posto que já consagrados na Constituição Federal brasileira (CFb) como direitos fundamentais, nos art. 5º, *caput* e inciso X. De qualquer forma, Dias e Bolesina afirmam que esses seriam, segundo a legislador brasileiro, os direitos fundamentais matrizes dos direitos específicos da lei de proteção de dados pessoais, que viriam nos art. 18 a 22.[339]

Não se pode olvidar que, tratando-se de um direito da personalidade, a regra é da sua irrenunciabilidade e intransmissibilidade, ressalvado os casos expressos em lei, sob pena de nulidade, conforme dispõe o art. 11 do Código Civil brasileiro (CCb)[340].

Diversos direitos são elencados no art. 18 da LGPD. Outros direitos previstos nas mais diversas legislações são assegurados, quando envolver uma relação jurídica estabelecida entre um titular dos dados pessoais e o controlador. O disposto no art. 64 da LGPD enfatiza que direitos e princípios nela expressos não excluem outros previstos no

---

[339] DIAS, Felipe da Veiga; BOLESINA, Iuri. Direito à proteção de dados pessoais no Brasil e os traços centrais de uma autoridade local de proteção. *E-Civitas - Revista Científica do Curso de Direito do UNIBH* - Belo Horizonte, jul. 2017, v. X, n. 1, [consultado 3 abril 2020], p. 1-26. cit. p. 11. Disponível na internet: <https://revistas.unibh.br/dcjpg/article/view/2165/1>. ISSN 1984-2716.

[340] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 10.406, de 10 de janeiro de 2002. Código Civil. *"D.O.U."* (11-01-2002). [Consultado 28 março 2020]. Disponível na internet: <http://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406.htm>. "Art. 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária."

ordenamento jurídico pátrio, relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte. Cite-se, por exemplo, os direitos e os princípios que constam no Marco Civil da Internet. Em relação aos princípios tem-se os do art. 3º, incisos II e III[341] e quanto aos direitos os do art. 7°, incisos I, II, III, VII, VIII, IX, X e art. 8º, todos do Marco Civil da Internet[342], sem sobreposição de uma lei sobre a outra, coexistindo ambas em harmonia.

Acrescente-se, entretanto, que uma enorme questão surge quanto à aplicabilidade dos direitos do art. 18 da LGPD, em razão do disposto nos parágrafos 3º e 5º do mesmo artigo. Em outras passagens do texto normativo, o legislador, ao tratar da regulamentação de um dispositivo, utilizou-se do termo "poderá", como o que ocorre nos os arts. 23, §1º e 30, ambos da LGPD[343]. Já o parágrafo §5º do art. 18 da LGPD, dispõe que o exercício de tais direitos será efetuado por requerimento do titular ou representante legal constituído perante o agente de tratamento, porém, nos prazos e termos previstos no regulamento. Assim, é possível a interpretação da existência de uma verdadeira condição suspensiva para o exercício de tais direitos reconhecidos na norma. Entretanto, pensamos que a melhor interpretação seja aquela que vislumbra que a lei se refere apenas à questão do prazo e do procedimento, não afetando o direito em si. Dessa forma, nada obsta ao titular buscar o Poder Judiciário, caso não seja atendido o direito perante o controlador, em um prazo razoável, diante dos princípios da transparência, do livre acesso, da boa-fé objetiva, previstos no art. 6º da LGPD. Corroborando tal

[341] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 12.965... op. cit. "Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: [...] II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei;"

[342] Ibid. "Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; [...] VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei; Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet. Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no caput, tais como aquelas que: I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil."

[343] BRASIL. PRESIDÊNCIA DA REPÚBLICA– Lei n.° 13.709... op. cit. "Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei n.° 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que: [...]§ 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento.[...] Art. 30. A autoridade nacional poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais."

entendimento, o § 8º do art. 18 da LGPD proclama que tais direitos poderão ser exercidos perante os órgãos de defesa do consumidor. Frise-se ainda que, o termo requerimento deve ser compreendido com requisição, não sendo uma faculdade para o controlador o seu processamento, somente podendo se opor nos casos expressos na LGPD.

Os dois primeiros direitos elencados no capítulo III da LGPD são o de confirmação de existência do tratamento e o de acesso, descritos no art. 18, incisos I e II. Tais direitos correlacionam-se como os princípios do livre acesso, qualidade dos dados e da transparência, descritos no art. 6º, incisos IV, V e VI da LGPD, respectivamente[344].

O direito de confirmação de existência do tratamento assegura ao titular a possibilidade de obter a confirmação de que os seus dados estão sendo tratados.

Já o direito de acesso, segundo Murillo e Piñar, garante ao titular dos dados obter a mais ampla informação sobre os dados objetos de tratamento.[345] Essas informações vão desde a origem, os responsáveis pelo tratamento, objetivos destes e outros. O acesso do titular dos dados será, nos termos do art. 19, *caput*, incisos I e II da LGPD, imediatamente em formato simplificado, ou, no prazo de 15 dias, quando se tratar de pleito de informações complexas. Entretanto, pode a autoridade nacional dispor sobre prazos específicos para cada setor, reconhecendo a lei a exiguidade dos prazos que lá constam, conforme o §4º. Para que possa o titular exercer esse direito de acesso, devem os dados serem armazenados de forma que seja possível o atendimento do pleito do titular, seguindo as orientações do §1º. As informações e os dados podem ser fornecidos por meio eletrónico ou de forma impressa, escolha que fica a cargo do titular. A questão é sobre os custos da forma impressa, diante da gratuidade estabelecida no art. 6º, inciso IV da LGPD. O direito de acesso, quando os dados tratados tenham por fundamento o consentimento ou contrato, assegura ao titular a obtenção de cópia eletrónica integral de seus dados pessoais, em formato que possibilite a utilização subsequente, inclusive em outras operações de tratamento, nos termos do art. 3º do art. 19 da LGPD. Limitação essa, a um fundamento, que não existe no RGPD. Segundo Feigelson e Siqueira, tal medida atende ao direito de portabilidade dos dados, que é tratado no art. 18, inciso V da

[344] Ibid.

[345] MURILLO DE LA CUEVA, Pablo de Lucas; PIÑAR MAÑAS, José Luís. *El derecho a la autodeterminación informativa.* Madrid: Fundación Coloquio Jurídico Europeo, 2009. p. 187. ISBN 978846133470-4.

LGPD.[346] O direito de acesso também é regulado no art. 9º da LGPD, ressaltando que as informações prestadas com base nesse direito devem ser fornecidas de forma clara, adequada e ostensiva. Diferenciando-se do RGPD, que o responsável pelo tratamento pode exigir uma taxa ou recusar a dar seguimento ao pleito, quando este for manifestamente infundado ou excessivo, notadamente devido ao seu caráter repetitivo, a LGPD nada dispõe a respeito.

O direito de retificação dos dados objeto de tratamento, previsto no art. 18, inciso III da LGPD, é aquele que possui o titular de completar aqueles inacabados, ou corrigir os inexatos ou desatualizados. Atende ao princípio da qualidade dos dados, descrito no art. 6º, inciso V da LGPD.

Quando os dados forem desnecessários, excessivos ou tratados de forma contrária a lei, o titular tem direito à anonimização, bloqueio ou eliminação dos dados desnecessários. Os conceitos de tais direitos estão dispostos no art. 5º, incisos XI, XII e XIV da LGPD.[347] Caberá ao controlador aplicar uma dessas medidas, seguindo os ditames da LGPD, mas atendendo também os seus interesses. Segundo Feigelson e Siqueira, tais direitos decorrem do princípio da necessidade, estampado no art. 6º, inciso III da LGPD.[348]

Dados anonimizados são aqueles em que não é possível a identificação do titular, considerando os meios técnicos disponíveis. Eles não mais serão objeto de tutela da LGPD, se esse processo não puder ser objeto de reversão. Nesse processo não é mais possível correlacionar o titular ao dado, de forma direta ou indireta. A anonimização é assegurada, sempre que possível, em tratamento de estudos por órgãos de pesquisa, seguindo o disposto nos arts. 7º, inciso IV, 11, inciso II, alínea c), 13 e 16, inciso II, todos da LGPD[349].

O bloqueio e a eliminação se assemelham, mas enquanto no bloqueio o tratamento é suspenso temporariamente, mantendo-se os dados, na eliminação descarta-se os

---

[346] FEIGELSON, Bruno; SIQUEIRA, Antônio Henrique Albani. *Comentário à lei geral de proteção de dados*: Lei 13.709/2018. São Paulo: Thomson Reuters Brasil, 2019. p. 122. ISBN 978855321439-6.

[347] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 13.709... op. cit. "Art. 5º Para os fins desta Lei, considera-se: XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;[...] XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados; XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;"

[348] FEIGELSON, op. cit., p. 124.

[349] BRASIL. PRESIDÊNCIA DA REPÚBLICA– Lei n.° 13.709... op. cit.

dados, é algo definitivo, sendo esta aplicada quando o tratamento for ilícito ou quando houver fim do tratamento, ressalvada a possibilidade de conservação dos dados, segundo o disposto no art. 16 da LGPD[350]. Mas além dessas duas hipóteses, existe um outro direito de eliminação dos dados, quando tratados com o consentimento do titular, independente do término do tratamento, estando previsto no art. 18, inciso VI da LGPD, o que assemelha-se com a hipótese de revogação de consentimento do art. 18, inciso IX e que conduz ao término do tratamento do art. 15, inciso III, levando à eliminação pelo art. 16.

Merece destaque, nesse contexto, o término do tratamento dos dados pessoais. Este é uma das causas geradoras do direito à eliminação dos dados pessoais para o titular. Elimina-se os dados devido a término do tratamento, objetivando-se evitar o uso indevido ou não autorizado. As hipóteses de término de tratamento dos dados pessoais estão descritas no art. 15º da LGPD e são em número de quatro: pelo esgotamento funcional (inciso I); pelo fim do prazo (inciso II); pela manifestação do titular, resguardado o interesse público (inciso III); em razão de ilegalidade (inciso IV). A primeira tem por limite a finalidade alcançada ou por não serem mais necessários os dados para aquela finalidade específica. Ela se justifica, pois o tratamento deve atender os princípios da finalidade, da adequação e da necessidade, descritos no art. 6º, incisos I, II e III da LGPD, respectivamente[351]. A segunda hipótese tem como limite o tempo. Guedes e Meireles afirmam que "[a]s duas primeiras hipóteses decorrem do princípio do consentimento ou autodeterminação informativa, como foi nomeado na seara da proteção de dados. A finalidade e o tempo constituem limites estabelecidos pela autodeterminação."[352] O consentimento amparado pela legislação é aquele direcionado a uma finalidade, consoante a exigência do art. 5º, inciso XII da LGPD. A terceira hipótese corresponde à comunicação do titular e revogação do consentimento, este de natureza qualificada, que

[350] Ibid. "Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: I - cumprimento de obrigação legal ou regulatória pelo controlador; II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados."

[351] Ibid. "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;"

[352] GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau. Término do tratamento de dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.) *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 219-241. cit. p. 223. ISBN 978855321663-5.

se atribui à vontade interna uma relevância acima do que a não verificada normalmente em relações de cunho patrimonial.[353] Por fim, a quarta hipótese do término do tratamento é por violação à LGPD, mediante a determinação da autoridade nacional. Entretanto, quatro exceções foram dispostas na lei, art. 16, em que inexiste o direito de eliminação dos dados, em que pese tenha encerrado o tratamento, uma vez que é autorizada a conservação, as quais devem ser interpretadas restritivamente: em cumprimento de obrigação legal ou regulatória pelo controlador; estudo por órgão de pesquisa com a anonimização dos dados pessoais; a transferência a terceiro, quando respeitados os requisitos legais de tratamento de dados; uso exclusivo do controlador, sendo anonimizados os dados, vedado seu acesso por terceiro. A LGPD não fixa prazo para a conservação, sendo que se deve adotar, com fundamento no diálogo das fontes, o disposto no Marco Civil da Internet que fixa seis meses de guarda de registos de acesso a aplicações de internet, pelo provedor de aplicações, no art. 15.[354]

Questão debatida é se esse direito de eliminação dos dados, com fundamento no término do tratamento, configuraria um direito ao esquecimento na seara digital. Manifesta-se afirmativamente Silva, para quem deve ser efetuada a ponderação com o direito à informação.[355] Contudo, entende-se de forma contrária. No Brasil o direito ao esquecimento é fruto de construção da doutrina e da jurisprudência, não havendo uma regulamentação legal, como resultado de interpretação dos direitos fundamentais constitucionais, especialmente uma decorrência da dignidade da pessoa humana, essencial ao livre desenvolvimento da personalidade. É acolhido na jurisprudência brasileira nas situações em que os indivíduos desejam obstar a divulgação de situações constrangedoras ou equívocos pretéritos que digam respeito à vida do indivíduo e que a sua divulgação corresponderia à eternização dos fatos, comprometendo o desenvolvimento da sua identidade pessoal, conforme explanou-se ao se discorrer sobre o apagamento dos dados no RGPD. Na seara da internet, o pedido geralmente inclui a desindexação de termos ou frases, a fim de dificultar ou impedir o acesso a tais

[353] Em decorrência do consentimento qualificado, surgem consequências jurídicas subjetivas: a manifestação de vontade tem que ser pessoal; essa vontade interna prevalece sobre a declarada e a possibilidade de revogação da vontade.
[354] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 12.965... op. cit.
[355] SILVA, Paula Jaeger da. Direito ao esquecimento: aumento da problemática com o advento da internet. *Revista Jurídica*, Síntese Editora, São Paulo, set. 2018, n. 491, p. 70. ISSN 0103-3379.

informações.[356] Dessa forma, não existe uma correlação de tal direito ao esquecimento com a eliminação dos dados pelo fim do tratamento. Conforme leciona Guedes e Meireles, a jurisprudência, em sede de direito a esquecimento, se concentra em fatos pretéritos e na questão desses fatos não serem objeto de divulgação eterna publicação, quando não haja um interesse legítimo, o que não corresponde ao disposto no art. 16 da LGPD e art. 7º do Marco Civil da Internet, sendo a Constituição Federal brasileira o verdadeiro fundamento do direito ao esquecimento.[357]

O que a LGPD e o RGPD sustentam é a eliminação dos dados, distanciando-se do direito ao esquecimento, no que tange ao conteúdo e aos fins mais imediatos, ainda que em ambos se vislumbre a tutela da dignidade da pessoa humana.[358]

Superada a questão do direito ao esquecimento, fazendo uma análise do direito ao apagamento do RGPD europeu e o direito à eliminação dos dados da LGPD brasileira têm-se: o apagamento dos dados tratados ilicitamente (art. 17º, n.° 1, alínea d) do RGPD) está prevista como a eliminação dos dados tratados em desconformidade com o disposto na lei (art. 18, IV da LGPD); a supressão do consentimento (art. 17º, n.° 1, alínea b) do RGPD) está descrita também na LGPD, art. 18, inciso VI; o apagamento pelos dados não serem mais necessários para a finalidade (art. 17º, n.° 1, alínea a) do RGPD), está descrita no art. 18, inciso IV da LGPD.

Assim, não existe uma grande distinção entre o direito à eliminação dos dados da LGPD com o direito ao apagamento do RGPD, ainda que esta derradeira legislação tenha utilizado a nomenclatura “direito a ser esquecido” paralela ao apagamento, posto que ambos os textos normativos têm tal direito de eliminação (apagamento) assentes em princípios da própria proteção dos dados, como licitude, autodeterminação informativa, finalidade, adequação e necessidade.

A portabilidade, transposição do dado de um fornecedor de produtos ou serviços para o outro, é outro direito assegurado ao titular dos dados pessoais no art. 18, inciso V

---

[356] BRASIL. Superior Tribunal de Justiça. Recurso especial n.° 1660168-RJ. Relator: Min. Nancy Andrighi. Brasília, DF, 8 de maio de 2018. [Consultado 25 março 2020]. Disponível em: <https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1628798&num_registro=201402917771&data=20180605&formato=PDF>.

[357] GUEDES, op. cit., p. 228.

[358] SCHREIBER, Anderson. Direito ao esquecimento e proteção de dados pessoais… op. cit., p. 377-380.

da LGPD.[359] É o que já se verifica há algum tempo no Brasil em relação aos números telefónicos. Tal direito é exercido mediante requisição expressa do titular ou representante legalmente constituído.

Segundo Cravo, enquanto o RGPD prevê, no art. 20, que esse direito pode ser exercido de três formas: direito de receber os dados fornecidos pelo titular; direito de transmitir esses dados a outro controlador e o direito de transmissão direta desses dados entre os controladores; a LGPD apenas tratou dessa última forma de exercício, mas, em face de uma interpretação sistemática é permitido ao titular exercer seu direito daquelas outras duas formas.[360] Para que atinja o seu desiderato, a portabilidade deve ser facilitada, daí porque a previsão "sem custos" do art. 18, §5º da LGPD, encontra-se em consonância com tal facilitação. Seguindo os ditames do RGPD, mais especificamente o Considerando 26, a LGPD deixa de fora da portabilidade os dados anónimos, conforme o art. 18, §7º, que exclui os dados que foram anonimizados. Porém, mantém-se esse direito aos dados pseudomizados. Diferentemente do regulamento europeu, que estabeleceu a portabilidade dos dados pessoais fornecidos pelo titular, a LGPD não faz tal restrição, gerando considerável amplitude ao direito, com aumento considerável dos custos. Frise-se, porém, que a portabilidade é dos dados pessoais e não o resultado do tratamento. Nesse sentido Cots e Oliveira citam exemplo que

> [...] determinado site de vendas, com base na navegação do usuário *logado,* cria um perfil de consumo por meio do qual oferece produtos de acordo com os interesses do cliente, utilizando-se, para isso, de estudo de mercado, *softwares* e outras técnicas. Se o titular solicitar a portabilidade, o *site* não é obrigado a reunir os dados e informações oriundos do tratamento, mas somente os dados pessoais coletados. Isso para que não haja a violação do segredo comercial e o beneficiamento injusto do site receptor dos dados.[361]

Enquanto a LGPD estabelece que a autoridade nacional poderá dispor sobre padrões de interoperabilidade, com vistas à portabilidade, o RGPD, em seu Considerando 68, apenas estimula os responsáveis a desenvolver tais padrões.

O direito à portabilidade pode entrar em conflito com outros direitos, como

[359] BRASIL. PRESIDÊNCIA DA REPÚBLICA– Lei n.° 13.709... op. cit. "Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;"

[360] CRAVO, op. cit., p. 360-361.

[361] COTS, op. cit., p. 131.

segredo industrial, comercial, produção intelectual e até privacidade de terceiros, podendo ser sustentado pelo responsável o art. 18, §4º ou a parte final do art. 18, inciso V da LGPD. Mas a preponderância desses direitos sobre o direito de portabilidade somente ocorrerá se aqueles forem atingidos de forma injustificada ou ilegítima, em um juízo de ponderação caso a caso.[362]

Quanto ao compartilhamento dos dados pessoais, este é permitido, nos termos da LGPD, mas a ele se segue o direito do seu titular de ser informado sobre a finalidade e alcance, como uma decorrência do princípio da transparência. Embora o inciso VII do art. 8º da LGPD não esclareça quanto à necessidade de informação da qualificação das entidades públicas e privadas com quem os dados foram compartilhados, entende-se ser ela obrigatória, caso contrário o titular não teria mais o controlo sobre os seus dados, o que vai de encontros aos objetivos legais. Isso deve ocorrer mesmo que a personalidade do receptor no uso compartilhado seja decorrente de segredo de negócio ou industrial.[363]

Correlacionado com os direitos de direito de correção, anonimização, de bloqueio, de eliminação e no dever de controlo que deve existir no compartilhamento com terceiros, existe a obrigação do controlador de informar os agentes de tratamento, com os quais tenha realizado uso compartilhado de dados, a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, salvo quando a comunicação é comprovadamente impossível ou implique esforço desproporcional.[364] A impossibilidade é ônus da prova do controlador, não apenas de mencionar a situação, como, por exemplo, as tentativas de notificação nos endereços desses terceiros.

O titular dos dados pessoais tem o direito de ser informado da sua liberdade de não conceder o consentimento para tratamento dos seus dados e quais seriam as consequências dessa negativa, que podem ser, por exemplo, a não possibilidade da celebração de um negócio jurídico. Mas a exigência não pode ser desarrazoada, devendo-se atentar para os princípios da necessidade, finalidade e adequação. Pode ser que o

---

[362] CRAVO, op. cit., p. 361-362.

[363] COTS, op. cit., loc. cit.

[364] BRASIL. PRESIDÊNCIA DA REPÚBLICA– Lei n.° 13.709... op. cit. "Art. 18 [...]§ 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional."

consentimento se dê por etapas, em dados básicos primeiramente, seguindo-se a mais dados nas etapas subsequentes, sendo que a advertências do não consentimento também deve se operar por etapas. Porém, no que tange a contratos, o consentimento é dispensável quando o tratamento for para a execução do mesmo ou de procedimentos preliminares relacionados a ele, contrato, em que o titular é parte, a pedido do titular de dados, tendo em vista do disposto no art. 7º inciso V da LGPD[365].

Também, quanto ao consentimento, o titular dos dados tem direito à revogação desse (art. 18, inciso IX), seguindo o art. 8º, §5º da LGPD, a qualquer momento de forma gratuita e facilitada, estando ratificados os tratamentos realizados sob o amparo do consentimento anterior.

Em relação às decisões automatizadas, o titular dos dados tem o direito se solicitar a revisão daquelas que tenham sido tomadas exclusivamente por esse meio e que afetem o seu interesse, inclusive a definição de perfis. Diferentemente o RGPD europeu que, no art. 22, n.° 1 afirma que 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, ressalvadas as exceções do n.° 2, a LGPD não proíbe. Mas ambas as legislações asseguram o direito de pedir revisão. Porém, surge outro distanciamento entre as normas, uma vez que o RGPD assegura a intervenção humana nessa revisão, enquanto que a LGPD assim não mais dispõe no art. 20, *caput*, pois a expressão "´por pessoa natural", que constava na redação original da lei, foi excluída pela MP n.° 869/2018, convertida em Lei n.° 13.853/2019. Tal alteração afeta de forma negativa esse direito de revisão, sendo que não houve um motivo cristalino para a exclusão da atuação humana na revisão.

Quanto à existência do direito à explicação das decisões automatizadas, ele encontra-se disposto no art. 20, §1º da LGPD, sendo que o controlador deve fornecer "informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados". Tal direito visa solucionar a opacidade das decisões automatizadas e das consequências

[365] Ibid. "Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;"

advindas do seu desacerto. Ou seja, deve o controlador expor as justificativas, as razões que levaram a essa decisão. Segundo Doshi-Velez e Kortz, a decisão encontra-se explicada quando se consegue responder, pelo menos, uma das seguintes perguntas: quais são os principais fatores que conduziram à decisão?; caso se modifique os fatores determinantes, a decisão mudaria? ou por que casos semelhantes tiveram decisões distintas?[366] Conforme já disposto, o RGPD também prevê tal direito, mas a LGPD foi muito mais incisiva, referindo-se a informações correspondes a critérios e a procedimentos.

Segundo Rodotà, esse direito do titular de informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para as decisões automatizadas trata-se de um enriquecimento e de um fortalecimento do direito de acesso, permitido àquele conhecer e valorar como têm sido tratadas suas informações.[367]

O art. 21 da LGPD, ao dispor que os dados pessoais que se referem ao exercício regular dos direitos pelo titular não podem ser utilizados em seu prejuízo, é um exemplo de má técnica legislativa, diante da sua obscuridade. Deve-se compreendê-lo no sentido de que o titular não pode ser prejudicado por exercer alguns dos direitos previstos na lei. Daí porque Feigelson e Siqueira afirmam que o artigo inclui "[...] não só utilizações ilegais dos dados, mas também o condicionamento do exercício dos direitos do Capítulo III à alguma situação desfavorável ao titular."[368]

O direito de acesso a jurisdição de forma individual ou coletiva está previsto no art. 22 da LGPD.[369] Tal dispositivo é uma cópia do art. 81 do Código de Defesa do Consumidor[370], demonstrando o elo entre as duas legislações, mas não o suficiente para igualar o tipo de responsabilidade civil, conforme se verá.

3.2.3 A regulação sectorial pela autoridade de controlo e o regime sancionatório e jurisdicional

---

[366] DOSHI-VELEZ, Finale; KORTZ, Mason. Accountability of AI Under the Law: the Role of explanation apud FEIGELSON, op. cit., p. 129.
[367] RODOTÀ, Stefano. *A vida na sociedade de vigilância…* op. cit. p. 69.
[368] FEIGELSON, op. cit., p. 133.
[369] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 13.709... op. cit. "Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva."
[370] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 8.078... op. cit . "Art. 81. A defesa dos interesses e direitos dos consumidores e das vítimas poderá ser exercida em juízo individualmente, ou a título coletivo.

Algumas políticas públicas podem ser formuladas, concretizadas e fiscalizadas pela própria administração direta, com um grau maior ou menor de descentralização, como a saúde e a educação. Porém, existem outras que, em razão da necessidade de conhecimento técnico específico, atuação frequente e célere, proteção constante a desmandos políticos, ausência de competitividade no setor, postulam a adoção de solução diversa, como o que ocorre com a proteção de dados.[371]

Para que uma política de proteção de dados se desenvolva a contento, o responsável institucional pela sua promoção, fiscalização, aplicação e cumprimento da norma deve ser estruturado de forma a atingir seu desiderato, dotado de independência, especialização técnica e competências pertinentes. Não existe uma única solução, poder-se-ia adotar um modelo fragmentado, como o norte americano, ou o centralizado e especializado, como o europeu.

Esse órgão responsável deve proporcionar o equilíbrio das partes envolvidas no tratamento de dados pessoais, não apenas refreando o tratamento de dados pessoais de modo ilegal e/ou desproporcional, mas também empoderando os titulares com formas de gestão de seus dados pessoais. Mas além dessa tutela geral e continuada da Autoridade, qualquer pessoa natural pode pleitear a tutela individual. Em qualquer delas, a tutela pode ocorrer de modo pré-violatório ou pós-violatório.[372]

Seguindo a batuta do modelo europeu, de sucesso internacional, a LGPD prevê um órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. Tal órgão intitulado de "Autoridade Nacional" pelo art. 5º, inciso XIX, foi criado pelo art. 55-A, e denomina-se Autoridade Nacional de Proteção de Dados (ANPD), com autonomia técnica e decisória (ar. 55-B), como órgão da administração pública federal, integrante da Presidência da República.[373]

O grande desafio instaurado pela LGPD, com relação a um órgão responsável, é o de aspirar pela proteção e gestão de dados pessoais, adequandas a práticas emancipatórias, cidadãs e democráticas, correspondentes à dignidade, a mecanismos utilitários e

---

[371] VASCONCELOS, BETO; PAULA, Felipe de. A autoridade nacional de proteção de dados: origem, avanços e pontos críticos. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.) *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 717-739. cit. p. 721. ISBN 978855321663-5.

[372] DIAS, Felipe da Veiga; op. cit., p. 15-16.

[373] BRASIL. PRESIDÊNCIA DA REPÚBLICA– Lei n.° 13.709... op. cit.

eficazes.[374]

Mas a autonomia técnica e decisória prevista em um texto normativo muitas vezes não é suficiente para que essa autonomia se verifique em termos práticos. Diferente do órgão europeu, nasce tal autoridade brasileira com sua autonomia, independência funcional, administrativa e financeira comprometida, posto que deverá atender às diretrizes do órgão Presidência da República, não possuindo personalidade jurídica da administração indireta e nem competência para proposição orçamentária. Ademais, os nomes do conselho diretor são indicados pela Presidência, sem sabatina, votação e aprovação pelo Senado, bem como o órgão não detém carreira própria de servidores concursados.

Era fundamental que tal autoridade fosse dotada de independência e autonomia. A independência, de estar submetida apenas à Constituição Federal e à legislação. Já a autonomia, essa se subdivide em: institucional (organização interna e eleição dos membros); económica-financeira (orçamento próprio e com poder de gestão); funcional-decisória (poder de investigação, intervenção, sanção, execução, solução de conflitos e emissão de pareceres) e regulamentar (sobre a proteção de dados pessoais).[375]

Dispõe, ainda, o art. 55-A: "Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD) [...]", o que, se por um lado demonstra certa responsabilidade fiscal, por outro revela um desprestigio ao órgão e desvalorização da sua função. Ressalte-se, porém, a possibilidade de transformação da Autoridade em entidade da administração pública indireta, em até dois anos,[376] com personalidade jurídica própria, conferindo uma maior autonomia. Essa autonomia relativa tem reflexo direto na proteção dos dados dos cidadãos.

Não se poderia deixar de mencionar a revogação de dois dispositivos, os parágrafos primeiro e segundo do art. 7º da LGPD, sendo que o primeiro determinava que o Poder Público deveria informar ao titular dos dados as hipóteses em que seria admitido o tratamento de dados, necessário à execução de políticas públicas previstas em leis,

[374] DIAS, Felipe da Veiga; op. cit., p. 14.
[375] Ibid., p. 14.
[376] BRASIL. PRESIDÊNCIA DA REPÚBLICA– Lei n.° 13.709... op. cit. "Art. 55-A. [...] § 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República. § 2º A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD."

regulamentos e convénios; já o segundo conferia poder à ANPD de especificar a forma de disponibilização das informações aos respectivos titulares dos dados sobre o tratamento dos dados pelo Poder Público. Com tal conduta legislativa, na primeira hipótese, fragilizou-se o direito à informação e a transparência ao titular dos dados; na segunda, restringiu-se a competência regulamentar da ANPD. Segundo Vasconcelos e De Paula, houve uma criação de uma assimetria regulatória injustificável, com a redução do grau de *accountability* por parte do Poder Público.[377] A tutela dos dados pessoais, este como um direito fundamental, deve ser realizada não apenas contra o particular, mas especialmente contra o Poder Público como agente de tratamento. Os direitos e garantias fundamentais têm em sua génese a proteção do cidadão frente ao Estado.

O art. 55-C da LGPD dispõe quais órgãos compõe a ANPD, não fixando a competência de cada um, a qual será objeto de regulamento via regimento interno, seguindo o disposto no art. 55-G[378].

O Conselho Diretor, formado de cinco diretores, incluído o Diretor-Presidente, é o órgão máximo da ANPD, sendo que tais membros ocuparão cargo em comissão, com mandato de quatro anos, a partir da finalização dos primeiros.[379] Em que pese a ocupação de cargo em comissão, não se aplica em relação a tais diretores a regra da livre nomeação e exoneração, do art. 37, inciso II da Constituição Federal, posto que são detentores de estabilidade no período do mandato, somente perdendo o cargo em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar.[380] A justificativa de tal estabilidade é assegurar a independência no exercício da função, evitando ingerências de autoridades públicas e do capital privado. Nas lições de Cots e Oliveira: "Tal regra é benéfica para preservar a independência do conselheiro, que suportará com maior desenvoltura eventuais pressões

---

[377] VASCONCELOS, op. cit., p. 733.

[378] BRASIL. PRESIDÊNCIA DA REPÚBLICA– Lei n.° 13.709... op. cit. "Art. 55-C. A ANPD é composta de: I - Conselho Diretor, órgão máximo de direção; II - Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; III - Corregedoria; IV - Ouvidoria; V - órgão de assessoramento jurídico próprio; e VI - unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei. [...] Art. 55-G. Ato do Presidente da República disporá sobre a estrutura regimental da ANPD."

[379] Ibid. "Art. 55-D. O Conselho Diretor da ANPD será composto de 5 (cinco) diretores, incluído o Diretor-Presidente. § 1º Os membros do Conselho Diretor da ANPD serão escolhidos pelo Presidente da República e por ele nomeados, após aprovação pelo Senado Federal, nos termos da alínea 'f' do inciso III do art. 52 da Constituição Federal, e ocuparão cargo em comissão do Grupo-Direção e Assessoramento Superiores - DAS, no mínimo, de nível 5. § 3º O mandato dos membros do Conselho Diretor será de 4 (quatro) anos."

[380] Ibid. "Art. 55-E. Os membros do Conselho Diretor somente perderão seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar. § 1º Nos termos do caput deste artigo, cabe ao Ministro de Estado Chefe da Casa Civil da Presidência da República instaurar o processo administrativo disciplinar, que será conduzido por comissão especial constituída por servidores públicos federais estáveis."

e lobbies políticos."

À ANPD, de uma forma geral, se aplicam os princípios constitucionais da administração pública do art. 37 da Constituição Federal, ou seja, legalidade, impessoalidade, moralidade, publicidade e eficiência. E, com fulcro na impessoalidade e moralidade, é que aos membros do Conselho Diretor aplicam-se as vedações dispostas no art. 6º da Lei n.° 12.813/2013, sendo que a violação se configura improbidade administrativa.[381]

O art. 55-J da LGPD dispõe sobre as funções, na verdade poderes administrativos da ANPD. Nesse ponto sobressaem-se os poderes de regulamentar (normativo) e o de polícia.

A Administração Pública é dotada de poderes para conseguir os seus objetivos, fazendo valer o interesse público. Nesse sentido Alexandrino e Paulo

> [o]s poderes administrativos representam instrumentos que, utilizados isolada ou conjuntamente, permitem à administração cumprir suas finalidades. Trata-se, assim, de poderes instrumentais, aspecto em que diferem dos poderes políticos – Legislativo, Judiciário e Executivo-, os quais são Poderes estruturais, dizem com a própria estrutura do estado, estabelecida diretamente pela Constituição.[382]

O poder normativo é aquele a ANPD detém de editar atos administrativos normativos, ou seja, com determinações gerais e abstratas, sem destinatários determinados e incidindo sobre todos os fatos que se enquadrem na hipótese descrita.

É possível se vislumbrar tal poder normativo nos incisos X, XIII, XVIII do art. 55-J da

---

[381] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 12.813, de 16 de maio de 2013. Dispõe sobre o conflito de interesses no exercício de cargo ou emprego do Poder Executivo federal e impedimentos posteriores ao exercício do cargo ou emprego; e revoga dispositivos da Lei n.° 9.986, de 18 de julho de 2000, e das Medidas Provisórias n.os 2.216-37, de 31 de agosto de 2001, e 2.225-45, de 4 de setembro de 2001. [Consultado 15 março 2020]. *"D.O.U."* (17-05-2013). Disponível na internet: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12813.htm>. "Art. 6º Configura conflito de interesses após o exercício de cargo ou emprego no âmbito do Poder Executivo federal: I - a qualquer tempo, divulgar ou fazer uso de informação privilegiada obtida em razão das atividades exercidas; e II - no período de 6 (seis) meses, contado da data da dispensa, exoneração, destituição, demissão ou aposentadoria, salvo quando expressamente autorizado, conforme o caso, pela Comissão de Ética Pública ou pela Controladoria-Geral da União: a) prestar, direta ou indiretamente, qualquer tipo de serviço a pessoa física ou jurídica com quem tenha estabelecido relacionamento relevante em razão do exercício do cargo ou emprego; b) aceitar cargo de administrador ou conselheiro ou estabelecer vínculo profissional com pessoa física ou jurídica que desempenhe atividade relacionada à área de competência do cargo ou emprego ocupado; c) celebrar com órgãos ou entidades do Poder Executivo federal contratos de serviço, consultoria, assessoramento ou atividades similares, vinculados, ainda que indiretamente, ao órgão ou entidade em que tenha ocupado o cargo ou emprego; ou d) intervir, direta ou indiretamente, em favor de interesse privado perante órgão ou entidade em que haja ocupado cargo ou emprego ou com o qual tenha estabelecido relacionamento relevante em razão do exercício do cargo ou emprego."

[382] ALEXANDRINO, Marcelo; PAULO, Vicente. *Direito administrativo descomplicado.* 25ª ed. rev. e atual. Rio de Janeiro: Forense; São Paulo: Método, 2017. p.270-271. ISBN 978853097474-9.

LGPD.[383] Ainda que não disposto de forma expressa, cabe à ANPD, diante do disposto no art. 55-J, inciso XIII, elaborar a Política Nacional de Proteção de Dados Pessoais e da Privacidade, com a colaboração do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPDPP). Segundo o §1º do mesmo artigo, a intervenção regulatória deve ser mínima em atenção ao interesse público, observando-se os fundamentos, princípios e direitos dos titulares.

A LGPD estabeleceu a coordenação das atividades entre a ANPD e demais órgãos e entidades públicos que regulam setores específicos, a fim de compatibilizar o cumprimento das atribuições e o funcionamento dos setores, atendendo tanto a legislação específica, quanto a presente lei. Isso se justifica, uma vez que poderia haver conflito de normas estabelecidas entre ANPD e os órgãos de setores altamente regulados, como: saúde (Agência Nacional de Saúde- ANS), energia (Agência Nacional de Energia Elétrica - ANEEL), telecomunicações (Agência Nacional de Telecomunicações -ANATEL), bancário (Banco Central – BACEN).

O Poder de Polícia, por sua vez, é uma função estatal que, com fulcro no interesse coletivo, estabelece restrições e limitações a liberdades e a demais direitos individuais. Para Carvalho Filho seria "[...] a prerrogativa de direito público que, calcada na lei, autoriza a Administração Pública a restringir o uso e gozo da liberdade e da propriedade em favor do interesse da coletividade."[384]

Na seara do Poder de Polícia na LGPD, a ANPD possui competência de: zelar pela proteção dos dados pessoais; fiscalizar e aplicar sanções; apreciar petições de titular contra controlador, caso não solucionada por este a reclamação; realizar auditorias ou determinar a sua realização; comunicar a autoridades a prática de infrações penais e aos órgãos de controlo interno o descumprimento do disposto nesta lei pelos órgãos da administração pública. Tais competências encontram-se, respectivamente, nos incisos I, IV, V, XVI, XXI e XXII, todos do art. 55-J da LGPD. Ressalte-se que somente a ANPD pode

[383] BRASIL. PRESIDÊNCIA DA REPÚBLICA– Lei n.° 13.709... op. cit. "Art. 55-J. Compete à ANPD: X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial; XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei;"

[384] CARVALHO FILHO, José dos Santos. *Manual de direito administrativo*. 25ª ed. rev., atual. e ampl. São Paulo: Atlas, 2012. p. 75. ISBN 978852246927-7.

aplicar sanções em termos administrativos.

Questão interessante diz respeito à relação entre a ANPD e as microempresas, empresas de pequeno porte, e as iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem *startups* ou empresas de inovação. O art. 55-J, inciso XVIII da LGPD é taxativo em afirmar que, para tais empresas, deve a ANPD "editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos [...]. Tal dispositivo encontra-se em consonância com os arts. 170, inciso IX, 179 e 218, todos da Constituição Federal[385], uma forma de tratamento mais favorecido, como forma de impulso à livre iniciativa e à inovação.

Nesse ponto é acertada a crítica feita por Cots e Oliveira de que, enquanto os conceitos de microempresa e empresas de pequeno porte[386] encontram-se definidos na legislação, não existe um conceito definido de "iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação", sendo que nessa derradeira hipótese utilizou-se o legislador o critério da autodeclaração, a qual deve estar ancorada em critérios objetivos, a fim de que possam ser conferidos.[387]

Ademais, o favorecimento de *startups* e empresas de inovação, sem um critério e sem uma análise individualizada, provoca desigualdade no sistema, posto que nem sempre existirá uma possível vulnerabilidade dessas empresas, muitas delas com patrimônio vultoso.

Além da ANPD, a LGPD criou o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPDPP), composto por 23 representantes titulares, com a origem de

---

[385] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Constituição da República Federativa do Brasil. Op. cit. "Art. 170. A ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, tem por fim assegurar a todos existência digna, conforme os ditames da justiça social, observados os seguintes princípios: [...] X - tratamento favorecido para as empresas de pequeno porte constituídas sob as leis brasileiras e que tenham sua sede e administração no País. [...] Art. 179. A União, os Estados, o Distrito Federal e os Municípios dispensarão às microempresas e às empresas de pequeno porte, assim definidas em lei, tratamento jurídico diferenciado, visando a incentivá-las pela simplificação de suas obrigações administrativas, tributárias, previdenciárias e creditícias, ou pela eliminação ou redução destas por meio de lei. [...] Art. 218. O Estado promoverá e incentivará o desenvolvimento científico, a pesquisa, a capacitação científica e tecnológica e a inovação. "

[386] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei Complementar n.° 123, de 14 de dezembro de 2006. Institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte. *"D.O.U."* (15-12-2006). [Consultado 5 março 2020]. Disponível na internet: < http://www.planalto.gov.br/ccivil_03/Leis/LCP/Lcp123.htm>. "Art. 3º Para os efeitos desta Lei Complementar, consideram-se microempresas ou empresas de pequeno porte, a sociedade empresária, a sociedade simples, a empresa individual de responsabilidade limitada e o empresário a que se refere o art. 966 da Lei n° 10.406, de 10 de janeiro de 2002 (Código Civil), devidamente registrados no Registro de Empresas Mercantis ou no Registro Civil de Pessoas Jurídicas, conforme o caso, desde que: I - no caso da microempresa, aufira, em cada ano-calendário, receita bruta igual ou inferior a R$ 360.000,00 (trezentos e sessenta mil reais); e II - no caso de empresa de pequeno porte, aufira, em cada ano-calendário, receita bruta superior a R$ 360.000,00 (trezentos e sessenta mil reais) e igual ou inferior a R$ 4.800.000,00 (quatro milhões e oitocentos mil reais)." (Redação dada pela Lei Complementar n.° 155, de 2016) Produção de efeito.

[387] COTS, op. cit., p. 234.

seus integrantes bem diversificada, fundamental para a questão da proteção de dados por carrearem experiências diversificadas, com participantes da administração pública e do setor privado.[388] Trata-se de serviço público relevante, sem remuneração.

Em relação à competência do CNPDPP, tem-se um rol taxativo de cinco atribuições, dispostas no art. 58-B da LGPD.[389] Tais atribuições descritas no artigo são límpidas. Entretanto, analisando tais atribuições em conjunto com os demais artigos da LGPD, apenas no presente artigo, incisos I e II, é que o texto legal menciona uma Política Nacional de Proteção de Dados Pessoais e da Privacidade. Trata-se de uma atividade necessária, tendo em vista que a atividade legislativa não consegue abranger todas as situações e a amplitude da matéria, que afetará o setor privado e público, cabendo ao Conselho apenas propor as diretrizes, estratégias, estudos e relatórios para subsidiar a elaboração da política nacional de proteção de dados, a cargo da ANPD.

No que tange às sanções passíveis de aplicação ao agente de tratamento infrator da norma protetiva dos dados, o art. 52 da LGPD elenca, nos seus incisos, um total de nove, todas de natureza administrativa e aplicadas pela ANPD. São elas: advertência, com indicação de prazo para realização de medidas corretivas; multa simples; multa diária; publicização da infração após devidamente apurada e confirmada a sua ocorrência; bloqueio dos dados pessoais a que se refere a infração até a sua regularização; eliminação dos dados pessoais a que se refere a infração; suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período e proibição parcial ou total do exercício de atividades

---

[388] BRASIL. PRESIDÊNCIA DA REPÚBLICA– Lei n.° 13.709... op. cit. "Art. 58-A. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto de 23 (vinte e três) representantes, titulares e suplentes, dos seguintes órgãos: I - 5 (cinco) do Poder Executivo federal; II - 1 (um) do Senado Federal; III - 1 (um) da Câmara dos Deputados; IV - 1 (um) do Conselho Nacional de Justiça; V - 1 (um) do Conselho Nacional do Ministério Público; VI - 1 (um) do Comitê Gestor da Internet no Brasil; VII - 3 (três) de entidades da sociedade civil com atuação relacionada a proteção de dados pessoais; VIII - 3 (três) de instituições científicas, tecnológicas e de inovação; IX - 3 (três) de confederações sindicais representativas das categorias econômicas do setor produtivo; X - 2 (dois) de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais; e XI - 2 (dois) de entidades representativas do setor laboral."

[389] Ibid. "Art. 58-B. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade: I- propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD; II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; III - sugerir ações a serem realizadas pela ANPD; IV - elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e V - disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população."

relacionadas a tratamento de dados.[390]

Trata-se de um rol exaustivo de natureza administrativa, ressalvado, a concomitância com as estabelecidas no Código de Defesa do Consumidor brasileiro (CDCb) e em leis específicas, conforme o §2º do art. 52.

Em que pese as sanções administrativas poderem apresentar, de um modo geral, natureza ressarcitória ou retributiva, todas aquelas previstas no art. 52 da LGPD possuem natureza retributiva, pois visam punir, restringir liberdades, impondo deveres, e não reparar o titular do direito lesado, como ocorre com as primeiras.

Segundo Mello:

> A sanção administrativa retributiva esgota-se na aplicação de um mal ao infrator. Trata-se de medida de simples retribuição pela prática da infração, sem qualquer pretensão de ressarcimento do dano causado pela conduta delituosa ou de restauração do *status quo ante*.[391]

Mas tem-se que reconhecer que a finalidade de tal sanção retributiva não é apenas punir. Visa também desestimular a prática de novos ilícitos.

Pressuposto geral para a aplicação de todas as sanções do art. 52 da LGPD é a prática de alguma conduta que viole a LGPD, ainda que não haja um dado material ou moral a um sujeito. Nesse sentido Cots e Oliveira lecionam: "Não há distinção no artigo, ou seja, caracterizada qualquer infração à LGPD, incluindo no que toca à matéria menos objetiva, como a observação de princípios, por exemplo, já submete o infrator às sanções previstas."[392]

Em que pese a clareza das sanções administrativas previstas no art. 52 da LGPD, deve-se tecer algumas considerações.

À sanção de multa foi acrescentada a qualificação de "simples", unicamente para distinguir da próxima sanção prevista, a multa diária, estando aquela limitada a 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, e no total de R$ 50.000.000,00 (cinquenta

---

[390] Ibid.

[391] MELLO, Rafael Munhoz de. Sanção administrativa e o princípio da culpabilidade. *Revista de Direito Administrativo e Constitucional*, Belo Horizonte, out./dez. 2005, n. 22, [consultado 6 março 2020], p. 25-57, cit. p. 29. Disponível na internet: <file:///C:/Users/TJMA/Documents/624-252-1-PB.pdf>. ISSN 1516-3210.

[392] COTS, op. cit., p. 208.

milhões de reais) por infração, segundo o art. 52, inciso II da LGPD. Ou seja, pela letra da lei, o limite é por infração e não por investigação, denúncia ou caso concreto como um todo. Porém, pensa-se que se deve, nesse ponto, fazer uma interpretação teleológica do dispositivo, no sentido de que se deve considerar o caso concreto como um todo e não a violação de cada item legal. Tal interpretação está em consonância com os fundamentos do desenvolvimento económico e tecnológico e da livre iniciativa do art. 2º, inciso V e VI da LGPD, com fito de se preservar a existência da atividade económica. Cots e Oliveira afirmam: "Assim, parece claro que, se uma única fiscalização houver a cumulação da multa por item violado da LGPD, muitos negócios poderão simplesmente deixar de existir, ante a soma que se alcançará com a cumulação."[393]

A sanção de publicização da infração, prevista no inciso IV do art. 52 da LGPD é outra que pode trazer consequências perenes e devastadoras. Como a legislação não especifica como ela ocorrerá, pode ela se operar em *sites* públicos ou privados, do próprio agente. E dessa forma, estando na rede mundial de computadores, poderá ser replicada, eternizando a punição, comprometendo a imagem da empresa, ainda que a mesma nunca mais vez a infringir a legislação.

As sanções de bloqueio e de eliminação dos dados pessoais, previstas, respectivamente, nos incisos V e VI do art. 52 da LGPD, tem seus conceitos fixados no art. 5º, incisos XIII e XIV, respectivamente, sendo que enquanto no bloqueio atinge apenas o tratamento, suspensão temporária, sem a exclusão dos dados, a eliminação é de natureza definitiva, com eliminação daqueles.

Por fim, as três derradeiras sanções, previstas nos incisos X, XI e XII do art. 52 da LGPD são: suspensão parcial do funcionamento do banco de dados a que se refere a infração por, no máximo, seis meses; a suspensão do exercício de atividade de tratamento de dados, por no máximo 6 meses, prorrogável por igual período; proibição parcial ou total das atividades relacionadas ao tratamento de dados. Essas três sanções foram vetadas pelo Presidente da República, mais tais vetos foram derrubados pelo Congresso Nacional, sendo restabelecidas. Devido à magnitude dessas três sanções, elas possuem uma peculiaridade em relação à demais, qual seja, de somente serem passiveis

[393] Ibid., p. 211.

de incidência se preenchidos dois pressupostos: já ter sido aplicada ao infrator alguma sanção distinta da de advertência para o mesmo caso concreto – espécie de reincidência – e que o responsável seja controlado por outros órgãos com competência sancionatória, órgãos estes que devem ser ouvidos, como, *verbi gratia,* bancos, áreas da saúde, energia e de telefonia. Em relação ao primeiro pressuposto, deve-se entender como mesmo caso concreto a prática de mesma infração em circunstâncias idênticas. Acrescente-se que a possibilidade de dupla punição também é iminente, pelo mesmo fato, pela ANPD e pelo órgão controlador, diante de uma mesma infração. Dessa forma, deve-se seguir-se pela razoabilidade e evitar-se o *bis in idem*. Nas lições de Cots e Oliveira, a ANPD não deve optar uma sanção que gere consequência sociais maiores que o tratamento inadequado, devendo pautar-se pela eficiência com menores impactos sociais.[394] Seguindo o disposto no art. 5º, inciso LIV da CFb, cláusula de reserva jurisdicional, a LGPD não estabeleceu como sanção administrativa a apreensão do banco de dados, posto que esse pertence ao responsável pelo tratamento, em que pese dos dados em si pertençam ao titular.

O §1º do art. 52 da LGPD fixa critérios para a aplicação das sanções administrativas, deixando claro a possibilidade de cumulação e a exigência de um processo administrativo com o resguardo da ampla defesa.[395] Trata-se do estabelecimento de parâmetros ao aplicador da sanção como forma de individualizá-la ao caso concreto, à conduta do infrator, atual e pretérita, sua condição económica, a sua boa-fé, gravidade do ato e consequências, danos e vantagens. Seguiu a LGPD critérios semelhantes aos previstos pelo RGPD em relação à aplicação das coimas no art. 83º.

Aqui princípios como a razoabilidade e a proporcionalidade devem ser utilizados, observando inclusive o interesse coletivo.

Conforme leciona Alexandrino e Paulo

> A imposição de uma limitação à esfera dos direitos individuais que não resulte para o grupo social em vantagem suficiente para compensar os efeitos

[394] Ibid., p. 213.

[395] BRASIL. PRESIDÊNCIA DA REPÚBLICA– Lei n.° 13.709... op. cit. "§ 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios: I - a gravidade e a natureza das infrações e dos direitos pessoais afetados; II - a boa-fé do infrator; III - a vantagem auferida ou pretendida pelo infrator; IV - a condição econômica do infrator; V - a reincidência; VI - o grau do dano; VII - a cooperação do infrator; VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei; IX - a adoção de política de boas práticas e governança; X - a pronta adoção de medidas corretivas; e XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção."

> deletérios da mesma limitação invalida o fundamento do interesse público do ato de polícia, por ofensa ao princípio da proporcionalidade.[396]

Em relação aos destinatários das sanções, o art. 52 dispõe que serão aplicadas contra os agentes de tratamento. Agentes de tratamento são o controlador e o operador, seguindo os conceitos legais dispostos no art. 5º, incisos VI, VII e IX da LGPD[397]. Ficou o encarregado, do art. 5º, inciso VIII, de fora das sanções administrativas.

Entidades e órgão públicos também são destinatários das sanções administrativas, excluindo-se apenas a multa simples e a multa diária, uma vez que as atividades dos órgãos públicos não têm por objetivo o lucro, sendo que afetaria ainda mais os cofres do próprio Estado e, consequentemente, o serviço prestado. Deve a ANPD, quando da aplicação de sanções aos órgãos públicos, observar que o exercício de tal poder não pode resultar em comprometimento dos serviços essenciais, como, por exemplo, saúde e educação.

O §7º do art. 52 da LGPD previu a possibilidade do infrator ficar infenso das sanções administrativas retributivas. Seriam as hipóteses de vazamentos individuais ou acessos não autorizados do art. 46, *caput* da mesma lei, desde que haja acordo do controlador com o titular dos dados. Em que pese atitude do legislador mereça aplausos, como forma de estimular a conciliação, uma forma de pacificação extrajudicial dos conflitos, sua redação peca por não deixar claro se os acessos não autorizados são somente individuais ou se alcançam também os coletivos. Entende-se que a melhor interpretação seja aquela que o parágrafo também se aplicaria apenas a acessos não autorizados de natureza individual, posto que o acesso coletivo indevido, pode trazer consequências sociais devastadoras, especialmente para empresas detentoras de enorme banco de dados, o que não se coadunaria com os princípios protetivos da LGPD.

Acrescente-se que todas as sanções administrativas ainda estão pendentes de regulamentação pela ANPD, regulamento que inclusive deve ser objeto de consulta pública, conforme o art. 53 da LGPD. Cots e Oliveira esclarecem

---

[396] ALEXANDRINO, op. cit., p. 299.

[397] BRASIL. PRESIDÊNCIA DA REPÚBLICA– Lei n.° 13.709... op. cit. "[...] VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; [...] IX - agentes de tratamento: o controlador e o operador;"

> [a]pós a aprovação do regulamento, deverá haver publicação para a ciência geral, especificamente dos controladores, apresentando as formas de dosimetria de sanções, valores-base, fundamentação detalhada, em que hipóteses serão aplicadas multas simples e diárias, entre outras informações descritas nos parágrafos do artigo. [398]

A LGPD deu atenção especial à sanção multa. Além de mencionar no art. 53 e parágrafos, de forma expressa, que o regulamento deve conter a metodologia e, nessa metodologia deve ser levada em consideração, objetivamente, as formas e as dosimetrias para o cálculo do valor-base das sanções de multa, com fundamentação de todos os elementos e critérios legais, além das circunstancias e condições para a adoção da multa simples ou diária, fixou, ainda, no parágrafo único do artigo seguinte (art. 54), regra específica de que a intimação da multa diária deve conter, no mínimo, a obrigação imposta, o valor e o prazo razoável para o cumprimento da obrigação. Portanto, não pode haver incerteza quanto à obrigação a ser cumprida, uma vez que ela somente incidirá após decorrido o prazo concedido. Já o disposto no *caput* do art. 54 da LGPD é desnecessário, uma vez que repete parte dos parâmetros exigidos para aplicação de qualquer sanção do art. 52, §1º e a necessidade de fundamentação, já prevista no art. 53, §1º, ambos da mesma lei.

Nada obsta, ainda, a possibilidade de aplicação de sanções civis e criminais ao infrator.

Na seara judicial, seguindo o disposto no art. 139, inciso IV do Código de Processo Civil brasileiro (CPCb), o magistrado também pode aplicar medidas para assegurar cumprimento de ordem judicial.

Além de tais medidas, a LGPD dispôs, na Secção III do Capítulo VI, sobre a responsabilidade civil, o ressarcimento dos danos, a cargo daqueles que violaram os preceitos legais de proteção aos dados pessoais e praticaram dano. Tais regras da responsabilidade civil estão dispostas apenas em quatro artigos, sendo inspirada no RGPD europeu. Entretanto, de início, merece críticas a LGPD nessa seara, por não definir se a responsabilidade do causador do dano por violação àquela norma será de natureza objetiva ou subjetiva. Em prol da responsabilidade objetiva sustenta-se a analogia com o

[398] COTS, op. cit., p. 218.

Código de Defesa do Consumidor brasileiro (CDCb), uma vez que vários dispositivos da LGPD foram inspirados naquela Lei, como a inversão do ônus da prova do art. 42, §2º da LGPD. Ademais, presente a semelhança entre os artigos 43 da LGPD[399] e o art. 12, §3º do CDCb, especialmente os incisos I e III[400]. Fundamenta-se também na teoria do risco, que seria intrínseco à atividade de tratamento de dados.[401] *A contrario sensu,* em prol da responsabilidade subjetiva, ou seja, fundamentada na culpa, posição que se adota, milita os diversos deveres impostos e padrões de conduta esperados pelo controlador e operador. A análise do cumprimento de deveres ou de padrões, como programas, políticas internas, procedimentos, métodos de supervisão, é típica da responsabilidade subjetiva, com a análise da culpa, um padrão de comportamento esperado nas circunstâncias concretas. Ademais, no projeto original da lei, no Capítulo sobre transferências internacionais, havia previsão expressa de responsabilidade solidária e objetiva dos agentes de tratamento pelos dados causados no art. 35, a qual foi excluída. Ressalte-se o disposto no art. 43, inciso II da LGPD, o qual exclui de responsabilidade os agentes que, embora tenham realizado o tratamento de dados pessoais, não violaram à legislação de proteção de dados, ou seja cumpriram o disposto na lei, o comportamento esperado, não praticando conduta culposa. Guedes e Meireles lecionam que

> [o] inciso II reflete, portanto, o regime subjetivo de responsabilidade, adotado pela LGPD, porque está intrinsecamente vinculado ao elemento culpa e, exatamente por isso, sua redação não se assemelha à do CDC. Enquanto o CDC isenta de responsabilidade o fornecedor que demonstra que o defeito inexiste, que é um parâmetro mais objetivo a LGPD exime do dever de indenizar o agente de tratamento que não tiver violado a lei. [402]

Já em relação ao tratamento dos dados sensíveis, conforme o tipo de tratamento, sendo considerado ele uma atividade de risco, seria possível se vislumbrar a

---

[399] Ibid. "Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem: I - que não realizaram o tratamento de dados pessoais que lhes é atribuído; II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro."

[400] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 8.078... op. cit. "Art. 12. O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos. § 3° O fabricante, o construtor, o produtor ou importador só não será responsabilizado quando provar: I - que não colocou o produto no mercado; II - que, embora haja colocado o produto no mercado, o defeito inexiste; III - a culpa exclusiva do consumidor ou de terceiro."

[401] MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova lei geral de proteção de dados. *Revista de direito do consumidor*, Editora Revista dos Tribunais, São Paulo, nov./dez. 2018, v. 120, p. 473. ISSN 1415-7705.

[402] GUEDES, op. cit., p. 236.

responsabilidade objetiva do causador do dano, com fulcro no art. 927, parágrafo único, do Código Civil brasileiro (CCb)[403], que estabelece uma cláusula geral de responsabilidade objetiva em situações dessa natureza.

Assim, por pressupostos da responsabilidade civil têm-se: a conduta com violação à lei de forma culposa em razão do tratamento de dados, o dano e o nexo causal. A conduta com violação à norma de ser praticada em razão da prática de uma das operações do art. 5º, inciso X da LGPD[404]. O dano é a lesão que pode ser de natureza patrimonial ou extrapatrimonial, individual ou coletiva. Por fim, o nexo é o elo que liga a conduta contrária à norma e o dano.

A princípio a responsabilidade civil do controlador – aquele que detém o poder decisório sobre o tratamento – e do operador – aquele que executa as ordens daquele em razão de uma parceria ou prestação de serviços – não é solidária, tanto que o art. 42, *caput* utiliza o conectivo "ou", respondendo cada um pelos seus atos. Segue-se aqui o disposto o art. 186 e 927 do CCb[405].

Porém, a LGPD criou duas situações de responsabilidade solidária, em que o credor lesado pode cobrar a dívida toda de apenas um dos responsáveis, conforme o art. 264 do CCb[406].

A primeira quando mais de um controlador participou do tratamento que resultou dano, assegurado, contudo a ação de regresso, conforme o §4º do art. 42 da LGPD, seguindo os moldes do art. 934 do CCb[407].

A segunda, de responsabilidade conjunta de controladores e operadores desde que: o operador tenha descumprido as obrigações legais ou não tiver seguido as instruções

---

[403] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 10.406... op. cit. "Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem."

[404] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 13.709... op. cit. "Art. 5º Para os fins desta Lei, considera-se: X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;"

[405] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 10.406... op. cit. "Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito. Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo."

[406] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 10.406... op. cit. "Da Solidariedade Passiva Art. 275. O credor tem direito a exigir e receber de um ou de alguns dos devedores, parcial ou totalmente, a dívida comum; se o pagamento tiver sido parcial, todos os demais devedores continuam obrigados solidariamente pelo resto."

[407] Ibid. "Art. 934. Aquele que ressarcir o dano causado por outrem pode reaver o que houver pago daquele por quem pagou, salvo se o causador do dano for descendente seu, absoluta ou relativamente incapaz."

lícitas do controlador diretamente. Esses requisitos podem ocorrer conjuntamente ou isoladamente. A responsabilidade do operador pelo descumprimento da lei demonstra a exigência de que este deve conhecer o texto legal. Já a responsabilidade do operador por descumprimentos das instruções lícitas do controlador no tratamento dos dados é justificável pois, assim agindo, aquele se equiparar a controlador, arvorando-se de poder decisório.

Sábia a lição de Cots e Oliveira: "[...] se as instruções do controlador forem contrárias à LGPD, o operador deve se recusar a cumpri-las? Sim, salvo se desejar assumir com o controlador o risco do tratamento irregular."[408]

O art. 43 da LGPD dispõe de três hipóteses de exclusão da responsabilidade dos agentes de tratamento, ou seja do controlador e do operador, cabendo a estes a prova: a não realização do tratamento atribuído; ainda que realizado o tratamento, não houve a violação à lei de proteção de dados ou o dado decorre de culpa exclusiva do titular dos dados ou de terceiro. A primeira funda-se na inexistência do ato em si de tratamento, uma vez que, se esse inexistiu, não houve a conduta. A segunda é a inexistência da violação da norma. Houve o tratamento, mas não a violação à lei geral de proteção de dados. Por derradeiro, tem-se a culpa exclusiva do titular ou terceiro. A redação dessa última excludente assemelha-se à prevista no art. 14, §3º, inciso II do CDCb[409]. A culpa exclusiva do titular ocorre quando, por exemplo, o titular fornece seus dados a terceiros ou não guarda seus documentos de forma adequada. Já a culpa exclusiva de terceiro pode gerar dúvidas, posto que ela terá que ser exclusiva daquele, para que o controlador e o operador fiquem isentos da responsabilidade. Ocorre que não existe sistema invulnerável, o que poderia conduzir ao entendimento da sempre contribuição dos responsáveis pelo tratamento.

Nesse ponto, o ônus da prova é assunto de extrema relevância. De regra, seguindo o disposto no CPCb, art. 373[410], cabe ao autor a prova do fato constitutivo do seu direito e ao réu a prova da existência de fato impeditivo, modificativo ou extintivo do direito do

---

[408] COTS, op. cit., p. 181.

[409] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 8.078... op. cit .

[410] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 13.105, de 16 de março de 2015. Código de Processo Civil. *"D.O.U."* (17-03-2015). [Consultado 7 março 2020]. Disponível na internet: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Lei/L13105.htm>. "Art. 373. O ônus da prova incumbe: I - ao autor, quanto ao fato constitutivo de seu direito; II - ao réu, quanto à existência de fato impeditivo, modificativo ou extintivo do direito do autor."

autor. Mas o § 1º do mesmo artigo assegurou a possibilidade da distribuição do ônus dinâmico da prova nos casos previstos em lei ou diante de peculiaridades da causa relacionadas à impossibilidade ou à excessiva dificuldade de cumprir o encargo nos termos do caput ou à maior facilidade de obtenção da prova do fato. O ordenamento jurídico brasileiro, em matéria consumerista, já previa possibilidade de inversão do ônus probatório no art. 6, inciso VIII do CDCb[411], quando fosse verossímil a alegação ou for o consumidor hipossuficiente, segundo as regras ordinárias de experiência.

Seguindo essa toada, art. 42, §2º da LGPD, não criado nada inédito, previu a possibilidade do magistrado inverter esse ônus em três situações: for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa. Trata-se de uma forma de facilitar a defesa do titular de dados pessoais em juízo, reconhecendo a lei que, geralmente, estará ele em situação de desvantagem em relação aos responsáveis pelo tratamento.

A lei prevê expressamente a responsabilidade do controlador e do operador quando o tratamento dos dados for irregular. A noção de irregularidade é mais ampla do que a verificação das hipóteses que autorizam os agentes de tratamento a realizá-lo. Irregular é o tratamento que é realizado sem a base legal do art. 7º da LGPD, mas também aquele que não fornece a segurança esperada pelo titular, considerando as circunstâncias relevantes. O §4º do art. 44 da LGPD cita três circunstâncias: o modo pelo qual é realizado; o resultado e os riscos que razoavelmente dele se esperam e as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.[412] A expectativa segurança esperada pelo titular, sua expectativa, somente pode ser obtida no caso concreto, sob a noção do homem-médio, quanto ao tratamento de dados. Não pode se esperar a mesma segurança de um banco de dados da Receita Federal e o de uma pequena farmácia local. As técnicas de tratamentos disponíveis na época da sua realização também são essenciais. “A palavra ‘disponíveis’ enaltece que é preciso levar em consideração a possibilidade ou não de o controlador ter acesso a determinado

[411] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 8.078... op. cit. “Art. 6º São direitos básicos do consumidor: [...] VIII - a facilitação da defesa de seus direitos, inclusive com a inversão do ônus da prova, a seu favor, no processo civil, quando, a critério do juiz, for verossímil a alegação ou quando for ele hipossuficiente, segundo as regras ordinárias de experiências;”

[412] BRASIL. PRESIDÊNCIA DA REPÚBLICA– Lei n.° 13.709... op. cit.

sistema, não o simples fato de ele existir ou ser comercializado fora dos padrões económicos do controlador sob análise."[413]

Um negócio jurídico pode atrair mais de uma lei. O tratamento pode ocorrer durante uma relação de consumo, o que é muito comum. Nesse contexto, o art. 45 da LGPD estabeleceu que se aplicam, em termos de responsabilização, também as regras consumeristas. As principais situações de responsabilização dos fornecedores para com os consumidores, dizem respeito a defeito e vício do produto e do serviço[414], situações descritas no CDCb, arts. 12 e 14 (defeito do produto e do serviço)[415] e 18 e 19 (vício do produto e do serviço)[416].

Portanto, em relação à responsabilidade civil, pode o titular de dados, em uma relação de consumo, se valer das regras do CDCb para postular a indenização. Da mesma forma, pode o controlador ou o operador se utilizar das regras dos §§2º e 3º do art. 14 do CDCb[417] para excluir a sua responsabilidade civil.

---

[413] COTS, op. cit., p. 186.

[414] Enquanto o vício é inerente ao produto ou serviço em si, na qualidade ou na quantidade, não afetando outros bens do consumidor, materiais ou imateriais, o defeito do produto ou serviço vai além e atinge outros bens do consumidor, sejam materiais ou imateriais, como o estético, a moral e a imagem.

[415] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 8.078... op. cit. "Art. 12. O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos. § 1° O produto é defeituoso quando não oferece a segurança que dele legitimamente se espera, levando-se em consideração as circunstâncias relevantes, entre as quais: I - sua apresentação; II - o uso e os riscos que razoavelmente dele se esperam; III - a época em que foi colocado em circulação. § 2º O produto não é considerado defeituoso pelo fato de outro de melhor qualidade ter sido colocado no mercado. 3° O fabricante, o construtor, o produtor ou importador só não será responsabilizado quando provar: I - que não colocou o produto no mercado; II - que, embora haja colocado o produto no mercado, o defeito inexiste; III - a culpa exclusiva do consumidor ou de terceiro. [...] Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos. § 1° O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais: I - o modo de seu fornecimento; II - o resultado e os riscos que razoavelmente dele se esperam; III - a época em que foi fornecido. § 2º O serviço não é considerado defeituoso pela adoção de novas técnicas. § 3° O fornecedor de serviços só não será responsabilizado quando provar: I - que, tendo prestado o serviço, o defeito inexiste; II - a culpa exclusiva do consumidor ou de terceiro. [...]

[416] Ibid. "Art. 18. Os fornecedores de produtos de consumo duráveis ou não duráveis respondem solidariamente pelos vícios de qualidade ou quantidade que os tornem impróprios ou inadequados ao consumo a que se destinam ou lhes diminuam o valor, assim como por aqueles decorrentes da disparidade, com a indicações constantes do recipiente, da embalagem, rotulagem ou mensagem publicitária, respeitadas as variações decorrentes de sua natureza, podendo o consumidor exigir a substituição das partes viciadas. [...] Art. 20. O fornecedor de serviços responde pelos vícios de qualidade que os tornem impróprios ao consumo ou lhes diminuam o valor, assim como por aqueles decorrentes da disparidade com as indicações constantes da oferta ou mensagem publicitária, podendo o consumidor exigir, alternativamente e à sua escolha: I - a reexecução dos serviços, sem custo adicional e quando cabível; II - a restituição imediata da quantia paga, monetariamente atualizada, sem prejuízo de eventuais perdas e danos; III - o abatimento proporcional do preço. § 1° A reexecução dos serviços poderá ser confiada a terceiros devidamente capacitados, por conta e risco do fornecedor. § 2° São impróprios os serviços que se mostrem inadequados para os fins que razoavelmente deles se esperam, bem como aqueles que não atendam as normas regulamentares de prestabilidade."

[417] Ibid. "Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.[...] § 2º O serviço não é considerado defeituoso pela adoção de novas técnicas. § 3° O fornecedor de serviços só não será responsabilizado quando provar: I - que, tendo prestado o serviço, o defeito inexiste; II - a culpa exclusiva do consumidor ou de terceiro."

4. OS DESAFIOS DA DIGITALIZAÇÃO E DA INTEROPERABILIDADE ADMINISTRATIVA PARA A PROTEÇÃO DE DADOS PESSOAIS EM FACE DA DATIFICAÇÃO DA VIDA [418]

A sociedade atual está sedimentada sobre uma forma organizacional em que a informação se constitui como o núcleo para o desenvolvimento económico e social, diferente do que ocorria nas sociedades agrícola, industrial e pós-industrial. Essas sociedades anteriores eram baseadas em algo material e palpável: a agrícola, na terra e na produção agrícola; a industrial, nas máquinas e na eletricidade; e a pós-industrial, na prestação de serviços, nos setores securitário, bancário, de transporte, de saúde e de assistência jurídica.[419]

Nessas sociedades anteriores, a informação também era vista como um fator relevante para a produção de riqueza. Na sociedade industrial, por exemplo, o engenheiro norte-americano Frederick Taylor (1856-1915), que é considerado o "*pai da administração científica"* das empresas, ou do *Taylorismo,* em sua obra Princípios de Administração Científica (1911) concentra o estudo na eficiência da produção e da riqueza, o que seria necessário, em relação ao trabalho, não apenas selecionar adequadamente o operário, como fornecer a este treinamento adequado específico para a função.[420]

Mas o protagonismo da informação operou-se com a mudança da forma como ela é

---

[418] Datificação é o ato de datificar, de fazer constar em dados quase toda vida do indivíduo. Tal termo corresponde ao fenómeno de crescente importância dos dados em todos os setores da vida em sociedade, com o surgimento de um novo paradigma. A expressão foi usada e correlacionada com o Big Data por Mayer-Schönberger e Cukier. MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. *Big data*: a revolution will transform how we live, work and think. Boston: Houghton Mifflin Harcourt, 2014. p. 91. ISBN 978054422775-0.

[419] MELODY, Willian H. Markets and Policies in New Knowledge Economies. In: MANSEL, Robin et al. (Org.). *The Oxford Handbook of Information and Communication Technologies*. New York: Oxford University Press, 2007, p. 59. ISBN 978019926623-4. "In an agricultural economy, land is the most valuable resource attracting investment capital. In an industrial economy, manufacturing plants, machinery, and other forms of physical capital are the focal points of investment activity. In the evolving knowledge economy, the expectation is that skilled and well-trained people, and the information and communication tools they use, will be the central resource attracting investment because knowledge is produced, stored, and applied primarily by humans. [...] One important distinction between the industrial economy and the evolving new knowledge economy is the shift in emphasis from a primary focus on the transformation of material resources, that is, the physical production of goods, to a focus on improving and facilitating transaction capabilities, that is, generating and communicating information to facilitate exchange transactions" "Em uma economia agrícola, a terra é o recurso mais valioso que atrai capital de investimento. Em uma economia industrial, fábricas, máquinas e outras formas de capital físico são os pontos focais da atividade de investimento. Na economia do conhecimento em evolução, a expectativa é de que pessoas qualificadas e bem treinadas e as ferramentas de informação e comunicação que elas usam sejam o recurso central para atrair investimentos, porque o conhecimento é produzido, armazenado e aplicado principalmente pelos seres humanos. [...] Uma distinção importante entre a economia industrial e a nova economia do conhecimento em evolução é a mudança de ênfase, de um foco principal para a transformação de recursos materiais, isto é, a produção física de bens, para um foco em melhorar e facilitar as capacidades de transação, ou seja, gerando e comunicando informações para facilitar transações." (tradução nossa).

[420] DRUCKER, Peter. A sociedade pós-capitalista. Tradução: Nivaldo Montingelli Junior. 3ª ed. São Paulo: Pioneira, 1993. p. 15-25. ISBN 852241825-X.

armazenada e transmitida. Se anteriormente o armazenamento e a transmissão da informação se operavam em algo material, como um livro, ficheiro ou papel em geral, através da escrita, esta passou a ser armazenada em um sistema binário, o bit[421]. Houve, assim, a desmaterialização da informação, ou seja, a sua digitalização, inclusive de imagens, de vídeo e de áudio.

Segundo Bioni, isso conduziu a uma guinada exponencial, tanto na quantidade, quanto na qualidade das informações processadas. Quantidade, posto que a informação poderia ser armazenada em diversas plataformas, com CDs, *pen drives*, computadores; qualidade, no que tange a organização, facilitando o acesso.[422] A evolução da virtualização da informação, a revolução binária, proporciona a transformação para a sociedade informacional.

Some-se a isso o desenvolvimento das tecnologias da informação e da comunicação (TICs), como computadores, internet, *softwares*, jogos eletrónicos, telemóveis, que levaram a informação a se constituir como fator preponderante sobre qualquer meio de produção. A economia e as reações sociais passam a ser interconectadas.

A internet, como elemento receptor e difusor de informação, produziu, na era pós-moderna, alterações em relação ao comportamento humano. Surgida no final dos anos 60, durante a guerra fria, foi criada pelo governo norte-americano com fins militares, visando meramente interligar bases militares das forças armadas e centros de pesquisa através de um sistema de comunicação. Mas a popularização da rede no mundo somente ocorreu com a criação da *Word Wide Web* (WWW) pelo físico inglês Tim Berners-Lee, no Laboratório Europeu de Partículas Físicas (CERN), na Suíça, em 1990.[423] Em seguida, com a tecnologia de hipertextos, que permitia a conexão entre diversos textos e arquivos, cada documento recebeu um endereço, *Uniform Resource Locator* (URL), com um identificador de hipertextos, *Hypertext Transfer Protocol* (HTTP) e um sinal de que estava disponível na *Web* (WWW).[424] Em 1993 foi desenvolvido, pelo norte-americano Marc Andreessen, o primeiro programa de navegação (*browser*), o qual permitia não apenas o

[421] Pode-se conceituar bit como a menor unidade de ”informação” armazenável (0 ou 1). Na verdade o bit é um dado que em conjunto formará a informação em si.
[422] BIONI, Bruno Ricardo. *Proteção de dados pessoais*...op. cit., p. 7.
[423] MARINELI, op. cit., p. 150-151.
[424] VIEIRA, Eduardo. *Os bastidores da internet no Brasil*. São Paulo: Manole, 2003. p. 6. ISBN 852041708-6.

compartilhamento de textos e arquivos, mas também imagens, gráficos e sons em locais de atualização dinâmica, ou seja, os *sites*.[425] E no início dos anos 90 surgem os grandes provedores de acesso.

Mas não é propriamente a troca de informação que gera a eficiência da economia e das relações sociais. Mas o conhecimento após o processamento dos dados que passa a ser aplicado, gerando a riqueza. Dos dados obtêm-se a informação que deve ser convertida em conhecimento aplicado, tornando a informação produtiva na seara empresarial. Nas lições de Castells: "O que está surgindo não é uma economia ponto.com, mas uma economia interconectada com um sistema nervoso eletrónico."[426]

Na base da informação e do conhecimento aplicado, encontram-se os dados pessoais dos indivíduos, digitalizados e fundamentais para a economia.

Na sociedade da informação há uma enorme quantidade de comportamentos pessoais que se transmutam em dados, em face do desenvolvimento das tecnologias de informação e da comunicação.

Assim os computadores podem processar, armazenar e efetuar a busca. As operadoras de telefonia dispõem de dados referentes ao endereço do utilizador, data, tempo e destinatário das ligações; os bancos detêm dados sobre a movimentação financeira do indivíduo, ativo, passivo, transferência de montante para a compra de bens, dependentes, despesas regulares, gastos com saúde, educação, locais onde esteve em determinado dia e hora ao realizar saques em caixa eletrónico; os aplicativos de celulares registam todo o percurso feito pelo indivíduo de posse do aparelho; as redes sociais de nome, número de telefone, idade, imagens, preferências, localização e outros.

O crescente aumento na utilização dos meios eletrónicos nas relações sociais conduz a um aumento dos cadastros onde constam tais bancos de dados. Segundo Marineli, é "[...] o que podemos denominar de uma demanda de registros."[427]

Nesse sentido, "[...] o ciberespaço é uma verdadeira plataforma eletrónica de transação onde os dados pessoais dos seus utilizadores se convertem num dos maiores

---

[425] Ibid., p. 7-8.

[426] CASTELLS, Manoel. *A galáxia da internet*: reflexões sobre a internet, os negócios e a sociedade. Tradução. Maria Luiza X. de A. Borges. Rio de Janeiro: Zahar, 2003. p. 57. ISBN 978857110740-3.

[427] MARINELI, op. cit., p. 136.

ativos económicos do mundo online, transformando-se na nova 'moeda' digital."[428] Na expressão de Matiuzzo, é o "varejo dos dados pessoais."[429]

Mas essa nova dinâmica de produção de riqueza não é propriamente uma economia da informação, mas do conhecimento, onde o seu processamento-organização é transmutado em um conhecimento a ser aplicado. Nesses termos, Amaral leciona que "[o] que faz a empresa ganhar dinheiro não é receber a informação em si própria. É transformar a sua informação em conhecimento que depois é aplicado. Falta-nos por isso introduzir a questão da transformação da informação em conhecimento."[430]

O mercado se sustenta nessa extração da informação a partir dos dados, fazendo com que o indivíduo se constitua com um expectador desse uso, uma "economia de vigilância". Ou seja, é uma observação perene do comportamento dos indivíduos que movimenta a economia, onde atores cooperam entre si transacionando os dados pessoais, a fim de que a mensagem publicitária direcionada seja a mais eficaz possível.

Bioni enfatiza: "Com a inteligência gerada pela ciência mercadológica, especialmente quanto à segmentação dos bens de consumo (*marketing*) e sua promoção (publicidade), os dados pessoais dos cidadãos converteram-se em fator vital para a engrenagem da economia da informação."[431]

E, cada vez mais, tais dados podem ser objeto de técnicas capazes de analisá-los em grandes quantidades, com diversidade e velocidade maiores, obtendo informações relevantes, que, em volumes menores, dificilmente seria possível. Nesse contexto, tem-se o *Big Data*. É que Bioni afirma ser a êxtase desse processo quantitativo e qualitativo da gestão da informação.[432] Isto porque o Big Data, diferente das outras tecnologias comuns de processamento, independe que os dados estejam estruturados em entidades ou atributos para minerá-los. Elimina-se essa etapa de estruturação. Este utiliza a linguagem definida como NoSQL (*not only structured query language*), enquanto a metodologia comum utiliza SQL (*structured query language).* Dados são analisados em toda a sua

---

[428] REBELO, Maria Paulo. Os desafios do Regulamento Geral de Proteção de Dados diante da nova tecnologia *blockchain. Anuário da Proteção de dados 2019*, CEDIS, Lisboa, 2019, [consultado 9 MARÇO 2020], p. 109-135. cit. p. 111. Disponível na internet: < http://cedis.fd.unl.pt/wp-content/uploads/2019/06/ANUARIO-2019-Eletronico_compressed.pdf>. ISSN 2184-5468.

[429] MATIUZZO, Marcela. Propaganda Online e Privacidade: O varejo de dados pessoais na perspectiva antitruste. In: *Ideias em Competição:* 5 anos do Prêmio Ibrac-Tim. São Paulo: Singular, 2015, p. 411-431. ISBN 978858662678-4.

[430] AMARAL, João Ferreira do. *Economia da informação e do conhecimento.* Coimbra: Almedina, 2009. p. 116. ISBN 978972403812-4.

[431] BIONI, Bruno Ricardo. *Proteção de dados pessoais...* op. cit., p. 12.

[432] Ibid., p. 34.

extensão, *posts*, *tweets*, clicks, e-mails, fotos. Da correlação entre todos esses dados, obtêm-se padrões, a recidiva de um evento, que permite induzir condutas ou acontecimentos futuros. Segundo Mayer-Schönberger e Cukier, não é um sistema inteligente de ensinar o computador a pensar de forma ou equivalente igual a um humano, mas trata-se de uma metodologia que processa e organiza dados para inferir a ocorrência de acontecimentos.[433] Não existe, portanto, a preocupação com a causa dos acontecimentos.

Se por um lado as empresas buscam tais dados como algo vital, por outro, em uma sociedade tecnológica, amplamente digital, onde se tem computadores, internet, *softwares*, jogos eletrónicos, celulares, e-mail, *sms*, redes sociais, jogos na internet, rádio e TV digital e compras *on-line*, como meios de comunicação, de compartilhamento e de entretenimento, a exposição dos dados pessoais dos indivíduos é cada vez maior diante da necessidade de se participar da vida social, ficando o indivíduo a mercê daqueles que armazenam tais dados.

Mas além dessa necessidade do indivíduo de expor os seus dados para poder participar da vida em sociedade, também não se pode esquecer de uma das facetas da sociedade pós-moderna, que seria a sociedade do espetáculo. Nessa sociedade, o realismo cede espaço à imagem e à representação, à ilusão, afetando a atividade de pensar e reagir. O espetáculo é a relação social entre indivíduos que passa a ser mediada por imagens. Os indivíduos abrem mão da realidade da vida, e passam a viver num mundo movido pelo consumo permanente de fatos, de notícias e de mercadorias. O filósofo francês Debord, que fincou as raízes do pensamento sobre espetáculo assim proclamou:

> 1- Toda a vida das sociedades nas quais reinam as condições modernas de produção se anuncia como uma imensa acumulação de espetáculos. Tudo o que era diretamente vivido se afastou numa representação. [...] 3- O espetáculo apresenta-se ao mesmo tempo como a própria sociedade, como uma parte da sociedade, e como instrumento de unificação. Enquanto parte da sociedade, ele é expressamente o setor que concentra todo o olhar e toda a consciência. Pelo próprio fato de este setor ser separado, ele é o lugar do olhar iludido e da falsa consciência; e a unificação que realiza não é outra coisa senão uma linguagem oficial da separação generalizada. 4- O espetáculo não é um conjunto de imagens, mas uma relação social entre pessoas, mediada por imagens.[434]

[433] MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. *Big data…* op. cit. p. 12.
[434] DEBORD, Guy. A sociedade do espetáculo. Rio de janeiro: Contraponto, 1997. p. 14. ISBN 858591017-8.

O valor principal, o lema, é a diversão. E não basta divertir-se. É necessária a exposição para terceiros dessa diversão, o compartilhamento. Essa exposição dos dados é a forma de participar do espetáculo. E quanto mais se é visto, mais se é exposto, melhor ainda.

Bauman frisa:

> [d]esse modo, o fazer sobre o qual se escrevem mensagens no Twitter talvez não signifique mais que dizer 'estou comendo pizza aos quatro queijos', ou 'estou olhando pela janela', ou 'com sono e indo pra cama', ou 'morto de tédio'. O que nós e todos os nossos iguais somos levados a compreender é que a única coisa que importa é saber e contar aos demais o que estamos fazendo – neste momento ou em qualquer outro; o que importa é 'ser visto'. Não tem importância alguma saber por que fazemos tal coisa, o que estamos pensando, desejando, sonhando, o que nos alegra ou entristece quando a fazemos, ou mesmo outras razões que nos inspiraram a usar o Twitter, além de manifestar nossa presença... O que se perde é a intimidade, a profundidade e durabilidade da relação e dos laços humanos.[435]

O indivíduo sente-se incomodado, deprimido, quando inexistem terceiros a desejar obter algum fato, aquele dado postado. Nessa sociedade, se de um lado considera-se normal a exposição dos seus dados como forma a participar do espetáculo e de "ser visto", atingindo a "fama", também se deseja conhecer o alheio, consumi-lo através da TV, radio, *site*, rede sociais, assim como expô-lo, tornando-se também famoso por revelá-lo. O modelo de sucesso mais propagado é ser uma celebridade. E para ser uma celebridade deve-se estar constantemente exposto aos olhos do público.[436]

Caracteriza-se ainda essa sociedade também pela divulgação de vídeos, imagens ou sons que humilham e denigrem o outro, posto que atende a um mesmo desejo e prazer dos membros da sociedade de visualizar a desgraça alheia, o prazer perverso. Tal prazer denominado de *Schadenfreude*[437], composta pelos termos *Schaden* (dano) e *Freude* (alegria), apresenta-se como uma característica humana que incide sobre cada um em diferentes níveis.

O desenvolvimento da tecnologia móvel em fusão com a internet fez com que o

---

[435] BAUMAN, Zygmunt. *44 cartas do mundo líquido moderno*. Rio de Janeiro: Zahar, 2011. p. 27-28. ISBN 853780681-1.

[436] Ibid., p. 41.

[437] SHAFFER, Andrew. A alegria de ver o sofrimento alheio: Shadenfreude e jogos vorazes In: DUNN George A; MICHAUD, Nicholas; e IRWIN, William (Orgs.). *Jogos vorazes e a filosofia*. Tradução: Patrícia Azeredo. Rio de Janeiro: Bestseller, 2013. p. 94. ISBN 857684644-6.

celular fosse alçado ao patamar de principal dispositivo de acesso à rede, se comparado com o computador. Considerando que esses dispositivos nos acompanham quase o tempo todo e o constante acesso, faz com que estejamos cada vez mais conectados, fazendo com que os ambientes *on-line* e *off-line* estejam cada vez mais interligados. Há uma verdadeira omnipresença na internet.

Além dos computadores e celulares, a expectativa é que os mais diversos objetos estejam conectados à internet. É o que se denomina de Internet das Coisas – *Internet of Things* (IoT) –, possível em razão da tecnologia da RFID, através da qual tais aparelhos se conectariam mediante um sistema de radiofrequência. Constitui-se na consagração da datificação, a vigilância, transportada do mundo *on-line* para o mudo físico dos objetos que circundam o nosso meio. Essa tecnologia seria possível com a implantação do IPV6 que possibilitará o aumento considerável no número de protocolos de comunicação (endereços de comunicação) em relação ao IPV4, possibilitando que cada utilizador tenha um endereço de IP (Internet Protocol) fixo, não se fazendo necessário o uso de IP dinâmico. Através da tecnologia RFID, poderia uma geladeira verificar quais alimentos faltantes e encontrá-los automaticamente em um *site* de supermercado, um despertador avisar uma cafeteira para preparo do café ou automóveis transmitindo dados de deslocamento, a fim de se administrar as melhores rotas de tráfego.[438]

Mas, por outro lado, ainda existem obstáculos que dificultam ou impossibilitam que as pessoas físicas e ou jurídicas tenham acesso a uma versão melhor dos bens e serviços públicos acessíveis através das plataformas digitais.[439]

Acrescente-se, ainda, que tecnologias como as Redes Sociais Virtuais, a Inteligência Artificial, a *Blockchain*, a Internet das Coisas conduzem a uma coleta cada vez maior dos dados pessoais, até de hábitos mais íntimos, estando as suas individualidades datificadas, uma extensão eletrónica que poderá decidir os aspectos da vida do indivíduo.

Retorna-se aí à questão de centro, que consiste no controlo da obtenção, do armazenamento e da utilização desses dados pessoais do indivíduo. Como se manter o

---

[438] BIONI, Bruno Ricardo. *Proteção de dados pessoais...* op. cit., p. 85-86.

[439] LEAL, Victor Moreira Mulin. A tecnologia Blockchain como plataforma de interoperabilidade na União Europeia? Um estudo a partir da Decisão (UE) 2015/2240. In: SILVEIRA, Alessandra; ABREU, Joana Covelo de; COELHO, Larissa (Coords.) *Unio e-book Interop 2019:* o mercado único digital da União Europeia como desígnio político: a interoperabilidade como o caminho a seguir. Braga: UNIO – EU Law Journal, 2019. [consultado 4 maio 2020]. p. 26-33. cit. p. 27. Disponível na internet: <http://repositorium.sdum.uminho.pt/bitstream/1822/61446/3/UNIO_EBOOK_INTEROP_2019.pdf >. ISBN 978989545871-4.

elevado nível de proteção em face de novas tecnologias e como elas podem contribuir para uma cidadania digital no contexto de Mercado Único Digital europeu.

4.1 A interoperabilidade administrativa no contexto do Mercado Único Digital

O Estado, considerado de forma individual, hodiernamente, não consegue atender interesses públicos primários globais, como saúde pública, meio ambiente, questões económicas e direitos fundamentais. Em razão desse fenómeno, competências típicas do Estado foram transpostas para um contexto transnacional, para entidades supranacionais.

A União Europeia, fruto dessa necessidade, como entidade transnacional, parte de uma noção de cidadania de mercado, a qual está relacionada com o exercício de direitos económicos para uma cidadania social, com o reconhecimento de direitos fundamentais além das atividades económicas. Nessa cidadania social, o cidadão é ator principal da construção de um mercado interno, cidadania essa que assenta em duas dimensões, uma nacional e outra supranacional. Essa cidadania supranacional, que atua de forma complementar à cidadania nacional e estabelece um elo entre os indivíduos de todos os Estados-Membros da UE, atribui direitos ao cidadão europeu. Para tanto, essa cidadania europeia, supranacional, consagrada no Tratado de Maastricht, expressou-se na Carta dos Direitos Fundamentais da União Europeia, tendo essa estabelecido, no art. 45º[440], que qualquer cidadão da União goza do direito de circular e de permanecer livremente em qualquer território dos Estados-Membros e também no artigo 20º do TFUE, adotado com o Tratado de Lisboa.

No âmbito digital, a União Europeia estabelece o Mercado Único Digital como um mecanismo para a superação da crise económica vivenciada, objetivando elevar a prosperidade económica e social, com a supressão de barreiras às transações em linha entre os Estados-Membros, sem descurar a proteção dos consumidores e dos seus dados como direito fundamental do cidadão.

[440] PARLAMENTO EUROPEU; CONSELHO – Carta dos direitos fundamentais da união europeia. Op. cit.

Eliminam-se, assim, com essa política, as fronteiras, em uma visão de mercado interno em que é assegurada a livre circulação de pessoas, capitais e serviços na seara digital, tendo por base jurídica o disposto nos arts. 4.º, n.° 2, alínea a), 26º, 27º, 114º e 115º do TFUE[441]. Portanto, esse mercado único assenta na ideia de que fronteiras físicas não podem ser um obstáculo à circulação dos bens, os quais se deseja que estejam em circulação. Para tal, a política de implementação leva em conta o potencial do mercado interno da União que permanece inexplorado.

Partindo-se da premissa de cidadania supranacional, em um contexto digital, a cidadania digital também deve ter como característica a supranacionalidade.

Durante anos, essa concretização de atualização digital ficou a cargo dos Estados-Membros. Entretanto, verificou-se que era necessário o estabelecimento de padrões comuns entre os Estados, diante de "descompassos e dificuldades de articulação entre as tecnologias implementadas." Dessa forma, a União chamou para si a responsabilidade, tendo sido estabelecida, em 6 de maio de 2015, a política de concretização do Mercado Único, e que caberia à Comissão Europeia, até janeiro de 2017, mobilizar o Parlamento Europeu e o Conselho, propondo os atos legislativos necessários, uma vez que a promoção do bom funcionamento do mercado interno é competência partilhada, segundo ao art. 4º, n.°2, alínea a) do TFUE.[442] Daí resultariam, não apenas, o RGPD e, em seguida, o Regulamento 2018/1725.

O Mercado Único Digital, fixado com uma política de interesse público primário pelos agentes políticos da União e nacionais, conduziu a interesses públicos secundários, em face dos objetivos, necessários à sua efetivação, dentre eles: a interoperabilidade administrativa que possibilite uma sintonia entre os órgãos nacionais e os da União e, de ambos, para com particulares; a fixação de um padrão elevado de proteção dos dados pessoais, para que se permita a livre circulação dos dados "em um ambiente controlado e protetivo", a fim de serem observadas as liberdades fundamentais.[443] Na busca do Mercado Único Digital, a proteção dos dados, disciplinada pelo RGPD e demais normas, e a interoperabilidade, em especial na administração pública, devem trilhar de forma

[441] UNIÃO EUROPEIA –Tratado sobre o funcionamento da união europeia. Op. cit.
[442] ABREU, Joana Covelo de. O mercado único digital e a interoperabilidade administrativa… op. cit., p. 211.
[443] Ibid., p. 212-213.

harmónica.

Ou seja, o Mercado Único Digital como um interesse público primário, tem por objetivos a fixação de soluções tangíveis como a Administração Pública em Linha. Mas para que a *e-Administração* funcione de forma adequada, prestando serviços públicos pela via eletrónica, de forma eficiente e eficaz, a interoperabilidade é o alvorecer de uma nova Administração Pública, mediante a efetivação da interconexão de informações, a criação de bases de dados e registos transnacionais comuns.

A interoperabilidade pode ser vista, sob a ótica da sociedade da informação, como a capacidade de múltiplos sistemas se relacionarem, trocando informações, sem custos de adaptação.

Na verdade, a interoperabilidade pode ser classificada como técnica, semântica e organizativa. A interoperabilidade técnica é a capacidade de sistemas e dispositivos realizarem a troca de dados e informações com confiabilidade e sem custos; a semântica é a capacidade de manutenção do significado da informação que está sendo proporcionada; e, por fim, a interoperabilidade organizativa é a capacidade de cooperação entre as organizações, mediante processos padronizados.[444]

Ela conduziria à conexão entre as diversas plataformas digitais, mediante o uso tecnológico que permita às autoridades de cada Estado e da União responsável, o acesso nos mais diversos campos e além das fronteiras de cada Estado-Membro, mas sempre observando o respeito à privacidade e à proteção de dados.

O progresso político, económico e social europeu têm por ponto chave a harmonização. E a interoperabilidade surge nesse contexto como forma de eliminar barreiras transfronteiriças de dados, aprimorando os serviços públicos.

Desde os primórdios dos anos 2000, os governos e organizações pregam que a interoperabilidade tornaria os serviços públicos melhores, além de facilitar a cooperação e a integração. Isso pode ser constado de forma hialina da leitura do Considerando 1 da

[444] ABREU, Joana Covelo de; ANDRADE, Francisco C. P. Da interoperabilidade à mediação eletrónica: um novo desafio para a Administração Pública". In: FONSECA, Isabel (coord.) A mediação administrativa: contributos sobre as (im) possibilidades. Coimbra: Almedina, 2019. p. 325-343. apud LEAL, op. cit., p. 27.

Decisão n.° 2015/2240[445].

Em outubro de 2009, foi editado o Regulamento n.° 1071/2009, "que estabelece regras comuns no que se refere aos requisitos para o exercício da actividade de transportador rodoviário", visando adaptar tal setor às regras de um mercado interno, conforme o Considerando 1[446]. A interoperabilidade administrativa nesse setor é ressaltada, uma vez que os registos eletrónicos nacionais dessas empresas, conectados entre os Estados-Membros, com troca de informações de forma mais rápida e eficaz, assegura a cooperação entre os entes estatais, com melhor fiscalização das empresas de transporte rodoviário, redução de custos administrativos para esse controlo, facilitando ainda o cumprimento e fiscalização das regras protetivas de dados estabelecida pela União, desestimulado a prática de infrações. Acrescente-se, ainda, a transparência que é proporcionada com tais registos, tanto para as empresas de transporte, quanto para o público, que poderá acender a certos dados a fim de verificar a regularidade daquelas.[447] Tal registo eletrónico nacional das empresas de transporte rodoviário, autorizadas a exercer a atividade de transportador rodoviário, é obrigatório para todos os Estados-Membros, sendo que o tratamento dos dados lá contidos deve estar sobre o controlo de uma autoridade, assim como deveriam estar interligados entre si através de pontos de contato até 31 de dezembro de 2012, seguindo o disposto no art. 16º.[448] Trata-se, portanto, da busca pela interoperabilidade decorrente da exigência do Mercado Único

[445] PARLAMENTO EUROPEU; CONSELHO – Decisão (UE) 2015/2240 de 25 de novembro de 2015 cria um programa sobre soluções de interoperabilidade e quadros comuns para as administrações públicas, as empresas e os cidadãos europeus (Programa ISA^2) como um meio para modernizar o setor público. "*J.O.U.E.*" (04-12-2015). [Consultado 11 maio 2020]. Disponível na internet: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32015D2240&from=PT>. "Considerando o seguinte: (1) Numa série de declarações ministeriais (Manchester, 24 de novembro de 2005; Lisboa, 19 de setembro de 2007; Malmö, 18 de novembro de 2009; e Granada, 19 de abril de 2010), os ministros convidaram a Comissão a facilitar a cooperação entre os Estados-Membros através da aplicação de soluções de interoperabilidade transfronteiriças e intersetoriais que permitam tornar os serviços públicos mais eficientes e mais seguros. Além disso, os Estados-Membros reconheceram que a oferta de serviços públicos de melhor qualidade deve ser feita com menos recursos, e que o potencial da administração pública em linha pode ser reforçado promovendo uma cultura de colaboração e melhorando as condições para a interoperabilidade nas administrações públicas europeias."

[446] PARLAMENTO EUROPEU; CONSELHO – Regulamento (EU) 1071/2009 de 21 de outubro de 2009 (estabelece regras comuns no que se refere aos requisitos para o exercício da actividade de transportador rodoviário e que revoga a Directiva 96/26/CE do Conselho). "*J.O.U.E.*" (14-11-2009). [Consultado 27 maio 2020]. Disponível na internet: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32009R1071&from=PT>. "Considerando o seguinte: [...] (1) A realização de um mercado interno do transporte rodoviário com condições de concorrência equitativas obriga à aplicação uniforme de regras comuns para o acesso à actividade de transportador rodoviário de mercadorias ou de passageiros ('actividade de transportador rodoviário'). Essas regras comuns contribuirão para aumentar o nível de qualificação profissional dos transportadores, para racionalizar o mercado, para melhorar a qualidade do serviço, no interesse dos transportadores rodoviários, dos clientes e da economia em geral, e para aumentar a segurança rodoviária. Facilitarão também o exercício efectivo do direito de estabelecimento dos transportadores rodoviários."

[447] Ibid., Considerandos 13, 14, 15 e 16.

[448] Ibid.

Digital em um setor específico.[449] [450]

Em 2010, a Comissão Europeia, na Comunicação de 19 de maio, sob o título "Uma Agenda Digital para a Europa" (ADE) "[...] sublinhou que a interoperabilidade é essencial para maximizar o potencial social e económico das tecnologias da informação e da comunicação (TIC) e que, por conseguinte, a agenda digital só poderá ser efetiva se a interoperabilidade estiver assegurada"[451], conforme a leitura do Considerando 2 da Decisão n.° 2015/2240.

Nessa Agenda, pretende-se estimular a economia europeia através da concretização de medidas de aprimoramento de tecnologias digitais pelas empresas, dos agentes e serviços públicos dos Estados-Membros e perante os cidadãos.[452]

Na seara da interoperabilidade administrativa é que a Administração Pública precisa se digitalizar, não apenas dispondo de meios tecnológicos, mas funcionando de uma forma inteligente e coordenada, seguindo os ditames do Plano de Ação Europeu (2016-2020) para a Administração Pública em Linha, observando-se novos princípios lá dispostos, a fim de que os serviços públicos sejam prestados de forma privilegiada por via eletrónica – através de um único ponto de contacto, de forma uniforme, aos diferentes canais do mercado único.[453]

---

[449] Em relação a tal Regulamento n.° 1071/2009, a República Portuguesa chegou a ser condenada em uma ação de incumprimento Após sucessivas notificações da Comissão, concedendo prazos, e a comunicação do parecer fundamentado, com prazo peremptório, proferido em 30 de abril de 2015, o qual também não foi cumprido, ficou a Comissão autorizada a dar início à fase contenciosa perante o TJUE. Ajuizada pela Comissão perante o TJUE, em 12 de novembro de 2015, e julgada em 5.10.2016, foi declarado que Portugal não teria cumprindo as obrigações previstas no direito da União de criação do registo eletrónico nacional das empresas de transporte rodoviário e consequente a interconexão com os demais registos dos Estados-Membros. Estava, assim, Portugal a dificultar a implementação da interoperabilidade e a cooperação entre os Estados-Membros. Cf. UNIÃO EUROPEIA. TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA (TJUE). Ação de incumprimento de Estado nos termos do artigo 258.° TFUE, processo C - 583/14. 10ª Secção. Data do acórdão: 5.10.2016. [Consultado 27 maio 2020]. Disponível na internet: <http://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&jge=&td=%3BALL&jur=C%2CT%2CF&num=C-583%252F15&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=pt&avg=&cid=1735999>.

[450] A ação de incumprimento está prevista nos arts. 258º a 260º do TFUE, dotada de duas fases, uma administrativa (pré-contenciosa), que tramita perante a Comissão, e outra judicial (contenciosa), que corre perante o TJUE, a fim de declarar que o Estado-Membro não cumpriu o Direito da União.

[451] PARLAMENTO EUROPEU; CONSELHO – Decisão (UE) 2015/2240… op. cit. Considerando 2.

[452] RODRIGUES, Laura Gomes. O princípio da autonomia procedimental e o procedimento para concessão de visto pelos Estados-Membros da União Europeia. Os novos desafios da interoperabilidade em matéria de vistos. In: SILVEIRA, Alessandra; ABREU, Joana Covelo de; COELHO, Larissa (Coords.) *Unio e-book Interop 2019:* o mercado único digital da União Europeia como desígnio político: a interoperabilidade como o caminho a seguir. Braga: UNIO – EU Law Journal, 2019. [Consultado 4 maio 2020]. p. 7-15. cit. p. 12. Disponível na internet: <http://repositorium.sdum.uminho.pt/bitstream/1822/61446/3/UNIO_EBOOK_INTEROP_2019.pdf>. ISBN 978989545871-4.

[453] FERREIRA, João. Pistas para uma cidadania à luz da interoperabilidade. In: SILVEIRA, Alessandra; ABREU, Joana Covelo de; COELHO, Larissa (Coords.) *Unio e-book Interop 2019:* o mercado único digital da União Europeia como desígnio político: a interoperabilidade como o caminho a seguir. Braga: UNIO – EU Law Journal, 2019. [Consultado 4 maio 2020]. p. 45-52. cit. p. 50-51. Disponível na internet: <http://repositorium.sdum.uminho.pt/bitstream/1822/61446/3/UNIO_EBOOK_INTEROP_2019.pdf >. ISBN 978989545871-4.

Tal Plano de Ação Europeu (2016-2020), seguindo os objetivos estratégicos do Mercado Único Digital de "modernizar a administração pública, obter interoperabilidade transfronteiras e facilitar uma interação fácil com os cidadãos", acabou por fixar medidas concretas de promoção de mobilidade transfronteiriça, através de serviços públicos digitais interoperáveis, de modernização da administração pública com as tecnologias da informação e comunicação e de facilitação da interação digital entre as administrações e os cidadãos/as empresas para serviços públicos de superior qualidade.[454]

Segundo Ferreira, as administrações devem estar em linha como forma de garantir a integração, como condições e normas comuns de intervenção.[455]

Estar em linha, ou propriamente em rede, significa que administrações públicas europeias devem cooperar entre si, trocando informações, uniformizando a sua atuação, havendo um reconhecimento mútuo de que suas decisões e atos são decisões e atos da União, alargando a confiança recíproca entre as Administrações. Para tanto, todas devem se encontrar em igualdade em termos tecnológicos.

A interoperabilidade, como um método, é capaz de afetar os serviços públicos na União em quatro dimensões, de acordo com o quadro europeu de interoperabilidade: na jurídica, vetando que a legislação crie obstáculos de forma desarrazoada ao reaproveitamento dos dados nas diferentes áreas de atuação; na organizacional, promovendo acordos formais entre as organizações, para fins de interação; na semântica, na uniformização de nomenclaturas, com "descrições comuns de dados trocados" e na técnica, permitindo o funcionamento dos sistemas de informação de forma ininterrupta.[456]

Mas se a interoperabilidade nacional não é algo fácil de ser implementada, o que se dirá da interoperabilidade transfronteiriça.

O cidadão, ao se deslocar no espaço único europeu, é portador de direitos, sendo que as administrações públicas devem garantir o exercício de direitos comuns a eles.

---

[454] COMISSÃO EUROPEIA. Plano de ação europeu (2016-2020) para a administração pública em linha: acelerar a transformação digital da administração pública. Bruxelas, 19 de abril de 2016. [Consultado 17 maio 2020]. Disponível na internet: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52016DC0179&rid=1>.

[455] FERREIRA, João. Pistas para uma cidadania à luz da interoperabilidade. Op. cit., p. 46.

[456] ABREU, Joana Covelo de. Os princípios gerais da Administração Pública em linha na União Europeia e a análise do artigo 14.º do CPA: revisitando as necessidades de literacia digital. In: GOMES, Carla Amado; SERRÃO, Tiago (Coords.). *Código de procedimento administrativo comentado*. AAFDUL, 2020, no prelo.

Portanto, os Estados devem trabalhar ao nível da União, entre sectores, com soluções compatíveis, a fim de evitar o surgimento de obstáculos à prestação de serviços públicos europeus, como a uniformização de informação de identificação ou sistemas de reporte comuns.[457]

Não se tem como ter um serviço público na modalidade transfronteiriça, sem a interoperabilidade, o que é indispensável ao Mercado Único, à liberdade de circulação e ao exercício da cidadania europeia.

A interoperabilidade está relacionada com os mais diversos sectores, tendo a Comissão afirmado que ela está ligada ao conjunto de informações que prestamos nos formulários em rede dos serviços públicos, e que é bastante variado na União, correspondentes à análise das mais diversas ocorrências da vida, como um início de uma atividade, a busca e perda de um emprego, a abertura de um negócio, estudar, a propriedade e autorização para dirigir um veículo.[458]

O debate sobre a interoperabilidade, proposto pela Comissão, com o auxílio das administrações nacionais, é fundamental para o exercício da cidadania na União e para a eliminação de obstáculos ao Mercado Único Digital, uma vez que aquelas, ao funcionarem de forma interoperável criarão, de forma gradativa, a confiança recíproca entre os agentes estatais dos diversos Estados-Membros, atuando mais como instituições funcionalmente europeias.[459]

Ademais, segundo Abreu "[...] a falta de interoperabilidade entre os serviços das entidades públicas e os operadores privados gera perdas em termos de transparência e cria dificuldades ao estabelecimento efetivo de um reconhecimento mútuo e de uma confiança recíproca."[460]

Visando proporcionar um programa de soluções de interoperabilidade e diretrizes comuns, tanto para as administrações públicas, como para as pessoas naturais e coletivas europeias, em atenção à modernização do setor público, emergiu a Decisão n.°

---

[457] FERREIRA, João. Pistas para uma cidadania à luz da interoperabilidade. Op. cit., p. 46.

[458] ABREU, Joana Covelo. O Mercado Único Digital e o seu desígnio político-constitucional: o impacto da Agenda Eletrónica Europeia nas soluções de interoperabilidade. *UNIO – EU Law Journal,* Braga, jan. 2017, v. 3, n. 1, [consultado 18 fevereiro 2020], p. 130-150, cit. p. 135. Disponível na internet: <https://revistas.uminho.pt/index.php/unio/article/view/20/52>. ISSN 2183-3435.

[459] FERREIRA, João. Pistas para uma cidadania à luz da interoperabilidade. Op. cit., p. 47.

[460] ABREU, Joana Covelo. O Mercado Único Digital e o seu desígnio político-constitucional… op. cit., p. 135.

2015/2240 (Programa ISA^2), apresentando inclusive um conceito para a interoperabilidade[461] e que é aplicável de 1 de janeiro de 2016 até 31 de dezembro de 2020. Esse programa visa a modernização das administrações públicas europeias e o estabelecimento do Mercado Único Digital. Ademais, demonstra o reconhecimento de que, em matéria de interoperabilidade, deve haver uma atuação efetiva da União, como forma de uniformizar a atuação dos Estados-Membros, evitando soluções díspares.

Segundo Abreu, tal programa proporciona

> [...] a interação entre as Administrações Públicas europeias, por um lado, e entre as Administrações Públicas europeias, as empresas e os cidadãos, por outro. Finalmente, também irá contribuir para uma administração eletrónica mais efetiva, simplificada e fácil de usar pelo utilizador (e-Administração) em todos os níveis onde a Administração Pública tem influência e exerce a sua atividade.[462]

Na Decisão n.° 2015/2240 percebem-se também vantagens da interoperabilidade na concretização de políticas públicas em três setores: no direito das sociedades; no livre acesso a documentos administrativos e no domínio da identificação eletrónica.

a) no direito das sociedades a interoperabilidade promoverá a segurança jurídica no meio empresarial, mediante a interligação dos registos das sociedades, como o intercâmbio transfronteiriço das informações e facilitará o acesso a pessoas físicas e jurídicas, no âmbito da União. Nessa seara, a Diretiva 2012/17/UE[463] do Parlamento Europeu e do Conselho impõe a interoperabilidade entre os registos centrais, registos comerciais e os registos das sociedades através de uma plataforma central, conforme o Considerando 6 da Decisão n.° 2015/2240[464];

b) no livre acesso aos documentos administrativos, ou seja, em relação às informações fornecidas pelo setor público, estes devem ser disponibilizados, sempre que possível, "em formatos abertos e compatíveis com a leitura por

---

[461] PARLAMENTO EUROPEU; CONSELHO – Decisão (UE) 2015/2240… op. cit. "Artigo 2º Definições. Para efeitos da presente decisão, entende-se por: 1) 'interoperabilidade', a capacidade de organizações díspares e diversas interagirem com vista à consecução de objetivos comuns com benefícios mútuos, definidos de comum acordo, implicando a partilha de informações e conhecimentos entre si, no âmbito dos processos administrativos a que dão apoio, mediante o intercâmbio de dados entre os respetivos sistemas de TIC;"

[462] ABREU, Joana Covelo. O Mercado Único Digital e o seu desígnio político-constitucional… op. cit., p. 136.

[463] PARLAMENTO EUROPEU; CONSELHO – Diretiva 2012/17/EU de 13 de junho de 2012 que altera a Diretiva 89/666/CEE do Conselho e as Diretivas 2005/56/CE e 2009/101/CE do Parlamento Europeu e do Conselho no que respeita à interconexão dos registos centrais, dos registos comerciais e dos registos das sociedades. *"J.O.U.E."* (16-06-2012). [Consultado 13 maio 2020]. Disponível na internet: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32012L0017>.

[464] PARLAMENTO EUROPEU; CONSELHO – Decisão (UE) 2015/2240… op. cit.

máquina, juntamente com os respectivos metadados, ao melhor nível de precisão e granularidade, num formato que garanta a interoperabilidade, a reutilização e a acessibilidade", seguindo a Diretiva 2013/37/EU[465], a teor do Considerando 13 da Decisão n.° 2015/2240[466];

c) em relação à identificação eletrónica, o Regulamento n.° 2014/910[467] estabelece a interoperabilidade de sistemas nacionais de identificação eletrónica, conforme narrado no Considerando 14 da Decisão n.° 2015/2240[468].

Em 2016, foi promovido pela Comissão um fórum, *Digital4EU Stakeholder Forum,* em que se estabeleceu que seria necessário, a atenção inicial e prioritária aos serviços públicos digitais, como forma de modernizá-lo, em razão de deficiência no que tange à qualidade e transparência, ressaltando a relevância do princípio específico da única vez, com a implementação da declaração única e possibilidade de reutilização dos dados, o que permitiria serviços públicos transfronteiriços.[469]

Seguindo essa toada, na República Portuguesa foi criada a Agência para a Modernização Administrativa (AMA), no ano de 2007, a qual é incumbida de efetuar a modernização na administração pública, aprimorando a prestação dos serviços públicos e a relação com os utilizadores, mediante o uso de tecnologias de informação e comunicação. Em 2011 foi criada a Plataforma de Interoperabilidade da Administração Pública, a qual possibilita a troca de informação eletrónica entre entidades públicas e privadas. Para 2019 os objetivos da AMA incluíam a melhora na qualidade serviços públicos, simplificando o relacionamento entre a administração e os cidadãos, com implementação de mecanismos tecnológicos, como o uso de plataformas como a Chave Móvel Digital e desenvolvendo novas aplicações *on-line*, e o auxílio governo na implementação de medidas de modernização e simplificação administrativas.[470]

---

[465] PARLAMENTO EUROPEU; CONSELHO – Diretiva 2013/37/UE de 26 de junho de 2013 que altera a Diretiva 2003/98/CE relativa à reutilização de informações do setor público. "*J.O.U.E.*" (27-06-2013). [Consultado 13 maio 2020]. Disponível na internet: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32013L0037>.

[466] PARLAMENTO EUROPEU; CONSELHO – Decisão (UE) 2015/2240… op. cit.

[467] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) n.° 910/2014 de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE. "*J.O.U.E.*" (28-08-2014). [Consultado 13 maio 2020]. Disponível na internet: <file:///C:/Users/Celeste/Downloads/I_25720140828pt00730114.pdf.pt.pdf >.

[468] PARLAMENTO EUROPEU; CONSELHO – Decisão (UE) 2015/2240… op. cit.

[469] ABREU, Joana Covelo de. Os princípios gerais da Administração Pública… op. cit.

[470] RODRIGUES, Laura Gomes. O princípio da autonomia procedimental… op. cit., p. 13.

Demanda-se, assim, a criação de meios capazes de proporcionar a interação tecnológica e bases de dados comuns pertencentes aos Estados-Membros e sua conexão com o órgão ou entidade da União competente, permitindo o acesso a documentos e dados transfronteiriços relevantes. Seria a constituição de uma base digital transfronteiriça.

A digitalização da Administração Pública objetiva a redução dos custos, a economia de tempo, o aumento da transparência e a melhora da qualidade dos dados e dos serviços públicos.[471]

A Administração Pública em Linha, como um paradigma a ser atingido, tem por necessidade a criação de soluções de interoperabilidade administrativa. Daí, a interoperabilidade, de um método eleito para se atingir a Administração Pública em Linha, torna-se um princípio da Administração Pública a ser observado. Mas não apenas ela se apresenta como um novo princípio.

Na perspectiva da Administração Pública em Linha, de acordo com o Plano de Ação, princípios específicos digitais podem ser identificados, além da transparência e acesso, confiança e segurança: o digital por definição (*digital by default*), o da acessibilidade e inclusão, o da uma única vez (*once-only principle*), o da interoperabilidade por definição (*interoperability by default*) e, por fim, o transfronteiriço por definição (*cross-border by default*).

Nessa senda, os princípios da confiança e segurança exigem que a utilização de novas tecnologias, em matéria de interoperabilidade, que sigam padrões elevados de segurança e de privacidade. Assim, deve-se atentar não apenas para normas de proteção de dados pessoais e da privacidade, mas também para as normas da segurança informática. Nesse sentido, Abreu leciona que a União aposta em estabelecer plataformas e sistemas confiáveis, que possam evitar intrusões ilícitas e crimes informáticos. Fomenta-se, seguindo a Estratégia Europeia para os Dados da Comissão[472], um Mercado Único de dados, mas com um corpo jurídico sólido de proteção de dados, de direitos fundamentais,

---

[471] FERREIRA, João. Pistas para uma cidadania à luz da interoperabilidade. Op. cit., p. 52.

[472] COMISSÃO EUROPEIA. Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões - Uma estratégia europeia para os dados. Bruxelas, 19 de fevereiro de 2020, COM(2020). [Consultado 7 julho 2020]. Disponível na internet: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020DC0066&from=EN>.

em segurança e cibersegurança, em um contexto de serviços públicos interoperáveis.[473] Nesse ponto, cite-se não apenas o RGPD, mas o "Regulamento Cibersegurança".[474]

Já os princípios da transparência e do acesso assegurariam ao titular a possibilidade de postular a correção, apagamento ou alteração dos dados perante a Administração Pública. Mas não apenas isso. Tais princípios permitem que os utilizadores acompanhem os procedimentos administrativos, proporcionando o surgimento de um clima de confiança com os utilizadores de tais serviços, além de uma administração pública aberta, com um maior controlo popular e combate à corrupção.

O princípio digital por definição (*digital by default*)[475] exige que as administrações públicas facultem os serviços públicos, prioritariamente, de forma digital e de um banco intuitivo e central, ainda que tenha que manter outros meios não digitais. O da uma única vez (*once-only principle*) estabelece que os particulares devem fornecer os dados uma única vez, sem a necessidade de novos fornecimentos, ou seja, os utilizadores, empresas e indivíduos, possuem tal expectativa de não mais providenciar alguns documentos, dados e informações que já tenham fornecido no passado, em face da utilização pela Administração Pública de TICs para reutilizar estes dados, evitando exigências desnecessárias para as pessoas naturais e empresas, mas com obediência às regras de proteção de dados. O da interoperabilidade por definição (*interoperability by default*), impõe que os serviços públicos estejam interligados e trabalhando de forma harmoniosa, em atenção à livre circulação de pessoas, serviços e bens na União.[476]

Seguindo o princípio do digital por definição e o da interoperabilidade por definição a Comissão Europeia criou o Portal *joinup*47, uma plataforma que compartilha as boas práticas em sede de interoperabilidade administrativa.[477]

No contexto da interoperabilidade, a Comissão enfatizou que os dados, por serem

---

[473] ABREU, Joana Covelo de. Os princípios gerais da Administração Pública… op. cit.

[474] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2019/881 de 17 de abril de 2019 (Relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n. o 526/2013 (Regulamento Cibersegurança)). *"J.O.U.E."* (07-06-2019). [Consultado 7 julho 2020]. Disponível na internet: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019R0881&from=PT>.

[475] Conforme o Relatório do Índice de Digitabilidade da Economia e da Sociedade (IDES) de 2020, que analisou os dados de 2019, em relação aos serviços públicos digitais, 67% dos cidadãos da União submeteram formulários em linha, um aumento de 10% em relação a 2014, que foi de 57%. Cf. COMISSÃO EUROPEIA. Digital Economy and Society Index Report 2020 - Digital Public Services. [Consultado 6 julho 2020]. Disponível na internet: <https://ec.europa.eu/digital-single-market/en/digital-public-services-scoreboard>.

[476] ABREU, Joana Covelo de. O mercado único digital e a interoperabilidade administrativa… op. cit., p. 217.

[477] Cf. COMISSÃO EUROPEIA. Portal *joinup*. [Consultado 7 julho 2020]. Disponível na internet: <https://joinup.ec.europa.eu/>.

produzidos pela sociedade, devem estar a serviço do interesse público mediante: "utilização de informações do setor público pelas empresas (partilha de dados entre a administração pública e as empresas – G2B); partilha e utilização de dados de bases privadas por outras empresas (partilha de dados entre empresas – B2B); utilização de dados de bases privadas por autoridades públicas (partilha de dados entre empresas e a administração pública – B2G) e a partilha de dados entre autoridades públicas."[478]

O princípio da acessibilidade e da inclusão determina que os serviços públicos sejam inclusivos por definição, a fim de atender as demandas de pessoas idosas e portadoras de deficiência, atentando para a sensibilidade digital dos cidadãos, qual desenvoltura possuem com os meios digitais.

Por sua vez, o princípio transfronteiriço por definição (*cross-border by default*) seria a exigência da Administração Pública de um Estado-Membro ser capaz de se relacionar com cidadãos e empresas estabelecidas em outros Estados-Membros, mediante o fornecimento de serviços públicos de forma internacional.

Segundo Ferreira,

> [d]eve a União providenciar por uma maior e melhor comunicação com e entre as administrações públicas e uma maior sensibilização das mesmas em matéria de interoperabilidade. Ao mesmo tempo, os serviços públicos nacionais têm de estar ligados e interligado, extravasando fronteiras que barrem a sua interconexão com outros do mesmo cariz ao nível da UE, aprofundando o mercado digital único.[479]

A aproximação entre os princípios do transfronteiriço por definição e o da uma única vez propiciam o exercício de direitos além das fronteiras, em um contexto de mercado interno, eliminando entraves burocráticos e a difícil compreensão do sistema organizacional público de um Estado-Membro. Essa inter-relação entre esses dois princípios é atestada pelo Relatório do Índice de Digitabilidade da Economia e da Sociedade (IDES), na secção "Serviços Públicos", que verifica e analisa a possibilidade de utilizadores de um Estado-Membro se valer de serviços públicos de outro Estado-Membro.[480]

---

[478] COMISSÃO EUROPEIA. Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico… op. cit., p. 6-8.
[479] FERREIRA, João. Pistas para uma cidadania à luz da interoperabilidade. Op. cit., p. 52.
[480] ABREU, Joana Covelo de. Os princípios gerais da Administração Pública… op. cit.

Nesse contexto de interoperabilidade e da Administração Pública em Linha, a nova Comissão Europeia, em 2020, estabeleceu, ainda, como ações prioritárias, um Plano de Ação de Educação Digital atualizado para "reforçar o acesso e a utilização dos dados como uma das suas principais prioridades, a fim de preparar as instituições de ensino e formação para a era digital e de as dotar das capacidades necessárias para tomar melhores decisões e aperfeiçoar aptidões e competências" e uma "Agenda de Reforço de Competências que definirá uma via que mostre de que forma a ação da UE e dos Estados-Membros pode aumentar a proporção da população da UE que detém competências digitais básicas, passando dos atuais 57% para 65% até 2025."[481] Segundo Abreu, essas duas ações são capazes de conferir aos indivíduos o entendimento e a compreensão do uso da tecnologia digital na prestação de serviços pela Administração Pública e, como consequência, a participação nas decisões administrativas, além de conduzir a uma melhor preparação dos funcionários públicos.[482] No contexto da sociedade digital e do paradigma da Administração Pública em Linha, objetiva-se em elevar o conhecimento digital e as competências em todos os graus de educação e, consequentemente, o empoderamento de toda a sociedade em matéria digital.

De nada adianta uma Administração Pública em Linha, sem que os utilizadores e os agentes públicos estejam aptos a interagir com as soluções digitais.[483]

Trata-se da promoção da literacia digital, tanto ativa (capacitação dos agentes públicos responsáveis pela condução do procedimento administrativo e de juízes que apreciarão lides decorrentes da atuação daqueles agentes), quanto passiva (elevação da competência digital pelos administrados), sob pena de restarem afetados a transparência, a celeridade e a participação ativa.[484]

Acrescente-se, ainda, como forma de se resguardar preceitos democráticos, qualquer providência adotada, a título de interoperabilidade, na instituição do Mercado Único Digital, deve levar em conta os princípios da proporcionalidade, da igualdade e da

[481] COMISSÃO EUROPEIA. Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico… op. cit., p. 21.
[482] ABREU, Joana Covelo de. Os princípios gerais da Administração Pública… op. cit.
[483] Segundo o Relatório do Índice de Digitabilidade da Economia e da Sociedade (IDES) de 2020, que analisou dados de literacia digital, "Em 2019, o percentual de pessoas que possuem pelo menos habilidades digitais básicas chegou a 58% (contra 55% em 2015). Uma grande parte da população da UE, no entanto, ainda carece de habilidades digitais básicas, embora a maioria dos empregos exija tais habilidades. (tradução nossa) "In 2019, the percentage of people that have at least basic digital skills reached 58% (up from 55% in 2015). A large part of the EU population, however, still lacks basic digital skills, even though most jobs require such skills." (no original) Cf. COMISSÃO. Digital Economy and Society *I*ndex Report 2020… op. cit.
[484] ABREU, Joana Covelo de. Os princípios gerais da Administração Pública… op. cit.

não discriminação.

Quanto ao princípio da proporcionalidade, o caminho a ser trilhado deve ser adequado (capaz de atingir os objetivos de acordo com o direito da União), necessário (o menos prejudicial de todas as propostas adequadas) e proporcional estrito senso (benefícios maiores que os prejuízos). Tal princípio, em termos da necessidade, consta no art. 5º, n.° 4º do Tratado da União Europeia[485]. Por sua vez, em relação à adequação e à proporcionalidade estrito senso, estabelecidos pelo TJUE[486], como princípios gerais de direito da União, devem ser sempre levados em conta, quando da implementação de medidas.

Já quanto os princípios da igualdade e da não discriminação, que se complementam, sendo esse último uma decorrência do primeiro, os dois lados de uma mesma moeda, as soluções de interoperabilidade devem tratar situações iguais de forma igual e situações desiguais de forma desigual. O princípio da igualdade é previsto como um valor universal no preâmbulo e no art. 2º do TUE. Também está esculpido no Título III e no art. 20º da CDFUE[487]. Já o princípio da não discriminação está previsto no art. 21º da CDFUE. Por sua vez, igualdade e não discriminação estão previstos, de forma conjunta, como objetivos da União no art. 3º, n.° 3 do TUE.

4.2 O nível de proteção adequado assegurado pelos RGPD e Regulamento n.° 2018/1725, na União, e pela LGPD, no Brasil, em um contexto de interoperabilidade

Se por um lado a União está interessada em uma interação digital pública através de bases de dados além das fronteiras de cada Estado-Membro, que assegure o acesso das autoridades de cada um deles e do órgão ou entidade da União responsável pelo

[485] UNIÃO EUROPEIA – Tratado da união europeia(versão consolidada). "*J.O.U.E.*" (07-6-2016). [Consultado 30 maio 2020]. Disponível na internet: <https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_2&format=PDF>.

[486] UNIÃO EUROPEIA. TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA (TJUE). Pedido de decisão prejudicial no processo C - 265/87. 5ª Secção. Data do acórdão: 11.7.1989. [Consultado 30 maio 2020]. Disponível na internet: <http://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&jge=&td=%3BALL&jur=C%2CT%2CF&num=C-265%252F87&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=pt&avg=&cid=2153787>.

[487] PARLAMENTO EUROPEU; CONSELHO – Carta dos direitos fundamentais da união europeia. Op. cit.

controlo desse sistema conectivo, por outro lado, a mesma União objetiva manter os padrões elevados de proteção desses dados.

E quando se fala em padrão mais elevado de proteção, perquirido pela União, tem-se em consideração duas normas principais, dois Regulamentos que tutelam a proteção dos dados em razão de novas exigências tecnológicas. Em termos de proteção de dados pessoais, enquanto as administrações públicas nacionais estão sob a batuta direta do RGPD, segundo o art. 4º, n.° 7º, as instituições, órgãos e organismos da União estão sob a regência do Regulamento n.° 2018/1725, conforme o art. 3º, n.° 8[488]. Ambas as normas são uma decorrência direta do art. 16º, n.° 2 do TFUE, mediante a atuação legislativa do Parlamento Europeu e do Conselho, através do procedimento legislativo ordinário.[489]

Tais normas são de direito administrativo global, posto que emanadas por entidade transnacional, observando-se, conforme leciona Rodrigues que: "[a] UE segue uma estrutura descentralizada da função administrativa, na medida em que o seu exercício cabe não só às suas próprias instituições, órgãos e organismos, como ainda é confiada às administrações públicas dos vários Estados-Membros (EM)."[490] Quando o direito é aplicado administrativamente pelas instituições, órgãos e organismos da União, denomina-se "administração organicamente europeia"; já quando o direito é aplicado pela Administração Pública dos Estados-Membros, denomina-se "administração funcionalmente europeia". Pode ainda ele ser aplicado com participação de ambos, de forma conjunta, como forma de chegar-se a uma decisão ou aplicação uniforme.

Tais Regulamentos procuram conciliar a promoção da atividade económica digital, que se concretiza com a implementação do Mercado Único Digital, com a proteção dos direitos fundamentais, especialmente o de proteção de dados como um direito autónomo. E isso se fazia necessário, considerando o aumento do tratamento dos dados

[488] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2018/1725 de 23 de outubro de 2018 (Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.° 45/2001 e a Decisão n.° 1247/2002/CE). *"J.O.U.E."* (21-11-2018). [Consultado 11 maio 2020]. Disponível na internet: < https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32018R1725&from=PT>.

[489] UNIÃO EUROPEIA – Tratado sobre o funcionamento da união europeia. Op. cit. "Artigo 16. o (ex-artigo 286. o TCE) 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. O Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes."

[490] RODRIGUES, Laura Gomes. O princípio da autonomia procedimental… op. cit., p. 9.

pessoais em face da sociedade da informação e da ascensão da economia digital. Frise-se que o Regulamento n.° 2018/1725 surge em substituição ao Regulamento n.° 45/2001, como uma forma de adequar os padrões de proteção dos dados pessoais aos ditames do RGPD, dados esses objeto de tratamento pelas instituições e órgãos da União e sobre a livre circulação desses dados entre esses órgãos e entidades, e desses com terceiros estabelecidos na União, conforme o art. 1º, n.°1 e 2[491].

A existência de ambos os Regulamentos demonstra a intenção da União de maximizar a proteção dos dados, no intuito de concretizar o princípio do "mais elevado âmbito de proteção" que é previsto no art. 53º da CDFUE[492]. Seguindo-se tal dispositivo, nas situações em que for possível aplicar mais de um padrão de proteção, deve-se aplicar a norma mais favorável, em um modelo de influências e correlação entre as normas de diferentes ordens jurídicas, sob a direção do que é plasmado pelo direito da União.

Na verdade, esse nível de proteção deve ser igualado, independentemente se o tratamento está sendo realizado pela administração pública nacional ou por um órgão ou entidade da União, com forma de se fixar um padrão de proteção maior, mais elevado, especialmente em face da interoperabilidade, que conduzirá ao compartilhamento de dados por autoridades nacionais e europeias.[493]

Mas esse "mais elevado âmbito de proteção" é assegurado também por aqueles que efetuam a aplicação das normas. Em relação às autoridades responsáveis pela proteção de dados, há uma interação entre as autoridades de controlo nacionais, o Comité Europeu e a Autoridade Europeia, estes dois derradeiros esclarecendo dúvidas quanto ao âmbito de aplicação de cada um dos regulamentos.

Ademais, com a implantação do Mercado Único, e a promoção do compartilhamento de dados de forma transfronteiriça, através de uma interoperabilidade, existe a tendência natural de uma interpretação e aplicação de forma uniforme e harmónica da legislação, e nesse ponto surge a atuação do TJUE, ícone na

[491] PARLAMENTO EUROPEU; CONSELHO – REGULAMENTO (UE) 2018/1725 de 23 de outubro de 2018… op. cit. "Artigo 1º Objeto e objetivos. 1. O presente regulamento estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos da União, e regras sobre a livre circulação de dados pessoais entre essas instituições e órgãos, ou entre essas instituições e órgãos e outros destinatários estabelecidos na União. 2. O presente regulamento protege os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais."

[492] PARLAMENTO EUROPEU; CONSELHO – Carta dos direitos fundamentais da união europeia. Op. cit.

[493] ABREU, Joana Covelo de. O mercado único digital e a interoperabilidade administrativa… op. cit., p. 233-234.

proteção jusfundamental da União. É bem verdade que na tutela do direito à proteção de dados atuam também os tribunais nacionais. Mas a fim de evitar diferentes graus de proteção, há um mecanismo cooperação entre o TJUE e os tribunais locais, que é o reenvio prejudicial[494], previsto no art. 267º do TFUE[495]. Segundo Abreu, este mecanismo é capaz de assegurar o nível de proteção desejado dos direitos fundamentais na União, ainda que não de forma exclusiva. Mas além desse instrumento, a relevância da atuação do TJUE se expande em face da sua competência para apreciar todos os litígios referentes ao Regulamento n.° 2018/1725, inclusive ações de indenização, recursos contra as decisões da Autoridade Europeia para a Proteção de Dados e da aplicação de coimas (art. 64º, n.^{os} 1, 2 e 3 do Regulamento n.° 2018/1725.[496] Sim, diante da possibilidade de julgamento de um maior número de casos, como instância inicial, e não apenas revisora, ter-se-á uma aplicação na jurisprudência do TJUE, que poderá ser aproveitada pelos Tribunais nacionais, nas lides que lhe são submetidas. Sem falar que poderá ser estabelecido um elo cooperativo entre o TJUE e os Tribunais nacionais, diante da coincidência entre as definições e direitos estabelecidos em ambos os regulamentos. Como se não bastasse, pode a Autoridade Europeia direcionar questões perante o TJUE (art. 58º, n.° 4 do Regulamento n.° 2018/1725), bem como atuar em processo, o que proporciona uma maior integração entre os órgãos, podendo ser obtida uma visão interpretativa do Tribunal.

Nesses termos é que Abreu entende que tais Regulamentos (RGPD e 2018/1725) proporcionam, no seu âmbito de aplicação, uma proteção adequada aos dados pessoais tratados em bases interoperáveis para fins de uma Administração Pública em Linha.[497]

Por sua vez, surge a indagação se a LGPD brasileira seria capaz de assegurar, em um contexto de interoperabilidade administrativa, a proteção dos dados pessoais de forma adequada.

De início, a LGPD fixa como objetivo, no seu art. 1º, a proteção dos direitos

---

[494] Reenvio prejudicial é um instrumento de cooperação que possibilita os Tribunais nacionais de demandarem perante a TJUE questões de interpretação e validade do direito da União, em um caso em concreto, sem que exista uma hierarquia entre as Cortes jurisdicionais.

[495] UNIÃO EUROPEIA –Tratado sobre o funcionamento da união europeia. Op. cit. "Artigo 267. o (ex-artigo 234. o TCE). O Tribunal de Justiça da União Europeia é competente para decidir, a título prejudicial: a) Sobre a interpretação dos Tratados; b) Sobre a validade e a interpretação dos atos adotados pelas instituições, órgãos ou organismos da União.

[496] ABREU, Joana Covelo de. O mercado único digital e a interoperabilidade administrativa… op. cit., p. 236-237.

[497] Ibid., p. 242.

fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, tendo em conta a proteção de dados como uma decorrência da privacidade.[498] Tal norma tem, por objeto, a proteção dos dados pessoais. Os fundamentos da lei, no art. 2º, refletem a harmonização do respeito à privacidade, à autodeterminação informativa, à inviolabilidade da intimidade, da honra e da imagem, aos direitos humanos, ao livre desenvolvimento da personalidade, à dignidade e ao exercício da cidadania pelas pessoas naturais, com o desenvolvimento económico e tecnológico, a inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor.

Tal norma brasileira é também aplicável ao tratamento de dados pessoais realizado por pessoa jurídica de direito público (art. 3º, art. 5º, inciso VI e VII e arts. 23 a 30, todos da LGPD).

A LGPD estabelece, em seu art. 6º, diversos princípios como: boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, prevenção, segurança, não discriminação, responsabilidade e prestação de contas.[499]

Os princípios da transparência e do acesso asseguram ao titular a possibilidade de postular a correção, o apagamento ou a alteração dos dados.

Os princípios da prevenção e da segurança impõem, em matéria de interoperabilidade administrativa, a observância de elevados padrões de segurança e de privacidade, conduzindo a princípios como o *privacy by design* e o *security by design*.

Os princípios da não discriminação e da igualdade, os quais devem ser levados em conta nas soluções de interoperabilidade, além de previstos na LGPD, estão dispostos na Constituição Federal brasileira: o da não discriminação encontra-se no art. 3º, inciso IV, sendo um dos objetivos fundamentais da República Federativa do Brasil, enquanto o princípio da igualdade se encontra no art. 5º, *caput*.[500]

Por sua vez, o princípio da proporcionalidade, que também é exigido nas soluções de interoperabilidade, é reconhecido no ordenamento jurídico brasileiro, tendo por fundamento os direitos fundamentais e o Estado de Direito.

---

[498] BRASIL. PRESIDÊNCIA DA REPÚBLICA– Lei n.° 13.709... op. cit.
[499] BRASIL. PRESIDÊNCIA DA REPÚBLICA– Lei n.° 13.709... passim.
[500] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Constituição da República Federativa do Brasil. Op. cit.

O modelo de proteção *ex ante* impede, mesmo em sistemas interoperáveis, o tratamento de dados sem uma base legal prevista específica.

A LGPD também adota a *accountability* como princípio*,* com previsões de códigos de boa conduta e certificações, podendo a autoridade nacional de proteção exigir, posteriormente, o relatório de impacto à proteção de dados, em que pese, ainda depender de regulamentação futura, em quais situações ele deve ser exigido e quais seriam as atividades de alto risco.

O sistema de *enforcement* centra-se em uma autoridade com independência, a Autoridade Nacional de Proteção de Dados (ANPD). Porém, nesse ponto, ainda pairam incertezas quanto à natureza jurídica da entidade, e, consequentemente, quanto ao grau de independência.

Nesses termos, entende-se que a LGPD também é capaz de acautelar a proteção de dados num contexto de interoperabilidade administrativa, em uma análise abstrata, posto que nada melhor de se verificar a eficácia de uma norma, quando de sua aplicação.

4.3 As novas tecnologias – a Blockchain –, o RGPD e a LGPD. Uma solução para a interoperabilidade?

O direito não possui a mesma celeridade que o desenvolvimento tecnológico.

Assim, novas tecnologias estão sempre exigindo da legislação novos desafios, sendo que em muitas situações as soluções jurídicas previstas não são capazes de surtir o efeito esperado de tutela dos direitos fundamentais e de resguardo dos direitos específicos previstos no RGPD e na LGPD.

Mas ao mesmo tempo em que uma inovação tecnológica pode se constituir em um desafio na sua conformidade com os direitos resguardados nas normas protetivas dos dados pessoais, pode essa inovação se constituir como um elemento de conformação de uma empresa ou ente governamental, responsável pelo tratamento de dados pessoais com aquelas mesmas normas protetivas.

Isto pode ser compreendido na medida em que para uma empresa privada ou ente

governamental, responsável pelo tratamento de dados, esteja em conformidade com o RGPD ou LGPD, não basta que sistemas/*softwares* contenham ferramentas endereçadas aos objetivos e direitos previstos naquelas normas. A conformidade de uma instituição com o RGPD e com a LGPD exige constante atualização, diante do surgimento regular de novas necessidades e novos desafios.

A conformidade assenta em três vertentes e não apenas na tecnologia: pessoas, processos e, por fim, na tecnologia através de sistemas e ferramentas. Em relação às pessoas, pode-se citar a conscientização, a instrução e a preparação para as mudanças advindas com a nova tecnologia ou norma. Em relação aos processos, tem a adoção e constante revisão do tratamento de dados pessoais, da sua classificação, da política de segurança e privacidade dos dados pessoais, da avaliação de impacto e das auditorias internas e externas e da aferição das garantias de conformidade prestadas pelos subcontratados e fornecedores com os quais a empresa ou a instituição governamental se relacionam. Quanto à tecnologia, é a utilização de sistemas e ferramentas que assegure e promovam o exercício dos direitos por parte dos titulares de dados, assim como de gerenciamento do consentimento e dos demais fundamentos que autorizam o tratamento dos dados pessoais, além de outros. [501]

Portanto, a tecnologia, como um dos elementos responsáveis pela conformação com o RGPD e a LGPD, age de forma a facilitar, agilizar e aprimorar esse processo de conformidade.

Daí o reconhecimento do art. 32º do RGPD[502] nesse ponto, no qual "[...] o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco [...]", isso levando em consideração 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 [...]"

---

[501] DIAS, Leandra. O papel da tecnologia na busca pela conformidade com o RGPD. In: SILVEIRA, Alessandra; ABREU, Joana Covelo de; COELHO, Larissa (Coords.) *Unio e-book Interop 2019:* o mercado único digital da União Europeia como desígnio político: a interoperabilidade como o caminho a seguir. Braga: UNIO – EU Law Journal, 2019. [Consultado 4 maio 2020]. p. 78-85. cit. p. 79-80. Disponível na internet: <http://repositorium.sdum.uminho.pt/bitstream/1822/61446/3/UNIO_EBOOK_INTEROP_2019.pdf >. ISBN 978989545871-4.

[502] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit.

A tecnologia atua na busca dessa conformidade, como no uso pelos responsáveis e subcontratantes de sistemas de antivírus e de bloqueio de *downloads* de fontes duvidosas, adoção de política de atualização de senhas, métodos de recuperação de dados, cifragem de dados (que torna os dados incompreensíveis para terceiros). Possibilita assim, ao responsável, atender a pleitos de utilizadores, no exercício de um direito, com menos custo, com redução dos erros e de forma mais célere. Dessa forma, otimizam-se também os recursos.

Dias ressalta que a tecnologia pode facilitar a prevenção e a identificação de falhas de segurança e violações de dados, com diminuição do risco de exposição destes. Outras técnicas seriam a encriptação de palavras-chave e de ficheiros, níveis de acesso à informação, definição de perfis e de *Logs*, os quais registam todas as operações, possibilitando identificar quem, onde, quando, a quê e o quê houve consulta ou execução sobre dados, possibilitando, assim, a identificação dos responsáveis. São todas elas evidências de conformidade da entidade.[503]

As empresas podem utilizar sistemas que efetuem um rastreamento de conformidade nas atividades de tratamento, permitindo a identificação de não conformidades, com notificações, e a consequente aplicação de medidas como forma de atenuá-las ou dirimi-las, servindo como um adjutório na tomada de decisões de realização ou não de avaliações de impacto.

A tecnologia poderá, inclusive, atuar na criação e desenvolvimento de sistemas como forma de controlar e fiscalizar os responsáveis pelos tratamentos, estando ao serviço das autoridades na deteção de falhas e ilegalidades perpetradas por aqueles.

Mas qualquer tecnologia deve atender a ditames éticos e legais. Sharma, discorrendo sobre a Inteligência Artificial, mas que se aplica às demais tecnologias, ressalta a necessidade de

> [p]rimeiro, garantir que há um grupo diversificado de pessoas a criar a tecnologia, não apenas tecnólogos como eu, mas também pessoas que compreendem a sociedade, as leis, a política. Em segundo lugar, quando desenhamos IA temos de pensar na ética desde o princípio. Que valores

[503] DIAS, Leandra. Op. cit., p. 81.

queremos?[504]

Deve haver, portanto, uma participação não apenas de tecnólogos, mas de juristas, empresas e demais representantes da sociedade civil na criação das tecnologias, como forma de ela atender aos direitos fundamentais e aos anseios sociais, a fim de que todos possam se beneficiar. E o que Dias denomina de "literacia digital ética"[505].

Nesse ponto, merece destaque a *Blockchain*, tecnologia essa sobre a qual se discorrerá de uma forma específica. Não que as demais tecnologias sejam menos relevantes, mas por necessidade de focalizar o âmbito da dissertação e de compreender como esta tecnologia será utilizada e se existe ou não a possibilidade de sua utilização em termos de interoperabilidade pela administração pública, como um dos objetivos do Mercado Único Digital Europeu.

A Decisão n.° 2015/2240 não fixou o meio tecnológico para se alcançar a interoperabilidade, razão pela qual a *Blockchain* surge como uma opção tecnológica e equacionar.

4.3.1 A tecnologia *Blockchain* – seu surgimento e a mudança de um paradigma

Na sociedade da informação, da era digital, tem-se a quarta revolução industrial, ou indústria 4.0, da valorização dos dados e da informação. Nessa nova era, surgiram ferramentas de dados, como o *Big Data*, a Internet das Coisas e os serviços de "nuvem", o que possibilita o aprendizado das máquinas através da inteligência artificial.

A quarta revolução industrial não é fruto de um acaso. Ela resulta da exigência dos consumidores em termos de celeridade na solução de suas demandas em conjugação com a praticidade. Os modelos de produção não são capazes de atender tais demandas a contento, fazendo com que a adaptação a essa nova realidade seja uma necessidade.

---

[504] SHARMA, Kriti. Jovens de hoje vão fazer trabalhos que ainda não existem. *Dinheiro Vivo*, 4 maio 2019. [Consultado 23 maio 2020]. Disponível na internet: <https://www.dinheirovivo.pt/vodafone-business-conference/kriti-sharma-jovens-de-hoje-vao-fazer-trabalhos-que-ainda-nao-existem/>.

[505] DIAS, Leandra. Op. cit., p. 85.

O surgimento da tecnologia *Blockchain* é resultado dessa exigência nesse contexto histórico, especialmente no que tange à interoperabilidade, melhor prestação de serviços aliada à necessidade de segurança e integridade dos dados. Isto pode ser atestado pela verificação de dois episódios ocorridos no mesmo ano, em 2008.

Em setembro de 2008, o Banco de Investimento Lehman Brothers Holdings Inc. pediu falência. Entretanto, em fevereiro de 2007 teria havido uma capitalização recorde de US$ 60 bilhões de dólares, tendo divulgado, em março de 2007, um lucro recorde no primeiro trimestre, que constava em seus livros fiscais.[506] Isto demonstra a possibilidade que as empresas possuem de, ao centralizarem dados, alterarem a contabilidade e os livros registrais, a fim de manter a sua boa imagem no mercado.

E nesse mesmo ano de 2008, tem-se o registo de nascimento da tecnologia *Blockchain*, com a divulgação do surgimento da criptomoeda *Bitcoin.* Essa criptomoeda e a tecnologia *Blockchain* teriam sido desenvolvidas por Satoshi Nakamoto[507], e funcionam através de um sistema de protocolos que operam P2P[508], sem a intervenção de uma entidade central que faça as operações, inexistindo o processamento por uma central.

Logo se observa que a necessidade de se resguardar a segurança nas relações jurídicas, diante da possibilidade de manipulação dos dados armazenados em sistemas centralizados, impulsiona um mercado financeiro alternativo.

Embora tenha surgido com o fim de realizar transações financeiras digitais, o seu uso não está limitado apenas àquela teleologia, posto que a sua utilização é verificada na Internet das Coisas (IoT), em transações digitais, nos domínios associados à Inteligência Artificial e até na seara da Administração Pública em Linha. A sua importância tem sido equiparada ao surgimento da própria internet, conforme leciona Rosic[509].

---

[506] LIOUDIS, Nick. The Collapse of Lehman Brothers: a case study. *Investopedia*, 26 nov. 2019. [Consultado 5 maio 2020]. Disponível na internet: < https://www.investopedia.com/articles/economics/09/lehman-brothers-collapse.asp>.

[507] Pseudônimo utilizado por inventor ou inventores desconhecidos.

[508] *Peer-to-peer*, ou pessoa a pessoa, tecnologia ponto a ponto. Rede sem ponto central de coordenação e sem uma base central de dados, onde cada um dos participantes (*peers*) é autónomo e pode ter acesso a outro participante, funcionando cada um desses, ao mesmo tempo, como cliente e servidor. Cf. MORAES, Alexandre Fernandes de. *Telemática:* convergência de dados, voz e imagem. São Paulo: Érica, 2014. [Consultado 4 maio 2020], p. 92-93. Disponível na internet: <https://books.google.com.br/books?id=a46wDwAAQBAJ&printsec=frontcover&hl=pt-BR&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false>. ISBN 978853652531-0.

[509] ROSIC, Ameer. What is Blockchain technology the new internet? A step-by-stepguide for beginners. *Blockgeeks*, 2016. [Consultado 5 maio 2020]. Disponível na internet: <https://blockgeeks.com/guides/what-is-blockchain-technology/>. "Is Blockchain Technology the New Internet? By allowing digital information to be distributed but not copied, blockchain technology created the backbone of a new type of internet. Originally devised for the digital currency, Bitcoin blockchain, (Buy Bitcoin) the tech community has now found other potential uses for the technology." "A tecnologia Blockchain é a nova Internet? Ao permitir que a informação digital

Trata-se de uma ferramenta de armazenamento de dados que diverge do padrão atual utilizado nos mais diversos setores, inclusive com o sistema de contabilidade que existente há séculos, possuindo, portanto, um caráter disruptivo, capaz de aliar a segurança da criptografia com uma modificação na forma de armazenamento de dados.[510] Verdadeira mudança de paradigma no modelo de confiança.

A confiança é pressuposto da convivência em sociedade, sendo necessária à cooperação.

Sob o ponto de vista humano, está correlacionada ao sentimento de segurança em uma determinada situação, para satisfação de uma expectativa. Já sob o aspecto matemático ou computacional "[...] é um nível particular de probabilidade subjetiva, na qual um agente acredita que outro agente realizará uma ação em particular, que está sujeita a uma verificação e que influencia na própria ação do agente em si".[511]

Enquanto nos sistemas tradicionais de armazenamento de dados o modelo de confiança consiste na centralização da confiança perante uma entidade, como um banco, um cartório ou o governo, havendo uma dependência desse agente centralizador, na *Blockchain* segue-se um modelo distribuído, sendo os dados transmitidos de maneira direta e segura.

Mas a tecnologia *Blockchain* carrega consigo um paradoxo. Se, por um lado, proporciona a segurança nas relações jurídicas e a proteção dos dados, em face de terceiros, e uma interoperabilidade nos sistemas, por outro impõe desafios de sua compatibilização com diversos direitos elencados no RGPD e na LGPD.

---

seja distribuída, mffas não copiada, a tecnologia blockchain criou a espinha dorsal de um novo tipo de internet. Originalmente concebido para a moeda digital, Bitcoin Blockchain, (Compra de Bitcoin) a comunidade tecnológica encontrou agora outros usos potenciais para a tecnologia." (tradução nossa)

[510] CORTIZO, Lucas Silvestre. Blockchain e e-Government: paradigmas e perspectivas. In: SILVEIRA, Alessandra; ABREU, Joana Covelo de; COELHO, Larissa (Coords.) *Unio e-book Interop 2019:* o mercado único digital da União Europeia como desígnio político: a interoperabilidade como o caminho a seguir. Braga: UNIO – EU Law Journal, 2019. [Consultado 4 maio 2020]. p. 16-25. cit. p. 17-18. Disponível na internet: <http://repositorium.sdum.uminho.pt/bitstream/1822/61446/3/UNIO_EBOOK_INTEROP_2019.pdf >. ISBN 978989545871-4.

[511] ALBUQUERQUE, Robson de Oliveira. *Uma proposta de um modelo de confiança computacional para grupos em sistemas distribuídos*. Tese de Doutorado em Engenharia Elétrica, Faculdade de Tecnologia da Universidade de Brasília, Brasília, 2008. 171f. [Consultado 7 maio 2020], cit. p. 12. Disponível na internet: <https://repositorio.unb.br/bitstream/10482/5674/1/2008_RobsonOAlbuquerque.pdf>.

4.3.2 Conceito e estrutura da tecnologia *Blockchain*

O nome *Blockchain* resulta da fusão de dois termos: *block* (bloco) e *chained* (sequência contínua).

A *Blockchain* é uma sequência de blocos que consegue, mediante a descentralização, proporcionar a autenticidade e a segurança das operações. Assemelha-se a um livro de milhares de páginas, sendo que cada página corresponderia a uma sequência linear de quadrados ou blocos, com certo número de dados, acorrentados. Esse livro vai ser acessado, em tempo real, por todos os utilizadores.[512]

No dizer de Rebelo: "[p]or outras palavras, é uma base de dados digital, partilhada, descentralizada e sincronizada que se mantém à base de um algoritmo consensual e armazenada em diversos *nodes* (computadores individuais/usuários)."[513]

A *Blockchain* é um livro-razão virtual distribuído, uma modalidade de DLT (*distributed ledger technology*)[514], utilizando o protocolo P2P, uma vez que possui uma cópia de todo o livro nos computadores dos utilizadores, não sendo administrado e nem armazenado por uma autoridade central. Essa descentralização dos dados funciona em um sistema de blocos imutáveis, sendo que todos os registos nesse sistema são criptografados, utilizando a função criptográfica *hash*, razão pela qual cada documento ou informação possui uma espécie de "impressão digital", tornado-se incorruptível. Funciona como um registo aberto e confiável de armazenamento de informações realizadas de um nódulo (*node*) para outro, ou seja, de um utilizador para outro.[515]

Mougayar sustenta três definições para a *Blockchain*, uma para cada das três perspectivas, a saber: a técnica, a corporativa e a legal. Sob uma perspectiva técnica, ela seria uma base de dados de *back-end* que mantém um registo distribuído abertamente. Sob uma perspectiva corporativa, a *blockchain* é uma rede de trocas para valores em movimento entre partes. Por fim, sob uma perspectiva legal essa tecnologia seria um

[512] CORTIZO, op. cit., p. 17.
[513] REBELO, op. cit., p. 113.
[514] Tecnologia de Registo Distribuído (tradução nossa).
[515] LEAL, op. cit., p. 29.

mecanismo de validação de transações que não necessita de intermediários.[516]

A *Blockchain* pode ser pública (*permissionless ledger*) ou privada (*permissioned ledger*).

A pública é aquela que possibilita que qualquer indivíduo ser um nódulo, lance dados e informações no livro-razão (*ledger*), como ocorre com as criptomoedas *Bitcoin e Ethereum*, sendo que todos que possuem aquele livro detêm uma cópia idêntica.

Já na privada, semelhante a uma intranet, havendo uma restrição daqueles que poderiam ser utilizadores. Essa restrição abarca o acesso, envio e verificação dos dados e informações que estejam disponibilizados na plataforma privada.[517] É necessária uma permissão ou convite para ingresso e acesso aos dados da rede, havendo uma certa fragilização no que tange à descentralização, com a manutenção da criptografia e da auditabilidade e consequentemente com uma segurança bem maior do que o método centralizado de armazenamento. Segundo Rebelo, as "[...] *blockchain* privadas em pouco se distinguem de bases de dados privadas; a verdadeira revolução que esta tecnologia trouxe para o plano digital centra-se, verdadeiramente, nas cadeias de blocos públicas e na possibilidade de tornar qualquer registo imutável."[518]

Na *Blockchain* pública, como não existe uma confiança prévia entre os utilizadores da rede, o modelo de consenso (algoritmo de consenso) utilizado é o de prova de trabalho (*prof of work*) ou o de prova de participação (*prof of stake*). Já no caso da *Blockchain* privada, o modelo de consenso apropriado é designado de prova de autoridade (*proof of authority*) ou Round Robin.

Borges e Revoredo fracionam a classificação estabelecida acima, segundo a qual as *Blockchains* podem ser: públicas (abertas) quando qualquer um pode ser utilizador da rede; privadas (fechadas) quando apenas utilizadores pré-selecionados podem participar da rede; permissionadas, somente podem participar do consenso entidades pré-selecionadas; não-permissionadas, qualquer pessoa pode participar do processo de

---

[516] MOUGAYAR, W. Blockchain para negócios: promessa, prática e aplicação da nova tecnologia da internet. Rio de Janeiro: Alta Books Editora, 2018 apud SAKAMOTO, Sarah Gomes. *Segurança, privacidade e blockchain no contexto de internet das coisas*. Monografia do Curso de Especialização em Internet das Coisas, Universidade Tecnológica Federal do Paraná - UTFPR, Curitiba, 2020. 64 f. [Consultado 19 maio 2020], cit. p. 28. Disponível na internet: <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/16143/1/CT_CEIOT_II_2019_10.pdf >.

[517] LEAL, op. cit., p. 30.

[518] REBELO, op. cit., p. 115.

consenso.[519]

Em relação aos nódulos (*nodes*), os utilizadores ou computadores conectados à plataforma, podem ser integrais ou parciais.

Os nódulos integrais (*full nodes*), também denominados de mineradores, são aqueles que possuem uma cópia de todo o registo da *Blockchain*, diante do grande poder computacional e de processamento. São os responsáveis por alcançar o consenso dos dados e informações enviados e pela publicação dos novos blocos. Esse consenso, de responsabilidade dos nódulos integrais, é o conjunto de regras e diretrizes que determinam a forma, o momento e os requisitos de validação de dados e informações no livro-razão.[520] Eles resolvem os enigmas criptográficos indispensáveis à consistência da *Blockchain*, legitimando as transações.

Segundo Brito e Castillo, discorrendo sobre a moeda *Bitcoin*, o protocolo foi projetado para que cada minerador contribua com o poder de processamento de um computador para manter a infraestrutura necessária para suportar e autenticar a rede monetária. Os mineradores são premiados com bitcoins recém-criados por contribuir com seu poder de processamento para manter a rede e verificar transações na cadeia de blocos. E à medida que mais poder de processamento é dedicado à mineração, o protocolo aumentará a dificuldade do problema matemático, garantindo que os bitcoins sejam sempre minerados a uma taxa previsível e limitada.[521]

A ideia do consenso distribuído baseia-se no Problema dos Generais Bizantinos (*Byzantine Fault Tolerance*). A fim de que uma cidade possa ser conquistada, é necessário que os generais promovam o ataque de forma simultânea, entretanto, nem todos os generais são passíveis de confiança. Quando da recepção da ordem de ataque ou não,

---

[519] BORGES Rodrigo; REVOREDO, Tatiana. Blockchain e as leis de proteção de dados: incompatíveis? *Cio from IDG*, 2018. [Consultado 20 maio 2020]. Disponível na internet: < https://cio.com.br/blockchain-e-as-leis-de-protecao-de-dados-incompativeis/>.

[520] LEAL, op. cit., p. 29-30.

[521] BRITO, Jerry; CASTILLO, Andrea. Bitcoin: a primer for policymakers. Arlington: Mercatus Center at George Mason University, 2016. [Consultado 6 maio 2020]. p. 9. Disponível na internet: < https://www.mercatus.org/system/files/gmu_bitcoin_042516_webv3_0.pdf>. ISBN 978194295116-2. "So, the protocol was designed so that each miner contributes a computer's processing power toward maintaining the infrastructure needed to support and authenticate the currency network. Miners are awarded newly created bitcoins for contributing their processing power toward maintaining the network and verifying transactions in the block chain. And as more processing power is dedicated to mining, the protocol will increase the difficulty of the math problem, ensuring that bitcoins are always mined at a predictable and limited rate." "Portanto, o protocolo foi projetado para que cada minerador contribua com o poder de processamento de um computador para manter a infraestrutura necessária para dar suporte e autenticar a rede monetária. Os mineradores recebem bitcoins recém-criados por contribuir com seu poder de processamento para manter a rede e verificar as transações na cadeia de blocos. E quanto mais poder de processamento for dedicado à mineração, o protocolo aumentará a dificuldade do problema matemático, garantindo que os bitcoins sejam sempre minerados a uma taxa previsível e limitada." (tradução nossa).

cada general deve transmitir a informação aos generais mais próximos a ele, sendo que, finalmente, deve haver uma concordância.[522]

Já os nódulos parciais (*lightweight nodes*), utilizadores parciais, são aqueles que não armazenam uma cópia integral dos registos, por não deterem tanto poder computacional, encaminham os dados e as informações, ajudam e apoiam os nódulos integrais no processamento das transações e possuem visualização.

Nesse contexto, a *Blockchain* possui três pilares: a descentralização, a transparência e a imutabilidade.

O primeiro pilar é a descentralização, a principal distinção do sistema tradicional de realização de transações digitais.

No sistema centralizado, tradicional, o modelo de serviço se desenvolve em uma relação cliente-servidor, na qual o cliente encaminha uma mensagem ao servidor, esse recebe e, posteriormente, devolve a informação, como ocorre com pleito em um *site* de busca.

Outro exemplo desse sistema é o ICP (Infraestrutura de Chave Pública) ou PKI (*Public Key Infrastructure)*, que se utiliza de criptografia assimétrica. Esse sistema assenta em dois elementos fundamentais: a autoridade certificadora e o certificado digital. A autoridade certificadora é aquela que personifica a confiança e é responsável pela emissão do certificado digital. Ela é a retratação da autoridade de confiança e responsável por emitir o certificado digital. Já o certificado digital é o documento que identifica de maneira segura e manifesta uma pessoa natural ou coletiva.[523]

No sistema centralizado, diversas vulnerabilidades podem ser expostas: *primus*, em face da centralização da informação em um único local, tem-se a facilidade de ataques de *hackers* e daqueles que tenham por objetivo obstar o funcionamento de um servidor; *secundus,* a paralisação provisória, em razão da necessidade de atualização de um *software*, ou definitiva do sistema do sistema, gera a impossibilidade de acesso à informação que consta no banco de dados; *tertius,* na hipótese de o banco centralizado ser corrompido ou violado, corre-se o risco de que todos os dados sejam afetados. Isso

[522] SAKAMOTO, op. cit., p. 30.
[523] Ibid, p. 29.

não ocorre com o sistema descentralizado, onde todos os utilizadores são donos da informação e interagem diretamente, sem a interferência de um terceiro.

Na *Blockchain* a descentralização é verificada, posto que a informação se localiza em todos os computadores dos utilizadores, os quais se combinam ao mesmo tempo, confirmando, reiteradas vezes, que todos fazem parte da mesma base de dados, assegurando a veracidade da informação disposta. Essa descentralização é algo oposto do que ocorre de regra com a grande concentração de dados em prestadores de serviços *on-line* como Google, Facebook e Apple. Portando, ela confere uma repartição do poder dos dados com todos os participantes da comunidade digital em oposição ao processamento e armazenamento de dados em servidores centrais. Em face da ausência de uma autoridade centralizadora, o sistema caracteriza-se pela democratização, onde o que é feito na cadeia de blocos tem a conferência dos demais e todos são responsáveis por suas ações.

Nesse sentido, Rosic enfatiza que:

> [o] banco de dados blockchain não é armazenado em qualquer local único, o que significa que os registos que ele mantém são verdadeiramente públicos e facilmente verificáveis. Não existe uma versão centralizada dessas informações para que um hacker corrompa. Hospedado por milhões de computadores simultaneamente, seus dados são acessíveis a qualquer pessoa na internet.[524]

Acrescente-se que, como não existe uma unidade centralizadora os dados, estes somente são inseridos após a confirmação da maioria dos utilizadores da rede. Portanto, novas transações, novos blocos, não são anexadas de forma automática na cadeia de blocos, permanecendo armazenadas, aguardando a decisão majoritária dos utilizadores, sendo que no *Bitcoin* é cerca de dez minutos, e, após essa autorização, é que serão anexadas. Tem-se uma democracia consensual no armazenamento de dados. [525]

Segundo Rebelo, "[...] na blockchain, a prova criptográfica e os algoritmos digitais substituem a confiança tradicional depositada em intermediários."[526]

O compartilhamento de documentos, nos bancos de dados tradicionais, ocorre da

[524] ROSIC, op. cit. "The blockchain database isn't stored in any single location, meaning the records it keeps are truly public and easily verifiable. No centralized version of this information exists for a hacker to corrupt. Hosted by millions of computers simultaneously, its data is accessible to anyone on the internet." (no original).
[525] CORTIZO, op. cit., p. 20.
[526] REBELO, op. cit., p. 115.

seguinte forma: primeiro envia-se aquele documento para o destinatário e, somente após esse devolver, é que o remetente poderá fazer alguma alteração. Ou seja, o remetente precisa aguardar a devolução para ver o que foi alterado pelo destinatário. Isso porque o documento fica bloqueado até que a parte contrária termine. É impossível que remetente e destinatário manipulem um documento ao mesmo tempo. Em transferências bancárias, a instituição financeira bloqueia o acesso (ou diminuem o saldo) durante a operação, atualizam o outro lado, e autorizam novamente o acesso (ou atualizam novamente). Já na Blockchain todas as partes têm acesso ao mesmo documento, em uma versão única, ao mesmo tempo, na modalidade de um livro compartilhado.

O segundo pilar da tecnologia é a transparência. Em que pese a identidade do utilizador estar escondida, em razão da criptografia, poderão ser vistas todas as transações realizadas pelo seu endereço público. Ademais, considerando que os utilizadores (*nodes*) armazenam, de forma idêntica e atualizada, o registo do livro-razão, há possibilidade de realização de auditorias a qualquer momento, por qualquer pessoa, proporcionado uma maior transparência[527], um dos princípios do RGPD e da LGPD.

O terceiro pilar é a imutabilidade ou integridade. O que é inserido na cadeia de blocos não pode ser modificado. Segundo Leal, diante da imutabilidade, um dado não poder ser desfeito após ele ter sido enviado, processamento, validado e registado, sendo um dos principais aspectos elementos que conduzem à confiabilidade.[528] Empresas não poderão adulterar os livros, evitando-se assim, desfalques financeiros. Essa imutabilidade é obtida em razão da *hash* criptográfica, uma classe especial de funções *hash*, ideal para criptografia. Na *Blockchain* existe uma lista vinculada que contém dados em um bloco e um ponteiro *hash* que aponta para seu bloco anterior, que em vez de conter apenas o endereço do bloco anterior, também contém dentro o *hash* dos dados do bloco anterior, criando assim a cadeia. Pequena adulteração dos dados em um bloco gera um efeito enorme em toda a cadeia, que alterará os dados e o *hash* armazenado nos demais blocos. A informação deixa ser passível de manipulação, posto que ao entrar no bloco a informação se anexa à informação já existente no anterior, em uma sequência ininterrupta, sendo que não podem ser removidos.

[527] LEAL, op. cit., p. 29.
[528] Ibid., p. 30.

Conforme escreve Cortizo,

> [a] maneira como o registro é feito em cada bloco é o que garante a autenticidade e integridade do sistema *Blockchain*: dentro do bloco, além dos dados a serem registrados, há um resultado da operação *hash* do bloco imediatamente anterior, ou seja, um algoritmo matemático que recebe um *input* de dados de determinado tamanho e comprime a um tamanho fixo em uma 'função *one-way*', matematicamente irreversível. Trata-se, então, de uma função criptográfica que reúne dados e faz uma 'digestão', transformando-os sempre numa sequência de igual tamanho (o '*digest*'). Cada bloco carrega a '*message digest*' do bloco imediatamente anterior, o que liga os blocos entre si, e pelo fato da *Blockchain* ser uma estrutura linear, consegue-se a imutabilidade não apenas dos dados inseridos, mas da ordem temporal da cadeia inteira. No final das contas, não é possível falsificar os dados de um bloco, afinal teria que alterar o bloco posterior e depois o posterior ao posterior e assim sucessivamente: para adulterar um bloco precisa alterar toda a cadeia de blocos.[529]

Ou seja, a imutabilidade decorre da função criptográfica *hash* utilizada, posto que cada bloco contém um *digest* próprio, de acordo com o conteúdo, e que se apresenta no subsequente. Tentativas de modificação do conteúdo de um bloco gerariam um novo *digest*, que entraria em choque com o *hash* original.

Ademais, a criptografia, que equivale ao procedimento de geração de códigos, possibilita que um dado ou informação permaneça em segredo, informação que somente poderá ser descodificada por aquele que possui autorização, impossibilitando intromissões indevidas.

A identificação dos utilizadores na *Blockchain* é representada por um par de chaves criptográficas, uma pública e outra privada. A primeira é utilizada para assinar as transações na rede, enquanto a segunda representa o utilizador. Assim, o funcionamento, na prática, ocorre em duas fases: cada utilizador tem uma chave pública e uma chave privada, ambas com sequência alfanumérica. A chave pública é a conta, que é compartilhada com terceiros para realizar as transações; já a chave privada equivale à senha (*password*), que é sigilosa. Operações matemáticas permitem que as chaves se relacionem, possibilitando à privada desencriptar os dados mediante a chave pública.

Essas chaves, que são utilizadas em sede de verificação da assinatura da transação, possuem um tamanho de 512-bits. Dessa forma, detém um tamanho "grande", o que não

[529] CORTIZO, op. cit., p. 17.

permite o caminho inverso, ou seja, a descoberta da chave a partir do *digest* criado pelo *hash*. Segundo Casey apud Cortizo, a rede, de acordo com a capacidade computacional atual (de todos os computadores), demoraria "4,500 trilhões trilhões trilhões de anos" para quebrar o *hash* algorítmico SHA-256, protetor dos dados da *Bitcoin*.[530]

Assim, resguarda-se o anonimato, a integridade e a autenticidade, proporcionando a segurança das operações e a interoperabilidade.

4.3.3 A tecnologia *Blockchain* e a incidência do RGPD e da LGPD

A tecnologia *Blockchain* e as normas protetivas dos dados pessoais refletem interesses comuns. Nesse ponto podemos citar: a confiança e a transparência; a restituição do controlo dos dados pessoais aos titulares, com a eliminação de grandes empresas concentrando o tratamento e a livre circulação de dados.

Antes de se analisar uma possível compatibilidade ou não da tecnologia *Blockchain* com a gama de direitos protetivos dos dados pessoais, deve-se testar se a sua estrutura e funcionamento é passível de enquadramento naquelas normas protetivas, ou seja, no conceito de dados pessoais e no procedimento de tratamento.

O RGPD (art. 1º, n.°1 c/c art. 4º, n.°1)[531] e a LGPD (art.1º, c/c art. 5º, inciso I)[532] tutelam os dados pessoais de pessoa natural identificada ou identificável.

Na *Blockchain* podem-se armazenar dados de três maneiras distintas no *ledger*[533]: texto, de forma criptográfica ou por *hashing.* A de texto qualquer pessoa pode ler os dados, no caso das *blockchain* públicas. Na forma criptográfica, têm-se duas fases: um cabeçalho (*header*) que contém o registo da data e hora, o IP (*Internet Protocol*) e o *hash* do bloco anterior, que não são criptografados; e os dos dados que serão armazenados na *Blockchain*, denominado de *payload*, que é criptografado. Somente quem detenha a chave privada pode desencriptar a informação. Por fim, ao invés de lançar os dados

[530] Ibid., p. 20.
[531] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit.
[532] BRASIL. PRESIDÊNCIA DA REPÚBLICA– Lei n.° 13.709... op. cit.
[533] Livro- razão, onde constam as transações e que cada um dos computadores possui uma cópia.

criptografados, pode-se ainda transformar o conteúdo em *hashes* e depois lançar estas ao invés do texto. Contudo, os *hashes* não podem ser desencriptados por chaves privadas.[534]

Portanto, há a possibilidade de inserção de informações pessoais na cadeia de blocos vista por todos, o que permitiria a identificação imediata do titular, o que é denominado de "envenenamento por privacidade" ou "*blockchain privacy poisoning"*.[535]

Todas as três formas de inserção de dados na *Blockchain* estão sujeitas ao RGPD e à LGPD. Os dados de texto correspondem a pessoas identificadas; os criptografados também atraem a incidência do RGPD e da LGPD, por pertencerem a uma pessoa identificável, diante da possibilidade de rastreamento dos IPs e os *hashes*, também conduzem à incidência das leis protetivas, posto que a pessoa pode ainda ser rastreada e identificada.

Quanto às chaves públicas, estas apesar de não serem dados da transação em si, mas um conjunto alfanumérico capaz de identificar o utilizador de forma pseudonimizada, apesar de serem criptografadas, permitem a identificação do sujeito, considerando que sua utilização se vincula a um endereço de IP de um utilizador.[536]

Em relação aos IPs dos utilizadores estes também devem ser vistos como dados pessoais, ainda que dinâmicos. O IP é um conjunto de números que permite identificar o computador do utilizador e que são encaminhados ao servidor do *site*, para fins de transmissão de dados. Estes podem ser estáticos, ou seja, sem modificação, ou dinâmicos, que modificam a cada acesso. A dúvida maior é se o IP dinâmico poderia ser considerado um dado pessoal, diante da sua mutabilidade e da necessidade de se

[534] REBELO, op cit., p. 116.

[535] SAKAMOTO, op. cit., p. 52.

[536] FINCK, Michèle. Blockchains and Data Protection in the European Union. *Max Planck Institute for Innovation and Competition Research Paper,* nov. 2017, n.° 18-01, [consultado 9 março 2020], p. 13-14. Disponível na internet: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080322>. ISSN 2184-5468. "Academic research has moreover shown that public keys can be traced back to IP addresses, aiding identification. What is more, where a user transmits a transaction to the network, they usually connect directly to the network and reveal their IP address. The GDPR leaves no doubt that personal data that has 'undergone pseudonymisation, which could be attributed to a natural person by the use of additional information' qualifies as personal data. To determine whether a person can be identified on the basis of pseudonymous data account has to be taken of 'all the means reasonably likely to be used'. Considering that public keys are in fact being used to identify individuals, they should be presumed to be a means 'reasonably likely to be used." "A pesquisa académica também mostrou que as chaves públicas podem ser rastreadas até endereços IP, auxiliando na identificação. Além disso, quando um usuário efetua uma transação na rede, ele geralmente se conecta diretamente à rede e revela seu endereço IP. O RGPD não deixa dúvidas de que os dados pessoais 'submetidos à pseudonimização, que poderiam ser atribuídos a uma pessoa física pelo uso de informações adicionais' se qualificam como dados pessoais. Para determinar se uma pessoa pode ser identificada com base em uma conta de dados pseudonimizados deve-se considerar 'todos os meios razoavelmente prováveis de serem utilizados'. Considerando que as chaves públicas estão de fato sendo usadas para identificar indivíduos, presume-se que elas sejam um meio 'razoavelmente provável de ser utilizado." (tradução nossa)

recorrer ao provedor de acesso, a fim de obter uma informação complementar como forma de identificar o computador do utilizador. Nesse contexto, o TJUE, ainda sob a vigência da Diretiva 95/46/CE, manifestou-se no sentido de que o IP dinâmico configuraria como dado pessoal.[537]

Diante da possibilidade de identificação do titular dos dados, utilizador da tecnologia *Blockchain*, passa-se, em seguida, à verificação se há ou não operação de tratamento de dados na citada tecnologia.

Seguindo o disposto no RGPD, art. 4º, n.° 2, tratamento é

> uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.[538]

De forma semelhante dispõe a LGPD.[539]

Na *Blockchain,* cada chave pública está vinculada a uma chave privada entregue aos utilizadores, sendo que, os utilizadores, dotados de uma chave pública, se controlam mutuamente e fazem a verificação de validade da autorização das transações, estas automatizadas. Ainda que automatizada, a verificação de validade enquadra-se como tratamento, nos termos do art. 4º, n.° 2 do RGPD e art. 3º e art. 5º, inciso X, ambos da LGPD.

Quanto aos dados transacionais (*transactional data)*, estes são objeto de operações

---

[537] UNIÃO EUROPEIA. TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA (TJUE). Pedido de decisão prejudicial no processo C - 582/14. 2ª Secção. Data do acórdão: 19.10.2016. [Consultado 19 maio 2020]. Disponível na internet: <http://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&jge=&td=%3BALL&jur=C%2CT%2CF&num=C-582%252F14&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=pt&avg=&cid=890482>. “À luz do que foi exposto, proponho que o Tribunal de Justiça responda às questões submetidas, nos seguintes termos: “1) De acordo com o artigo 2.°, alínea a), 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 respeito ao tratamento de dados pessoais e à livre circulação desses dados, um endereço IP dinâmico por meio do qual um utilizador tenha acedido à página Internet de um fornecedor de um meio de comunicação eletrónico constitui para este um ‘dado pessoal’ na medida em que um fornecedor de acesso à Internet disponha de outras informações suplementares que, associadas ao endereço IP dinâmico, permitam a identificação do utilizador. 2) O artigo 7.°, alínea f), da Diretiva 95/46 deve ser interpretado no sentido de que, em princípio, o objetivo de garantir o funcionamento do meio de comunicação eletrónico pode ser considerado um interesse legítimo, cuja prossecução justifica o tratamento desse dado pessoal, desde que prevaleça sobre os interesses ou os direitos fundamentais da pessoa em causa. Uma disposição nacional que não permita tomar em consideração esse interesse legítimo é incompatível com o referido artigo.” (Tradução nossa)

[538] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit.

[539] BRASIL. PRESIDÊNCIA DA REPÚBLICA– Lei n.° 13.709... op. cit. “Art. 5º, [...] X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;”

de tratamento, na modalidade de uso e armazenamento, uma vez que são armazenados em um bloco, anexados e distribuídos a todos os utilizadores.

Por fim, em relação aos utilizadores (*nodes*) e endereços, cada um possui cópia e registo com todos os outros membros, se comunicando, realizando tratamento na modalidade de armazenamento.

Visando excluir tais dados da incidência do RGPD e da LGPD, pode-se sustentar a seguinte alteração. Em relação aos dados transacionais, eles seriam armazenados não na cadeia, mas apenas vinculados ao livro-razão através de um *hash*, sendo que no livro-razão constaria apenas um dado alfanumérico que ficaria visível, sendo que os dados correspondentes ao *hash* estariam armazenados fora da cadeia de blocos. Mas aí exige-se a presença de um terceiro para efetuar a gestão desse banco de dados fora da cadeia de blocos, banco esse passível de edição, comprometendo a segurança e a descentralização, embora chamando a colação a existência de um responsável pelo tratamento cingindo-se a tais operações.

Já as chaves públicas não podem ser transpostas para fora da cadeia de blocos, pela razão de serem necessárias à validação e ao funcionamento da tecnologia.

4.3.4 A dificuldade de compatibilização da *Blockchain* com alguns direitos do RGPD e da LGPD

Em regra, os utilizadores da rede desconhecem quais os dados pessoais que são lançados nos blocos, em face da criptografia, os *hashes*, que são códigos alfanuméricos. Entretanto, como o uso dessa tecnologia pode operar-se das mais variadas formas, pelos mais diversos utilizadores, contendo quaisquer tipos de dados, pessoais ou não, tem-se a dificuldade de se construir mecanismos de defesa e proteção, impostos pelo art. 25º do RGPD e art. 46 da LGPD.

O certo é que o RGPD e a LGPD foram idealizados para sistemas centralizados, onde os utilizadores participam interagindo, especialmente em redes sociais e serviços em nuvem (*cloud),* não para *Blockchains* públicas, onde a informação é replicada por toda a rede, ainda que criptografada, havendo a dificuldade de identificação de todos os

responsáveis, até para fins de aplicação de sanções. Nesse sentido, Borges e Revoredo afirmam que "[...] importante perceber que a GDPR foi elaborada para proteger a privacidade e a liberdade de indivíduos que há muito sofriam por abusos e falhas relacionadas a sistemas "centralizados" de transmissão e armazenamento de dados."[540]

Surgem, assim, dificuldades no que tange: ao apagamento e à retificação; à transferência de dados; ao controlo e à limitação do tratamento.

Desde já, ressalte-se que, embora a *Blockchain* proporcione, a certo modo, a restituição do controlo dos dados aos seus titulares, ela possui, em sua essência, a garantia da autenticidade através da imutabilidade, sendo necessária a adoção de ferramentas técnicas complementares como forma de sua compatibilização com o âmbito legal.

Em relação ao direito ao apagamento ou de eliminação, o art. 16 da LGPD dispõe que "[o]s dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades..."[541] Já o RGPD também o prevê no art. 5º, n.° 1, alínea d) e art. 17º.[542] A dificuldade é aqui imposta pela imutabilidade e descentralização.[543] Na *Blockchain* não existe de um controlo único, uma entidade, diante da pluralidade de sujeitos (todos os membros), que não se tem como identificar. E ainda que fosse possível a identificação de todos os utilizadores, estes não teriam como modificar ou apagar o dado armazenado. Isto porque, nas *Blockchains* públicas as transações são registadas na cadeia, não podendo ser modificadas ou apagadas em definitivo, posto que a transação seguinte, ainda que modifique a anterior, será ela um novo bloco anexado ao *hash* original criptográfico que, além de registar a nova operação, reproduz e ratifica a anterior. Nesse ponto, haveria a incompatibilidade com o direito de remoção de determinados dados dos motores de busca, nas hipóteses resguardadas ao titular, direito esse reconhecido pelo TJUE, ainda sob a vigência da Diretiva 95/46/CE, no caso da *Google Spain* e a *Google Inc.*

[540] BORGES, op. cit.
[541] BRASIL. PRESIDÊNCIA DA REPÚBLICA– Lei n.° 13.709... op. cit.
[542] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit.
[543] SAKAMOTO, op. cit., p. 52.

versus Agência Espanhola de Proteção de Dados e Mario González.[544]

Primeiramente, deve-se estabelecer de que modo estaria resguardado o direito ao apagamento ou à eliminação, se seria realmente necessário o desaparecimento total dos dados do sistema, ou bastaria a adoção de técnicas que impeçam a sua localização ou de proteção, com uma criptografia irreversível. Pensa-se que essa segunda opção (técnicas de não localização ou de proteção) seria uma forma de compatibilização da tecnologia com as normas protetivas.

Aliás, em termos compatibilização dessa tecnologia com o direito ao apagamento, alternativas estão sendo propostas.

Em relação aos dados transacionáveis, estes seriam armazenados num banco encriptado e introduzido um *hash* desse mesmo banco na cadeia de blocos. Assim seria mantida a integralidade e integridade do teor dos dados sem os tornar visíveis na *Blockchain*. Ou seja, os dados pessoais não constariam na cadeia de blocos, sendo armazenados em bancos de dados fora da cadeia. Mas, de qualquer forma, a descentralização de dados P2P é afetada de forma significativa.[545]

Esse armazenamento de dados pessoais sensíveis, de forma *off chain,* em uma rede

---

[544] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA (TJUE). Pedido de decisão prejudicial no processo C - 131/12. Grande Secção. Data do acórdão: 13.05.2014. Disponível na internet: <http://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&jge=&td=%3BALL&jur=C%2CT%2CF&num=C-131-12&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=pt&avg=&cid=4858444>. Acesso em: 27 de abr..2020. " 1) O artigo 2.°, alíneas b) e d), 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 respeito ao tratamento de dados pessoais e à livre circulação desses dados, deve ser interpretado no sentido de que, por um lado, a atividade de um motor de busca que consiste em encontrar informações publicadas ou inseridas na Internet por terceiros, indexá-las automaticamente, armazená-las temporariamente e, por último, pô-las à disposição dos internautas por determinada ordem de preferência deve ser qualificada de «tratamento de dados pessoais», na aceção do artigo 2.°, alínea b), quando essas informações contenham dados pessoais, e de que, por outro, o operador desse motor de busca deve ser considerado «responsável» pelo dito tratamento, na aceção do referido artigo 2.°, alínea d). [...] 3) Os artigos 12.°, alínea b), e 14.°, primeiro parágrafo, alínea a), da Diretiva 95/46 devem ser interpretados no sentido de que, para respeitar os direitos previstos nestas disposições e desde que as condições por elas previstas estejam efetivamente satisfeitas, o operador de um motor de busca é obrigado a suprimir da lista de resultados, exibida na seqüência de uma pesquisa efetuada a partir do nome de uma pessoa, as ligações a outras páginas *web* publicadas por terceiros e que contenham informações sobre essa pessoa, também na hipótese de esse nome ou de essas informações não serem prévia ou simultaneamente apagadas dessas páginas *web,* isto, se for caso disso, mesmo quando a sua publicação nas referidas páginas seja, em si mesma, lícita. 4) Os artigos 12.°, alínea b), e 14.°, primeiro parágrafo, alínea a), da Diretiva 95/46 devem ser interpretados no sentido de que, no âmbito da apreciação das condições de aplicação destas disposições, importa designadamente examinar se a pessoa em causa tem o direito de que a informação em questão sobre a sua pessoa deixe de ser associada ao seu nome através de uma lista de resultados exibida na seqüência de uma pesquisa efetuada a partir do seu nome, sem que, todavia, a constatação desse direito pressuponha que a inclusão dessa informação nessa lista causa prejuízo a essa pessoa. Na medida em que esta pode, tendo em conta os seus direitos fundamentais nos termos dos artigos 7.° e 8.° da Carta, requerer que a informação em questão deixe de estar à disposição do grande público devido à sua inclusão nessa lista de resultados, esses direitos prevalecem, em princípio, não só sobre o interesse económico do operador do motor de busca mas também sobre o interesse desse público em aceder à informação numa pesquisa sobre o nome dessa pessoa. No entanto, não será esse o caso se se afigurar que, por razões especiais como, por exemplo, o papel desempenhado por essa pessoa na vida pública, a ingerência nos seus direitos fundamentais é justificada pelo interesse preponderante do referido público em ter acesso à informação em questão, em virtude dessa inclusão. "

[545] REBELO, op. cit., p. 128-129.

tradicional, é uma alternativa viável de compatibilidade. Borges e Revoredo afirmam que a adoção desse sistema tem se tornado cada vez mais popular em razão de: maior privacidade (os danos não são visíveis na *Blockchain)*; baixo custo (sem intermediários para validar transações) e velocidade da operação (as transações são registadas imediatamente, não havendo necessidade confirmação na rede).[546]

Outra possibilidade é a criação de uma *Blockchain* paralela (*side chain*), independente, que funciona ao lado da *Blockchain* principal, sendo que o grau de privacidade nas transações realizadas nas *side chains,* vai depender de qual tecnologia usada.

Finck cita a proposta de que, em procedimentos realizados em ambientes supervisionados e seguros, poderia ser assegurado ao titular dos dados a possibilidade de eliminar a sua chave privada, impedindo o acesso àqueles dados, uma vez que somente ele titular poderia desencriptar a informação. Mas aí o apagamento não seria total, conforme citado, mas haveria apenas uma impossibilidade de acesso aos dados.[547] Cita-se ainda a possibilidade dos chamados *chameleon-hashes* que reeditariam o teor dos blocos armazenados na *Blockchain*, mas sob restrições e fiscalização de determinadas autoridades, o que levaria à interferência de uma terceira autoridade, que não os utilizadores da cadeia, perdendo a essência do *Blockchain.*

Outro problema de compatibilização de tecnologia com o RGPD e com a LGPD é quanto às exigências para transferência dos dados para fora da União Europeia ou do Brasil. O RGPD aplica-se ao tratamento de dados quando o responsável pelo tratamento ou o subcontratante estejam situados no território da União, independentemente de o tratamento ocorrer dentro ou fora da União, ou que o titular se encontre na União

---

[546] BORGES, op. cit.

[547] FINCK, op. cit., p. 24. “Here, the question arises as to whether the reference to ‘available technology’ could lead to an interpretation of the GDPR that dispenses from outright erasure in light of blockchains’ technical limitations in favour of an alternative solution. Some have moreover suggested that formalized procedures of transmitting a key to the data subject or deleting the private key in a supervised setting could amount to erasure for the purposes of the GDPR. Unlike outright erasure the encrypted data would still exist on-chain but could only be accessed by the data subject (through her exclusive control of the private key) or simply no longer be accessed at all. [...] A further option would be the use of chameleon-hashes to re-write the content of blocks on a DLT by authorized authorities under specific constraints, and with full transparency and accountability.” “Aqui, surge a questão de saber se a referência à 'tecnologia disponível' poderia levar a uma interpretação do RGPD que dispensa o apagamento total à luz das limitações técnicas das cadeias de blocos em favor de uma solução alternativa. Além disso, alguns sugeriram que procedimentos formalizados de transmissão de uma chave para o titular dos dados ou exclusão da chave privada em um ambiente supervisionado podem ser apagados para os fins do RGPD. Ao contrário do apagamento total, os dados criptografados ainda existiriam na cadeia, mas somente poderiam ser acessados pelo titular dos dados (através de seu controlo exclusivo da chave privada) ou simplesmente não poderiam mais ser acessados. [...] Uma outra opção seria o uso de hashes-camaleão para reescrever o conteúdo dos blocos em um DLT pelas autoridades autorizadas sob restrições específicas, com total transparência e responsabilidade.” (tradução nossa).

Europeia, nos termos do art. 3º, n.^{os} 1 e 2[548]. Já a lei brasileira, a LGPD, aplica-se aos tratamentos realizados no território nacional ou quando o titular se localize no território nacional ou quando os dados pessoais objeto do tratamento tenham sido coletados no território nacional, segundo o art. 3º, incisos I, II e III da LGPD[549]. Ocorre que, para que possam ser realizadas transferências de dados para outros países de fora da União ou do Brasil é necessário que sejam respeitadas diversas condições previstas, a fim de que não reste comprometido o nível de proteção das pessoas singulares previsto nas normas.[550] [551]

Só que por essa tecnologia não se tem como determinar onde se encontra o utilizador/*node*, que por sinal todos são responsáveis pelo tratamento e, geralmente, se localizam nos mais diversos países. Até mesmo os mineradores (*miners*) – que resolvem os problemas matemáticos para o lançamento de dados e armazenam cópia integral do livro-razão –, podem se localizar em qualquer local do mundo. Aí não se tem como ter um controlo dos dados do utilizador, os quais foram transferidos, ao mesmo tempo, para os mais diversos países.

Diante da dificuldade de se estabelecer, na prática, uma uniformidade de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas semelhantes, tem-se sido exigido o consentimento expresso para a transferência dos dados a terceiros, com informação prévia acerca dos possíveis riscos envolvidos, seguindo-se o art. 49º, n.°

---

[548] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit.

[549] BRASIL. PRESIDÊNCIA DA REPÚBLICA– Lei n.° 13.709... op. cit.

[550] PARLAMENTO EUROPEU; CONSELHO – Regulamento (UE) 2016/679… op. cit. "Artigo 44º Princípio geral das transferências. Qualquer transferência de dados pessoais que sejam ou venham a ser objeto de tratamento após transferência para um país terceiro ou uma organização internacional só é realizada se, sem prejuízo das outras disposições do presente regulamento, as condições estabelecidas no presente capítulo forem respeitadas pelo responsável pelo tratamento e pelo subcontratante, inclusivamente no que diz respeito às transferências ulteriores de dados pessoais do país terceiro ou da organização internacional para outro país terceiro ou outra organização internacional. Todas as disposições do presente capítulo são aplicadas de forma a assegurar que não é comprometido o nível de proteção das pessoas singulares garantido pelo presente regulamento."

[551] BRASIL. PRESIDÊNCIA DA REPÚBLICA– Lei n.° 13.709... op. cit. "Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos: I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais dequado ao previsto nesta Lei; II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de: a) cláusulas contratuais específicas para determinada transferência;b) cláusulas-padrão contratuais; c) normas corporativas globais; d) selos, certificados e códigos de conduta regularmente emitidos; III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional; IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro; V - quando a autoridade nacional autorizar a transferência; VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional; VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei."

1, a) do RGPD[552] e art. 33, inciso VIII da LGPD[553].

Outro problema é a dificuldade de identificação do responsável pelo tratamento (*data controller*) e o subcontratante (*data processor*), que realiza o tratamento sob as instruções do primeiro, para fins de controlo. Na *Blockchain* privada não existe o problema, pois aquele que é o destinatário dos dados é o responsável pelo tratamento. Todavia, nas *Blockchains* públicas, todos tratam dados de todos. Nessa seara pensa-se que não podem eles ser considerados responsáveis, posto que não agem intencionalmente e de forma independente, realizando o tratamento, sequer existe a vontade direcionada a tratar os dados de terceiros. Ademais, reconhecer os utilizadores/*nodes* como responsáveis conjuntos pelo tratamento, seguindo o art. 26.º, n.º 1 do RGPD, também não seria a melhor solução, posto que eles não determinam as finalidades e os meios de tratamento conjuntamente. Poderia ser levantada a possibilidade de o criador da *Blockchain* ser o responsável, uma vez que ele determina os objetivos do *software*, o que não facilita as coisas, posto que não é fácil encontrá-lo. Poderia se vislumbrar os *nodes* como subcontratantes, já que processam dados pessoais de terceiros em nome dos outros utilizadores. Mas os seguintes problemas surgem: os utilizadores poderem se encontrar fisicamente em qualquer país, com identidade encriptada, havendo dificuldade de se lhes aplicar sanções; são apenas utilizadores de um programa desenvolvido por terceiro, com autonomia apenas para entrar, fornecer os dados e sair do *software*, mas não estabelecem os objetivos, pois não desenvolvem os algoritmos; as cópias dos dados do *ledger* nos seus computadores estão em versão criptografada ou em *hashing,* sem poder de edição; o RGPD e a LGPD exigem garantias dos subcontratantes para implementar soluções técnicas de proteção de dados pessoais, passadas diretamente pelo responsável pelo tratamento, via algoritmo, sendo que

[552] FINCK, op. cit., p. 19-20. "A more realistic solution is enshrined in Article 49(1)(a) GDPR that foresees the possibility of a data subject providing explicit consent for such a transfer, subject to being informed about possible risks. This could be easily implemented on a private blockchain where access is controlledand can be subjected to terms and conditions but it is not obvious how such consent could be acquired in respect of a permissionless chain. In attempting to determine the GDPR's personal, material and jurisdictional scope, we have observed that the EU's data protection regime, fashioned for the centralized collection, storage and processing of data, cannot be easily transposed to decentralized digital ledgers. An analysis of the application of the Regulation's substantive rights to distributed ledgers further validates this conclusion." "Uma solução mais realista está consagrada no Artigo 49 (1) (a) do RGPD, que prevê a possibilidade de um titular de dados fornecer consentimento explícito para essa transferência, desde que seja informado sobre possíveis riscos. Isso pode ser facilmente implementado em uma *blockchain* privada onde o acesso é controlado e pode estar sujeito a termos e condições, mas não é óbvio como esse consentimento pode ser adquirido em relação a uma cadeia não permissionada. Ao tentar determinar o escopo pessoal, material e jurisdicional do GDPR, observamos que o regime de proteção de dados da UE, criado para a coleta, armazenamento e processamento centralizados de dados, não pode ser facilmente transposto para ledgers digitais descentralizados. Uma análise da aplicação dos direitos substantivos do regulamento aos livros distribuídos valida ainda mais essa conclusão." (tradução nossa)

[553] BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 13.709... op. cit.

inexiste esse contrato com o criador e há a impossibilidade de proceder a essas alterações.

Por fim, existe certa dificuldade de compatibilização da *Blockchain* com o princípio da limitação das finalidades do art. 5.º, n.º 1, alínea b) do RGPD e do art. 6º, inciso I da LGPD. Os dados recolhidos têm que obedecer a finalidades determinadas, explícitas e legítimas, não podendo ser tratados para outros fins. Entretanto, a cadeia de blocos de dados é irremovível, sendo apenas objeto de acréscimos aos dados anteriores, além de cada utilizador armazenar todos os dados lançados.

Segundo Rebelo, a sujeição da tecnologia *Blockchain* ao RGPD é um fato inegável, posto que os dados pessoais constantes na cadeia dos blocos são pseudonimizados, onde se realiza tratamento na modalidade de uso e de armazenamento por todos, independente de alguns utilizadores/*nodes* não se encontrarem na União. Mas acrescenta que, adequações ao Regulamento devem ser efetuadas, a fim de possibilitar a sua compatibilização com o sistema de proteção de dados europeu, quer pela via técnica, com modificação do algoritmo ou fugas ao livro-razão, quer por meios legais, com a atenuação do sentido de eliminação.[554]

Em verdade, é fundamental o diálogo entre sociedade, empresas, Estados, União, estes dois últimos responsáveis pela edição das normas protetivas, e os responsáveis pela criação e desenvolvimento dessa tecnologia, a fim de compatibilizar a proteção dos dados pessoais e demais direitos fundamentais do cidadão com essa inovação tecnológica.

4.3.5 A *Blockchain* e sua aplicação na Administração Pública – a consolidação da cidadania nacional e supranacional

O uso da *Blockchain* na Administração Pública, mais do que nunca, possui um caráter disruptivo.

Para tanto, deve-se verificar como surgiu e em que consiste o sistema utilizado pelas Administrações Públicas.

---

[554] REBELO, op. cit., p. 134-135.

O conhecimento contábil-matemático europeu tem seu nascimento com o livro *Liber Abaci*, em 1202, de autoria do mercador Italiano, natural da cidade de Pisa, Leonardo Fibonacci ou Leonardo Pisano, responsável por trazer dos árabes a aritmética, introduzindo o conhecimento dos algarismos arábicos na Europa. Isto proporcionou um grande desenvolvimento comercial no continente. O desenvolvimento comercial conduz ao surgimento de um grande número de dados que necessitam ser armazenados.

Mais adiante, Luca Pacioli, em 1494, criou o sistema de partidas dobradas – *Double-entry Bookkeping* (DeB) – que possibilita o armazenamento de dados mediante livros de registo que são armazenados por entidades de confiança e é desse método, ou técnica, que se origina a ciência contábil. De imediato, esse método, além de proporcionar o desenvolvimento das relações económicas, possibilitou a evolução na estrutura de governo dos Estados, vigente ainda hodiernamente, com implantação inédita na cobrança de tributos na administração pública francesa.[555]

O modelo de Administração Pública tradicional, de forma burocrática, assenta nesse sistema, no qual as informações constantes nos livros-registo gozam de presunção relativa, *iuris tantum,* de veracidade.

Portugal foi um dos primeiros países europeus a adotar o DeB como modelo contábil oficial do Tesouro Real, o que se verificou a partir de 1761, sob a gestão do Primeiro-Ministro Sebastião José de Carvalho e Melo, o Marquês de Pombal e Conde de Oeiras.[556]

A *Blockchain* anunciaria uma mudança, tanto do ponto de vista administrativo-burocrático, na forma de armazenamento dos dados, quanto sob um ponto de vista de confiabilidade social, de natureza psicológica, uma vez que existe um costume social de

---

[555] CORTIZO, op. cit., p. 18.

[556] GOMES, Delfina Rosa da Rocha. *Accounting change in central government: the institutionalization of double entry bookkeeping at the Portuguese Royal Treasury (1761-1777).* Tese de doutoramento em ciências empresariais, especialização em contabilidade, Universidade do Minho, Braga, 2007. 292 f. [Consultado 15 maio 2020], cit. p. 124-125. Disponível na internet: <http://repositorium.sdum.uminho.pt/handle/1822/6754>. "Pombal played a key role in all the reforms implemented in Portugal in the beginning of the second half of the eighteenth century. Among the different reforms adopted, accounting assumed a significant role and specific measures were put into practice in order to improve commercial and accounting knowledge of Portuguese merchants and also of public employees. Accounting change in central government was part of a major reform within Portuguese public administration, which resulted in the adoption of DEB at the Royal Treasury in 1761 [...]" "Pombal desempenhou um papel fundamental em todas as reformas implementadas em Portugal no início da segunda metade do século XVIII. Entre as diferentes reformas adotadas, a contabilidade assumiu um papel significativo e foram adotadas medidas específicas para aprimorar o conhecimento comercial e contábil dos comerciantes portugueses e também dos funcionários públicos. A mudança contábil no governo central fez parte de uma grande reforma na administração pública portuguesa, que resultou na adoção do DEB no Tesouro Real em 1761 [...]"(tradução nossa).

confiar em documentos emitidos por um órgão centralizado, no qual reside um original do qual se extrai uma cópia chancelada ou certidão.

Em matéria eleitoral, a primeira vez que se utilizou tal tecnologia foi em março de 2018, em Serra Leoa.[557] Posteriormente, nos Estados Unidos, na West Virginia, verificou-se a primeira eleição realizada naquele país, em que se utilizou parcialmente a *Blockchain*.[558]

Na vanguarda da utilização da *Blockchain* na Administração Pública, em termos nacionais, está a Estónia, como forma de implantação da Administração Pública em Linha. Para tanto foi criada a KSI *Blockchain*, um sistema de autenticação que pode ser ampliado para todos os utilizadores da internet. Ela serve para verificação de todos os atos e processos do governo. Nesse país, cerca de 99% dos serviços públicos são disponíveis *on-line*, todos os dias da semana e a qualquer hora, salvo casamentos, divórcios e transações de segurança nacional. Como se não bastasse, a Estónia criou a *Government Cloud*, como forma de arquivar dados, um portal que possibilita a realização de eleições, o *i-voting*, mediante o uso de uma assinatura eletrónica individual para cada eleitor e um *site* de serviços, o *e-services*, em que se soluciona problemas cotidianos perante a administração pública, mediante o uso de uma assinatura criptografada. Criou-se também os *e-Cabinet*, mediante a utilização de um aparelho audiovisual e um software que possibilita que decisões possam ser tomadas de maneira remota. Além disso, no contexto da interoperabilidade administrativa e da Administração Pública em Linha, bases de dados públicas e privadas foram interligadas, como forma de que os dados dos cidadãos sejam requisitados "uma única vez", em atenção ao princípio digital na mencionado, mas com troca de informações assinadas e criptografadas como forma de garantir a segurança.[559]

Além da Estónia, vislumbra-se a utilização da tecnologia *Blockchain* na Administração Pública no mundo europeu: em Malta, na emissão e verificação de certificados académicos em um portal aberto; na Suíça, na emissão de identidades em um portal público denominado *uPort* e na Finlândia, através do sistema MONI's, em serviços

[557] CHOHAN, Usman W. Blockchain enhancing political accountability? Sierra Leone 2018 Case. *SRRN*, 2018. [Consultado 15 maio 2020]. Disponível na internet: <https://ssrn.com/abstract=3147006>.

[558] WOOD, Aaron. Secretário de estado da Virgínia Ocidental relata votação bem-sucedida em blockchain em eleições do meio do mandato de 2018. *Cointelegraph Brasil*, 17 nov. 2018. [Consultado 15 maio 2020]. Disponível na internet: <https://cointelegraph.com.br/news/west-virginia-secretary-of-state-reports-successful-blockchain-voting-in-2018-midterm-elections>.

[559] CORTIZO, op. cit., p. 21-22.

de emigração.

A China também tem mirado na interoperabilidade administrativa e na dotação de uma Administração Pública em Linha, tendo desenvolvido o projeto *Guangdong Province Big Data Comprehensive Experimental Area*, que objetiva a criação o estabelecimento de uma única plataforma em que os cidadãos podem ter acesso a diversos serviços públicos.[560]

Em termos da União Europeia, a Decisão n.° 2015/2240 estabeleceu alguns princípios no art. 4º: segurança, respeito da privacidade e proteção de dados, transparência, salvaguarda da informação, modernização administrativa, transparência e abertura, os quais devem ser observados com a implantação da interoperabilidade na Administração Pública.[561]

Frise-se o Plano de Ação Europeu (2016-2020) para a Administração Pública em Linha, como forma de acelerar a transformação digital da administração pública, modernizando-a, eliminando as barreiras, seguindo a estratégia do Mercado Único Digital. Segundo Rodrigues, "[...] com este programa pretende-se a modernização das administrações públicas europeias e consequentemente o estabelecimento do Mercado Único Digital."[562]

Tal plano descreveu alguns princípios, conforme já foi mencionado: abertura e transparência[563], transfronteiriço por definição[564], interoperabilidade por definição[565], credibilidade e segurança[566].

A doutrina tem defendido o uso da tecnologia *Blockchain* como uma trilha adequada na busca por um serviço público mais eficiente, com maior transparência e

---

[560] CORTIZO, op. cit., p. 22.

[561] PARLAMENTO EUROPEU; CONSELHO – Decisão (UE) 2015/2240… op. cit.

[562] RODRIGUES, Laura Gomes. O princípio da autonomia procedimental… op. cit., p. 12.

[563] COMISSÃO EUROPEIA. Plano de ação europeu (2016-2020)… op. cit. "Abertura e transparência: as administrações públicas devem partilhar informações e dados entre si e permitir que os cidadãos e as empresas acedam, controlem e corrijam os próprios dados; permitir que os utilizadores acompanhem os respetivos processos administrativos; interagir e criar um clima de confiança com as partes interessadas (tais como empresas, investigadores e organizações sem fins lucrativos) na conceção e na prestação de serviços."

[564] Ibid. "Transfronteiriço por definição: as administrações públicas devem disponibilizar os serviços públicos digitais relevantes internacionalmente e evitar o surgimento de uma maior fragmentação, facilitando assim a mobilidade no Mercado Único."

[565] Ibid. "Interoperabilidade por definição: os serviços públicos devem visar trabalhar uniformemente no Mercado Único e através de domínios organizacionais, com base na livre circulação de dados e serviços digitais na União Europeia."

[566] Ibid. "Credibilidade e segurança: Todas as iniciativas devem ir além da simples conformidade com o quadro jurídico relativo à proteção de dados pessoais e da privacidade, bem como da segurança informática, mediante a integração desses elementos na fase de conceção. Estas constituem condições prévias importantes para o aumento da confiança nos serviços digitais e a adoção dos mesmos."

cooperação, a fim de resgatar a confiança do cidadão com o serviço público, sem falar que as informações podem ser trocadas e armazenadas de forma segura. O uso de ferramentas de Tecnologia da Informação, como a *Blockchain*, conduziria à interoperabilidade e à Administração Pública em Linha, esta como sendo a faceta visível daquela.

Em relação ao Plano de Ação Europeu citado, Cortizo discorre:

> [...] todo o Plano gira em torno de uma modernização da Administração Pública no âmbito europeu em que a Blockchain aparenta ser o vetor tecnológico crucial buscado pela Comissão. Ao que parece, a Comissão sinaliza compatibilidade com as benesses que a Blockchain é capaz de trazer; afinal, mesmo tendo surgido no contexto financeiro, já se percebe seu potencial no contexto da Administração Pública.[567]

Além disso, a União considera-a fundamental, pois vai permitir um intercâmbio transfronteiriço de informações, além da facilitação do acesso facilitado aos serviços administrativos.

Em 2016, um relatório do consultor científico do chefe do governo do Reino Unido conclui que a DLT (*distributed ledger technology*) reduz fraudes, erros e custos de prestação de serviços.[568]

No mesmo ano, foi editada pelo Parlamento Europeu a Resolução n.° 2016/2007[569], sobre moedas virtuais, que reconheceu as potencialidades de tal tecnologia para "além do domínio dos pagamentos". Assim, a norma: incentiva os serviços do Estado a testar a tecnologia, análises de impacto, como forma de aprimorar a prestação de serviços aos cidadãos e a oferta de soluções de administração em linha, em conformidade com as normas de proteção de dados da União Europeia, reconhecendo melhorias no sistema

---

[567] CORTIZO, op. cit., p. 23.

[568] GOVERNMENT-OFFICE FOR SCIENCE UK. *Distributed Ledger Technology: beyond block chain*. A report by the UK Government Chief Scientific Adviser. 2016. [Consultado 17 maio 2020]. p. 71. Disponível na internet: < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf>. "Distributed ledgers undoubtedly hold value for government, offering new ways of operating that reduce fraud, error and the costs of delivering services to underserved users. At the same time, these technologies offer new forms of innovation and the ability to reduce transaction costs for SMEs in the UK. This chapter has highlighted only some of the possible use cases. As distributed ledgers are adopted more widely, it is likely that a new form of operating government services will emerge." "Sem dúvida, os livros distribuídos são valorosos para o governo, oferecendo novas formas de operação que reduzem fraudes, erros e custos de prestação de serviços a utilizadores mal atendidos. Ao mesmo tempo, essas tecnologias oferecem novas formas de inovação e a capacidade de reduzir os custos de transação para as Pequenas e Médias empresas (PMEs) no Reino Unido. Este capítulo destacou apenas alguns dos possíveis casos de uso. À medida que os livros distribuídos são adotados mais amplamente, é provável que uma nova forma de operação dos serviços governamentais surja." (tradução nossa)

[569] PARLAMENTO EUROPEU – *Resolução n.° 2016/2007 (INI), sobre moedas virtuais.* Bruxelas, 26 de maio 2016. [Consultado 17 maio 2020]. Disponível na internet: <https://www.europarl.europa.eu/doceo/document/TA-8-2016-0228_PT.html?redirect>.

cadastral (art. 12); admite a possibilidade da tecnologia ajudar as autoridades estatais a combater o branqueamento de capitais, a fraude e a corrupção (art. 11); reconhece que a tecnologia poderá ser utilizada facilitar o fluxo de dados, a transparência e a confiança entre governo, cidadãos e empresas (art. 8); ressalta o seu auto grau de privacidade e de proteção da vida privada, sem proporcionar o anonimato, colaborando de forma positiva para o bem-estar dos cidadãos e o desenvolvimento económico (art. 1, alínea d) e e)); além de ressaltar a capacidade dessa tecnologia de "acelerar, descentralizar, automatizar e normalizar", a baixo custo, os processos de tratamento dados, conduzindo a uma alteração na maneira de transferir os ativos e de manter os registos, com consequências para o setor privado e para o setor público, este como "prestador de serviços, como supervisor e como legislador"(art. 5)[570].

Assim, um Observatório e um Fórum específico para tecnologia *Blockchain* foram criados em 2018[571], nesse contexto de Administração Pública em Linha e da interoperabilidade no Mercado Único Digital.

A utilização dessa tecnologia reforça a transparência e a cooperação entre os Estados-Membros da União. O fato dos Estados-Membros armazenarem cópia do livro-razão íntegro resguarda o princípio da transparência na esfera pública, com a possibilidade de realização de auditorias. A descentralização, no armazenamento dos dados, evita ataques cibernéticos, posto que seria necessário um ataque simultâneo em todos os nódulos integrais, que interagem entre si. Sem falar na imutabilidade criptográfica que impede o apagamento dos dados, com foco na segurança.[572]

Além do conhecimento que seria compartilhado, haveria uma restrição na burocracia, em consonância com a Decisão n.° 2015/2240, em uma interoperabilidade nos três setores (direito das sociedades, informações fornecidas pelo setor público e identificação eletrónica) de natureza transfronteiriça.

Portanto, as características da *Blockchain* demonstram a sua compatibilidade com os Princípios do Plano de Ação Europeu (2016-2020) de abertura, transparência, credibilidade e segurança. Além disso, seria uma ferramenta de modernização da

[570] Ibid.
[571] EU BLOCKCHAIN OBSERVATORY AND FORUM. [Consultado 13 maio 2020]. Disponível na internet: < https://www.eublockchainforum.eu/>.
[572] LEAL, op. cit., p. 32.

Administração Pública de uma forma uniforme em toda a União, um dos objetivos desta. Ademais, possibilita o intercâmbio transfronteiriço de informações, com acesso facilitado e implantação da interoperabilidade. Assim, trilha-se na implementação de um Mercado Único Digital e na concretização da Administração Pública em Linha em termos de União.

Para Marchionni, a *Blockchain* privada seria mais adequada para a implantação no setor público, por permitir uma melhor adaptação à forma de gestão dos governos e dos processos decisórios.[573]

A preferência pela utilização da *Blockchain* privada, no setor público é justificável. A utilização dos modelos de prova de autorização *Round Robin*, próprio dessa espécie de *Blockchain*, permite que se fixe quais utilizadores podem aceder e verificar os dados e as informações ali dispostas. Ademais, é possível estabelecer que apenas os Estados-Membros sejam nódulos integrais, processando e registando dados. Seriam eles os responsáveis por armazenar, cada um, a cópia integral do livro-razão. Já as pessoas naturais, coletivas e demais entidades públicas seriam nódulos parciais, encaminhando e visualizando as informações.

Porém, não existe um consenso na utilização da *Blockchain* privada, como forma de implantação de uma Administração Pública em Linha. Leal sustenta tratar-se de uma "opção não adequada", até que haja uma harmonização entre a tecnologia e os dispositivos legais. Isto porque a Administração Pública tem por características a atualização, o apagamento e a retificação de dados, sendo estes direitos previstos no RGPD, legislação a que estão sujeitas a entidades públicas, havendo um conflito entre o direito fundamental, incluindo os direitos concretizadores, e a estrutura de funcionamento da *Blockchain*.[574]

Já Cortizo ressalta que as indagações sobre a conformação entre o uso da tecnologia *Blockchain* na Administração Pública com assuntos de soberania, controlo de interesse público de rede descentralizada, o consentimento expresso e o direito ao esquecimento, ou apagamento previstos no RGPD devem ser respondidas mediante estrutura técnica maleável desenvolvida, com permissões de acesso controladas (nas

[573] MARCHIONNI, Pietro. The next Generation e-government. Linkedin, 2018. [Consultado 6 maio 2020]. Disponível na internet: < https://www.linkedin.com/pulse/next-generation-e-government-pietro-marchionni>.
[574] LEAL, op. cit., p. 31.

Permissioned ledgers), em um dos sistemas de verificação, distinto do protocolo *Proof of Work* da *Bitcoin* e de uma forma que os dados registados permaneçam íntegros, embora não visíveis.[575]

O certo é que com a cidadania desprovida de um território estatal específico, em uma modalidade supranacional e com surgimento de novos direitos fundamentais, especialmente o de proteção de dados pessoais, programas de interoperabilidade devem ser implementados, e, nesse ponto, a *Blockchain* se apresenta como uma tecnologia viável, não de uma forma isolada por cada Estado, mas de uma maneira coordenada, em que haja participação de técnicos, da União e da administração pública de cada um dos Estados, a nível nacional e subnacional.

Só assim pode-se sustentar um livre fluxo de dados e informações, a portabilidade de direitos, exigência de uma cidadania digital em termos supranacionais, além do desenvolvimento económico e social.

[575] CORTIZO, op. cit., p. 24.

5. CONCLUSÃO

Na sociedade informacional, os titulares dos dados são pessoas datificadas na medida em que se verifica um crescente aumento do tratamento dos dados pessoais através das tecnologias da informação e comunicação.

A preocupação com a proteção dos dados decorre do reconhecimento que o tratamento é uma atividade de risco, diante da possibilidade de situações danosas aos titulares em seus direitos fundamentais e na perceção da potencialidade e da amplitude de controlo e de manipulação da sociedade e do mercado.

Tais situações danosas são evidenciadas das mais diversas formas: o uso abusivo ou indevido, a utilização sem o conhecimento, a atribuição de dados falsos a um titular, a seleção de utilizadores de maneira discriminatória, a exposição indiscriminada do nome ou imagem e até a criação indevida ou errónea de um perfil virtual. No que tange, especificamente, à definição de perfis, os titulares são verdadeiras vítimas de algoritmos que ditam não apenas a publicidade dirigida, mas também a vida das pessoas, com relação às oportunidades como, por exemplo, quanto a processos seletivos empregatícios, à concessão ou não de crédito, à fixação do valor do prémio em contratos securitários, ao acesso à informação, dentre outros casos.

O direito à proteção dos dados pessoais, em uma só toada, resguarda o controlo dos mesmos por parte dos titulares e assegura a utilização desses dados por terceiros seguindo os ditames constitucionais da licitude, observando-se a dignidade da pessoa humana, a boa-fé, a segurança e a transparência.

Tamanha relevância na tutela de tal direito elevou a proteção de dados à categoria de fundamental, tanto formal, quanto material, além de ser reconhecido como um direito da personalidade.

O reconhecimento dessa fundamentalidade é resultado da evolução das relações sociais e económicas, quando ele passa a ser visto como essencial para a existência, desenvolvimento e interação do ser humano, tornando-se, ainda, fator de legitimação da atuação estatal, restringindo, impedindo ou exigindo, por parte desse, alguma conduta.

É um direito fundamental formal, diante da sua previsão expressa em textos

normativos constitucionais e supranacionais; é um direito fundamental material, por ter em seu epicentro a dignidade da pessoa humana, a qual tem, na sua essência, a potencialidade de o homem se autodeterminar e de ser livre. E mais, por se apresentar como um direito fundamental, o direito à proteção de dados é dotado de características e regime jurídico próprio: a universalidade, a inalienabilidade, a historicidade, a força vinculativa e a aplicabilidade imediata.

Não se pode olvidar que tal direito também se apresenta como um direito da personalidade, uma vez que tais dados e informações sobre uma pessoa natural constituem um corpo latente, uma extensão, uma projeção da personalidade, os quais merecem igual proteção a qualquer outro direito da personalidade, como: o direito à vida e à integridade física (corpo vivo, sem lesões, ao corpo morto, voz, com o combate a tortura, lesão corporal, abandono de incapaz); o direito à integridade psíquica (direito à privacidade – intimidade –, à liberdade, ao sigilo, à sociabilidade) e o direito à integridade moral (direito à reputação, ao respeito, à consideração, à boa fama e à estima que a pessoa desfruta nas relações sociais).

A forma como esse direito se estabelece e se consagra como um direito fundamental não se opera de forma idêntica em todos os ordenamentos jurídicos. Enquanto no ordenamento jurídico brasileiro não existe uma disposição expressa na Constituição relativa ao direito à proteção de dados, resultando de uma interpretação extensiva do direito fundamental à intimidade da vida privada e familiar, este sim previsto expressamente no art. 5º, inciso X da Constituição Federal brasileira, no ordenamento jurídico da União ele se apresenta como um direito fundamental autónomo, distinto da privacidade. Tamanha autonomia é resultado das tradições constitucionais comuns aos Estados-Membros, de Tratados e de Convenções internacionais de proteção aos direitos humanos e da atividade jurisprudencial correspondente a eles, a qual é reconhecida na CDFUE, Carta essa que passou a deter força juridicamente vinculativa com o Tratado de Lisboa.

A autonomia do direito à proteção dos dados pessoais se justifica, uma vez que, i) diferentemente da privacidade, não há o amparo na dicotomia público e privado, não importa se o dado é íntimo ou não, privado ou não, havendo o balizamento no conceito de dado pessoal; ii) presentes se fazem princípios próprios, como o da publicidade ou da

transparência, da exatidão, da finalidade, do livre acesso e da proteção física e lógica; iii) existem direitos concretizadores específicos; e iv) por fim, além de tutelar a privacidade, o direito à proteção de dados também ampara direitos como o de igualdade, de não discriminação, de liberdade de escolha, de expressão, de acesso à informação e de capacidade de autodeterminação informativa.

Se, por um lado, existe o interesse de proteção dos dados pessoais, como um direito fundamental da personalidade do titular, por outro, esses dados se apresentam como essenciais para o desenvolvimento económico e para a elaboração de políticas públicas. Pode-se afirmar que o sistema de proteção de dados pessoais atua em dupla função: a proteção da pessoa, do titular dos dados pessoais, contra os riscos decorrentes do tratamento, e a promoção da livre circulação de informações e de bens entre países com nível de proteção adequado e equivalente. O RGPD europeu e a LGPD brasileira são reflexos dessa inquietude.

Em que pese a influência do RGPD na LGPD brasileira, a diferença na técnica legislativa se manifesta de forma hialina. Enquanto o RGPD é o resultado de um longo caminho de debates e estudos sobre a necessidade de uma tutela efetiva e uniforme da proteção de dados pessoais em toda a União, o que conduziu a uma norma com 99 (noventa e nove) artigos e 173 (cento e setenta e três) considerandos com orientações interpretativas; a LGPD possui apenas 65 (sessenta e cinco) artigos, sem considerando algum, conferindo ao intérprete uma maior labuta, posto que esse terá de trilhar a sua jornada sem pistas interpretativas dispostas na sua parte preliminar.

Mas a verificação do nível de equivalência de ambos pode ser obtida não pela técnica legislativa ou quantitativa, mas através da análise qualitativa que perpassa pela racionalidade regulatória, onde se verifica a convergência no que tange aos princípios e direitos, no modelo *ex-ante* de proteção, no papel essencial da *accountability,* sendo que, nesse último, a calibração da equivalência será dada pela Autoridade Nacional de Proteção de Dados Pessoais. No que tange ao *enforcement*, as incertezas pairam em face do disposto na legislação brasileira. E nesse sentido pensa-se pela possibilidade de obtenção do nível de equivalência entre as duas normas.

Esse nível de equivalência entre os sistemas normativos de proteção, uma verdadeira interoperabilidade dos sistemas normativos, é fundamental para que eles

alcancem o seu desiderato de proteção dos dados pessoais e do livre fluxo de informações e bens, especialmente em uma era tecnológica em que os dados podem fluir através das fronteiras dos Estados, sem obstáculo algum, inclusive mediante o uso de base de dados compartilhada por controladores e operadores situados em diversos países. Até mesmo porque o paradigma da revolução tecnológica da informação, na sociedade informacional, consiste na possibilidade da informação e das relações ocorrerem no ciberespaço, local onde os dados são tratados, independentemente da nacionalidade e da localização do titular. Trata-se de uma sociedade estruturada em rede, interconectada.

Tal necessidade de estruturação em rede também se expande para a seara administrativa pública, em uma noção de que um órgão de um Estado, ou, até mesmo um Estado, de forma isolada, não é capaz de atender a interesses públicos primários globais, como saúde pública, meio ambiente, questões económicas e direitos fundamentais. Eis aí a relevância da interoperabilidade administrativa nacional e supranacional.

Em termos da União Europeia, o Mercado Único Digital, como uma política pública de interesse primário, assenta na noção de cidadania social, em que o cidadão é ator principal da construção de um mercado interno, dotado de uma dimensão nacional e outra supranacional. Emergem daí dois interesses públicos secundários: a proteção dos dados pessoais mediante um padrão elevado num ambiente controlado e a interoperabilidade administrativa que possibilite interconexão de informações, a criação de bases de dados e registos transnacionais comuns, a fim de que serviços públicos sejam prestados pela via eletrónica, de forma eficiente e resolutiva. O RGPD e Regulamento 2018/1725 são fruto da política pública deste Mercado Único Digital.

Essa interoperabilidade é indispensável ao Mercado Único Digital europeu, à liberdade de circulação e ao exercício da cidadania europeia e deve se operar de três aspectos: técnico (capacidade de sistemas e dispositivos trocarem dados e informações sem custos e de forma confiável); semântico (mantendo o significado da informação) e organizativo (capacidade de cooperação entre as organizações).

A Decisão n.° 2015/2240 (Programa ISA^2), que tem por objetivo a modernização das administrações públicas europeias e o estabelecimento do Mercado Único Digital, proclama que, em relação à interoperabilidade administrativa, deve haver uma atuação

efetiva da União a fim de uniformizar a atuação do Estados-Membros. Ademais, pode-se atestar que da decisão emergem vantagens em políticas públicas em relação à segurança jurídica no meio empresarial, ao livre acesso a documentos administrativos e à identificação eletrónica.

O Plano de Ação Europeu em matéria de Administração Pública em linha (2016-2020) também fixou medidas concretas de modernização da administração pública, de serviços públicos digitais interoperáveis, no contexto de promoção de mobilidade transfronteiriça e interação digital entre as administrações e os cidadãos, as empresas e os serviços públicos.

Ademais, a União, através de um Plano de Ação de Educação Digital e de uma Agenda de Reforço de Competências, estabelecido no corrente ano, também mira no empoderamento da sociedade em literacia digital, a fim que todos possam relacionar-se com a prestação dos serviços públicos em linha de forma efetiva.

A interoperabilidade, mais que um método, é um princípio da Administração Pública, que conduz à necessidade de criação de soluções que promovam a observância do paradigma da Administração Pública em linha.

Nesse contexto de interoperabilidade administrativa, o RGPD e o Regulamento 2018/1725, aplicáveis, respectivamente, às administrações públicas nacionais e aos órgãos e instituições da União, asseguram um nível de proteção adequado aos dados pessoais, o que é alcançado com o auxílio do TJUE, responsável pela aplicação uniforme e harmónica do direito da União, na busca do mais elevado âmbito de proteção, seguindo os ditames do art. 53º da CDFUE. Da mesma forma, pensa-se que a LGPD é também capaz de assegurar um nível de proteção adequado, considerando o modelo de proteção *ex ante*, a *accountability*, os princípios e direitos concretizadores ali dispostos.

No anseio pela proteção dos dados pessoais e pela interoperabilidade administrativa, a Decisão n.° 2015/2240 (Programa ISA^2) não fixou um meio tecnológico específico, razão pela qual a *Blockchain,* especialmente a privada, é uma alternativa viável e eficaz.

Tal tecnologia, a qual tem por registo de nascimento a divulgação do surgimento da

criptomoeda *Bitcoin,* surge no contexto de exigência de uma melhor prestação de serviço aliada à necessidade de segurança e de integridade dos dados. Possui ela um caráter disruptivo, tanto em relação à burocracia administrativa de armazenamento de dados, quanto de confiança social em um órgão central, por seguir um modelo distribuído de armazenamento, associado à segurança da criptografia. Assenta em três pilares: a descentralização, a transparência e a imutabilidade.

A *Blockchain* atrai a incidência do RGPD e da LGPD. Os dados lá armazenados são pessoais, ainda que pseudonimizados, uma vez que os utilizadores são passíveis de identificação. As chaves públicas e o IP também correspondem a dados pessoais, sendo que, na *Blockchain*, ocorrem as mais diversas operações de tratamento. Portanto, deve haver uma harmonização entre o funcionamento de tal tecnologia com as normas protetivas jusfundamentais em matéria de dados pessoais.

Como forma de se compatibilizar a *Blockchain* com o direito ao apagamento ou de eliminação, considerando a imutabilidade e a descentralização como características daquela tecnologia, podem-se adotar algumas medidas como i) armazenar os dados fora da cadeia *Blockchain;* ii) adotar uma *Blockchain* paralela; iii) assegurar ao titular dos dados a possibilidade de eliminar a sua chave privada, o que não permitiria desencriptar a informação e a adoção de *chameleon-hashes* que reeditariam o teor dos blocos armazenados na *Blockchain*, sob restrições e fiscalização de determinadas autoridades.

Quanto às exigências impostas pelo RGPD e pela LGPD para transferência dos dados para fora da União Europeia ou do Brasil, uma forma de compatibilizar tais normas com a citada tecnologia é exigir o consentimento expresso para a transferência dos dados a terceiros, com informação prévia acerca dos possíveis riscos envolvidos, seguindo-se o art. 49º, n.° 1, a) do RGPD e art. 33, inciso VIII da LGPD.

Em relação à dificuldade de identificação do responsável pelo tratamento e do subcontratante, que realiza o tratamento sob as instruções do primeiro, para fins de controlo, tal não se opera com a *Blockchain* privada, que possui um ou mais destinatários certos.

A opção pela *Blockchain* privada para a Administração Pública em linha se justifica. Ainda que haja uma certa restrição no que tange à descentralização no armazenamento

dos dados, ela possibilita que apenas os Estados-Membros ou órgãos destinatários sejam nódulos integrais, armazenando cópia integral do livro-razão*,* enquanto os utilizadores (pessoas naturais, coletivas e demais entidades públicas) apenas encaminhariam e acederiam aos dados, na qualidade de nódulos parciais. Pode-se ainda estabelecer quais utilizadores podem aceder e a quais dados eles teriam acesso.

Ademais, princípios previstos no plano de ação europeu (2016-2020) e na Decisão n.° 2015/2240 para uma da Administração Pública em linha, restariam consagrados com o uso da *Blockchain:* i) desde logo, o princípio da interoperabilidade por definição técnica, semântica e organizativa; ii) os princípios da transparência e da abertura, pois os Estados-Membros armazenarão cópia do livro-razão íntegro, o que permite auditorias, com possibilidade dos utilizadores acederem e controlarem em todas as fases o tratamento; iii) o princípio do transfronteiriço por definição, com a prestação de serviços públicos de forma transfronteiriça, proporcionando a mobilidade; iv) os princípios da confiança e da segurança, posto que a descentralização evita ataques cibernéticos e a criptografia impede o apagamento, evitando fraudes e erros, proporcionando um clima de credibilidade por parte dos utilizadores e dos Estados-Membros, uns para com os outros; v) o princípio da declaração única, posto que se fará desnecessário o fornecimento de mais de uma vez dos dados, face o compartilhamento dos mesmos; e vi) o princípio do digital por definição, posto que mais serviços serão prestados, prioritariamente, por meios digitais.

A interoperabilidade promovida pela *Blockchain,* especificamente a privada, proporciona ainda que instituições estatais ajam como instituições funcionalmente europeias, devido a transparência, a cooperação entre os Estados-Membros como nódulos integrais e o grau de confiança gerado. Além do conhecimento distribuído, haveria uma retração da burocracia, dos desacertos e dos custos.

Porém, a implantação da tecnologia *Blockchain* deve ser realizada de forma organizada e coordenada, com participação da União e da administração pública de cada um dos Estados, a nível nacional e subnacional, por ser essencial ao livre fluxo de dados e informações, à portabilidade de direitos, à cidadania digital em termos supranacionais e ao desenvolvimento económico e social, mas com observância das normas de tutela

jusfundamental, em especial de proteção de dados, como forma de concretização do Mercado Único Digital.

Posto isto, a experiência europeia poderia ser devidamente enquadrada – sobretudo dadas as sensibilidades que aí já se colheram em matéria de proteção de dados – para a realidade brasileira. Na realidade, o caminho também deverá pautar-se por mais dinâmicas interoperáveis no ordenamento jurídico brasileiro e, por sua vez, também este deverá ser equacionado e enquadrado num mundo globalizado e impactado pelas novas tecnologias de informação e de comunicação.

REFERÊNCIAS

Doutrina e Jurisprudência

ABREU, Joana Covelo de. O mercado único digital e a interoperabilidade administrativa: a proteção dos dados pessoais na articulação entre administrações públicas nacionais e as instituições e órgãos da União Europeia – reflexões prospectivas. In: GOMES, Carla Amado et al. (Coord.) *O direto administrativo nos 30 anos da constituição brasileira de 1988*: um diálogo luso-brasileiro. Lisboa: ICJP/CIDP, 2019. [Consultado 8 maio 2020]. p. 206-242. Disponível na internet: <https://www.icjp.pt/sites/default/files/publicacoes/files/ebook_da30anoscb_icjp15mar2019.pdf> ISBN 978989872236-2.

_____. O mercado único digital como o novo mundo para a união europeia: repercussões na estrutura regulatória social e institucional – a redefinição do serviço universal e do organismo de reguladores europeus das comunicações eletrónicas (ORECE). *UNIO – EU Law Journal,* Braga, jul. 2018, v. 4, n. 2, [consultado 18 fevereiro 2020], p. 59-72. Disponível na internet: <https://revistas.uminho.pt/index.php/unio/article/view/20/52>. ISSN 2183-3435.

_____. O Mercado Único Digital e o seu desígnio político-constitucional: o impacto da Agenda Eletrónica Europeia nas soluções de interoperabilidade. *UNIO – EU Law Journal,* Braga, jan. 2017, v. 3, n. 1, [consultado 18 fevereiro 2020], p. 130-150. Disponível na internet: <https://revistas.uminho.pt/index.php/unio/article/view/20/52>. ISSN 2183-3435.

_____. Os princípios gerais da Administração Pública em linha na União Europeia e a análise do artigo 14.º do CPA: revisitando as necessidades de literacia digital. In: GOMES, Carla Amado; SERRÃO, Tiago (Coords.). *Código de procedimento administrativo comentado*. AAFDUL, 2020, no prelo.

ALBUQUERQUE, Robson de Oliveira. *Uma proposta de um modelo de confiança computacional para grupos em sistemas distribuídos*. Tese de Doutorado em Engenharia Elétrica, Faculdade de Tecnologia da Universidade de Brasília, Brasília, 2008. 171 f. [Consultado 7 maio 2020]. Disponível na internet: <https://repositorio.unb.br/bitstream/10482/5674/1/2008_RobsonOAlbuquerque.pdf>.

ALEXANDRINO, Marcelo; PAULO, Vicente. *Direito administrativo descomplicado.* 25ª ed. rev. e atual. Rio de Janeiro: Forense; São Paulo: Método, 2017. ISBN 978853097474-9.

AMARAL, João Ferreira do. *Economia da informação e do conhecimento.* Coimbra: Almedina, 2009. ISBN 978972403812-4.

ANDRADE, José Carlos Vieira de. *Os direitos fundamentais na constituição portuguesa de 1976*. 5ª ed. reimpressão. Coimbra: Almedina, 2017. ISBN 978972404669-3.

BAUMAN, Zygmunt. *44 cartas do mundo líquido moderno*. Rio de Janeiro: Zahar, 2011. ISBN 853780681-1.

BIONI, Bruno Ricardo. *Proteção de dados pessoais:* a função e os limites do consentimento. 2ª ed. rev., atual. e refor. Rio de Janeiro: Forense, 2020. ISBN 978853098862-3.

BIONI, BRUNO Ricardo; MENDES, Laura Schertel. Regulamento europeu de proteção de dados pessoais e a lei geral brasileira de proteção de dados: mapeando divergências na direção de um nível de equivalência. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.) *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 797-819. ISBN 978855321663-5.

BITTAR, Carlos Alberto. *Os direitos da personalidade.* 5ª ed. Rio de Janeiro: Forense Universitária, 2001. ISBN 852180285-4.

BLUM, Renato Opice; ARANTES, Camila Rioja. Autoridades de controle, atribuições e sanções. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords.) *Comentários ao GDPR:* Regulamento Geral de Proteção de Dados da União Europeia. São Paulo: Thomson Reuters Brasil, 2018. p. 227-252. ISBN 978855321230-9.

BOLESINA, Iuri. *O direito à extimidade:* as inter-relações entre identidade, ciberespaço e privacidade. Florianópolis: Empório do Direito, 2017. ISBN 978859477084-4.

BORGES Rodrigo; REVOREDO, Tatiana. Blockchain e as leis de proteção de dados: incompatíveis? *Cio from IDG*, 2018. [Consultado 20 maio 2020]. Disponível na internet: < https://cio.com.br/blockchain-e-as-leis-de-protecao-de-dados-incompativeis/>.

BRASIL. Supremo Tribunal Federal. Recurso Extraordinário n.° 511.961-SP. Relator: Min. Gilmar Mendes. Brasília, DF, 17 de junho de 2009. [Consultado 31 março 2020]. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=605643>.

_____. Superior Tribunal de Justiça. Recurso especial n.° 1660168-RJ. Relator: Min. Nancy Andrighi. Brasília, DF, 8 de maio de 2018. [Consultado 25 março 2020]. Disponível em: <https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1628798&num_registro=201402917771&data=20180605&formato=PDF>.

BRITO, Jerry; CASTILLO, Andrea. Bitcoin: a primer for policymakers. Arlington: Mercatus Center at George Mason University, 2016. [Consultado 6 maio 2020]. p. 9. Disponível na internet: <https://www.mercatus.org/system/files/gmu_bitcoin_042516_webv3_0.pdf>. ISBN 978194295116-2.

CANOTILHO, José Joaquim Gomes. *Direito constitucional e teoria da constituição*. 7ª ed. Coimbra: Almedina, 2003. ISBN 978972402106-5.

CANOTILHO, José Joaquim Gomes; MOREIRA, Vital. *Constituição da república portuguesa anotada.* 3ª ed. Coimbra: Coimbra, 1993. ISBN 972320592-0.

CAPEZ, Fernando. *Curso de direito penal:* parte especial. 15ª ed. São Paulo: Saraiva, 2015. v.2. ISBN 978850261905-0.

CARDOSO, Vladimir Mucury. O abuso do direito na perspectiva Civil-Constitucional. In: MORAES, Maria Celina Bodin de (Coord.). *Princípios do direito civil contemporâneo*. Rio de Janeiro: Renovar, 2006. p. 61-110. ISBN 857147575-X.

CARVALHO FILHO, José dos Santos. *Manual de direito administrativo*. 25ª ed. rev., atual. e ampl. São Paulo: Atlas, 2012. ISBN 978852246927-7.

CASTELLS, Manoel. *A galáxia da internet*: reflexões sobre a internet, os negócios e a sociedade. Tradução. Maria Luiza X. de A. Borges. Rio de Janeiro: Zahar, 2003. ISBN 978857110740-3.

CHOERI, Raul Cleber da Silva. *O direito à identidade na perspectiva civil-constitucional.* Rio de Janeiro: Renovar, 2010. ISBN 978857147789-6.

CHOHAN, Usman W. Blockchain enhancing political accountability? Sierra Leone 2018 Case. *SRRN*, 2018. [Consultado 15 maio 2020]. Disponível na internet: <https://ssrn.com/abstract=3147006>.

CODERCH, Pablo Salvador. *El derecho de la libertad.* Madrid: Centro de Estudios Constitucionales, 1993. ISBN 978842590947-4.

CORDEIRO, A. Barreto Menezes. Repercussões do RGPD sobre a responsabilidade civil. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.) *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 777-795. ISBN 978855321663-5.

CORTIZO, Lucas Silvestre. Blockchain e e-Government: paradigmas e perspectivas. In: SILVEIRA, Alessandra; ABREU, Joana Covelo de; COELHO, Larissa (Coords.) *Unio e-book Interop 2019:* o mercado único digital da União Europeia como desígnio político: a interoperabilidade como o caminho a seguir. Braga: UNIO – EU Law Journal, 2019. [Consultado 4 maio 2020]. p. 16-25. Disponível na internet: <http://repositorium.sdum.uminho.pt/bitstream/1822/61446/3/UNIO_EBOOK_INTEROP_2019.pdf >. ISBN 978989545871-4.

COTS, Márcio; OLIVEIRA, Ricardo. *Lei geral de proteção de dados pessoais comentada*. 3ª ed. São Paulo: Thomson Reuteres Brasil, 2019. ISBN 978855321959-9.

CRAVO, Daniela Copetti. O direito à portabilidade na lei de proteção de dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.) *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 347-365. ISBN 978855321663-5.

CUNHA JÚNIOR, Dirley da. *Curso de direito constitucional*. 12ª ed. rev., ampl. e atual. Salvador: JUSPODIVM, 2018. ISBN 978854421926-3.

DEBORD, Guy. A sociedade do espetáculo. Rio de janeiro: Contraponto, 1997. ISBN 858591017-8.

DIAS, Felipe da Veiga; BOLESINA, Iuri. Direito à proteção de dados pessoais no Brasil e os traços centrais de uma autoridade local de proteção. *E-Civitas - Revista Científica do Curso de Direito do UNIBH* - Belo Horizonte, jul. 2017, v. X, n. 1, [consultado 3 abril 2020], p. 1-26. Disponível na internet: <https://revistas.unibh.br/dcjpg/article/view/2165/1>. ISSN 1984-2716.

DIAS, Leandra. O papel da tecnologia na busca pela conformidade com o RGPD. In: SILVEIRA, Alessandra; ABREU, Joana Covelo de; COELHO, Larissa (Coords.) *Unio e-book Interop 2019:* o mercado único digital da União Europeia como desígnio político: a interoperabilidade como o caminho a seguir. Braga: UNIO – EU Law Journal, 2019. [Consultado 4 maio 2020]. p. 78-85. Disponível na internet: <http://repositorium.sdum.uminho.pt/bitstream/1822/61446/3/UNIO_EBOOK_INTEROP_2019.pdf >. ISBN 978989545871-4.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Revista Espaço Jurídico.* Joaçaba, jul./dez. 2011*,* v. 12, n. 2, [consultado 8 janeiro 2020], p. 91-108. Disponível na internet: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315/658>. ISSN 2179-7943.

_____. *Da privacidade à proteção dos dados pessoais:* elementos da formação da lei geral de proteção de dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019. ISBN 978855321957-5.

DOTTI, René Ariel. *Proteção da vida privada e liberdade de informação*: possibilidades e limites. São Paulo: Revista dos Tribunais, 1980. ISBN 852030036-7.

DRUCKER, Peter. A sociedade pós-capitalista. Tradução: Nivaldo Montingelli Junior. 3ª ed. São Paulo: Pioneira, 1993. p. 15-25. ISBN 852241825-X.

FARIÑAS MATONI, Luis Maria. *El derecho a la intimidad*. Madrid: Trivium, 1983. ISBN 848614408-6.

FEIGELSON, Bruno; SIQUEIRA, Antônio Henrique Albani. *Comentário à lei geral de proteção de dados*: Lei 13.709/2018. São Paulo: Thomson Reuters Brasil, 2019. ISBN 978855321439-6.

FERRAZ JUNIOR, Tércio Sampaio. A liberdade como autonomia recíproca de acesso a informação. In: GRECO, Marco Aurélio; MARTINS, Ives Gandra da Silva (Coord.). *Direito e Internet:* relações jurídicas na sociedade informatizada. São Paulo: Revista dos Tribunais, 2001. ISBN 852032034-1.

_____. *Direito constitucional*: liberdade de fumar, privacidade, estado direitos humanos e outros temas. Barueri, SP: Manole, 2007. ISBN 978852042451-3.

_____. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito da Universidade de São Paulo*, São Paulo, 1993, v. 88, [consultado 14 fevereiro 2020], p. 439-459. Disponível na internet: <http://www.revistas.usp.br/rfdusp/article/view/67231/69841>. ISSN 0303-9838.

FERREIRA, João. Pistas para uma cidadania à luz da interoperabilidade. In: SILVEIRA, Alessandra; ABREU, Joana Covelo de; COELHO, Larissa (Coords.) *Unio e-book Interop 2019:* o mercado único digital da União Europeia como desígnio político: a interoperabilidade como o caminho a seguir. Braga: UNIO – EU Law Journal, 2019. [Consultado 4 maio 2020]. p. 45-52. Disponível na internet: <http://repositorium.sdum.uminho.pt/bitstream/1822/61446/3/UNIO_EBOOK_INTEROP_2019.pdf >. ISBN 978989545871-4.

FINCK, Michèle. Blockchains and Data Protection in the European Union. *Max Planck Institute for Innovation and Competition Research Paper,* nov. 2017, n.° 18-01, [consultado 9 março 2020]. Disponível na internet: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080322>. ISSN 2184-5468.

FRAZÃO, Ana. Objetivos e alcance da lei geral de proteção de dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.) *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 99-129. ISBN 978855321663-5.

FREITAS, Pedro Miguel. Regulamento geral de proteção de dados: uma visão portuguesa sobre o regime sancionatório*. UNIO – EU Law Journal,* Braga, jul. 2018, v. 4, n. 2, [consultado 18 fevereiro 2020], p. 113-118. Disponível na internet: <https://revistas.uminho.pt/index.php/unio/article/view/24/56 >. ISSN 2183-3435.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. *Novo curso de direito civil:* parte geral. 8ª ed. rev., atual. e reform. São Paulo: Saraiva, 2007. v. 1. ISBN 850205748-0.

GAMIZ, Mário Sergio de Freitas. *Privacidade e intimidade*: doutrina e jurisprudência. Curitiba: Juruá, 2012. ISBN 978853623785-5.

GEDIEL, José Antônio Peres; CORRÊA, Adriana Espíndola. Proteção jurídica de dados pessoais: a intimidade sitiada entre o estado e o mercado. *Revista da Faculdade de Direito Universidade Federal do Paraná,* Curitiba, jun. 2008, n. 47, [consultado 15 fevereiro 2020], p. 141-153. Disponível na internet: <https://revistas.ufpr.br/direito/article/view/15738>. ISSN 2236-7284.

GOMES, Delfina Rosa da Rocha. *Accounting change in central government: the institutionalization of double entry bookkeeping at the Portuguese Royal Treasury (1761-1777).* Tese de doutoramento em ciências empresariais, especialização em contabilidade, Universidade do Minho, Braga, 2007. 292 f. [Consultado 15 maio 2020]. Disponível na internet: <http://repositorium.sdum.uminho.pt/handle/1822/6754>.

GOMES, Orlando. *Introdução ao direito civil.* 19ª ed. Rio de Janeiro: Forense, 2007. ISBN 978853092582-6.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau. Término do tratamento de dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.) *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 219-241. ISBN 978855321663-5.

JABUR, Gilberto Haddad. *Liberdade de pensamento e direito à vida privada:* conflito entre direitos da personalidade. São Paulo: Revista dos Tribunais, 2000. ISBN 852031928-9.

LEAL, Victor Moreira Mulin. A tecnologia Blockchain como plataforma de interoperabilidade na União Europeia? Um estudo a partir da Decisão (UE) 2015/2240. In: SILVEIRA, Alessandra; ABREU, Joana Covelo de; COELHO, Larissa (Coords.) *Unio e-book Interop 2019:* o mercado único digital da União Europeia como desígnio político: a interoperabilidade como o caminho a seguir. Braga: UNIO – EU Law Journal, 2019. [Consultado 4 maio 2020]. p. 26-33. Disponível na internet: <http://repositorium.sdum.uminho.pt/bitstream/1822/61446/3/UNIO_EBOOK_INTEROP_2019.pdf >. ISBN 978989545871-4.

LEONARDI, Marcel. *Tutela e privacidade na internet.* São Paulo: Saraiva, 2011. ISBN 978850200000-0.

LIMA, Caio César Carvalho. Objeto, Aplicação material e Aplicação territorial. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords.) *Comentários ao GDPR:* Regulamento Geral de Proteção de Dados da União Europeia. São Paulo: Thomson Reuters Brasil, 2018. p. 23-36. ISBN 978855321230-9.

LIOUDIS, Nick. The Collapse of Lehman Brothers: a case study. *Investopedia*, 26 nov. 2019. [Consultado 5 maio 2020]. Disponível na internet: < https://www.investopedia.com/articles/economics/09/lehman-brothers-collapse.asp>.

LOPES, Tereza Vale. Responsabilidade e governação das empresas no âmbito do novo regulamento sobre a proteção de dados. *Anuário da Proteção de dados 2018.* Lisboa:

CEDIS, 2018. [Consultado 20 março 2020]. p. 45-69. Disponível na internet: <http://cedis.fd.unl.pt/wp-content/uploads/2018/04/ANUARIO-2018-Eletronico.pdf>. ISBN 978972993995-2.

MACHADO, Diego Carvalho et al. *GDPR e suas repercussões no direito brasileiro*: primeiras impressões de análise comparativa. Instituto de Referência em Internet e Sociedade: Belo Horizonte, 2018. [Consultado 19 março 2020]. Disponível na internet: <https://irisbh.com.br/wp-content/uploads/2018/06/GDPR-e-suas-repercussões-no-direito-brasileiro-IRIS-1.pdf>.

MALDONADO, Viviane Nóbrega. Direitos dos titulares dos dados. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords.) *Comentários ao GDPR:* Regulamento Geral de Proteção de Dados da União Europeia. São Paulo: Thomson Reuters Brasil, 2018. p. 85-109. ISBN 978855321230-9.

MARCHIONNI, Pietro. The next Generation e-government. Linkedin, 2018. [Consultado 6 maio 2020]. Disponível na internet: <https://www.linkedin.com/pulse/next-generation-e-government-pietro-marchionni>.

MARINELI, Marcelo Rumão. *Privacidade e redes sociais virtuais:* sob a égide da Lei n.° 12.965/2014- Marco civil da internet. Rio de Janeiro: Lumen Juris, 2017. ISBN 978855190053-6.

MARMELSTEIN, George. *Curso de direitos fundamentais.* 5ª ed. São Paulo: Atlas, 2014, p. 308. ISBN 978852248805-6.

MATIUZZO, Marcela. Propaganda Online e Privacidade: O varejo de dados pessoais na perspectiva antitruste. In: *Ideias em Competição:* 5 anos do Prêmio Ibrac-Tim. São Paulo: Singular, 2015, p. 411-431. ISBN 978858662678-4.

MATOS, Ana Carla Harmatiuk; RUZYK, Carlos Eduardo Pianovski. Diálogos entre a lei geral de proteção de dados e a lei de acesso à informação. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.) *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 199-218. ISBN 978855321663-5.

MAYER-SCHÖNBERGER, Viktor. *Delete:* the virtue of forgetting in the digital age. New Jersey: Princeton University, 2009. ISBN 978069113861-9.

_____. General development of data protection in Europe. In: AGRE, Phillip; ROTENBERG, Marc (Org.). *Technology and privacy*: The new landscape. Cambridge: MIT Press, 1997. ISBN 978026201162-4.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. *Big data*: a revolution will transform how we live, work and think. Boston: Houghton Mifflin Harcourt, 2014. ISBN 978054422775-0.

MELLO, Rafael Munhoz de. Sanção administrativa e o princípio da culpabilidade. *Revista de Direito Administrativo e Constitucional*, Belo Horizonte, out./dez. 2005, n. 22, [consultado 6 março 2020], p. 25-57, cit. p. 29. Disponível na internet: <file:///C:/Users/TJMA/Documents/624-252-1-PB.pdf>. ISSN 1516-3210.

MELODY, Willian H. Markets and Policies in New Knowledge Economies. In: MANSEL, Robin et al. (Org.). *The Oxford Handbook of Information and Communication Technologies*. New York: Oxford University Press, 2007. ISBN 978019926623-4.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de direito constitucional.* 13ª ed. rev. e atual. São Paulo: Saraiva, 2018. ISBN 978854722974-0.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova lei geral de proteção de dados*. Revista de direito do consumidor*, Editora Revista dos Tribunais, São Paulo, nov./dez. 2018, v. 120, p. 473. ISSN 1415-7705.

MENEZES, Joyceane Bezerra de; COLAÇO, Hian Silva. Quando a lei geral de proteção de dados não se aplica? In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.) *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p.157- 197. ISBN 978855321663-5.

MIRABETE, Julio Fabbrini. *Manual de direito penal.* 24ª ed. São Paulo: Atlas, 2006. v. 2. ISBN 852244316-5.

MIRANDA, Jorge. *Manual de direito constitucional*. 4ª ed. Coimbra: Coimbra Editora, 2008. t. 4. ISBN 978972321613-4.

MIRANDA, Jorge; RODRIGUES JUNIOR, Otavio Luiz; FRUET Gustavo Bonato. Principais problemas dos direitos da personalidade e estado da arte da matéria no direito comparado. In: MIRANDA, Jorge; RODRIGUES JUNIOR, Otavio Luiz; FRUET Gustavo Bonato (Coord.). *Direitos da Personalidade*. São Paulo: Atlas, 2012. ISBN 978852247134-8.

MONIZ, Graça Canto. Direitos do titular dos dados pessoais: o direito à portabilidade. *Anuário da Proteção de dados 2018*, Lisboa: CEDIS, 2018. [Consultado 20 março 2020]. p. 11-34. Disponível na internet: <http://cedis.fd.unl.pt/wp-content/uploads/2018/04/ANUARIO-2018-Eletronico.pdf>. ISBN 978972993995-2.

_____. Finalmente: coerência no âmbito de aplicação do regime da União Europeia de proteção de dados pessoais! O fim do enigma linguístico do artigo 3.º, n.º 2 do RGPD. *UNIO – EU Law Journal*, Braga, jul. 2018, v. 4, n. 2, [consultado 18 fevereiro 2020], p. 119-131. Disponível na internet: <https://revistas.uminho.pt/index.php/unio/article/view/25/57>. ISSN 2183-3435.

MONTEIRO FILHO, Carlos Edison do Rêgo; CASTRO, Diana Paiva de. Potencialidades do direito de acesso na nova lei geral de proteção de dados (Lei 13.709/2018). In: TEPEDINO,

Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.) *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 323-345. ISBN 978855321663-5.

MORAES, Alexandre de. *Direito Constitucional.* 24ª ed. São Paulo: Atlas, 2009. ISBN 978852245401-3.

MORAES, Alexandre Fernandes de. *Telemática:* convergência de dados, voz e imagem. São Paulo: Érica, 2014. [Consultado 4 maio 2020]. p. 92-93. Disponível na internet: <https://books.google.com.br/books?id=a46wDwAAQBAJ&printsec=frontcover&hl=pt-BR&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false>. ISBN 978853652531-0.

MURILLO DE LA CUEVA, Pablo de Lucas; PIÑAR MAÑAS, José Luís. *El derecho a la autodeterminación informativa.* Madrid: Fundación Coloquio Jurídico Europeo, 2009. ISBN 978846133470-4.

NORONHA, Edgard Magalhães. *Direito Penal:* dos crimes contra a pessoa; dos crimes contra o patrimônio. 33ª ed. São Paulo: Saraiva, 2003. v. 2. ISBN 850204313-7.

NUNES JUNIOR, Vital Serrano. *A proteção constitucional da informação e o direito à crítica jornalística.* São Paulo: Editora FTD, 1997. ISBN 853223758-4.

OST, François. *O tempo do direito.* Tradução: Élcio Fernandes. Bauru: Edusc, 2005. ISBN 978857460127-4.

PASQUALE, Franck. *The black box society*: The secret algorithms that control money and information. Cambridge: Harvard University Press, 2015. ISBN 978067436827-9.

PEREIRA, Marcelo Cardoso. *Direito à intimidade na internet.* Curitiba: Juruá, 2011. ISBN 853620516-4.

PÉREZ LUÑO, Antônio Henrique. *Derechos Humanos, Estado de Derecho y Constitutión.* 7ª ed. Madrid: Tecnos, 2001. ISBN 843093723-4.

REBELO, Maria Paulo. Os desafios do Regulamento Geral de Proteção de Dados diante da nova tecnologia *blockchain. Anuário da Proteção de dados 2019*, CEDIS, Lisboa, 2019, [consultado 9 MARÇO 2020], p. 109-135. Disponível na internet: <http://cedis.fd.unl.pt/wp-content/uploads/2019/06/ANUARIO-2019-Eletronico_compressed.pdf>. ISSN 2184-5468.

RODOTÀ, Stefano*. A vida na sociedade de vigilância:* a privacidade hoje. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: renovar, 2008. ISBN 978857147688-2.

_____. *Repertorio di fine secolo*. Bari: Laterza, 1999. ISBN 978884205859-5.

_____. *Tecnologie e diritti*. Bologna: Mulino, 1995. ISBN 978881504855-4.

RODRIGUES, Laura Gomes. O princípio da autonomia procedimental e o procedimento para concessão de visto pelos Estados-Membros da União Europeia. Os novos desafios da interoperabilidade em matéria de vistos. In: SILVEIRA, Alessandra; ABREU, Joana Covelo de; COELHO, Larissa (Coords.) *Unio e-book Interop 2019:* o mercado único digital da União Europeia como desígnio político: a interoperabilidade como o caminho a seguir. Braga: UNIO – EU Law Journal, 2019. [Consultado 4 maio 2020]. p. 7-15. Disponível na internet: <http://repositorium.sdum.uminho.pt/bitstream/1822/61446/3/UNIO_EBOOK_INTEROP_2019.pdf>. ISBN 978989545871-4.

ROSIC, Ameer. What is Blockchain technology the new internet? A step-by-stepguide for beginners. Blockgeeks, 2016. [Consultado 5 maio 2020]. Disponível na internet: <https://blockgeeks.com/guides/what-is-blockchain-technology/>.

SAKAMOTO, Sarah Gomes. *Segurança, privacidade e blockchain no contexto de internet das coisas*. Monografia do Curso de Especialização em Internet das Coisas, Universidade Tecnológica Federal do Paraná - UTFPR, Curitiba, 2020. 64 f. [Consultado 19 maio 2020]. Disponível na internet: <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/16143/1/CT_CEIOT_II_2019_10.pdf >.

SANCHÍS, Luís Pietro. *Estudios sobre derechos fundamentales.* Madrid: Debate, 1990. ISBN 978847444443-8.

SCHREIBER, Anderson. *Direitos da personalidade.* 3ª ed. rev., atual. São Paulo: Atlas, 2014. ISBN 978852249343-2.

_____. Direito ao esquecimento. In: SALOMÃO, Luís Felipe; TARTUCE, Flávio.(Coord.). *Direito Civil:* diálogos entre a doutrina e jurisprudência. São Paulo: Atlas, 2018. ISBN 978859701465-5.

_____. Direito ao esquecimento e proteção de dados pessoais na Lei n.° 13.709/2018: distinções e potenciais convergências. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.) *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 367-384. ISBN 978855321663-5.

SHAFFER, Andrew. A alegria de ver o sofrimento alheio: Shadenfreude e jogos vorazes In: DUNN George A; MICHAUD, Nicholas; e IRWIN, William (Orgs.). *Jogos vorazes e a filosofia*. Tradução: Patrícia Azeredo. Rio de Janeiro: Bestseller, 2013. ISBN 857684644-6.

SHARMA, Kriti. Jovens de hoje vão fazer trabalhos que ainda não existem. *Dinheiro Vivo*, 4 maio 2019. [Consultado 23 maio 2020]. Disponível na internet: <https://www.dinheirovivo.pt/vodafone-business-conference/kriti-sharma-jovens-de-hoje-vao-fazer-trabalhos-que-ainda-nao-existem/>.

SILVA, Paula Jaeger da. Direito ao esquecimento: aumento da problemática com o advento da internet. *Revista Jurídica*, Síntese Editora, São Paulo, set. 2018, n. 491, p. 70. ISSN 0103-3379.

SILVEIRA, Alessandra; FROUFE, Pedro. Do mercado interno à cidadania de direitos: a proteção de dados pessoais como a questão jusfundamental identitária dos nossos tempos*. UNIO – EU Law Journal,* Braga, jul. 2018, v. 4, n. 2, [consultado 18 fev. 2020], p. 4-20. Disponível na internet: <https://revistas.uminho.pt/index.php/unio/article/view/16/48>. ISSN 2183-3435.

SOLOVE, Daniel J. *Understanding privacy*. Cambridge: Harvard University Press, 2008. ISBN 978067403507-2.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.) *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 287-322. ISBN 978855321663-5.

UNIÃO EUROPEIA. TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA (TJUE). Ação de incumprimento de Estado nos termos do artigo 258.° TFUE, processo C - 583/14. 10ª Secção. Data do acórdão: 5.10.2016. [Consultado 27 maio 2020]. Disponível na internet: <http://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&jge=&td=%3BALL&jur=C%2CT%2CF&num=C-583%252F15&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=pt&avg=&cid=1735999>.

_____. Pedido de decisão prejudicial no processo C - 265/87. 5ª Secção. Data do acórdão: 11.7.1989. [Consultado 30 maio 2020]. Disponível na internet: <http://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&jge=&td=%3BALL&jur=C%2CT%2CF&num=C-265%252F87&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=pt&avg=&cid=2153787>.

_____. Pedido de decisão prejudicial no processo C - 180/95: Pedido de decisão prejudicial: Arbeitsgericht Hamburg - Alemanha. Data do acórdão: 22.4.1997. [Consultado 26 março 2020]. Disponível na internet: <http://curia.europa.eu/juris/showPdf.jsf?text=&docid=100350&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=914963>.

_____. Pedido de decisão prejudicial no processo C - 212/13. 4ª Secção. Data do acórdão: 11.12.2014. [Consultado 20 março 2020]. Disponível na internet: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=160561&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=143990>.

UNIÃO EUROPEIA. TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA (TJUE). Pedido de decisão prejudicial no processo C - 217/05: Tribunal Supremo - Espanha. 3ª Secção. Data do acórdão: 14.12.2006. [Consultado 20 março 2020]. Disponível na internet: < http://curia.europa.eu/juris/showPdf.jsf?text=&docid=66539&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=139883>.

_____. Pedido de decisão prejudicial no processo C - 295/04: Pedido de decisão prejudicial: Giudice di pace di Bitonto - Itália. 3ª Secção. Data do acórdão: 13.7.2006. [Consultado 26 março 2020]. Disponível na internet: < http://curia.europa.eu/juris/document/document.jsf?text=&docid=56474&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=916296>.

_____. Pedido de decisão prejudicial no processo C - 494/16: Tribunal de Trapani - Itália-Espanha. 1ª Secção. Data do acórdão: 7.3.2018. [Consultado 26 março 2020]. Disponível na internet: < http://curia.europa.eu/juris/document/document.jsf?text=&docid=200013&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=911006>.

_____. Pedido de decisão prejudicial no processo C - 557/12: Pedido de decisão prejudicial: Oberster Gerichtshof (Áustria). 5ª Secção. Data do acórdão: 5.6.2014. [Consultado 26 março 2020]. Disponível na internet: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=153312&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=920778>.

_____. Pedido de decisão prejudicial no processo C - 582/14. 2ª Secção. Data do acórdão: 19.10.2016. [Consultado 19 maio 2020]. Disponível na internet: <http://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&jge=&td=%3BALL&jur=C%2CT%2CF&num=C-582%252F14&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=pt&avg=&cid=890482>.

URIBE, Carlos Enrique Serra. *Derecho a la intimidad y videovigilancia policial*. Madrid: Laberinto, 2006. ISBN 978848483221-8.

VASCONCELOS, BETO; PAULA, Felipe de. A autoridade nacional de proteção de dados: origem, avanços e pontos críticos. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.) *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 717-739. ISBN 978855321663-5.

VERONESE, Alexandre. Os direitos de explicação e de oposição frente às decisões totalmente automatizadas: comparando o RGPD da União Europeia com LGPD brasileira. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coords.) *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019. p. 385-415. ISBN 978855321663-5.

VERONESE, Alexandre; CUNHA, Marcele. Desafios do comércio eletrónico no Brasil: integração vertical entre fornecedores e meios de pagamentos, proteção de dados pessoais e cooperação regulatória internacional*. UNIO – EU Law Journal,* Braga, jul. 2018, v. 4, n. 2, [consultado 18 fevereiro 2020], p. 73-89. Disponível na internet: <https://revistas.uminho.pt/index.php/unio/article/view/23/53>. ISSN 2183-3435.

VIEIRA, Eduardo. *Os bastidores da internet no Brasil*. São Paulo: Manole, 2003. ISBN 852041708-6.

WARREN, Samuel D. e BRANDEIS, Louis D. The rigth of privacy. *Harvard Law Review,* Boston, dez. 1890, v. 4, n. 5, [consultado 11 março 2020], p. 193-220. Disponível na internet: <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>.

WOOD, Aaron. Secretário de estado da Virgínia Ocidental relata votação bem-sucedida em blockchain em eleições do meio do mandato de 2018. *Cointelegraph Brasil*, 17 nov. 2018. [Consultado 15 maio 2020]. Disponível na internet: <https://cointelegraph.com.br/news/west-virginia-secretary-of-state-reports-successful-blockchain-voting-in-2018-midterm-elections>.

ZANON, João Carlos. *Direito à proteção dos dados pessoais.* São Paulo: Revista dos Tribunais, 2013. ISBN 978852034905-2.

Legislação e documentos institucionais

ALEMANHA. PARLAMENTO FEDERAL ALEMÃO – Lei Fundamental da República Federal da Alemanha. Tradução: Assis Mendonça. Promulgada (23-05-1949). [Consultado 12 março 2020]. Disponível na internet: <https://www.btg-bestellservice.de/pdf/80208000.pdf>.

BRASIL. PRESIDÊNCIA DA REPÚBLICA – Constituição da República Federativa do Brasil. "*D.O.U.*" (05-10-1988). [Consultado 20 março 2020]. Disponível na internet: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>.

_____ – Decreto n.° 7.962, de 15 de março de 2013. Regulamenta a Lei n.° 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. *"D.O.U."* (15-03-2013). [Consultado 20 janeiro 2020]. Disponível na internet: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D7962.htm>.
BRASIL – Decreto-Lei n.° 4.657, de 4 de setembro de 1942. Lei de Introdução às normas do Direito Brasileiro. *"D.O.U."* (09-09-1942). [Consultado 28 março 2020]. Disponível na internet: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del4657compilado.htm>.

BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. *"D.O.U."* (12-09-1990). [Consultado 20 janeiro 2020]. Disponível na internet: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>.

_____ – Lei n.° 8.080/1990, de 19 de setembro de 1990. Dispõe sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes e dá outras providências. *"D.O.U."* (20-09-1990). [Consultado 31 março 2020]. Disponível na internet: <http://www.planalto.gov.br/ccivil_03/leis/ l8080.htm>.

_____ – Lei n.° 8.142/1990, de 28 de dezembro de 1990. Dispõe sobre a participação da comunidade na gestão do Sistema Único de Saúde (SUS) e sobre as transferências intergovernamentais de recursos financeiros na área da saúde e dá outras providências. *"D.O.U."* (31-12-1990). [Consultado 31 março 2020]. Disponível na internet: <http://www.planalto.gov.br/ccivil_03/leis/L8142.htm>.

_____ – Lei n.° 9.610, de 19 de fevereiro de 2018. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. *"D.O.U."* (20-02-1998). [Consultado 31 março 2020]. Disponível na internet: < http://www.planalto.gov.br/ccivil_03/leis/l9610.htm>.

_____ – Lei n.° 10.406, de 10 de janeiro de 2002. Código Civil. "*D.O.U*." (11-01-2002). [Consultado 28 março 2020]. Disponível na internet: <http://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406.htm>.

_____ – Lei n.° 12.529, de 30 de novembro de 2011. Estrutura o Sistema Brasileiro de Defesa da Concorrência; dispõe sobre a prevenção e repressão às infrações contra a ordem econômica...; *"D.O.U."* (01-11-2011). [Consultado 20 março 2020]. Disponível na internet: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12529.htm>.

_____ – Lei n.° 12.813, de 16 de maio de 2013. Dispõe sobre o conflito de interesses no exercício de cargo ou emprego do Poder Executivo federal e impedimentos posteriores ao exercício do cargo ou emprego; e revoga dispositivos da Lei n.° 9.986, de 18 de julho de 2000, e das Medidas Provisórias n.^{os} 2.216-37, de 31 de agosto de 2001, e 2.225-45, de 4 de setembro de 2001. [Consultado 15 março 2020]. *"D.O.U."* (17-05-2013). Disponível na internet: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12813.htm>.

_____ – Lei n.° 12.965, de 23 de abril de 2014. Estabelece princípios garantias, direitos e deveres para o uso da internet no Brasil. *"D.O.U."* (24-04-2014). [Consultado 20 fevereiro 2020]. Disponível na internet: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>.

_____ – Lei n.° 13.105, de 16 de março de 2015. Código de Processo Civil. *"D.O.U."* (17-03-2015). [Consultado 7 março 2020]. Disponível na internet: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Lei/L13105.htm>.

BRASIL. PRESIDÊNCIA DA REPÚBLICA – Lei n.° 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). *"D.O.U."* (15-08-2018). [Consultado 15 janeiro 2020]. Disponível na internet: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>.

_____ – Lei n.° 13.853, de 08 de julho de 2019. Altera a Lei n.° 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. *"D.O.U."* (20-12-2019). [Consultado 20 fevereiro 2020]. Disponível na internet: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm>.

_____ – Lei Complementar n.° 105, de 10 de janeiro de 2001. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. *"D.O.U."* (11-01-2001). [Consultado 20 janeiro 2020]. Disponível na internet: <http://www.planalto.gov.br/ccivil_03/LEIS/LCP/Lcp105.htm>.

_____ – Lei Complementar n.° 123, de 14 de dezembro de 2006. Institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte. *"D.O.U."* (15-12-2006). [Consultado 5 março 2020]. Disponível na internet: < http://www.planalto.gov.br/ccivil_03/Leis/LCP/Lcp123.htm>.

BRASIL. SENADO FEDERAL – Proposta de emenda à constituição n.° 17, de 2019. Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. [Consultado 12 março 2020]. Disponível na internet: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1571776979155&disposition=inline>.

COMISSÃO EUROPEIA. Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões - Uma estratégia europeia para os dados. Bruxelas, 19 de fevereiro de 2020, COM(2020). [Consultado 7 julho 2020]. Disponível na internet: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020DC0066&from=EN>.

_____. Digital Economy and Society Index Report 2020 - Digital Public Services. [Consultado 6 julho 2020]. Disponível na internet: <https://ec.europa.eu/digital-single-market/en/digital-public-services-scoreboard>.

_____. *Do we always have to delete personal data if a person asks?* [Consultado 19 março 2020]. Disponível na internet: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/do-we-always-have-delete-personal-data-if-person-asks_en>.

_____. Plano de ação europeu (2016-2020) para a administração pública em linha: acelerar a transformação digital da administração pública. Bruxelas, 19 de abril de 2016.

[Consultado 17 maio 2020]. Disponível na internet: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52016DC0179&rid=1>.

COMISSÃO EUROPEIA. Portal *joinup*. [Consultado 7 julho 2020]. Disponível na internet: <https://joinup.ec.europa.eu/>.

CONSELHO DA EUROPA. Convenção n.° 108. Estrasburgo, 28 de janeiro de 1981. [Consultado 26 março 2020]. Disponível na internet: <https://www.cnpd.pt/home/legis/internacional/Convencao108.htm>.

_____. Convenção n.° 108+. Estrasburgo, 18 de maio de 2018. [Consultado 31 março 2020]. Disponível na internet: <https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf>.

_____. Convenção Europeia dos Direitos do Homem. Estrasburgo, 2 de outubro de 2013. [Consultado 30 março 2020]. Disponível na internet: <https://www.echr.coe.int/Documents/Convention_POR.pdf >.

DÉCIMO TERCEIRO CUMBRE IBERO-AMERICANA DE CHEFES DE ESTADO E DE GOVERNO. *Declaração de Santa Cruz de La Sierra.* Bolívia, 14 e 15 de novembro de 2003. [Consultado 18 fevereiro 2020]. Disponível na internet: <https://www.segib.org/wp-content/uploads/DECLARASAO-STA-CRUZ-SIERRA.pdf>.

ESPANHA. ASSEMBLEIA CONSTITUINTE – Constitución Española. *"B.O.E"* (29-12-1978). [Consultado 20 março 2020]. Disponível na internet: <http://www.lamoncloa.gob.es/documents/constitucion_es1.pdf>.

EU BLOCKCHAIN OBSERVATORY AND FORUM. [Consultado 13 maio 2020]. Disponível na internet: <https://www.eublockchainforum.eu/>.

GOVERNMENT-OFFICE FOR SCIENCE UK. *Distributed Ledger Technology: beyond block chain*. A report by the UK Government Chief Scientific Adviser. 2016. [Consultado 17 maio 2020]. Disponível na internet: < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf>.

GRUPO DE PROTEÇÃO DAS PESSOAS NO QUE DIZ RESPEITO A TRATAMENTO DE DADOS PESSOAIS (GT29). *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.* [Consultado 18 fevereiro 2020]. Disponível na internet: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053>.

_____. *Guidelines on the Lead Supervisory Authority (wp244rev.01).* [Consultado 2 março 2020]. Disponível na internet: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235>.

GRUPO DE PROTEÇÃO DAS PESSOAS NO QUE DIZ RESPEITO A TRATAMENTO DE DADOS PESSOAIS (GT29). *Guidelines on the right to data portability.* [Consultado 18 fevereiro 2020]. Disponível na internet: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233>.

_____. *Guidelines on Transparency under Relugation 2016/679.* [Consultado 10 fevereiro 2020]. Disponível na internet: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227>.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* [Cited 28 march 2020]. Available from internet: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>.

PARLAMENTO EUROPEU – *Resolução n.° 2016/2007 (INI), sobre moedas virtuais.* Bruxelas, 26 de maio 2016. [Consultado 17 maio 2020]. Disponível na internet: <https://www.europarl.europa.eu/doceo/document/TA-8-2016-0228_PT.html?redirect>.

PARLAMENTO EUROPEU; CONSELHO – Carta dos direitos fundamentais da união europeia. "*J.O.U.E.*" (07-06-2016).[Consultado 30 março 2020]. Disponível na internet: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR>.

_____ – Decisão (UE) 2015/2240 de 25 de novembro de 2015 cria um programa sobre soluções de interoperabilidade e quadros comuns para as administrações públicas, as empresas e os cidadãos europeus (Programa ISA^2) como um meio para modernizar o setor público. "*J.O.U.E.*" (04-12-2015). [Consultado 11 maio 2020]. Disponível na internet: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32015D2240&from=PT>.

_____ – Directiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995 relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. "*J.O.C.E.*" (23-11-1995). [Consultado 30 março 2020]. Disponível na internet: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT>.

_____ – Diretiva 2012/17/EU de 13 de junho de 2012 que altera a Diretiva 89/666/CEE do Conselho e as Diretivas 2005/56/CE e 2009/101/CE do Parlamento Europeu e do Conselho no que respeita à interconexão dos registos centrais, dos registos comerciais e dos registos das sociedades. "*J.O.U.E.*" (16-06-2012). [Consultado 13 maio 2020]. Disponível na internet: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32012L0017>.

_____ – Diretiva 2013/37/UE de 26 de junho de 2013 que altera a Diretiva 2003/98/CE relativa à reutilização de informações do setor público. "*J.O.U.E.*" (27-06-2013).

[Consultado 13 maio 2020]. Disponível na internet: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32013L0037>.

PARLAMENTO EUROPEU; CONSELHO – Directiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002 relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas). *"J.O.C.E."* (31-07-2002). [Consultado 31 março 2020]. Disponível na internet:<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0058&from=EN>.

_____ – Regulamento (UE) n.° 910/2014 de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE. *"J.O.U.E."* (28-08-2014). [Consultado 13 maio 2020]. Disponível na internet: <file:///C:/Users/Celeste/Downloads/l_25720140828pt00730114.pdf.pt.pdf>.

_____ – Regulamento (EU) 1071/2009 de 21 de outubro de 2009 (estabelece regras comuns no que se refere aos requisitos para o exercício da actividade de transportador rodoviário e que revoga a Directiva 96/26/CE do Conselho). *"J.O.U.E."* (14-11-2009). [Consultado 27 maio 2020]. Disponível na internet: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32009R1071&from=PT>.

_____ – Regulamento (UE) 2016/679 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). *"J.O.U.E."* (04-05-2016). [Consultado 12 janeiro 2020]. Disponível na internet: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=pt>.

_____ – Regulamento (UE) 2018/1725 de 23 de outubro de 2018 (Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.° 45/2001 e a Decisão n.° 1247/2002/CE). *"J.O.U.E."* (21-11-2018). [Consultado 11 maio 2020]. Disponível na internet: < https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32018R1725&from=PT>.

_____– Regulamento (UE) 2019/881 de 17 de abril de 2019 (Relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n. o 526/2013 (Regulamento Cibersegurança)). *"J.O.U.E."* (07-06-2019). [Consultado 7 julho 2020]. Disponível na internet: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019R0881&from=PT>.

PORTUGAL – Código Civil - Decreto-Lei n.º 47344. *"D.G."* (25-11-1966). [Consultado 26 março 2020]. Disponível na internet: < https://dre.pt/web/guest/legislacao-consolidada/-/lc/123928118/202003261339/diploma?did=34509075&_LegislacaoConsolidada_WAR_drefrontofficeportlet_rp=indice>.

PORTUGAL. ASSEMBLEIA CONSTITUINTE – Constituição da República Portuguesa. *"D.R."* (10-04-1976). [Consultado 20 março 2020]. Disponível na internet: <https://dre.pt/legislacao-consolidada/-/lc/34520775/view>.

_____ – Constituição da República Portuguesa. *"D.R."* (10-04-1976) (Versão Original). [Consultado 12 março 2020]. Disponível na internet: <http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=4&tabela=lei_velhas&nversao=1&so_miolo= >.

UNIÃO EUROPEIA – Tratado da união europeia(versão consolidada). "*J.O.U.E."* (07-6-2016). [Consultado 30 maio 2020]. Disponível na internet: <https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_2&format=PDF>.

_____ – Tratado sobre o funcionamento da união europeia (versão consolidada). "*J.O.U.E."* (07-6-2016).[Consultado 30 março 2020]. Disponível na internet: <https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF>.

UNITED STATES OF AMERICA. Records, Computers and The Rights of Citizens – *Report of the Secretary's Advisory Committee on Aumomated Personal Data Systems*. 1973. [Cited 15 march 2020]. Available from internet: <https://aspe.hhs.gov/report/records-computers-and-rights-citizens>.