Universidade do Minho
Escola de Direito

Weder de Lacerda Silva

O Regime Jusfundamental da Proteção de Dados Pessoais no Brasil

julho de 2020

O Regime Jusfundamental da Proteção de Dados Pessoais no Brasil
Weder de Lacerda Silva
UMinho | 2020

Universidade do Minho
Escola de Direito

Weder de Lacerda Silva

O Regime Jusfundamental da Proteção de Dados Pessoais no Brasil

Dissertação de Mestrado
Mestrado em Direitos Humanos

Trabalho efetuado sob a orientação da
Professora Doutora Alessandra Silveira

julho de 2020

AGRADECIMENTOS

Gratidão é a palavra que resume a experiência, que foi iniciar e finalizar esse mestrado na Universidade do Minho em Braga, Portugal.

Antes de agradecer a qualquer pessoa, quero agradecer a DEUS, pois, Ele tem me guiado desde o dia que decidi me candidatar a esse programa de mestrado e tem me ajudado desde então em todas as coisas.

Amar a Deus sobre todas as coisas é o que me ensinou a confiar nEle e ter Fé, e pela Fé, todas as outras coisas aconteceram. Quando eu achei que não conseguiria, bastou uma oração e confiar, que Deus concedeu. Gratidão à Deus pelos dias vividos em Portugal, pela experiência e principalmente pelo aprendizado.

Depois de agradecer a Deus, e não menos importante, quero agradecer aos meus Pais, José Carlos e Ana Lucia, que, mesmo do outro lado do Atlântico, torceram e oraram por mim todos os dias, para que todas as coisas saíssem bem. Assim como minha irmã, que acreditou em mim e me deu forças para deixar a vida no Brasil e realizar meu sonho de morar fora.

Agradeço também ao meu amigo e companheiro Cleolenes Junior, que, ainda que por um curto período de estada, fizeram dos meus dias mais engraçados, feliz e leve.

Quero agradecer ainda a minha família portuguesa, que de portuguesa não tinha nada, além dos vinhos. Gratidão pela oportunidade de ter conhecido o Gabriel Centenaro, a Nicole Paganini, o casal maravilhoso Ana e Gabriel, que foram meus companheiros nos dias de inverno e primavera, durante sua breve estadia em Braga.

Com toda certeza, os vinhos, os queijos, os Unus, as brincadeiras e os passeios não seriam os mesmos sem vocês. A vida em Portugal é muito atrativa, mas sem uma boa companhia, nem o melhor vinho alegra o dia.

Quero agradecer a todos os professores que lecionaram durante o primeiro ano, foi um prazer e uma honra poder expandir e crescer diante de conhecimento tão único, durante esse mestrado. Em especial a professora Alessandra Silveira, minha orientadora, que confiou e acreditou em mim, desde a minha primeira apresentação em sala e me convidou para falar sobre esse tema que eu desconhecia e passei a amar. Na verdade, um caso sério de amor e ódio (sobre os dados pessoais), mas qual relacionamento, não é assim?! Mas eu venci!

Por fim, quero agradecer a minha filha Lavínia Antonelli Lacerda, que tão pequenina e inocente, suportou minha ausência e me dava forças, contribuindo com seu amor para me aquecer nos dias frios

e chuvosos de Braga. Foi por mim e por ela que decidi entrar de cabeça nesta experiência, que ao mesmo tempo foi a realização de um sonho.

Um abraço apertado em Braga. Guardarei comigo memorias, fotografias e lembrança dessa terra maravilhosa que, por um curto período de tempo, eu pude desbravar.

Assim, apenas gratidão por ter sido agraciado com essa experiência na qual, eu jamais esquecerei.

DECLARAÇÃO DE INTEGRIDADE

Declaro ter atuado com integridade na elaboração do presente trabalho académico e confirmo que não recorri à prática de plágio nem a qualquer forma de utilização indevida ou falsificação de informações ou resultados em nenhuma das etapas conducente à sua elaboração.

Mais declaro que conheço e que respeitei o Código de Conduta Ética da Universidade do Minho.

O REGIME JUSFUNDAMENTAL DA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

RESUMO

A presente dissertação tem por objetivo afirmar a dimensão jusfundamental do direito à proteção de dados pessoais no ordenamento jurídico brasileiro, perspectivando-o como o direito fundamental que efetivamente é. Apesar da ausência de consagração expressa neste sentido – algo que será brevemente ultrapassado por força de emenda constitucional em tramitação no Congresso Nacional (PEC n.º 17/2019) – o direito à proteção de dados pessoais possui inegável dimensão jusfundamental, sob pena da sua fragilização no confronto com outros direitos fundamentais. Nesta medida, analisaremos todo o percurso do direito à proteção de dados pessoais no ordenamento brasileiro, desde as primeiras formulações associadas à proteção da vida privada, até a atual iminência de reconhecimento formal pelo constituinte, procurando identificar o que distingue o direito à proteção de dados pessoais do direito à proteção da privacidade – ou seja, qual o seu âmbito de aplicação, o que protege, o que proíbe. Para tanto, foi adotada a metodologia indutiva, com base no estudo de fontes primárias (instrumentos normativos de âmbito internacional – tratados internacionais de proteção aos direitos humanos –, normas constitucionais, leis infraconstitucionais, jurisprudências) e fontes secundárias (doutrinas, artigos e trabalhos acadêmicos de autores brasileiros e estrangeiros). A dissertação está dividida em três capítulos. No primeiro capítulo será abordada a recepção dos direitos humanos no ordenamento jurídico brasileiro desde o direito à vida privada até o direito à proteção de dados pessoais. No segundo capítulo será apresentado o conceito de dados pessoais – inclusivamente no que tange aos dados de caráter sensível e aos dados anônimos –, bem como a relevância dos mesmos para o mercado digital, salientando ainda a importância da regulamentação do direito à proteção de dados pessoais em decorrência da sua dimensão jusfundamental. No terceiro capítulo será demonstrado como encontra-se disposto o direito à proteção de dados pessoais no ordenamento jurídico brasileiro, desde a Constituição da República Federativa do Brasil (CRFB) de 1988 até a Lei Geral de Proteção de Dados Pessoais (LGPD). Por fim, no capitulo final, será apresentado os impactos do COVID-19 sobre a LGPD, com ênfase final na Proposta de Emenda à Constituição (PEC) n.º 17/2019 e a decisão inédita do STF em discussão do Direito Fundamental à Proteção de Dados Pessoais.

Palavras-chave: Direitos humanos; Direitos fundamentais; Dados pessoais; Lei Geral de Proteção de Dados Pessoais (LGPD); PEC n.º 17/2019.

THE JUSFUNDAMENTAL REGIME FOR THE PROTECTION OF PERSONAL DATA IN BRAZIL

ABSTRACT

This dissertation aims to affirm the fundamental dimension of the right to protection of personal data in the Brazilian legal system, viewing it as the fundamental right that it effectively is. Despite the absence of express consecration in this sense – something that will soon be overcome due to a constitutional amendment pending in the National Congress (PEC n.º 17/2019) – the right to the protection of personal data has an undeniable jusfundamental dimension, under penalty of its fragility in the confrontation with other fundamental rights. To this extent, we will analyze the entire path of the right to protection of personal data in the Brazilian system, from the first formulations associated with the protection of private life, to the current imminence of formal recognition by the constituent, seeking to identify what distinguishes the right to data protection. personal rights to the protection of privacy – that is, what is its scope, what protects, what it prohibits. For that, the inductive methodology was adopted, based on the study of primary sources (normative instruments of international scope – international treaties for the protection of human rights –, constitutional norms, infraconstitutional laws, jurisprudence) and secondary sources (doctrines, articles and academic works Brazilian and foreign authors). The dissertation is divided into three chapters. The first chapter will address the reception of human rights in the Brazilian legal system, from the right to private life to the right to the protection of personal data. In the second chapter, the concept of personal data will be presented – including with regard to sensitive data and anonymous data -, as well as their relevance to the digital market, also emphasizing the importance of regulating the right to protection of personal data. due to its fundamental dimension. In the third chapter, it will be demonstrated how the right to protection of personal data is provided for in the Brazilian legal system, from the Constitution of the Federative Republic of Brazil (CRFB) of 1988 to the General Law of Protection of Personal Data (LGPD). Finally, in the final chapter, the impacts of COVID-19 on the LGPD will be presented, with final emphasis on the Proposed Amendment to the Constitution (PEC) n.º 17/2019 and the unprecedented decision of the STF in discussion of the Fundamental Right to Protection Personal Data.

Keywords: Human rights; Fundamental rights; Personal data; General Law on Protection of Personal Data (LGPD); PEC n.º 17/2019.

ÍNDICE

LISTA DE ABREVIATURAS E SIGLAS

AC – Ação Civil Pública

ADIn – Ação Direta de Inconstitucionalidade

ANATEL – Agencia Nacional de Telecomunicações

ANPD – Agência Nacional de Proteção de Dados

Art. – Artigo

CADH – Convenção Americana de Direitos Humanos

CC – Código Civil

CDC – Código de Defesa do Consumidor

CE – Comissão Europeia

CEDH – Convenção Europeia dos Direitos do Homem

Cf. – Conforme

CGI – Comitê Gestor da Internet

CIA – Central Intelligence Agency

CNJ – Conselho Nacional de Justiça

COOPA – Children's Online Privacy Protection Act

COVID-19 – Coronavirus Disease 2019

CPF – Cadastro de Pessoas Físicas

CRFB – Constituição da República Federativa do Brasil

D2D – Device to Device

Dje – Diário da Justiça Eletrônico

DNA – Ácido desoxirribonucleico

DOU – Diário Oficial da União

DUDH – Declaração Universal dos Direitos Humanos

ECA – Estatuto da Criança e do Adolescente

Ed. – Edição

Ement. – Ementa

EPDB – Comitê Europeu para a Proteção de Dados

Et al. – Et alii

Etc. – Et Cetera

EU – União Europeia

EUA – Estados Unidos da América

GPS – global positioning system

IBGE – Instituo Brasileiro de Geografia e Estatística

INDA – Infraestrutura Nacional de Dados Abertos

IoT – Internet of Things

IP – Internet Protocol

LAI – Lei de Acesso à Informática

LGPD – Lei Geral de Proteção de Dados Pessoais

MP – Ministério Público

MPF – Ministério Público Federal

MPFDFT – Ministério Púnico do Distrito Federal e Territórios

MPFPI – Ministério Público Federal do Piauí

MProv. – Medida Provisória

MS – Mandado de Segurança

N.º – Número

NSA – National Security Agency

OMS – Organização Mundial de Saúde

ONU – Organização das Nações Unidas

Op. cit. – opera citato

P. – Página

PEC – Proposta de Emenda à Constituição

PIDCP – Pacto Internacional dos Direitos Civis e Políticos

PIDESC – Pacto Internacional dos Direitos Econômicos, Sociais e Culturais

PL – Projeto de Lei

PLS – Projeto de Lei do Senado

Pp. – Páginas

PROCON – Programa de Proteção e Defesa do Consumidor

REsp. – Recurso Especial

RG – Registro Geral

RGPD – Regulamento Geral sobre a Proteção de Dados

RJ – Rio de Janeiro

RJET – Regime Jurídico Emergencial e Transitório das relações Jurídicas de Direito Privado

RMS – Recurso Mandado de Segurança

RO – Recurso Ordinário

S/a – Autor Desconhecido

S/d – Sem data

SeNaCon – Secretaria Nacional do Consumidor

SES – Secretaria de Saúde

SIC – Serviço de Informação ao Cidadão

Sinaes – Sistema Nacional de Avaliação da Educação Superior

SPC – Serviço de Proteção ao Crédito

STF – Supremo Tribunal Federal

STJ – Superior Tribunal de Justiça

TFUE – Tratado sobre o Funcionamento da União Europeia

TJUE – Tribunal de Justiça da União Europeia

TRF1 – Tribunal Regional Federal da 1ª Região

Ún. – Único

Vol. – Volume

§ – Parágrafo

INTRODUÇÃO

Desde a década de 1990, a comunicação via internet vem crescentemente ganhando destaque e se consolidando. É impossível imaginar o mundo atual sem a internet. Ela invadiu a vida moderna e adentrou à casa de cada indivíduo – o que facilitou o contato e o acesso aos diferentes tipos de informação. Da mesma forma com que facilitou o contato entre pessoas naturais, a internet impulsionou também o relacionamento entre e com pessoas coletivas (pessoas jurídicas). Nesse sentido, contribuiu para a criação de um mercado dados[1] – que através do *e-commerce*[2] movimenta diariamente milhares de dólares. Esse mercado se baseia no tráfego de dados, em larga medida de natureza pessoal, inclusivamente aqueles considerados como sendo de caráter sensível e extremamente valiosos (nos sentidos financeiro e moral).

A forma com que essa circulação de dados acontece tem sido alvo de grandes discussões jurídicas[3], na medida em que a simples inserção de uma informação (dado pessoal) na *web* – através do preenchimento de formulários, fichas cadastrais, cupons, currículos e outros – pode conduzir à vulnerabilidade do titular dos dados pessoais. A fim de compreender o que acontece nesse universo virtual – e suas implicações no real –, e de que forma o legislador está a se mover para alcançar a efetiva proteção dos dados pessoais, faz-se necessário explanar inicialmente sobre tal conceito.

Por dados entende-se "um conjunto de registros sobre fatos, passíveis de serem ordenados, analisados e estudados para se alcançar conclusões[4]". Os dados, quando "organizados e ordenados de forma coerente e significativa para fins de compreensão e análise[5]", são chamados de informação.

---

1 Cf. SILVA, Camila, "O mercado de dados no Brasil", *in E-commerce Brasil*, 2014, texto disponível em https://www.ecommercebrasil.com.br/artigos/o-mercado-de-dados-brasil/ [07.11.2019].

2 "*O comércio eletrônico, ou e-commerce, é um ambiente digital em que ocorrem operações de compra e venda, troca e prestação de serviço com suporte de equipamentos e programas de informática, por meio dos quais se possibilita realizar a negociação, a conclusão e até a execução do contrato, quando for o caso de bens intangíveis via download. No fundo o e-commerce é uma extensão do comércio convencional. Apesar de o ambiente virtual propiciar os mais variados tipos de contratos, públicos e privados, como, por exemplo: negócios entre empresas (B2B - business to business) e entre particulares no âmbito da contratação civil (C2C - consumer to consumer), sem dúvida a grande massa de negócios eletrônicos são entre fornecedor e consumidor (B2C - business to consumer)".* Cf. TEIXEIRA, Tarcísio. *"Aspectos atuais do e-commerce",* São Paulo, *in Jornal Carta Forense*, 2014, texto disponível em http://www.cartaforense.com.br/conteudo/entrevistas/aspectos-atuais-do-e-commerce/14650 [10.02.2019].

3 *"No Brasil a discussão começa agora, com aproximadamente 40 anos de atraso em relação aos países europeus e aos Estados Unidos, que têm legislações específicas desde a década de 70. No final de 2010, através de uma iniciativa do Ministério da Justiça em parceria com o Observatório Brasileiro de Políticas Digitais do Centro de Tecnologia e Sociedade da FGV, foi proposto um debate com a sociedade através do blog http://culturadigital.br/dadospessoais sobre o anteprojeto de lei de proteção de dados pessoais que foi encaminhado ao legislativo no segundo semestre de 2011, que, teve aprovação somente em julho de 2018".* Cf. SARDETO, Patrícia Eliane da Rosa, *"A proteção de dados pessoais em debate no Brasil",* Florianópolis, *in Âmbito Jurídico*, 2011, texto disponível em http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=9455 [13.02.2019].

4 Cf. LACOMBE, Francisco José Masset et al., *Administração Princípios e Tendências*, São Paulo, Saraiva, 2003, p. 490.

5 Cf. LACOMBE, Francisco José Masset et. al. *Administração Princípios...* op. cit., p. 490.

O termo dados pessoais foi balizado por uma diretiva europeia – e refere-se à qualquer informação relativa a uma pessoa singular identificada ou identificável. É considerado identificável todo aquele que possa ser identificado, direta ou indiretamente – nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social[6].

A inserção desses dados na internet, bem como a sua consulta e divulgação, cria uma teia de informações – também conhecida como rede de dados –, que movimenta o mercado de dados. Por rede de dados entende-se a "infraestrutura cuja concepção possibilita a transmissão de informação através da troca de dados. Cada uma dessas redes foi concebida especificamente para satisfazer os seus objetivos, com uma determinada arquitetura para facilitar a troca de conteúdo[7]".

O mundo virtual, referido aqui como a internet, é alimentado diariamente por dados pessoais fornecidos, em sua grande maioria, pelo próprio titular/usuário. A inserção dos dados pode dar-se através das redes sociais (Facebook, Instagram, Twitter, WhatsApp, etc.), empresas privadas que se utilizam de uma espécie de banco de dados (Amazon, Google, Apple, etc.), bem como por empresas específicas em armazenamento de currículos *online*, dentre outros. Com o acesso à tecnologia avançada de celulares tipo *smartphones* e o fácil acesso à rede de dados móveis, a transmissão de dados pessoais em tempo real torna-se praticamente incontrolável.

Em algumas situações, o tratamento indevido dos dados pessoais acaba por violar direitos fundamentais consagrados pela Carta Magna brasileira desde 1988, tais como o direito à intimidade e à vida privada[8], reconhecidos universalmente como pertencente ao rol dos direitos humanos[9]. No entanto, na literalidade da legislação brasileira, não há nada formalmente disposto a propósito de um direito fundamental específico e autônomo à proteção de dados pessoais. Vai daí a necessidade premente da regulamentação desse direito, não somente pelo fato de algumas normas internacionais já o reconhecerem enquanto tal, mas também levando em consideração a sua inegável dimensão

---

6 Cf. UNIÃO EUROPEIA, "*Directiva 95/46/CE do Parlamento Europeu e do Conselho da União Europeia, 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"*, diretiva disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT [07.11.2019].

7 Cf. S/A, "*Conceito de rede de dados*", *in Conceito.de,* 2014, texto disponível em https://conceito.de/rede-de-dados [14.01.2019].

8 *"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: (...) X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; (...)".*

9 "*Artigo XII - Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques".* Cf. ORGANIZAÇÕES DAS NAÇÕES UNIDAS, *Declaração Universal dos Direitos Humanos*, Paris, 1948, texto disponível em http://www.onu.org.br/img/2014/09/DUDH.pdf [13.02.2019].

jusfundamental, sob pena da fragilização do direito à proteção de dados pessoais no confronto com outros direitos fundamentais.

A principal problemática no tratamento e divulgação indevida dos dados pessoais ocorre pelos efeitos negativos que causam ao seu titular – que, em algumas situações, nem sequer consentiu naquele tratamento. Um exemplo de tratamento de dados pessoais de forma ilícita veio à tona com o vazamento das informações de dados "espionados" pela NSA e CIA, em 2013, denunciado por Edward Snowden[10] – que acabou por despertar na sociedade mundial a consciência sobre o controlo sobre seus dados pessoais, assim como a necessidade de criação de normas que regulamentassem o seu tratamento de forma efetiva.

SILVEIRA e FROUFRE fazem analogia a esse despertar quando escrevem sobre o Regulamento Geral sobre a Proteção de Dados (RGPD) – Regulamento (UE) 2016/679 –, recorrendo à metáfora da princesa adormecida[11] do conto infantil, que acaba por perceber (aqui a princesa refere-se ao titular dos dados) que é dona dos dados que lhe digam respeito e que os mesmos possuem um valor. Neste sentido, num âmbito global, vários países já regularam o direito em questão, tendo como destaque países integrantes da União Europeia que, atualmente, possuem respaldo do RGPD[12], em vigor desde maio de 2016, mas que somente passou a ser aplicado em 25 de maio de 2018.

Diferentemente de Portugal e demais países integrantes da União Europeia, bem como alguns países da América do Sul – Argentina, Bolívia, Chile, Colômbia, Guatemala e Peru –, o Brasil tratou do direito à proteção de dados pessoais na internet, até o ano de 2018, de forma muito tímida e rasa, tendo como base legal principal a Lei n.º 12.965, de 23 de abril de 2014[13], conhecida como Marco Civil da Internet. Cumpre salientar que esse panorama jurídico atualmente está a se reconfigurar. Isso porque a

---

10 *"O ex-técnico da CIA Edward Snowden, de 29 anos, foi acusado de espionagem por vazar informações sigilosas de segurança dos Estados Unidos e revelar em detalhes alguns dos programas de vigilância que o país usa para espionar a população americana – utilizando servidores de empresas como Google, Apple e Facebook – e vários países da Europa e da América Latina, entre eles o Brasil, inclusive fez o monitoramento de conversas da presidente Dilma Rousseff com seus principais assessores".* Cf. G1, *Entenda o caso de Edward Snowden, que revelou espionagem dos EUA*, São Paulo, *in G1*, 2013, texto disponível em http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html [03.08.2019].

11 Cf. SILVEIRA, Alessandra e FROUFRE, Pedro, *"Do mercado interno à cidadania de direitos: a proteção de dados pessoais como a questão Jusfundamental identitaria dos nossos tempos"*, Braga, UNIO - EU Law Journal, Vol. 4, N.º 2, 2018, p. 5.

12 Cf. UNIÃO EUROPEIA, "*Regulamento (UE) 2016/679 Do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)",* 2016, regulamento disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN [03.08.2019]

13 Cf. BRASIL, Lei n° 12.965, de 23 de abril de 2014, *"Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil"*, 2014, texto disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.html [14.01.2019].

Lei n.º 13.709[14] – Lei Geral de Proteção de Dados Pessoais (LGPD) –, publicada em 14 de agosto de 2018, entrará em vigor em sua totalidade[15] em 03 de maio de 2021, com inicio da aplicação das sanções somente a partir de 1º de agosto de 2021.

Para melhor compreensão da dimensão jusfundamental do direito à proteção de dados pessoais – tal como defendemos –, a presente dissertação foi organizada em três capítulos. No primeiro capítulo será exposto historicamente o recepcionamento dos direitos humanos no ordenamento jurídico brasileiro, dando ênfase à consagração do direito fundamental à vida privada pela Carta Magna. Insta salientar que o reconhecimento desse direito ocorreu, a nível internacional, muito antes da CRFB de 1988. Na verdade, em 1948, o direito à vida privada foi reconhecido no artigo XII da Declaração Universal dos Direitos Humanos[16] (DUDH) da Organização das Nações Unidas (ONU). Os direitos humanos seriam reafirmados em 1966 pelos Pacto Internacional dos Direitos Civis e Políticos (PIDCP) e o Pacto Internacional dos Direitos Econômicos, Sociais e Culturais (PIDESC), bem como pela Convenção Americana de Direitos Humanos (CADH) de 1969, também conhecida como Pacto de San José da Costa Rica, ratificado pelo Brasil em 25 de setembro de 1992.

No segundo capítulo será abordado, de maneira minuciosa, o conceito de dados pessoais, esclarecendo o sentido de dados sensíveis e anônimos, e mostrando qual a sua importância e valor para o mercado de dados. O objetivo é evidenciar em que medida os dados pessoais hão de ser protegidos autonomamente em relação aos direitos à privacidade ou à intimidade, bem como defender a sua dimensão jusfundamental, através da doutrina e do ordenamento jurídico brasileiro e internacional.

Será demonstrado também em que medida a rede de dados inseridos na *web* depende crescentemente de algoritmos de aprendizagem que possibilitam o desenvolvimento e aperfeiçoamento da chamada economia digital. Tais algoritmos aprendem a partir dos dados que lhes são facultados – ou seja, os dados dos titulares/usuários/consumidores inseridos na internet –, com a finalidade de aprimoramento das tarefas que lhe são designadas. Neste rol de inserção e captura indireta de dados, também entra em cena o papel das redes sociais (Facebook, Instagram, Twitter, WhatsApp, etc.) e os motores de buscas (Google, Yahoo, Amazon, Apple, etc.) detentores do maior acervo de dados existente atualmente no mundo. Por de trás do viés aparentemente gratuito da sua atividade, tais gigantes da

---

14 Cf. BRASIL, *Lei nº 13.709, de 14 de agosto de 2018, "Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet)"*, 2018, lei disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.html [28.02.2019].

15 *"Art. 65. Esta Lei entra em vigor: (Redação dada pela Lei nº 13.853, de 2019) I - dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e (Incluído pela Lei nº 13.853, de 2019) I-A – dia 1º de agosto de 2021, quanto aos arts. 52, 53 e 54; (Incluído pela Lei nº 14.010, de 2020) II - em 3 de maio de 2021, quanto aos demais artigos. (Redação dada pela Medida Provisória nº 959, de 2020)."*

16 Cf. ORGANIZAÇÕES DAS NAÇÕES UNIDAS, "*Declaração Universal dos Direitos...", op. cit.,* artigo XII.

internet acabam por encobrir seu real interesse/modelo de negócio – qual seja, a recolha e venda de dados pessoais com o fito de que empresas terceiras definam perfis consumeristas específicos para oferecer produtos e serviços direcionados. Afinal, "não existem almoços grátis[17]".

No capítulo três (último capítulo) serão apresentados os projetos legislativos, bem como as normas relacionadas com a proteção de dados pessoais, desde a promulgação da CRFB de 1988, passando pela Lei n.º 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), inclusivamente à luz do seu enquadramento internacional –, até a PEC n.º 17/2019. O propósito que nos move é aquele de apresentar o direito à proteção de dados pessoais como um direito fundamental, reconhecendo-o na sua devida importância e autonomia em relação a outros direitos, e ressaltando o que tal direito protege, o que proíbe e principalmente o que o distingue de outros direitos considerados como análogos.

17 ***"There is no free lunch",*** faz referência ao Teorema de David Wolpert, afirmando que por trás de todo "grátis" há uma moeda de troca como pagamento revestida de uma falsa gratuidade. (Itálico Nosso)

CAPÍTULO I

O PERCURSO JURÍDICO DO DIREITO À VIDA PRIVADA ATÉ O DIREITO À PROTEÇÃO DE DADOS PESSOAIS COMO UM DIREITO FUNDAMENTAL

1. Do reconhecimento universal aos direitos humanos

Através da história, nota-se uma linha crescente de valorização das ideias ligadas aos direitos humanos. Importante salientar ainda que as crenças religiosas ou culturais também contribuíram com esse papel, afinal, reafirmavam a existência de direitos de proteção ao ser humano e a sua essência, por meio de um direito natural, ou seja, não positivado, regido pelo bom senso e a boa-fé, dentre outros, como por exemplo, advindos ou refletidos de uma vontade divina – afinal, durante anos a fio, a igreja regeu as leis humanas.

O primeiro registro escrito encontrado no mundo acerca da proteção de direitos humanos é datado de 539 anos antes de Cristo. Esse apontamento foi conhecido como o "Cilindro de Ciro[18]", escrito por Ciro, o Grande, na época em que fora rei da Pérsia. Muito embora exista ainda correntes que discordem de tal fato, o Cilindro de Ciro é considerado como o primeiro registro escrito precursor de direitos humanos.

À época do Iluminismo, filósofos desenvolveram teorias da lei natural, que influenciaram diretamente na adoção de outros documentos, como por exemplo a Declaração de Direitos de 1689[19],

18 O Cilindro de Ciro é um cilindro de argila, atualmente dividido em vários fragmentos, no qual está escrita uma declaração em grafia cuneiforme acadiana, em nome do xá, Ciro, o Grande. Ele data do século VI a.C. (539 a.C.), e foi descoberto nas ruínas de Babilônia na Mesopotâmia (atual Iraque) em 1879. É possessão do Museu Britânico (British Museum), que patrocinou a expedição responsável pela descoberta do cilindro. O artefato foi criado após a conquista persa da Babilônia em 539 a.C., quando o exército persa, sob Ciro, o Grande, invadiu e conquistou o império caldeu, trazendo-o sob o controle do Império Persa. (...) O Cilindro também foi interpretado por alguns estudiosos como um "precursor da carta de direitos humanos", embora o Museu Britânico e outros estudiosos rejeitem tal interpretação como sendo anacrônica e equivocada.

19 Cf. REINO UNIDO, "*Declaração de Direitos de 1689, considerando que o falecido Rei Jaime II, com a ajuda de diversos maus conselheiros juízes e ministros empregados por ele, empenhou-se em destruir e extirpar a religião protestante, e as leis e liberdades deste reino",* 1689, declaração disponível em http://www.direitoshumanos.usp.br/index.php/Documentos-anteriores-%C3%A0-cria%C3%A7%C3%A3o-da-Sociedade-das-Na%C3%A7%C3%B5es-at%C3%A9-1919/a-declaracao-inglesa-de-direitos-1689.html [25.09.2019].

da Inglaterra, a Declaração dos Direitos do Homem e do Cidadão de 1789[20], da França e, por fim, a Carta de Direitos de 1791[21], dos Estados Unidos.

Na intenção de se criar uma missão da manutenção da paz por parte da Liga das Nações, em 1945, foi criada uma nova organização internacional, a Organização das Nações Unidas (ONU), que, por meio de uma Carta, reforçou a necessidade de integração e internacionalização de garantias e direitos a todos os cidadãos, momento em que a humanidade presenciou a normatização e a internacionalização da proteção dos direitos humanos, tendo como marco inicial o reconhecimento e valoração da Carta das Nações Unidas.

A Carta das Nações Unidas[22] trouxe, em seu texto, reconhecimento a uma classe de direitos universais, tratadas como direitos humanos. O texto legal da carta, no ponto 3 do artigo 1.º, declara um dos propósitos da ONU, que é: "[c]onseguir uma cooperação internacional para resolver os problemas internacionais de caráter econômico, social, cultural ou humanitário, e para promover e estimular o respeito aos direitos humanos e às liberdades fundamentais para todos, sem distinção de raça, sexo, língua ou religião".

Mais adiante, ainda na mesma Carta, em seu artigo 56, disciplina a necessidade de os Estados-parte da Organização tomarem ações individualmente e em parceria com a ONU para atingir os objetivos já determinados no artigo 55, os quais se tratam, em linhas gerais, de direitos humanos, sem distinção de qualquer espécie ou território de origem. Por meio dos artigos 55 e 56, esses direitos ficaram conhecidos como *golden thread – fio dourado* –, o que indica que os direitos humanos seriam uma matéria digna da preocupação global, e que as ações de cada Estado estariam limitadas a obrigações legais exigíveis perante a comunidade internacional.

A partir disso, vários movimentos deram o pontapé no intuito da proteção dos direitos humanos, não somente para os povos que sofreram diretamente durante a guerra, mas a fim de assegurar direitos a nível mundial.

---

20 Cf. FRANÇA, "*Declaração dos Direitos do Homem e do Cidadão de 1789, (...) o esquecimento ou o desprezo dos direitos do homem são as únicas causas dos males públicos e da corrupção dos Governos, resolveram declarar solenemente os direitos naturais, inalienáveis e sagrados do homem, a fim de que esta declaração, sempre presente em todos os membros do corpo social, lhes lembre permanentemente seus direitos e seus deveres; a fim de que os atos do Poder Legislativo e do Poder Executivo, podendo ser a qualquer momento comparados com a finalidade de toda a instituição política, sejam por isso mais respeitados (...)*", 1789, declaração disponível em http://www.direitoshumanos.usp.br/index.php/Documentos-anteriores-%C3%A0-cria%C3%A7%C3%A3o-da-Sociedade-das-Na%C3%A7%C3%B5es-at%C3%A9-1919/declaracao-de-direitos-do-homem-e-do-cidadao-1789.html [25.09.2019].

21 Cf. ESTADOS UNIDOS DA AMÉRICA, Carta dos Direitos dos Estados Unidos de 1789, *"A Carta de Direitos é formada pelas dez primeiras Emendas à Constituição dos Estados Unidos da América. Foi redigida pelo Congresso dos EUA em 1789 e ratificada pelos estados em 15 de dezembro de 1791"*, 1789, texto disponível em http://www.dhnet.org.br/direitos/anthist/marcos/carta_direitos_eua_1789.htm [25.09.2019].

22 Cf. CARTA DAS NAÇÕES UNIDAS, *Organização das Nações Unidas - ONU*, 1945, texto disponível em https://nacoesunidas.org/wp-content/uploads/2017/11/A-Carta-das-Na%C3%A7%C3%B5es-Unidas.pdf [25.09.2019]

Assim, a Declaração Universal dos Direitos Humanos (DUDH) começou a ser pensada quando o mundo ainda estava sobre os efeitos da guerra.

Após a Segunda Grande Guerra Mundial (1939 – 1945) o mundo tomou conhecimento das maiores atrocidades cometidas pela Alemanha nazista, e percebeu-se então que a Carta das Nações Unidas não tinha definido suficientemente os direitos a que se referia[23]. De forma latente, restou claro que uma declaração universal deveria existir e que essa deveria especificar os direitos individuais.

Foi a partir desse momento que a Declaração Universal dos Direitos Humanos (DUDH) começou a ser pensada, quando o mundo ainda sentia os efeitos negativos da Segunda Grande Guerra Mundial, que se findou em 1945.

A ideia foi apresentada na primeira Assembleia Geral das Organizações das Nações Unidas (ONU), no ano de 1946, sendo repassada à comissão de Direitos Humanos ainda no mesmo ano, para que encabeçasse o início de uma Declaração Internacional de Direitos Humanos.

No ano de 1947, durante a primeira sessão da comissão de Direitos Humanos presidida por Eleanor Roosevelt (viúva do presidente americano Franklin D. Roosevelt), fora elaborado, pelos membros da comissão[24], um "rascunho preliminar da Declaração Internacional dos Direitos Humanos".

Importante salientar que, à época, a comissão dos direitos humanos já era um braço das Nações Unidas, e foi constituída para começar o trabalho daquilo que foi inicialmente recebido apenas como uma Carta de Direitos.

Em setembro do ano de 1948 foi apresentado o rascunho final da DUDH, o qual contou com a ajuda na sua elaboração de mais de 50 (cinquenta) países.

Com 48 (quarenta e oito) votos a favor, nenhum voto contra e 8 (oito) abstenções[25], em 10 de dezembro de 1948, a Declaração Universal dos Direitos Humanos (DUDH) foi adotada pela Assembleia Geral.

Urge reconhecer a importância desses acontecimentos para a judicialização dos crimes contra a humanidade no plano internacional com a criação do sistema global de proteção internacional dos

---

23 Cf. UDHR50, National Coordinating Committee for, "*Didn't Nazi tyranny end all hope for protecting human rights in the modern world? ",* Franklin and Eleanor Roosevelt Institute, 1998, texto disponível em https://archive.is/20120919000037/http://www.udhr.org/history/overview.htm#selection-553.0-553.43 [25.09.2019]

24 Membros de vários países foram designados para representar a comunidade global: Austrália, Bélgica, República Socialista Soviética da Bielorrússia, Chile, China, Cuba, Egito, França, Índia, Irã, Líbano, Panamá, Filipinas, Reino Unido, Estados Unidos, União das Repúblicas Socialistas Soviéticas, Uruguai e Iugoslávia. Membros conhecidos incluíam Eleanor Roosevelt dos Estados Unidos (esposa de Franklin D. Roosevelt), Jacques Maritain e René Cassin da França, Charles Malik do Líbano e P. C. Chang da China, entre outros.

25 As abstenções se deram pelos seguintes países (em sua maior parte do bloco soviético: Bielorrússia, Tchecoslováquia, Polônia, Ucrânia, União Soviética e Iugoslávia, além da África do Sul e Arábia Saudita.

direitos humanos. Assim, foi somente por meio da Declaração Universal dos Direitos Humanos (DUDH), de 1948, que se inaugurou a fase de positivação e universalização dos direitos humanos.

1.1. Do direito fundamental à vida privada na declaração universal dos direitos humanos (DUDH) de 10 de dezembro de 1948

Certamente a adoção da Declaração Universal dos Direitos Humanos em 1948 pela Assembleia Geral das Nações Unidas foi um divisor de águas no mundo jurídico, isso porque, através dela, houve, além do reconhecimento universal de uma carta de direitos considerados como básicos a qualquer individuo, a imposição desses direitos frente ao abuso cometido pelos Estados e/ou seus líderes. Desse modo, historicamente, foi e ainda é um documento precursor para os direitos humanos a nível internacional.

Desde a sua proclamação em 10 de dezembro de 1948, em Paris, na Assembleia Geral das Nações Unidas, a DUDH fora traduzida em mais de 500 idiomas[26], sendo considerado o documento com mais traduções no mundo[27].

Zeid Ra'ad Al Hussein (alto-comissário dos Direitos Humanos das Nações Unidas entre os anos de 2014 á 2018), assinala que o número crescente dessas traduções representa "o poder de suas palavras em ressoar poderosamente por todas as culturas e línguas[28]".

Reafirmado logo no preâmbulo da DUDH, a dignidade da pessoa humana é inalienável e constitui fundamento para a liberdade de todos e a garantia da justiça e paz no mundo. A DUDH é composta por 30 artigos que reconhecem e instituem os direitos fundamentais, ou seja, direitos básicos, que devem alcançar a todos, sem distinção em razão da origem, raça, cor, etnia ou religião. Conforme dispõe seu artigo I "[t]odos os seres humanos nascem livres e iguais em dignidade e direitos."

Corrobora ainda em seu artigo II, n.º 1, que o direito à igualdade abrange de modo geral a todos os indivíduos, isso porque dispõe que não haverá "distinção de qualquer espécie, seja de raça, cor, sexo, idioma, religião, opinião política ou de outra natureza, origem nacional ou social, riqueza, nascimento,

---

26 "*A Declaração Universal dos Direitos Humanos ganhou uma versão inédita no dialeto da língua indígena quechua falado por cerca de 116 mil pessoas no noroeste da Bolívia. Com a nova tradução oficial, o documento – que já era o mais traduzido em todo o mundo – está disponível em 501 idiomas".* Cf. NAÇÕES UNIDAS DO BRASIL, *"Declaração Universal dos Direitos Humanos está disponível em mais de 500 idiomas",* in Nações Unidas Brasil, 2016, texto disponível em https://nacoesunidas.org/declaracao-universal-dos-direitos-humanos-esta-disponivel-em-mais-de-500-idiomas/ [25.09.2019]

27 *"Em novembro de 1999, a instituição Guinness World Records afirmou que o texto era o documento mais traduzido no planeta, com um total de versões em 298 línguas à época. A certificação do organismo foi atualizada em 2009, quando o número de traduções chegou a 370".* Cf. NAÇÕES UNIDAS DO BRASIL, "*Declaração Universal dos Direitos...", op. cit.*

28 Cf. NAÇÕES UNIDAS DO BRASIL, "*Declaração Universal dos Direitos...", op. cit.*

ou qualquer outra condição". No n.º 2, ainda do artigo II, dispõe que o direito à igualdade deverá ultrapassar barreiras físicas, governos e até mesmo a condição política.

O artigo III reforça que o direito à vida é universal e através desse direito, o Estado deve garantir a todo ser humano, independente de sua origem, a sua liberdade e sua segurança pessoal.

Nos artigos IV ao XI percebe-se que a declaração de Direitos Humanos se preocupou em defender direitos universais que viessem proteger cada indivíduo frente a grande disparidade opressiva entre o abuso de poder do Estado, criando meios jurídicos pelo quais os lesados pudessem se valer de um devido processo legal e de um julgamento imparcial.

Como marco inicial da história do Direito à Proteção de Dados pessoais, nos importa apresentar o primeiro artigo que veio reconhecer a necessidade de proteção da identidade do ser humano, assim como as informações que lhe digam respeito, as situações relacionadas a sua vivência, suas comunicações e pessoas com quem se relaciona e o rodeiam.

O primeiro artigo inserido no rol de direitos humanos, como um direito fundamental que visava a proteção ora suscitada, foi o artigo XII que assim dispõe: "Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques."

No artigo citado, a declaração previu a existência de direitos que protegessem de fatores externos (ou terceiros) a personalidade do individuo como um todo, mesmo ante a complexidade que isso viesse representar. Para tanto, a declaração reconheceu um rol de direitos específicos, sendo eles: à vida privada; à intimidade; à honra e reputação; e à inviolabilidade do seu lar e comunicações, sendo apresentado de fato no artigo como a terminologia de correspondência, em razão de ser essa uma das poucas formas de trocar informações à época, uma vez que não era imaginado a internet como meio primordial de comunicações como atualmente o é.

Conforme se extrai do artigo XII, desde logo, o legislador se preocupou em apresentar a vida privada como um objeto diferente da intimidade, ainda que *prima facie*, a intimidade aparenta estar inserida de forma mais profunda dentro da vida privada. Contudo, importante expor que se trata de direitos de abrangência distinta que mais adiante será explanado. Esse artigo, de grande importância a esta dissertação – uma vez que se revela precursor da existência de um direito que nos dias atuais visa à proteção de dados pessoais – se revelou como um direito humano fundamental ligado à privacidade do indivíduo.

O direito apresentado no artigo XII da Declaração Universal dos Direitos Humanos de 1948 reflete a positivação da privacidade do individuo como um valor em si, que faz parte do desenvolvimento da sua

personalidade, apresentando-o como um ser dotado de direitos que visam compor a dignidade da pessoa humana. De modo mais profundo, o artigo XII veio relevar também a necessidade de proteção da intimidade do indivíduo, uma vez que ela é essencial para a realização da plenitude da dignidade da pessoa humana.

Nesse sentido, em meio ao caos que o mundo vivia pós segunda Guerra Mundial, assim como as pressões e opressões pelo Estado através das violações de direitos, era no lar de cada indivíduo que se encontrava seu refugio. Anos depois, a jurisprudência americana reconheceu como uma garantia constitucional o "*right to be alone*[29]" – ou seja, o direito de estar só, a fim de que o individuo tivesse espaço em meio à sociedade para tomar suas decisões e guardar para si aquilo que julga ser intimo e pessoal.

Dessa forma, o direito à vida privada, ou seja, à privacidade em si, passou a permitir que o indivíduo mantenha sob sua vontade (exclusiva) a exposição ou a omissão de qualquer conjunto de informações a seu respeito – sobre quem, onde, quando ou em que condições.

Muito embora as declarações não tenham força para coagir e/ou coibir, por serem meramente proclamadas, a Declaração Universal dos Direitos Humanos adquiriu relevância de costume internacional, o que a revestiu como norma vinculativa e, portanto, exigível perante à comunidade internacional. É oportuno salientar que, no sexto parágrafo do preâmbulo da DUDH, o conteúdo do artigo 56 da Carta da ONU é citado e reiterado para reconhecimento de direitos em caráter universal.

Vários outros documentos e tratados internacionais sobre o tema de direitos humanos que dizem respeito ao direito fundamental à vida privada, foram elaborados pela ONU, merecendo destaque o Pacto Internacional dos Direitos Civis e Políticos – PIDCP.

1.2. Do direito fundamental à vida privada no pacto internacional dos direitos civis e políticos (PIDCP), de 16 de dezembro de 1966

Em 1966, 18 (dezoito) anos depois da adoção na Assembleia Geral das Nações Unidas da DUDH, no auge da Guerra Fria, surge o Pacto Internacional dos Direitos Civis e Políticos (PIDCP)[30], com

29 *"The right to privacy is, as a legal concept, a fairly recent invention. It dates back to a law review article published in December of 1890 by two young Boston lawyers, Samuel Warren and Louis Brandeis*". Cf. GLANCY, Dorothy J., "*The Invention of the Right to Privacy*", Arizona Law Review, 1979, v. 21, nº. 21, pp. 1–39, texto disponível em https://web.archive.org/web/20100722230541/http://law.scu.edu/site/dorothy-glancy/File/Privacy.pdf [25.09.2019]

30 Cf. ORGANIZAÇÃO DAS NAÇÕES UNIDAS, "*Pacto Internacional dos Direitos Civis e Políticos – PIDCP, de 16 de dezembro de 1966, (...) Reconhecendo que estes direitos derivam da dignidade inerente à pessoa humana; Reconhecendo que, de acordo com a Declaração Universal dos Direitos do Homem, não se pode realizar o ideal do ser humano livre, gozando das liberdades civis e políticas, libertos do terror e da miséria, a menos que se criem condições que*

o intuito de reafirmar e dar legalidade internacional ao rol de Direitos Fundamentais descrito na DUDH, entretanto, condicionado à obrigatoriedade através de sua ratificação por Estados que o reconheça e se comprometa a cumpri-lo.

No que tange ao PIDCP, muito embora tenha sido aprovado em 1966, somente entrou em vigor na ordem jurídica internacional no ano de 1976, isso porque, de acordo com os termos do seu artigo 49[31], o presente pacto só entraria em vigor e teria eficácia três meses após o 35º (trigésimo quinto) instrumento de ratificação ou adesão.

Ante a grande importância do Pacto Internacional dos Direitos Civis e Políticos – PIDCP, não desmerecendo os artigos que tratam dos demais direitos fundamentais – merecedores de igual importância de estudo –, a essa dissertação importa expor o disposto no artigo 17, que assim diz:

> "1. Ninguém poderá ser objetivo de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais às suas honra e reputação.
>
> 2. Toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas."

Pelo que se demonstra cristalino, o ponto 1 do artigo 17 do PIDCP vem reafirmar o direito fundamental à vida privada tratado no artigo XII da DUDH, assim como os direitos inerentes a ele, tais como o direito à intimidade, ao sigilo das correspondências, dentre outros.

O que se percebe é que, a todo tempo, mesmo durante os períodos turbulentos vivenciados por uma parcela da população mundial diante do quase nulo direito à vida privada, quando da elaboração da DUDH até o PIDCP, à proteção a vida privada tornou-se ponto de partida para garantir de fato a dignidade da pessoa humana, que, à época se via fragilizada por falta de normatização desse direito pelo legislador.

Em decorrência do período vivenciado pelo Brasil durante a Ditadura Militar[32] (1964 – 1985), momento de repressão de direitos da maioria, não sendo a vida privada um direito assistido a todos, o PIDCP não fora ratificado logo no início de seu reconhecimento a nível internacional em 1976.

---

permitam a cada pessoa gozar dos seus direitos civis e políticos, assim como dos seus direitos económicos, sociais e culturais, (...)", texto disponível em http://www.cne.pt/content/onu-pacto-internacional-sobre-os-direitos-civis-e-politicos [25.09.2019].

31 "*ARTIGO 49 – 1. O presente Pacto entrará em vigor três meses após a data do depósito, junto ao Secretário-Geral da Organização das Nações Unidas, do trigésimo-quinto instrumento de ratificação ou adesão. 2. Para os Estados que vierem a ratificar o presente Pacto ou a ele aderir após o deposito do trigésimo-quinto instrumento de ratificação ou adesão, o presente Pacto entrará em vigor três meses após a data do deposito, pelo Estado em questão, de seu instrumento de ratificação ou adesão".*

32 "*Ditadura Militar foi o período da história brasileira que se estendeu de 1964 a 1985. Esse regime foi instaurado no poder de nosso país por meio de um golpe organizado tanto pelos meios militares quanto pelos civis. Esse golpe visou à derrubada do presidente João Goulart e deu início a um período de 21*

Na verdade, o Brasil somente ratificou o Pacto, quando seus principais direitos já se encontravam resguardados pela atual CRFB de 1988, em seu título II, intitulado como "Dos Direitos e Garantias Fundamentais", que, mais adiante será explanado.

O PIDCP, fora aprovado através do Decreto-Legislativo n.º 226[33], em 12 de dezembro de 1991, tendo o Brasil depositado sua Carta de Adesão junto à Secretária Geral da Organização das Nações Unidas em 24 de janeiro de 1992 e que, por força do artigo 49, entrou em vigor em 24 de abril do mesmo ano.

Muito embora já houvesse previsão legal na CRFB de 1988 de Direitos e Garantias Fundamentais inerentes a vida privada, foi somente a partir da implementação do PIDCP que o Brasil se tornou legalmente responsável pela aplicabilidade do direito à vida privada, direito esse já consagrado por outros tratados e a nível internacional.

Independente do tempo da aplicabilidade e da mudança de conduta de cada Estado Membro, o que realmente interessa é o compromisso assumido para assegurar direitos humanos. Certamente o Pacto Internacional dos Direitos Civis e Políticos, assim como a DUDH, teve sua devida importância por consagrar o direito à vida privada como um direito com garantia fundamental.

1.3. Da natureza jurídica dos direitos fundamentais – direito materialmente constitucional e formalmente constitucional

Atualmente, os direitos fundamentais dentro do ordenamento jurídico brasileiro são considerados como cláusulas pétreas[34], isto é, não podem ser suprimidos nem por emenda à constituição. Contudo, mesmo sendo considerados como cláusulas pétreas, esses direitos não são absolutos, pois, se fossem, em caso de conflito – fato rotineiro em um Estado democrático de direito –, seria impossível resolver tal conflito.

---

anos marcado pelo autoritarismo e pela repressão realizada pelo Estado. Encerrou-se em 1985, quando Tancredo Neves foi eleito presidente do Brasil". Cf. SILVA, Daniel Neves, *Ditadura Militar*, Brasil Escola, S/d, texto disponível em https://brasilescola.uol.com.br/historiab/ditadura-militar.html [07.08.2019].

33 Cf. BRASIL, *Decreto Legislativo nº 226, 12 de dezembro de 1991, "Aprova os textos do Pacto Internacional sobre Direitos Civis e Políticos e do Pacto Internacional sobre Direitos Econômicos, Sociais e Culturais, ambos aprovados, junto com o Protocolo Facultativo relativo a esse último pacto, na XXI Sessão (1966) da Assembléia-Geral das Nações Unidas",* texto disponível em https://www2.camara.leg.br/legin/fed/decleg/1991/decretolegislativo-226-12-dezembro-1991-358251-exposicaodemotivos-146136-pl.html [25.09.2019].

34 *"Dispositivo constitucional que não pode ser alterado nem mesmo por Proposta de Emenda à Constituição (PEC). As cláusulas pétreas inseridas na Constituição do Brasil de 1988 estão dispostas em seu artigo 60, § 4º. São elas: a forma federativa de Estado; o voto direto, secreto, universal e periódico; a separação dos Poderes; e os direitos e garantias individuais".* Cf. SENADO FEDERAL, "*Cláusula pétrea",* Agência Senado, texto disponível em https://www12.senado.leg.br/noticias/glossario-legislativo/clausula-petrea [10.02.2019].

É inegável que direitos fundamentais são essenciais para garantir o mínimo de dignidade à pessoa humana, e por esse motivo são considerados como direitos indisponíveis, ou seja, não se pode dele abrir mão.

Neste diapasão, segue o disposto na Jurisprudência do Supremo Tribunal Federal (STF), RMS 23.452/RJ[35]:

> "Os direitos e garantias individuais não têm caráter absoluto. Não há, no sistema constitucional brasileiro, direitos ou garantias que se revistam de caráter absoluto, mesmo porque razões de relevante interesse público ou exigências derivadas do princípio de convivência das liberdades legitimam, ainda que excepcionalmente, a adoção, por parte dos órgãos estatais, de medidas restritivas das prerrogativas individuais ou coletivas, desde que respeitados os termos estabelecidos pela própria Constituição. O estatuto constitucional das liberdades públicas, ao delinear o regime jurídico a que estas estão sujeitas – e considerado o substrato ético que as informa – permite que sobre elas incidam limitações de ordem jurídica, destinadas, de um lado, a proteger a integridade do interesse social e, de outro, a assegurar a coexistência harmoniosa das liberdades, pois nenhum direito ou garantia pode ser exercido em detrimento da ordem pública ou com desrespeito aos direitos e garantias de terceiros".

Nesse sentido, o interesse público estará sempre adstrito ao princípio do bem comum, como um dos principais vetores para a limitação dos direitos fundamentais.

Muito embora a regra da consagração de um direito fundamental só aconteça através da sua positivação na carta de direitos fundamentais de um Estado – conhecido assim como um direito formalmente constitucional –, é de todo oportuno expor que o reconhecimento a um direito fundamental também pode se dar mesmo quando não estiver disposição na carta magna, sendo assim reconhecido como um direito materialmente constitucional.

Quando se expõe que aquele direito em específico tem reconhecimento como um direito materialmente constitucional, isso quer dizer que a sua essência, substância e seu conteúdo é naturalmente constitucional. Desse modo, pode-se dizer que um direito materialmente constitucional é

35 Cf. SUPREMO TRIBUNAL FEDERAL – STF, "*Mandado de Segurança nº 23452 RJ, Relator: Celso de Mello, Data de Julgamento 16/09/1999, Tribunal Pleno, Data de Publicação: Dj 12-05-2000, PP-00020 Ement. Vol-01990-01 PP-00086*", texto disponível em https://stf.jusbrasil.com.br/jurisprudencia/738746/mandado-de-seguranca-ms-23452-rj [25.09.2019].

aquele que, em decorrência da sua importância, tem o reconhecimento equiparado a um direito formalmente constitucional, com a única diferença de não estar positivado – ainda.

Mesmo que não haja previsão constitucional, essas normas, devido a sua própria natureza, encontram-se implícitas no texto constitucional através de outros direitos. É o caso por exemplo do Direito à Proteção de Dados Pessoais, que, em decorrência dos direitos à vida privada, à intimidade e outros – já positivados rol de direitos e garantias fundamentais do artigo 5.º da CRFB de 1988 –, apresenta-se implícito no texto constitucional.

Entretanto, há de se expor que o Direito à Proteção de Dados Pessoais carrega, desde o inicio, uma dimensão jusfundamental, ou seja, independente de uma disposição formal, foi, é, e sempre será considerado como um direito com garantias fundamentais.

Contudo, é de todo oportuno expor que, mesmo que esse reconhecimento se dê de forma implícita – como dito a respeito do direito à vida privada, à intimidade e outros –, são direitos distintos e merecem igual atenção pelo legislador devido sua importância como um direito estritamente fundamental à dignidade da pessoa humana, o que justifica a necessidade da sua consagração.

Explanado o que é o direito materialmente constitucional, cabe agora expor o que se entende por direito formalmente constitucional. O direito constitucional formal, ou seja, as normas formalmente constitucionais são aquelas que estão formalizadas na constituição de um Estado, independente do seu conteúdo, essência ou substância.

De outra ótica – mais fácil de se assimilar –, são aquelas normas positivadas na carta magna de um Estado, que, por sua natureza, passam por um processo específico de elaboração, votação e aprovação pelo poder legislativo, que posteriormente são solenemente publicadas, para só então ter eficácia em certo ordenamento jurídico de um Estado. Dessa forma, são unicamente explicitas.

Exposto a natureza jurídica dos direitos fundamentais, bem como a diferença entre um direito materialmente constitucional de um direito formalmente constitucional, agora se faz necessário apresentar a origem do Direito à Proteção de Dados Pessoais e de que forma esse direito se encontra disposto no ordenamento jurídico brasileiro.

2. Da origem do direito à proteção de dados pessoais

O assunto relacionado à proteção da privacidade e dos dados pessoais tem, cada vez mais, sido palco de grandes discussões. A importância de se discutir tal assunto – legalmente falando – se justifica, pois, a sociedade vive constantemente desafiada a caminhar por caminhos novos frente as novas

questões relacionadas a informação digital e a tecnologia, sendo esse o atual panorama vivenciado pela sociedade mundial.

A importância de se discutir sobre temas relacionados à privacidade dos usuários no mundo digital tem gerado varias dúvidas acerca da existência de uma lei que viesse efetivamente trazer proteção a aqueles que dela precisam.

Ordinariamente, com o intuito de se ganhar o mercado e criar uma base sólida, bem como uma forma de aferir lucros, várias empresas no Brasil (e no mundo) coletam e tratam dados pessoais da forma que bem entendem, sem uma lei – por lei entende-se um regimento próprio e atual – que venha disciplinar a proteção desses dados, principalmente quando essas ações acontecem no meio digital, ou seja, na internet.

Até o presente momento, na história do direito à proteção de dados pessoais no Brasil, não havia uma política efetiva de proteção que pudesse tutelar os dados pessoais, isso porque, formalmente falando, a carta magna nunca tratou sobre o tema de forma explicita reconhecendo a dimensão jusfundamental desse direito.

Contudo, imperioso é destacar que, muito embora a letra da lei nunca tivesse tratado de forma clara a respeito de um direito à proteção de dados pessoais, desde o inicio do percurso jurídico constitucional brasileiro, tal direito já se fazia presente, porém de forma implícita, em decorrência da existência de um direito e garantia fundamental relacionado à vida privada de cada brasileiro.

Dessa forma, não é difícil expor e assimilar que as questões atuais que envolvem problemas relacionados à privacidade dos usurários da internet, têm, de fato, eficácia horizontal através de efeitos fundamentais ligados a direitos da personalidade, especialmente àqueles direitos relacionados à proteção da privacidade e da intimidade, bem como ao direito ao esquecimento, sigilo nas correspondências e troca de informações, dentre outros, que acabam por trazer à baila, com um enfoque constitucional, o direito à proteção de dados pessoais.

Desse modo, certo é assinalar que o ponto precursor do direito à proteção de dados pessoais foi a consagração do direito à vida privada, desde a DUDH, o PIDCP e as primeiras cartas magnas brasileiras como um direito com garantia fundamental, linha histórica que que agora passa-se a explanar.

2.1. Do direito fundamental à vida privada e o que ele tutela

É cediço que a personalidade de uma pessoa é composta por um conjunto de características, tanto internas (em sentido emocional), quanto externas (em sentido aparente). O ser humano é

individualizado pelo nome, raça, gostos, religião, idade, dentre outras características. Essas constitutivas se externam de acordo com sua manifestação na sociedade e cria assim uma personalidade única ante os demais.

O direito à vida privada, desde o inicio, foi pensado pelo legislador para abranger a tutela da privacidade, da honra, da intimidade e da imagem das pessoas. Porém, na prática, direitos como à privacidade e à intimidade são distintos, ainda que muito parecidos, mas, conforme aponta DOTTI, a intimidade se caracteriza como "a esfera secreta da vida do indivíduo na qual este tem o poder legal de evitar os demais[36]".

Para COSTA JUNIOR, "a expressão 'direito à intimidade' tutela dois interesses, que se somam: o interesse de que a intimidade não venha a sofrer agressões e o de que não venha a ser divulgada. O direito, porém, é o mesmo. (...) No âmbito do direito à intimidade, portanto, podem ser vislumbrados estes dois aspectos: a invasão e a divulgação não autorizada da intimidade legitimamente conquistada[37]".

Sendo assim, a intimidade se apresenta como uma esfera ainda mais reservada do que a privacidade em si, ou seja, como um direito ainda mais sensível, mais oculto, merecendo assim igual importância pela lei.

O reconhecimento ao direito à intimidade possibilita cada indivíduo o poder de optar por deixar à mostra algo seu ou impossibilitar essa exposição. Como a intimidade reflete a essência de cada indivíduo, ela integra sua orientação sexual, religião, partido político, preferências sociais de demais características que geralmente são formadoras de grupos e/ou oposições sociais.

Contudo, há aqueles que ainda tratam a privacidade e a intimidade como esferas da vida privada, como por exemplo SILVA, que defende que a vida privada é aquela que "integra a esfera íntima da pessoa, porque é repositório de segredos e particularidades do foro moral e íntimo do indivíduo[38]".

Diferentemente de dessa parte da doutrina, a legislação brasileira atual, ao tratar sobre o direito à intimidade e à vida privada, os apresenta como direitos distintos, ambos como direitos e garantias fundamentais, mas entrelaçados, ou seja, não há como se falar em intimidade sem mencionar a vida privada.

Desse modo percebe-se que o legislador teve o interesse de defender a ideia de que a vida do indivíduo compreende dois aspectos: o primeiro voltado para o interior (deixar expor ou preferir omitir

36 Cf. DOTTI, René Ariel, *Proteção da Vida Privada e Liberdade de Informação*, São Paulo, Revista dos Tribunais, 1980, p. 27.

37 Cf. COSTA JÚNIOR, Paulo José da, *O direito de estar só: tutela penal da intimidade,* São Paulo, Revista dos Tribunais, 1995, p. 34.

38 Cf. SILVA, José Afonso da, *Curso de Direito Constitucional Positivo,* São Paulo, Editora Malheiros, 38ª ed., 2014, p. 210.

certas informações acerca de si a terceiros ou ao próprio Estado); já o segundo aspecto é voltado para o exterior (membros da família e amigos), alegando que esse aspecto é inviolável.

O direito à vida privada teve então por preocupação principal proteger o direito à privacidade em si, de maneira abrangente, incluindo ainda os segredos que essa vida privada pode reservar, no intuito de protegê-la de terceiros e até mesmo do próprio Estado, uma vez que tais "segredos" compreendem ainda a expansão da personalidade de cada indivíduo, e reforça a ideia de que não podem sofrer os atentados (violações) de exposição indevida (levar ao conhecimento de terceiros eventos relevantes da vida pessoal e familiar) e da investigação (pesquisa de acontecimentos referentes à vida pessoal e familiar).

Muito embora, por anos, esse direito efetivamente tivesse trazido proteção aos brasileiros no que tange à privacidade da sua vida, em face da atual mudança global frente as novas tecnologias de informação, a internet e a inteligência artificial, ou seja, pela facilidade de acesso aos dados pessoais, esse direito encontra-se enfraquecido (por enfraquecido entende-se que não tem efetividade na tutela dos dados pessoais).

Tendo em vista a mudança na forma de relacionamento entre as pessoas frente a internet – isso por que há uma maior facilidade de acesso a informações pessoais –, nunca se fez tão necessário reconhecer a existência de um direito que que venha tutelar especificamente os dados pessoais, uma vez que o objeto de proteção dos direitos à intimidade e à privacidade não são os mesmos. Como o objeto em si a ser tutelado é os dados do próprio titular, e por esses integrarem a sua personalidade, não há como não reconhecer a sua dimensão jusfundamental.

2.2. Do direito à proteção de dados pessoais como um direito fundamental autônomo

Há muito se questiona sobre a efetividade do direito à privacidade e/ou direito à intimidade em relação à proteção de dados pessoais, uma vez que, por se tratar de institutos diversos, poderiam esses direitos tutelar o tratamento e guarda de dados pessoais?

Enquanto o direito à privacidade tutela as esferas intimas que envolvem a vida privada, o direito à proteção de dados pessoais, por sua vez, vem tutelar as informações pessoais que não são privadas, que, além de proteger de terceiros que poderiam vir a expor informações a seu respeito, com ou sem consentimento quando do tratamento dos seus dados pessoais, ter o direito de optar se tais dados podem ou não se tornar de conhecimento público, ou transferi-los para fins comerciais.

Conforme explanado até aqui – assunto ainda que será guerreado até o fim desta dissertação – os institutos relacionados à privacidade, à intimidade ou à vida privada diferem-se dos dados pessoais, isso porque, o objeto de proteção aqui engloba todas as informações que constroem o individuo e não somente as informações que são classificadas como privadas.

Antes mesmo da adoção da terminologia legal do Direito à Proteção de dados pessoais, já existia um direito análogo a este, o direito à vida privada (ventilados pela Carta da ONU na DUDH e por tratados internacionais como PIDCP, CADH entre outros), que por muito tempo foi utilizado pelo legislador para tutelar todas as esferas da privacidade e a intimidade, bem como a tudo que ela incluísse, a saber, violação de segredos, orientação sexual, situação familiar, casamento, dados pessoais, dentre outros.

Como dito alhures, a definição de Dado Pessoal poderia ser expressa como toda e qualquer informação ou conjunto de informações ligadas a uma pessoa singular pode identificá-la ou torná-la identificável por associação de conceitos e conteúdos. Esse conjunto de informações, por mais que se assemelhe com informações de outros indivíduos, quando agrupadas, criam uma identidade única e distinta das demais, assim como um DNA ou como um código de barras, que reconhece e passa a identificar aquela pessoa em específico.

As características comuns (internas e externas) aos indivíduos, tais como, nome e sobrenome, orientação sexual, religião, partido político, endereço de sua residência ou do seu trabalho, endereço de e-mail, número do Registro Geral (RG), número do Cadastro de Pessoas Físicas (CPF), Ips (protocolo de internet) do smartphone ou notebook, Cookies (rastros de sites acessados), número de telefone fixo ou móvel, dados médicos, dados trabalhistas, dados relativo à família, previdência social, nome em redes sociais, dentre outros, são dados pessoais que identificam uma pessoa em específico, ou seja, como a expõe como única. A importância do reconhecimento de um Direito à Proteção de Dados Pessoais tem como finalidade proteger a pessoa contra as ameaças derivadas do seu tratamento e uso indevido de seus dados por terceiros.

A definição de Dados Pessoais, inicialmente, não foi encontrada em doutrinas ou leis brasileiras, pelo contrário, o conceito legal de Dados Pessoais, tal qual conhecemos, vem de outro continente, e se encontra presente na Diretiva Europeia 95/46/CE, de 24 de abril de 1995, em seu artigo 2º, letra a. Vejamos:

> "«Dados pessoais», qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»); é considerado identificável todo aquele que possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais

> elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social".

O conceito normativo revela que "dados pessoais" são todas aquelas informações pessoais, que possuem ligação direta com uma pessoa específica, desse modo, cristalino é reconhecer que esse direito merece amparo legal, ou seja, a tutela do poder público, uma vez que o objeto do qual trata o direito é a própria pessoa em causa e sua individualidade. Portanto, o reconhecimento desse instituto como um direito autônomo tem como finalidade a preservação da sua própria personalidade.

Quando a Diretiva 95/46/CE, de modo inaugural, veio explanar um conceito de dados pessoais ainda na década de 90, a realidade enfrentada – mesmo já existindo a internet – era diversa da vivenciada atualmente, motivo esse que, a diretiva visou de modo abrangente a proteção de dados pessoais em relação ao dono e seu uso por terceiro ou pelo próprio Estado independente do meio do seu tratamento.

Contudo, levando em consideração a experiência vivida a nível global em relação ao uso da internet e das tecnologias de informação, há necessidade iminente do reconhecimento de um direito atual e específico, que venha tutelar os dados pessoais, principalmente na internet, uma vez que atualmente seu processamento é realizado por meio eletrônico – via internet – e são ilimitadamente armazenados, podendo ser consultados a qualquer momento, em diferentes locais do globo em segundos e sem nenhuma restrição.

Para os tribunais brasileiros as discussões a respeito de um direito específico à proteção de dados pessoais não aconteceram de forma tão precoce quanto na União Europeia. O primeiro registro que menciona dados pessoais junto as jurisprudências do Superior Tribunal de Justiça (STJ) brasileiro, é datado de 18/10/2001, e apresenta esse direito como pertencente a esfera da privacidade, como um sem autonomia, ou seja, vinculado e/ou dependente. Vejamos:

> "EXECUÇÃO – REQUISIÇÃO DE INFORMAÇÃO DE ENDEREÇO DO RÉU AO BANCO CENTRAL – IMPOSSIBILIDADE. 1. Embora na hipótese dos autos não se pretenda, através de requisição ao Banco Central, obter informações acerca de bens do devedor passíveis de execução, mas tão-somente o endereço, o raciocínio jurídico a ser adotado é o mesmo. 2. *O contribuinte ou o titular de conta bancária tem direito à privacidade em relação aos seus dados pessoais,* além do que não cabe ao Judiciário substituir a parte autora nas

diligências que lhe são cabíveis para demandar em juízo. 3. Recurso especial não conhecido[39].” (itálico nosso).

O ministro relator, no acórdão citado, entendeu que os dados pessoais estavam ligados ao direito à privacidade, e por esse motivo, merecia a proteção da lei, uma vez que tal direito fazia parte do rol dos direitos e garantias fundamentais consagrado pela CRFB de 1988.

Na mesma seara, o primeiro registro que menciona dados pessoais nas jurisprudências do Supremo Tribunal Federal (STF) brasileiro, é datado de 23/04/1998, e apresenta os dados pessoais como integrantes da esfera do direito à privacidade. Vejamos:

> “Protesto cambial: MProv. 1638-1/98: limitação de emolumentos relativos a protestos de que devedora microempresa ou empresa de pequeno porte (art. 6º) e disciplina do fornecimento de certidões diárias dos processos tirados e cancelamentos efetuados às entidades representativas da indústria ou do comércio e aos serviços de proteção do crédito (alteração, pelo art. 10, dos arts. 29 e 31 da L. 9.492/97): alegada inconstitucionalidade por ofensa dos arts. 62, 236, § 2º, 5º, X e XXXII, e 170, V, da Constituição: suspensão cautelar indeferida. 1. A idoneidade em tese da disciplina de matéria tributária em medida provisória é firme na jurisprudência do Tribunal, de que decorre a validade de sua utilização para editar norma geral sobre fixação de emolumentos cartorários, que são taxas. 2. Afirmada em decisão recente (ADIn MC 1.800) a validade em princípio da isenção de emolumentos relativos a determinados registros por lei federal fundada no art. 236, § 2º, da Constituição, com mais razão parece legítima a norma legal da União que, em relação a determinados protestos, não isenta mas submete a um limite os respectivos emolumentos, mormente quando o conseqüente benefício às microempresas têm o respaldo do art. 170, IX, da Lei Fundamental. 3. *A convivência entre a proteção da privacidade e os chamados arquivos de consumo, mantidos pelo próprio fornecedor de crédito ou integrados em bancos de dados, tornou-se um imperativo da economia da sociedade de massas: de viabilizá-la cuidou o CDC, segundo o molde das legislações mais*

39 Cf. SUPERIOR TRIBUNAL DE JUSTIÇA – STJ, Recurso Especial n.° 306.570/SP, Rel. Ministra Eliana Calmon, Segunda Turma, julgado em 18/10/2001, DJe 18/02/2002, p. 340, texto disponível em https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=IMG&sequencial=30922&num_registro=200100235255&data=20020218&formato=PDF [22.08.2019].

> *avançadas: ao sistema instituído pelo Código de Defesa do Consumidor para prevenir ou reprimir abusos dos arquivos de consumo*, hão de submeter-se as informações sobre os protestos lavrados, uma vez obtidas na forma prevista no edito impugnado e integradas aos bancos de dados das entidades credenciadas à certidão diária de que se cuida: *é o bastante a tornar duvidosa a densidade jurídica do apelo da argüição à garantia da privacidade, que há de harmonizar-se à existência de bancos de dados pessoais*, cuja realidade a própria Constituição reconhece (art. 5º, LXXII, in fine) e entre os quais os arquivos de consumo são um dado inextirpável da economia fundada nas relações massificadas de crédito.[40]" (itálico nosso)

No acórdão citado, o ministro relator entendeu que os dados pessoais estavam inseridos no que se tinha como visível à época como direito à privacidade, direito e garantia fundamental consagrado pela CRFB de 1988, que por sua vez, quando violado, levando ainda em consideração o fato da violação ocorrer em uma relação de consumo, também encontrava respaldo pelo Código de Defesa do Consumidor de 1990.

O que se percebe através dos acórdãos juntados é que, mesmo para o STF em 1998 e para o STJ em 2001, a confusão em relação a aplicação do direito à proteção dos dados pessoais acontecia porque havia o entendimento de que os dados eram informações pertencentes à esfera do direito à privacidade e por esse motivo também se estendiam a eles a mesma tutela à privacidade prestigiada pela CRFB.

Desse modo, percebe-se que à Proteção de Dados Pessoais se dava por equiparação ao Direito à Privacidade, e que, de forma implícita, se revestia como um Direito Fundamental, assim como efetivamente é. Nesse sentido, resta claro que, desde os primeiros julgados junto ao STJ e STF, o Direito à Proteção de Dados Pessoais era tratado como um Direito com dimensão jusfundamental, ainda que por equiparação a outros direitos já mencionados.

Contudo, os entendimentos mais recentes dos tribunais brasileiros revelam uma mudança quanto à aplicabilidade e à necessidade do reconhecimento de um Direito à Proteção de Dados Pessoais como um direito autônomo. Vejamos:

---

40 Cf. SUPREMO TRIBUNAL FEDERAL – STF, *"Ação Direta de Inconstitucionalidade n.º 1.790 MC, Relatora: Min. Sepúlveda Pertence, Tribunal Pleno, julgado em 23/04/1998, DJe 08-09-2000, PP-00004, EMENT VOL-02003-01, PP-00199"*, texto disponível em http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=347269 [22.08.2019].

"HABEAS CORPUS. CRIME CONTRA A LEI DE LICITAÇÕES. CONTRATO DE CONCESSÃO E ADITIVOS. COMPETÊNCIA. BUSCA E APREENSÃO. FUNDAMENTAÇÃO DA DECISÃO. EXISTÊNCIA. ACESSO AO CONTEÚDO DAS MÍDIAS APREENDIDAS. LEGALIDADE. HABEAS CORPUS DENEGADO.1. A complexidade das investigações pode ensejar o deslocamento da competência, nas hipóteses em que ela se firma pelo local do resultado do delito, a fim de tornar mais efetiva a produção dos elementos de informações, em se tratando de inquérito, ou de provas, quando já deflagrado o processo penal. Precedentes. 2. No caso, todos os fatos (atos de execução delito, o modus operandi e as empresas que participaram da licitação investigada) se deram em local diverso daquele em que supostamente ocorreu o resultado. Não há nenhuma circunstância – à exceção do malsinado resultado – que justifique fixar a competência pelo local do resultado em prejuízo de toda a investigação e, por que não dizer, da própria defesa dos investigados. 3*. Determinadas informações, por se entrelaçarem com aspectos ligados à personalidade, devem ser objeto de proteção em grau mais elevado. Por isso, a Constituição protege à intimidade e à vida privada (art. 5º, X da CF), que abrangem uma série de dados pessoais (bancários, fiscais etc), e também a comunicação de dados (art. 5º, XII, da CF), por via telefônica, telemática ou outro meio. Nesse contexto se insere a busca e apreensão domiciliar, que se sujeita à reserva absoluta de jurisdição (art. 5º, XI, da CF)*. A validade da busca e da apreensão somente é considerada legal quando imprescindíveis às investigações e condicionadas à existência de elementos concretos que as justifiquem. Precedentes. 4*. A cláusula absoluta de reserva de jurisdição se limita à comunicação dos dados – que deve ser compreendida como informações dinâmicas –, e não aos dados em si – considerados como informações estáticas –, que possuem proteção distinta, conforme entendimento jurisprudencial.* Isso significa que a existência de sigilo não deve ser confundida com cláusula de reserva de jurisdição. 5. Na hipótese de o equipamento (computador, pen drive, HD externo etc.) haver sido apreendido em busca e apreensão domiciliar, o próprio mandado judicial pode facultar o acesso às informações que nele constem. Por isso, não há óbice para que a autoridade

> policial ou o Ministério Público solicite, em sua representação pela autorização de busca e apreensão, que seja deferido o acesso aos dados estáticos contidos no material coletado. 6. As Leis n.º 12.965/2014 e 9.296/1996 possuem dispositivos legais que objetivam tutelar o fluxo das comunicações em sistemas de informática e telemática, isto é, proteger a fluência da comunicação em andamento, diversamente do que ocorre quando são recolhidos aparelhos informáticos em decorrência de busca e apreensão domiciliar, nos quais os dados são estáticos. Em virtude disso, é incorreta a avaliação dos requisitos necessários para a interceptação do fluxo de comunicações, a fim de aferir a possibilidade de acesso as informações estáticas que estão armazenadas em aparelhos recolhidos em busca e apreensão domiciliar. 7. Habeas corpus denegado.[41]" (itálico nosso).

Conforme visto no acórdão citado, o Direito à Proteção de Dados Pessoais alcançou visibilidade legal, sendo enfim citado como um direito autônomo com garantia fundamental materialmente constitucional, equiparado com os direitos já consagrados pela CRFB de 1988, direitos como à intimidade e à privacidade.

Muito embora nossos tribunais tenham por anos tentado tutelar os dados pessoais nas relações civis e comerciais, o ambiente de discussão e aplicação de proteção pela lei se dava nas relações físicas, contudo, conforme já salientado, atualmente, o ambiente de aplicação do direito à proteção de dados pessoais acontece em um ambiente novo e pouco regulamento, a internet.

Em face da ausência da consagração formal do Direito à Proteção de Dados Pessoais como um direito com garantia fundamental pela CRFB de 1988, urge a necessidade da criação de uma lei que venha apresentar um conceito amplo e direto acerca dos dados pessoais no ambiente virtual, independentemente de os dados dizerem respeito à vida intima e privada ou a fatos de conhecimento público e notório.

Desse modo, restou claro que o ambiente que necessita ser legislado na atualidade é o virtual, e por esse motivo, deve ainda o legislador expor um conceito amplo e claro que venha dispor e enquadrar as relações civis, comerciais e criminais nesse novo ambiente. Surge então novas preocupações frente as novas tecnologias e a forma de interação entre o legislador, a internet e o cidadão titular dos dados.

---

41 Cf. SUPERIOR TRIBUNAL DE JUSTIÇA – STJ, *"Habeas Corpus n.º 444.024/PR, Rel. Ministro Rogerio Schietti Cruz, Sexta Turma, julgado em 02/04/2019, DJe 02/08/2019"*, texto disponível em https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1769509&num_registro=201800782456&data=20190802&formato=PDF [22.08.2019].

É de todo oportuno salientar que, todo e qualquer acesso à internet gera rastros – e isso acontece através do endereço IP de cada usuário –, sendo ele o caminho pelo qual se consegue identificar quem acessou, manipulou e enviou dados. Nesse sentido, é importante questionar a ampliação do conceito de dados pessoais: o IP seria um dado pessoal? ~~A~~través dele é possível tornar uma pessoa identificada ou identificável?

A resposta para essas perguntas certamente é positiva, e isso justifica a necessidade de apresentar um novo conceito de dados pessoais, o Protocolo de Internet (IP) certamente deverá ser inserido no rol de características que possibilitam a identificação de uma pessoa.

Importante ressaltar ainda que, a identificação do endereço de IP fornece outras inúmeras informações de uma pessoa, isso porque, além das informações contratuais, tais como nome, sobrenome, Registro Geral (RG), Cadastro de Pessoas Físicas (CPF), endereço e outros, também possibilita saber através de qual computador ou smartphone identificar de onde foi realizado o acesso e em que local do globo ele ocorreu, através da sua geolocalização. Entretanto, imperioso é destacar que, quando o endereço de IP não for identificável[42] e não puder oferecer nenhum dado de uma pessoa determinada ou determinável, este deixará de estar inserido no rol de dados pessoais e passará a ser tratado como dados anônimos.

De acordo com o exposto até aqui, pode-se notar que a largos passos o conceito de dados pessoais caminhou um grande percurso para se ter reconhecimento por meio de normas legais, quer seja a nível internacional ou nacional. Durante todo o caminho percorrido pelo legislador, a luta travada teve como finalidade resguardar direito intrínseco a cada indivíduo, não só pela ausência de norma legal que trata diretamente sobre o tema, mas sim por que a falta de proteção viola diretamente direito fundamental ligado à personalidade.

Desse modo, necessário se faz apresentar como a lei trata o rol de dados pessoais, destacando que existem tipos de dados que merecem mais atenção de proteção do que outros, a exemplo, os dados de caráter sensíveis, da mesma forma que existem outros tipos de dados que, mesmo sendo dados

---

42 *"Uso de VPN – as VPNs são a forma mais sólida, segura e simples de esconder seu endereço IP. Elas também oferecem poderosos recursos de segurança que mantêm você seguro e anônimo. Proxy – os proxies são uma maneira simples de fazer parecer que você possui um endereço IP diferente. No entanto, eles podem deixar sua conexão bastante lenta, não criptografam sua atividade e não são uma boa opção para torrenting. Tor – o Tor é uma forma gratuita de manter sua atividade online totalmente anônima. Conectar-se através do Tor pode causar grande lentidão em sua conexão à internet, mas seu endereço IP se tornará indetectável. Public Wi-Fi – conectar-se a uma rede Wi-Fi pública é uma maneira simples de mascarar seu endereço IP, mas pode deixar você vulnerável a grandes ameaças de segurança. Esse método não o ajudará a contornar restrições geográficas".* Cf. VEALE, Kate, "*Como Esconder Seu IP – 4 Formas Rápidas e Fáceis",* in vpnMentor, S/d, texto disponível em https://pt.vpnmentor.com/blog/4-formas-faceis-de-ocultar-seu-endereco-ip/ [25.09.2019].

pessoais, desmerecem essa classificação por não ser possível a identificação da pessoa, como é o caso dos dados anônimos.

CAPÍTULO II

OS DADOS PESSOAIS E A SUA DIMENSÃO JUSFUNDAMENTAL

1. Os dados pessoais

Conforme já exposto, o primeiro regulamento jurídico que trouxe a baila o conceito de dados pessoais foi a Diretiva Europeia 95/46/CE, de 24 de abril de 1995. Segundo a letra "a" do artigo 2.º da diretiva mencionada, os dados pessoais são qualquer informação relativa a uma pessoa singular, que a torne identificava ou que possa ser identificável.

Desse modo, dados pessoais são qualquer informação singular ou um conjunto de diversas outras informações distintas que, quando combinadas leva à identificação de uma determinada pessoa. Por esse principal motivo é que se justifica expor a jusfundamentalidade do Direito à Proteção de Dados Pessoais.

Por essas razões é que se justifica o anseio da sociedade pela criação de uma lei própria que venha dispor de forma clara e precisa sobre o Direito à Proteção de dados pessoais, lei essa que venha tutelar os dados independentemente da tecnologia utilizada em seu tratamento – quer seja no mundo físico ou no mundo virtual.

Em relação aos dados pessoais há de se expor que podem ser divididos conjuntos de dados[43], como por exemplo os dados de caráter sensíveis e os dados anônimos, e que, por meio dessa subclassificação terão maior ou menor amparo da lei no que tange a proteção ao titular de dados levando em consideração o potencial ofensivo quando do tratamento inadequado desses dados. Sendo assim, necessário se faz apresentar que se entende por dados de caráter sensível e por dados anônimos.

1.1. Dados de caráter sensível, dados anônimos e o processo de anonimização

Nas páginas anteriores foi demonstrado o quão importante são os dados pessoais para seu titular, pois é através deles que é possível identificar um individuo perante a sociedade e o Estado.

43 *"(...) todo dado pessoal só pode ser tratado se seguir um ou mais critérios definidos pela LGPD, mas, dentro do conjunto de dados pessoais, há ainda aqueles que exigem um pouco mais de atenção: são os sobre crianças e adolescentes; e os "sensíveis", que são os que revelam origem racial ou étnica, convicções religiosas ou filosóficas, opiniões políticas, filiação sindical, questões genéticas, biométricas e sobre a saúde ou a vida sexual de uma pessoa."*, Cf. SERPRO, *"O que são dados sensíveis, de acordo com a LGPD"*, *in serpro.gov*, S/d, texto disponível em https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-sensiveis-lgpd [25.09.2019].

Contudo, os dados pessoais apresentam ainda outros valores – por valores entende-se não somente de importância relacionada à dignidade da pessoa humana, mas também na sua forma pecuniária.

Os dados pessoais são essenciais para a manipulação de transações na internet e por isso possui um valor (monetário) no mercado de dados, afinal, é assim, por exemplo, como veremos mais adiante, que é possível traçar um perfil específico de um consumidor e como uma empresa consegue alcançá-lo para expandir seus negócios para venda de produtos e serviços direcionados.

Nesse sentido, reconhecendo que os dados são o método que possibilita a individualização de pessoas, ou seja, as torna identificadas ou identificáveis, imperioso se faz expor que há dados pessoais que merecem mais atenção se comparado com outros dados, é o caso por exemplo dos dados de considerados como sensíveis.

As primeiras discussões acerca da maior fragilidade de alguns dados, aqueles apresentados pelo legislador como sensíveis, acompanharam a mesma trajetória do reconhecimento do Direito à Proteção dos Dados Pessoais ao redor do mundo. A partir das décadas de 60 e 70, com a chegada das tecnologias da informação, leis específicas de proteção de dados pessoais começaram a surgir e consequentemente a incluir os dados sensíveis como merecedores de maior atenção e proteção.

Embora o reconhecimento ao direito aos dados pessoais tenha se desenvolvido inicialmente nas jurisprudências norte-americanas, foi na Europa que as principais fontes legais e doutrinárias sobre proteção de dados emergiram durante os últimos anos, especialmente na década de 70.

Dentro das discussões acerca dos dados pessoais, a categoria dos dados sensíveis[44] foi reconhecida e consagrada pela primeira vez através do Conselho da Europa, por meio da Convenção 108[45]. A Convenção previu em seu artigo 6.º, uma "categoria especial de dados", e dispôs que os dados pessoais relativos à origem racial, saúde, vida sexual e condenações penais somente poderiam ser objeto de tratamento desde que o direito interno previsse as garantias adequadas para o seu processamento[46].

Nesse prisma, percebe-se que na União Europeia, o Conselho da Europa se encontra ativo em regular à proteção de dados sensíveis, depois, no âmbito da União Europeia, a Diretiva Europeia 95/46/CE, que trouxe um regime especial de proteção para a categoria dos dados pessoais, tendo

44 Cf. HIGUERAS, Manuel Heredero, *La Directiva Comunitaria de Protección de los datos de carater personal,* Madrid, Aranzadi Editorial, 1997, pp. 116 - 117.

45 Cf. CONSELHO DA EUROPA, Convenção 108, de 28 de janeiro de 1981, "*para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal"*, texto disponível em https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm [25.09.2019]

46 Cf. CONSELHO DA EUROPA, Convenção 108, de 28 de janeiro de 1981, *"para a proteção...",* op. cit., Artigo 6º.

continuidade no Regulamente Geral de Proteção de Dados Europeu (RGPD) UE 2016/679 em seu artigo 9.º[47].

Destaca-se que, desde então a União Europeia tem sido referência mundial em normas relativas à proteção de dados, possuindo o mais completo instrumento normativo em vigor – o RGPD.

No Brasil, o conceito de dados sensíveis foi disposto pela primeira vez através do Projeto de Lei n.º 5.276[48] de 15 de maio de 2016, que, no artigo 5.º, inciso III, assim se apresentava: dados sensíveis são "dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos".

Importante salientar que esse conceito – tal qual disposto pela primeira vez na legislação brasileira – encontra-se reafirmado na Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n.º 13.709[49], de 14 de agosto de 2018, através do artigo 5.º, inciso II, leis essa que tem como papel principal legislar a respeito do "tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural".

Nesse sentido, percebe-se que a legislação interna (nacional) seguiu o mesmo conceito encontrado na legislação internacional, principalmente no que tange ao conceito de dados de caráter sensível. Em outras palavras, é cristalino que houve uma cópia (*ipsis litteris*) por parte do legislador brasileiro das disposições europeias.

Conforme se nota, dentro da categoria de dados elencados como sensíveis, há sempre uma repetição de alguns tipos de dados, tais como, dados relacionados à origem racial, vida sexual e convicções religiosas e políticas. Isso acontece porque o armazenamento, o tratamento e a circulação de alguns desses dados podem constituir um risco à personalidade do individuo, principalmente quando a exposição desses dados tiver como finalidade o uso discriminatório.

Na realidade, o rol de dados considerados como sensível não deve ser taxativo, pois o que determina se o dado expõe a fragilidade do seu titular, é tipo de tratamento a que ele será submetido.

---

47 *"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."*

48 Cf. BRASIL, Câmara do Deputados, "*Projeto de Lei n° 5.276/2016, dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural",* texto disponível em https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=E0C5C0C9CEB5C726CC764F3E7AAB0B62.proposicoesWebExterno1?codteor=1457459&filename=PL+5276/2016 [26.08.2019].

49 Cf. BRASIL, Lei n° 13.709, de 14 de agosto de 2018, *"Dispõe sobre a proteção...", op. cit.,* artigo 50°, inciso II.

Outra classe de dados pessoais que também merece atenção são os dados anônimos. Muito embora se encontrem dispostos na doutrina como uma classe dos dados pessoais, há correntes que defendem que aqueles dados que tenham sido tornados anônimos, ou seja, anonimizados, deixam de serem considerados como dados pessoais.

Contudo, para que seja considerado realmente como um dado anônimo, a anonimização tem de ser irreversível. O processo de anonimização se baseia em métodos técnicos que de alguma forma vem impedir a identificação direta ou indireta do titular dos dados.

Na maioria dos casos, os dados anônimos são utilizados para o uso estatístico, mesmo que sejam carregados de informações pessoais, tais como dados sobre família, doença, partido político, intenção de voto, orientação sexual, dentre outros, de uma forma que não identifique ou torne identificável uma pessoa diretamente.

Atualmente é comum a existência de empresas que fazem o tratamento específico de anonimização e utilização dos dados anônimos. A exemplo disso, no Brasil, tem-se o Instituto Brasileiro de Geografia e Estatística (IBGE)[50], sendo o maior dos provedores de dados (anônimos) e informações, que tem por finalidade de atender às necessidades dos mais diversos segmentos da sociedade civil, bem como dos órgãos das esferas governamentais federal, estadual e municipal.

A principal missão do IBGE é identificar e analisar o território, contar a população e mostrar como a economia evolui através do trabalho e da produção das pessoas e ainda revelar como elas vivem.

Através dos dados pessoais que o IBGE expõe é possível demonstrar quantidade de pessoas por família, renda per capita, sexo ou orientação sexual, nível de escolaridade e outros dados que outrora são classificados como dados sensíveis, mas que, pelo simples fato de serem anonimizados, deixam de ser considerados dados pessoais e passam a não ter a mesma proteção pela lei.

Dessa forma concluir-se que os dados anonimizados (anônimos) são aqueles que realmente não têm como finalidade a identificação do seu titular, quer seja esta identificação direta ou indireta, de modo que, motivo esse que leva essa classe de dados a não ter o mesmo respaldo de proteção pelas leis vigentes, ou seja, por não apresentarem perigo direto ao titular do dados anonimizados, consequentemente não violam direitos fundamentais.

Uma vez defendido que os dados anonimizados não encontram respaldo de proteção legal pelas leis vigentes, necessário se faz expor que, se por algum motivo a anonimização puder ser revertida a fim

50 *"O IBGE é uma entidade da administração pública federal, vinculada ao Ministério do Planejamento, Orçamento e Gestão, que possui quatro diretorias e dois outros órgãos centrais".* Cf. IBGE, in IBGE.GOV, S/d, texto disponível em https://www.ibge.gov.br/institucional/o-ibge.html [26.08.2019].

de novamente indicar ou tornar identificável o titular dos dados, voltam assim a ter a mesma tutela de um dado comum.

No que diz respeito à anonimização de dados pessoais, a Lei Geral da Proteção de Dados Pessoais (LGPD), Lei n.º 13.709/2018, através do inciso XI, do artigo 5.º vem dispor que: "anonimização [é a] 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".

Como um dos principais objetivos da presente dissertação é expor o lado positivo do reconhecimento por meio de lei própria do direito à proteção de dados pessoais, principalmente diante da grande mudança na era digital, também há pontos suscetíveis de preocupação, a exemplo disso, é o que pode vir a acontecer com os dados anônimos, pois, em um futuro próximo, as técnicas utilizadas atualmente no processo de anonimização podem se tornar ineficientes, o que possibilitará a re-identificação do titular dos dados.

2. Os dados pessoais e seu tratamento no âmbito da internet

É cediço que o uso da internet – atualmente – é considerado importantíssimo ao exercício da cidadania, bem como ao acesso a diversas informações do dia-a-dia. Por esse motivo é que o tratamento de dados pessoais na internet deve ser regulado de forma clara e precisa para efetiva tutela dos interesses do titular dos dados.

Acerca do tratamento de dados, a LGPD, vem, em através do inciso X, no artigo 5.º, expor seu conceito no âmbito do uso dos dados pessoais da internet, sendo caracterizado como tratamento de dados "toda [e qualquer] 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 fato, o tratamento de dados pessoais é processo comum daqueles que utilizam o meio digital para transacionar dados, independente da sua finalidade, por esse motivo é que se justifica a sua regulamentação.

A respeito da transação e tratamento de dados, há que se expor que ela acontece por diversas finalidades, podendo ser apenas para fins de estatísticas, como acontece no caso do IBGE já citado; para fins de estudos, como acontece no caso das Universidades e até mesmo na área da saúde para fins de

estudo de novo medicamento, cura de doenças, relatórios de doentes e recuperados. A exemplo disso tem-se os relatórios de COVID-19 emitido pela OMS através de seu site oficial[51].

Conforme será exposto à frente, o tratamento de dados pessoais pode ser também o meio pelo qual pode, o controlador e o operador de dados – figuras exemplificadas pela lei que manuseiam os dados pessoais no âmbito digital – transacionar dados pessoais no intuito de aferir lucro.

Com o uso constante da internet, o titular dos dados deve sempre estar ciente dos termos de autorizações e consentimentos que dá desmedidamente para ter acesso a diversos tipos de conteúdos ou sites. Mesmo tendo, o titular, o direito – garantido pela lei – de acessar, corrigir, eliminar, anonimizar, bloquear seus dados, revogar consentimento e outros, há todo um mercado digital – voraz – que visa constantemente aferir lucro através da criação (através da captação dos dados na internet) de perfis consumeristas para oferecimento de produtos e serviços, e ó chamado mercado de dados.

2.1. O mercado digital, onde se transacionam dados pessoais

O meio em que os dados pessoais são armazenados e tratados é o desafio que a legislação moderna busca regulamentar, uma vez que, quando inseridos em uma rede de dados, o seu tratamento não acontece como em um armazenamento físico – ambiente com barreiras físicas que pode facilmente ser controlado. Porém, antes de adentrarmos ao mérito de fato, necessário se faz expor o que se entende por rede de dados.

Como o próprio nome denota, uma "Rede", no meio virtual, é uma estrutura que apresenta um padrão característico e uma arquitetura com ligação direta ou indireta com outros dispositivos interligados e que tenham a capacidade de firmar essa conexão. Os dados, em sentido amplo, são indicativos de qualquer tipo de informação, quer seja ela relacionada à área da informática ou como um dado pessoal.

Sendo assim, rede de dados é qualquer infraestrutura que viabiliza a transmissão em tempo real ou *offline* na troca de dados. Essa troca de informações, por meio da rede de dados, é criada especificamente para cumprir com seus objetivos, e quando online, ela acontece por meio da internet. A internet é a rede virtual que possibilita a ligação entre as redes de dados e os computadores.

Pierre LÉVY defende que, "[o] ciberespaço (que também chamarei de 'rede') é o novo meio de comunicação que surge da interconexão mundial dos computadores. O termo especifica não apenas a

51 Cf. WORLD HEALTH ORGANIZATION, "*Coronavirus Disease (COVID-19) Dashboard*", in OMS, S/d, texto disponível em https://covid19.who.int/ [22.06.2020]

infraestrutura material da comunicação digital, mas também o universo oceânico de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo[52]".

Para DOMINGOS, "sem ela [a internet], cada tipo de rede precisaria de um protocolo diferente para conversar com outros tipos (...). Os protocolos da internet são uma espécie de esperanto que dá a cada computador a impressão de estar conversando diretamente com outros computadores e permite que o correio eletrônico e a web ignorem os detalhes da infraestrutura física pela qual eles fluem[53]".

É esse o caminho que os dados percorrem, desde a sua inserção ou "captura", até o uso/divulgação, ou, até o seu local de armazenamento, caminho que está envolto de rastros, ou seja, de dados identificáveis. É de todo oportuno salientar que no meio virtual, através das ligações aos computadores e frente às novas tecnologias, é quase impossível para o homem conseguir controlar o fluxo de dados, e é nesse meio que se encontra e se movimenta o mercado digital.

É inegável em todo o mundo que, através dos dados pessoas, também já se afere lucro – não sendo essa a única finalidade de se transacionar dados. Desde o processo C-101/01 de 06 de novembro de 2003, o Tribunal de Justiça da União Europeia (TJUE) afastou a ideia de que o tratamento de dados teria uma dimensão exclusivamente económica. De qualquer forma, os dados são crescentemente utilizados para auferir lucro, podendo ser utilizados na formação de perfis para o direcionamento de produtos e serviços ao consumidor, movimentando assim o chamado mercado de dados. Neste subtítulo demonstraremos a grande importância dos dados pessoais para o mercado de dados.

A importância dos dados pessoais para o mercado digital é tamanha, que são considerados como o novo petróleo da era digital. Conforme aponta artigo publicado pela revista The Economist, *"[a] century ago, the resource in question was oil. Now similar concerns are being raised by the giants that deal in data, the oil of the digital era[54]".*

Retroceder à era do trabalho manual e braçal – onde o controle de todas as ações e informações se davam através de máquinas enormes, controladas pelo esforço humano limitado, lentas e sem ligação à internet – não é mais uma opção disponível para gerar riquezas e comodidade ao cidadão do mundo, motivo esse que justifica a criação de um mercado digital, que, aliás já se encontra operante, e é uma realidade que alavanca o mercado financeiro digital.

---

52 Cf. LÉVY, Pierre, *Cibercultura,* Tradução de Carlos Irineu da Costa, São Paulo, Editora 34, 2008, p. 17.

53 Cf. DOMINGOS, Pedro, *O Algoritmo Mestre: Como a busca pelo algoritmo de machine learning definitivo recriará nosso mundo*, São Paulo, Novatec, 2017, p. 263.

54 Cf. THE ECONOMIST, *"Regulating the internet giants. The world's most valuable resource is no longer oil, but data", in The Economist,* ed. 06 de maio de 2017, texto disponível em https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data [12.11.2019].

Indiscutível são os benefícios que o mercado digital traz dia após dia para a vida moderna, contudo, esse meio só trará confiança no relacionamento para com os cidadãos, se for muito bem regulamentado, afinal, a base do mercado digital são em sua grande parte, os próprios dados pessoais.

Ante a grande importância dos dados pessoais para o mercado digital – e não somente por esse motivo –, justifica-se mais uma vez a necessidade da consagração do Direito à Proteção de Dados Pessoais como um direito fundamental no ordenamento jurídico brasileiro pela Carta Magna brasileira de 1988, uma vez que, atualmente, seu reconhecimento dá-se apenas como um direito implícito, ou seja, como um direito fundamental materialmente constitucional.

A doutrina majoritária tem se manifestado no sentido de afirmar que, antes mesmo de uma possível positivação como um direito com garantia fundamental pela CRFB de 1988 (fato esse que logo será superado pela proposta de emenda à constituição PEC n.º 17/2019), o Direito à Proteção de Dados Pessoais já era considerado como um direito materialmente constitucional com garantia fundamental.

Ingo SARLET, desde 2014, tem assinalado que os dados pessoais mereciam assim ser considerados, por que englobam "o direito de acesso e conhecimento dos dados pessoais existentes em registros (banco de dados) públicos e privados; o direito ao não conhecimento, tratamento e utilização e difusão de determinados dados pessoais pelo Estado ou por terceiros, aqui incluído um direito de sigilo quanto aos dados pessoais; o direito ao conhecimento da identidade dos responsáveis pela coleta, armazenamento, tratamento e utilização dos dados; o direito ao conhecimento da finalidade da coleta e eventual utilização dos dados; o direito à retificação e, a depender do caso, de exclusão de dados pessoais armazenados em banco de dados[55];" são direitos ligados à personalidade do individuo e que permeia a sua vontade como fator primordial de expor ou deixar de expor informações a seu respeito, de modo que devem ser protegidos sem restrições pela Carta Magna brasileira.

De mesma sorte, no plano normativo internacional, a Comissão Europeia, "por meio da comunicação da comissão ao parlamento europeu, ao conselho, ao comité económico e social europeu e ao comité das regiões sobre a revisão intercalar relativa à aplicação da Estratégia para o Mercado Único Digital conectado para todos, COM(2017), 228, parte final, de 15 de maio de 2017, <<enfatiza que>> [a] vida privada não é um produto que deva ser comercializado. Pelo contrário, o respeito da vida privada e da proteção dos dados pessoais constitui uma condição para que poderem existir fluxos comerciais globais estáveis, seguros e competitivos[56]".

---

55 Cf. MARINONI, Luis Guilherme, et al., *Curso de Direito Constitucional,* São Paulo, Revista dos Tribunais, 2014, pp. 434-435.

56 Cf. COMISSÃO EUROPEIA, *"Comunicação da Comissão Europeia sobre a revisão intercalar relativa à aplicação da Estratégia para o Mercado Único Digital - Um Mercado Único Digital conectado para todos [COM(2017) 228 final]* de 10 de maio de 2017", Bruxelas, 2017, texto disponível em http://eur-lex.europa.eu/legal-content/PT/TXT/ HTML/?uri=CELEX:52017DC0228&from=PT [29.11.2019].

Por mais esse motivo, é que se justifica a criação de uma norma específica que venha regulamentar de forma clara e precisa o tratamento de dados pessoais no meio digital, uma vez que, ao mesmo tempo que assegurará o tratamento e armazenamento seguro dos dados, bem como o uso dos mesmos, também impulsionará com confiança o mercado digital.

2.2. O algoritmo de aprendizagem e a sua ligação com a internet das coisas (Internet of Things - IoT)

Atualmente, toda a internet encontra-se estruturada por meio de algoritmos que controlam e direcionam as informações que circulam por meio da rede de dados. A saber, um algoritmo é uma sucessão de diretrizes, finitas, que descrevem ao computador o que se deve fazer e como fazer.

Apesar de o algoritmo se apresentar de forma complexa, o seu conceito pode se apresentar de forma muito simples. DOMINGOS apresenta que "[u]m algoritmo é uma sequência de instruções dizendo a um computador o que fazer[57]".

O controle dos dados – no sentido amplo – na internet acontece por meio de algoritmos que foram criados com finalidade para alcançar o objetivo do uso desses dados. Quer seja na escolha de um filme na plataforma da NETFLIX, na escolha de um e-book na AMAZON, pedir um UBER, fazer com que uma Aeronave da AZUL Linhas Aéreas chegue ao seu destino através do piloto automático ou para destrancar a distância uma fechadura eletrônica da YALE, usando o reconhecimento digital por meio de leitura biométrica ou facial acionado por um smartphone, há algoritmos por trás dessas ações. Para DOMINGOS, "[s]e todos os algoritmos parassem de funcionar inesperadamente, o mundo que conhecemos chegaria ao fim[58]."

Em relação a sua estrutura, importante destacar que todo algoritmo é programado para receber um dado que é lançado através de um computador ou um smartphone e inserido por um usuário com vistas a trabalhar para produzir um resultado que foi indicado pelo comando do homem.

Nesse sentido, a máquina obedece a um comando humano e faz o trabalho que a ele caberia, porém de uma forma mais célere e com uma porcentagem menor de erros. É valido mencionar que os algoritmos estão ligados, ao *machine learning*[59] – algoritmo de aprendizagem –, o que faz com que a

57 Cf. DOMINGOS, Pedro, *O Algoritmo Mestre: Como a busca pelo algoritmo..., op. cit.* p. 24.

58 Cf. DOMINGOS, Pedro, *O Algoritmo Mestre: Como a busca pelo algoritmo..., op. cit.* p. 24.

59 *"A aprendizagem automática ou aprendizado da máquina (em inglês: "machine learning") é um subcampo da inteligência artificial dedicado ao desenvolvimento de algoritmos e técnicas que permitem ao computador aprender, isto é, aperfeiçoar seu desempenho em alguma tarefa."* Cf. DOMINGOS, Pedro, *O Algoritmo Mestre: Como a busca pelo algoritmo..., op. cit.* p. 24.

própria máquina aprenda através dos comandos humanos o que se fazer após a coleta e estudo desses dados.

Atualmente, é por meio de algoritmos de aprendizagem que empresas fazem as coletas de dados pessoais de todos os usuários da internet, bem como de pessoas que não consentiram o uso de seus dados, isso com o intuito de conhecer cada individuo e traçar um perfil para lhe oferecer serviços ou objetos para fomentar a venda direcionada.

Desse modo, o algoritmo de aprendizagem é o meio pelo qual se é possível criar uma descrição de necessidades de consumo, opiniões e outros, para apresentar um produto de forma mais apurada a fim de obter mais sucesso na hora da oferta e fechamento da venda.

Grandes empresas como Google, Bing e Yahoo, utilizam algoritmos de aprendizagem para conhecer o perfil dos usuários da internet através de seus buscadores de informações e por meio dos dados inseridos, e a partir dai, traçam um perfil do usuário para lhe oferecer uma resposta mais apurada daquilo que é procurado. Quando um usuário logado, pela primeira vez faz busca de algo relacionado ao seu interesse, o algoritmo de aprendizagem coleta os dados daquele indivíduo e começa a identificar seus gostos e repassa tais informações para o Google (por exemplo) que, por sua vez, entrega a uma empresa (por um valor previamente acordoado) o perfil traçado e como retorno (a empresa terceira) apresenta ao usuário produto ou serviços de "seu interesse".

Importante destacar que o Google possui atualmente os melhores algoritmos de aprendizagem disponíveis no mercado e conta com o maior aparato de aplicativos [Google Drive (armazenamento na nuvem), Google Maps (Gps), Google Chrome (Navegador), Gmail (e-mail), dentre outros], que também contribuem com a coleta de dados pessoais.

Para DOMINGOS "essas empresas aplicam algoritmos de aprendizagem às montanhas de dados acumulados e deixam que eles adivinhem o que os clientes querem. Os algoritmos de aprendizagem são os conciliadores: eles unem produtores e consumidores, rompendo a sobrecarga de informações. (...) Quando o inevitável ocorre e os algoritmos de aprendizagem se tornam o intermediário, o poder se concentra neles. Os algoritmos do Google determinam em grande parte quais informações uma pessoa deve encontrar; os da Amazon, quais produtos ela deve comprar; e os do site Match.com, com quem ela deve sair[60]. A última etapa é sempre nossa – escolher entre as opções apresentadas pelos algoritmos (...)".

Desse modo, a empresa que tiver maior concentração de dados pessoais, colhidos através de seus mecanismos de buscas ou comprado de terceiros, lucra mais em seus negócios, os quais foram

60 Cf. DOMINGOS, Pedro, *O Algoritmo Mestre: Como a busca pelo algoritmo..., op. cit.* p. 35.

fechados através das ofertas apresentadas aos usuários em seus sites. Aqui, encontra-se o verdadeiro mercado de dados.

O que há de importante nos dados pessoais na internet? Explica SILVEIRA e FROUFRE, que "[a] razão é simples: a livre circulação de dados é indispensável para o desenvolvimento da chamada economia digital. (...) Por isso se diz que os dados (inclusivamente os de caráter pessoal) estão na base da revolução algorítmica que está a mudar o mundo[61]".

Contudo, salientam que a "vida privada não é (e nem deve ser) um produto comercializável (sobretudo à revelia dos visados). E sabemos que a quebra de privacidade que crescentemente acompanha o uso universal da Internet garante a monitorização de cada gesto e ideia humana[62]". Porém, enfatizam que, "[n]ão há qualquer problema em comercializarmos os nossos dados desde que o façamos de forma livre e esclarecida, porém, (...) a maioria das pessoas não tem consciência da quantidade de dados que são diariamente recolhidos a seu respeito – nem dos potenciais custos e benefícios envolvidos – e enquanto isso as grandes empresas foram atuando sem dar nas vistas. Tudo isso faz parte de um modelo de negócio através do qual os internautas pagam com seus dados pessoais por um serviço[63]".

A coleta pelos dados pessoais tem se tornado diariamente uma corrida na busca de quem consegue chegar primeiro. Empresas como as citadas atribuem aos dados pessoais um valor e através dessas informações buscam aperfeiçoar seus produtos, bem como aprimorar seu método de oferta.

Cada vez que o usuário acessa algum dos sites das empresas que utilizam algoritmos de aprendizagem é coletado algum tipo de dado, e, aos poucos, se consegue montar um perfil contendo as suas preferências e aversões, tudo isso acontece após cada clique, graças aos algoritmos.

DOMINGOS possui uma ideia otimista em relação ao assunto e entende que, "[n]osso futuro digital começa com uma percepção: sempre que interagimos com um computador – seja smartphone ou um servidor a milhares de quilômetros de distância – o fazemos em dois níveis. O primeiro é obter o que queremos: uma resposta, um produto para comprar, um novo cartão de crédito. O segundo nível, que em longo prazo é o mais importante, é ensinar ao computador quem somos. Quanto mais ensinarmos, melhor ele poderá nos servir – ou nos manipular[64]."

Entretanto é em meio a essa corrida e colheita de dados que são utilizados pelos algoritmos que se esconde o real perigo do tratamento, armazenamento e uso indevido dos dados pessoais, com ou

---

61 Cf. SILVEIRA, Alessandra e FROUFRE, Pedro, *"Do mercado interno à cidadania de direitos: a proteção de dados pessoais como a questão Jusfundamental identitária dos nossos tempos",* Braga, UNIO - EU Law Journal, Vol. 4, n°. 2, julho 2018, pp. 5-6.

62 Cf. SILVEIRA, Alessandra e FROUFRE, Pedro, *"Do mercado interno...", op. cit.*, p. 6.

63 Cf. SILVEIRA, Alessandra e FROUFRE, Pedro, *"Do mercado interno...", op. cit.*, p. 11.

64 Cf. DOMINGOS, Pedro, *O Algoritmo Mestre: Como a busca pelo algoritmo..., op. cit.*, p. 291.

sem consentimento do usuário. Em grande parte, os dados inseridos na internet contêm o consentimento dos usuários, e esses dados são classificados por DOMINGOS em quatro tipos[65]: "O primeiro tipo inclui coisas como críticas do Yelp, da Amazon e do TripAdvisor, pontuações do feedback do Ebay (...) e assim por diante. Esses dados têm muito valor e são os menos problemáticos dos quatros."

No primeiro tipo de dados todos se beneficiam, pois tem como finalidade a melhora do serviço prestado e, principalmente, há consentimento direto pelo usuário para expor sua opinião e no fim as empresas ganham com tal ato, porque acabam por aperfeiçoar seus serviços.

"O segundo tipo de dado também não deve ser problemático (...). Compartilhamos atualizações e fotos com nossos amigos no Facebook, e eles compartilham conosco. Porém, todas as pessoas compartilham suas atualizações e fotos com o Facebook. (...) Dia após dia, o Facebook aprende muito mais sobre o mundo que qualquer outra pessoa. (...) O Facebook usa todo esse conhecimento principalmente para destinar propaganda para nós. (...) Esse é o intercâmbio que fazemos ao usar o Facebook. (...) O único problema é que o Facebook também pode fazer coisas com os dados e os modelos que não são de nosso interesse, e não temos como evitar."

No segundo tipo de dados também há consentimento do usuário, principalmente quando há o aceite para entrar no site ou na rede social, como é o caso do Facebook. Muito embora em sua tela inicial de login conste a seguinte informação "É gratuito e sempre será", na realidade não é.

Conforme explanado, o acesso "livre" ao Facebook acontece através da troca de dados que são comercializados por ele a empresas que, posteriormente oferecem seus produtos ao usuário através de propagandas com base em seu perfil, mesmo sem o seu consentimento. Apesar de ter sido apresentado por DOMINGOS como trocas de dados não problemático, a empresa é uma das que possui em seu currículo escândalos envolvidos com violação de dados pessoais, fatos esses que serão mostrados mais adiante.

O mesmo acaso acontece com as empresas que oferecem a guarda de dados na nuvem. Estas disponibilizam um espaço *online*, de forma gratuita, para a guarda e armazenamento de dados. Apresentam ainda "segurança" para garantir o acesso somente pelo usuário, porém elas fazem tudo isso para acumular nossos dados e distribuí-los – vendê-los – posteriormente para empresas criarem anúncios específicos focados na venda dos serviços ou produtos aos usuários titulares dos dados.

Ainda há o terceiro tipo que se refere àqueles que são compartilhados entre as empresas que buscam os dados diretamente e os comercializa. Entende-se, houve o consentimento, mesmo que nas entrelinhas pelo usuário. "(...) há uma corrida insana para a coleta de dados sobre você. Todos adoram

65 Cf. DOMINGOS, Pedro, *O Algoritmo Mestre: Como a busca pelo algoritmo..., op. cit.,* p. 298.

seus dados, e não é de surpreender: eles são a porta para o seu mundo, o seu dinheiro, o seu voto e até seu coração."

Nesse tipo de recolha do dado, a finalidade é especifica e acontece pela colheita e o repasse a um terceiro. "O Google vê suas buscas, a Amazon suas compras online, a AT&T seus telefonemas, a Capital One suas transações com cartão de crédito." Entretanto, como algumas vezes esses dados partem de escolhas aleatórias, nem sempre os perfis traçados condizem com a realidade.

O último tipo de dados se refere "àquele não compartilhado (...). Pode não nos ter ocorrido de fazê-lo, pode não haver uma maneira fácil, ou talvez simplesmente não tenhamos interesse em compartilhar. (...) Um exemplo já visto é o de pacientes com câncer, que poderiam contribuir com a cura da doença compartilhando o genoma e o histórico de tratamento de seus tumores[66]."

Nesse caso, o compartilhamento, ou seja, o tratamento desses dados está vinculado diretamente a dados sensíveis dos pacientes e que, muito embora possa vir ajudar a ciência com novos métodos de tratamento, estatística, ou até a cura, viola direitos fundamentais, como direito à privacidade, à intimidade, à proteção de dados pessoais, sobretudo por não carregar consigo o consentimento do titular sobre esses dados.

O principal perigo com o uso de forma indevida, mesmo que haja o consentimento inicial do usuário, se dá pelos danos morais e até materiais que pode causar ao titular de dados. DOMINGOS alerta que, "[a]tualmente, a maioria das pessoas não sabem quantos dados sobre elas estão sendo coletados nem quais são os possíveis custos e benefícios. As empresas parecem satisfeitas em continuar a agir em segredo, com medo de uma admoestação[67]."

Entretanto, mesmo estando (todos) alertados sobre os riscos, o mundo entra em um novo momento, carregado pela automatização das coisas, ligado diretamente à internet através da coleta de dados pessoais pelos algoritmos e a facilitação dos afazeres do dia a dia. Em outras palavras, e á era da internet das coisas.

A "Internet das coisas" faz referência a uma nova revolução desencadeada pela tecnologia e tem como finalidade ligar, através de conexão via internet, bluetooth ou wifi, objetos e itens que se usam no dia a dia à rede global de computadores.

Muito embora a revolução da internet das coisas seja ainda uma novidade, seu início aconteceu em 1991, quando a internet, como se conhece atualmente, começou a se popularizar. Bill Joy, co-

66 Cf. DOMINGOS, Pedro, *O Algoritmo Mestre: Como a busca pelo algoritmo..., op. cit.,* p. 299.

67 Cf. DOMINGOS, Pedro, *O Algoritmo Mestre: Como a busca pelo algoritmo..., op. cit.,* p. 303.

fundador da Sun Microsystems, foi a primeira pessoa a se pensar em uma conexão que mais aproximava à vida real com a virtual, através da conexão Device to Device[68] (D2D).

Entretanto, a terminologia "Internet das Coisas (IoT)" foi reconhecida somente em 1999[69] por Kevin Ashton, o precursor que criou um sistema de sensores omnipresentes com a finalidade de conectar o mundo real à internet, enquanto desenvolvia outro projeto de identificação por rádio frequência (RFID).

O primeiro aparelho doméstico ligado à internet no mundo foi apresentado durante a Feira Anual de Tecnologia da Informação de 1990, e desenvolvido por John Romkey e Simon Hackett. O dispositivo criado, foi uma torradeira elétrica que era ligada através da internet por meio de um computador via rede TCP/IP[70]. A ideia, bem como a apresentação do produto foi um sucesso. Um ano após a criação do primeiro aparelho ligado via tecnologia IoT, houve uma leve mudança, e a ele foi agregado uma pequena alavanca robótica que possibilitava, inclusive que o pão fosse colocado na torradeira, por meio de sistema totalmente automático[71]. Desde então, a ideia de minimizar o tempo gasto com os afazeres de casa e a possibilidade de controle à distância tem ganhado força e transformado o mundo.

A internet das coisas já é uma realidade vivenciada em vários países do mundo, isso porque, encontram-se disponíveis smart-tvs, smartphones, eletrodomésticos, computadores, fechaduras eletrônicas, dentre outros dispositivos que são conectados à internet, ou seja, a linha dos "smarts".

A ânsia pela aproximação do mundo físico com o digital tem ofertado aos homens experimentar situações que até então eram inimagináveis, como é o caso do Google Glass[72], que transmite em tempo real, por meio de um computador acoplado a um óculos, informações referente ao trabalho, clima, dentre

---

68 *"Device-to-Device (D2D) communication in cellular networks is defined as direct communication between two mobile users without traversing the Base Station (BS) or core network. D2D communication is generally non-transparent to the cellular network and it can occur on the cellular frequencies (i.e., inband) or unlicensed spectrum (i.e., outband. (May 2015")*. Cf. ASADI, Arash, et al., "*A Survey on Device-to-Device Communication in Cellular Networks", in IEEE Communications Surveys & Tutorials*, v. 16, Issue 4, 2014, texto disponível em https://ieeexplore.ieee.org/document/6805125/references#references [27.08.2019].

69 Cf. MANCINI, Mônica, *"Internet das Coisas: História, Conceitos, Aplicações e Desafios"*, São Paulo, *in Research Gate*, 2017, texto disponível em https://www.researchgate.net/publication/326065859_Internet_das_Coisas_Historia_Conceitos_Aplicacoes_e_Desafios [23.08.2019].

70 *"O TCP/IP (também chamado de pilha de protocolos TCP/IP) é um conjunto de protocolos de comunicação entre computadores em rede. Seu nome vem de dois protocolos: o TCP (Transmission Control Protocol - Protocolo de Controle de Transmissão) e o IP (Internet Protocol - Protocolo de Internet, ou ainda, protocolo de interconexão). O conjunto de protocolos pode ser visto como um modelo de camadas (Modelo OSI), onde cada camada é responsável por um grupo de tarefas, fornecendo um conjunto de serviços bem definidos para o protocolo da camada superior. As camadas mais altas, estão logicamente mais perto do usuário (chamada camada de aplicação) e lidam com dados mais abstratos, confiando em protocolos de camadas mais baixas para tarefas de menor nível de abstração"*. Cf. FERREIRA, Rubem E, "*Linux: Guia do Administrador do Sistema*", São Paulo, Novatec, 2ª ed., 2013, p. 8.

71 Cf. SRISHTI Deoras, "*Primeiro dispositivo IoT - "The Internet Toaster"*, in ldapwiki.com, 2018, texto disponível https://ldapwiki.com/wiki/Internet%20Toaster [23.08.2019].

72 *"O Glass Enterprise Edition 2 é um dispositivo vestível que ajuda as empresas a melhorar a qualidade de sua produção e ajuda seus funcionários a trabalhar de maneira mais inteligente, rápida e segura. Ele fornece aos trabalhadores e profissionais de mão-de-obra uma assistência ativada por voz que é projetada para ser usada durante todo o dia com seu perfil leve e confortável"*. Cf. S/A, *"Glass Enterprise Edition 2", in Google*, texto disponível em https://www.google.com/glass/tech-specs/ [27.08.2019].

outras, assim como os Smartwatchs que permitem conexão com a internet como um smartphone e que ainda possibilitam a execução de exames cardíacos, acionam o serviço de emergência em caso de queda ou sintomas ligado a arritmia cardíaca, chamadas por voz e liberação por desbloqueio de outros dispositivos.

Quem não se sente atraído por um refrigerador que pode ser controlado pelo smartphone e escolher enquanto vai para casa após um cansativo dia de trabalho a temperatura da cerveja para o happy-hour[73]? Ou procurar uma receita apenas com um toque na porta do refrigerador enquanto prepara as refeições? Essas e outras atrações já são facilmente encontradas para se comprar. A Inteligência das coisas é real e além dos benefícios, traz consigo também grandes preocupações em relação às informações que seus proprietários inserem sobre si nesses produtos.

Além dos riscos de acesso indevido – não consentido – aos dados pessoais de seus titulares, ficam ainda à mercê de assaltos, sequestros, devido aos dados de localização, que podem ser acompanhados em tempo real via gps, bem como roubo de senhas de cartões e clonagem de dados.

Em todos esses casos, principalmente os relacionados à Internet das Coisas, faz-se presente o algoritmo de aprendizagem que estuda cada dia mais sobre o usuário/titular e se aprimora para poder oferecer um atendimento mais personalizado, e ao mesmo tempo, repassa tudo que aprendeu ao seu criador, fato esse que, quando não regulamentado por lei específica, pode vir a violar o Direito à Proteção de Dados Pessoais.

3. O tratamento e conservação de forma ilícita de dados – implicações e consequências legais

A fim de realmente proteger os dados pessoais, não é somente com a forma de atuação do algoritmo de aprendizado que se deve preocupar o legislador. Dentro dos serviços de tratamento de dados existem outros pontos ainda que merecem devida atenção, um deles, por exemplo, é o serviço prestado pelo buscador que, caso não seja bem regulamentado, fragiliza a segurança dos dados dos consumidores/titulares, e ao mesmo tempo enriquece as grandes empresas.

Em relação à fragilidade e à intensificação em massa da relação entre consumidor/usuário e empresas detentoras dos dados, SILVEIRA e FROUFRE apontam um perigo, alegando que "[u]m mercado e uma sociedade intensamente conectados são mais vulneráveis a ciberataques – o que prejudica as

73 Cf. LUIGGI, Mirella, *"Vale a pena investir em uma geladeira inteligente?"*, São Paulo, *in UOL*, 2017, texto disponível em https://www.uol.com.br/tilt/noticias/redacao/2018/06/23/vale-a-pena-investir-em-uma-geladeira-inteligente-conheca-os-recursos.html [26.08.2019].

empresas de todas as dimensões e compromete a confiança na economia digital e nas instituições democráticas[74]".

Em relação a uma das formas de captação de dados, a princípio, apresenta-se o buscador como um motor inteligente de buscas, e tem como finalidade auxiliar na procura de informações que estão dispostas na rede mundial de internet, busca essa que pode ser realizada partir de um simples smartphone ou de um computador pessoal em rede online e até mesmo em uma rede de computadores offline.

O buscador permite que o usuário solicite conteúdo específico, que pode ser através de palavras isoladas ou frases, então o algoritmo de aprendizado procura o que se encontrar disposto na rede mundial acerca do assunto e lhe apresenta uma lista de referências na forma de catálogo. O resultado da busca é aprimorado sempre que o buscador tiver mais informações do usuário (dados pessoais), principalmente quando este estiver logado ou pelos cookies armazenados.

A figura do algoritmo é extremante eficaz e, sem sombra de dúvidas aprimora dia após dias a forma com que o mercado digital se apresenta. Mas qual o perigo em transacionar dados pessoais? Há casos em que há a violação no tratamento e uso de dados pessoais mesmo com o consentimento do titular de dados?

3.1. O caso Facebook e Cambridge Analytica

O caso mais recente que abalou a confiabilidade dos usuários da internet ficou conhecido como "Facebook - The Great Hack (Nada é Privado): O Escândalo da Cambridge Analytica[75]", sendo o último e maior escândalo relacionado à violação de Direito à Proteção de Dados Pessoais, assim como à Privacidade dos usuários da internet.

Em 4 de fevereiro de 2004 surge o Facebook, como assim é conhecido mundialmente, sendo ele, operado pela Facebook Inc., que também tem seu domínio e propriedade. Fundado por Mark Zuckerberg e seus colegas de quarto (á época) Eduardo Saverin, Dustin Moskovitx e Chris Hughes[76], inicialmente, com o objetivo de ser um site de acesso somente aos estudantes da Universidade de

74 Cf. SILVEIRA, Alessandra e FROUFRE, Pedro, *"Do mercado interno...", op. cit.*, p. 6.

75 Cf. VIEIRA, João Estróia, *"The Great Hack: uma visão sobre o escândalo da Cambridge Analytica", In Comunidade Cultura e Arte*, 2019, texto disponível em https://www.comunidadeculturaearte.com/the-great-hack-uma-visao-sobre-o-escandalo-da-cambridge-analytica/ [04.09.2019].

76 Cf. CARLSON, Nicholas, "*At last - the full story of how Facebook was founded*", In Business Insider, 2010, texto disponível em https://www.businessinsider.com/how-facebook-was-founded-2010-3 [04.09.2019].

Harvard, logo iniciou sua expansão a outras universidades estadunidenses atendendo a diversos alunos e por fim, em 2005, abriu acesso a estudantes do mundo todo.

O nome da maior rede social do mundo não foi escolhido por acaso. Facebook, nos Estados Unidos é o nome dado por algumas Universidades a um anuário, ou seja, um livro com foto de todos os alunos matriculados para facilitar o contato entre eles.

Em 4 de outubro de 2012 o Facebook alcançava o maior número de usuários em uma rede social no mundo, com 1 (um) bilhão de contas ativas, situação esta superada em 27 de junho de 2016 quando ultrapassou a marca de 2 (dois) bilhões[77] de contas ativas, número que, em julho de 2019, já era superior a 2,3 (dois vírgula três) bilhões de usuários[78].

Desde o ano de 2013, o Brasil já era considerado o segundo país com mais contas registradas na rede social Facebook, à época com mais de 71 (setenta e um) milhões de contas ativas[79]. Atualmente, o Brasil ocupa a terceira posição no ranking de contas registradas no Facebook, com o expressivo número de mais de 130 (cento e trinta) milhões de usuários. Perde apenas para a Índia, líder do ranking, que conta com mais de 300 (trezentos) milhões de usuários e o Estados Unidos, que ocupa o segundo lugar com mais de 210 (duzentas e dez) milhões de usuários na referida rede social[80].

Em meio a tantos usuários, a capacidade de armazenamento e tratamento de dados pessoais passa a ser uma preocupação frente às violações ao Direito à Privacidade e ao Direto à Proteção de Dados Pessoais, que já ocorriam no meio *web*, fato que veio à tona e expôs o escândalo entre o Facebook e a Cambridge Analytica.

Em 17 de março de 2018, Christopher Wylie, ex-funcionário da Cambridge Analytica revelou aos jornais The New York Times e The Gardian que a empresa obteve ilegalmente dados dos usuários do Facebook. Quase 87 (oitenta e sete) milhões de usuários[81] tiveram suas informações coletadas indevidamente – sem consentimento – pela Cambridge Analytica, com o aval do Facebook, informações essas que eram recolhidas desde o ano de 2014. A alegação à época foi que os dados foram recolhidos

---

77 Cf. G1, "*Facebook atinge os 2 bilhões de usuários*", in G1, 2017, texto disponível em https://g1.globo.com/tecnologia/noticia/facebook-atinge-os-2-bilhoes-de-usuarios.ghtml [04.09.2019].

78 Cf. CLEMENT, James, "*Most famous social network sites worldwide as of July 2019, ranked by number of active users (in millions)", in Statista*, 2019, texto disponível em https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ [04.09.2019].

79 Cf. VOLTILINI, Ramon, "*Brasil é o segundo país com mais contas registradas no Facebook", in Tecmundo,* 2013, texto disponível em https://www.tecmundo.com.br/facebook/38693-brasil-e-o-segundo-pais-com-mais-contas-registradas-no-facebook.html [04.09.2019].

80 Cf. R7, "*Brasil é o 3º país com o maior número de usuários do Facebook*", *in R7*, 2019, texto disponível em https://noticias.r7.com/tecnologia-e-ciencia/brasil-e-o-3-pais-com-o-maior-numero-de-usuarios-do-facebook-02032019 [04.09.2019].

81 Cf. SOLON, Olivia, "*Facebook says Cambridge Analytica may have gained 37m more users' data*", *in The Guardian*, 2018, texto disponível em https://www.theguardian.com/technology/2018/apr/04/facebook-cambridge-analytica-user-data-latest-more-than-thought [04.09.2019].

com a finalidade de influenciar a opinião dos eleitores em vários países para afetar as eleições presidenciais.

Após as revelações a respeito da coleta e uso indevido de dados pessoais, o Facebook fez pedido público de desculpas e se defendeu alegando que a Cambridge Analytica coletava os dados pessoais de seus usuários de forma "inadequada[82]".

Em dezembro de 2015, os principais jornais dos Estados Unidos informavam que o Facebook se valia de tal prática (coleta de dados) para fins políticos[83]. Era cristalino a violação ao Direito à privacidade e ao Direito à Proteção de Dados Pessoais dos usuários do Facebook, pois tiveram suas informações roubadas com a finalidade de serem influenciados na escolha de seu voto[8485].

A violação ao Direito à Proteção de Dados Pessoais dos usuários do Facebook, bem como à privacidade dos mesmos, incitou no mundo todo, discussões acerca das atitudes das duas empresas em relação às leis de proteção aos direitos fundamentais violados, bem como levantou insegurança quanto a real proteção aos usuários da maior rede social do mundo.

Por fim, o proprietário do Facebook, em 25 de março de 2018, Mark Zuckerberg, veio a público pedir desculpas por todo o ocorrido e prometeu fazer as alterações necessárias com a finalidade de impedir outras infrações relacionadas à violação de dados pessoais e à privacidade de seus usuários.

Além dos processos judiciais que o Facebook responde pela clara violação ao Direito à Proteção de Dados Pessoais e à Privacidade dos seus usuários, também perdeu mais de 35 (trinta e cinco) bilhões de dólares na bolsa de valores[86].

3.2. "A Google lê todos os seus e-mails." – O caso Google no Brasil

Atualmente o principal e o mais conhecido buscador de informações disposto na rede mundial de internet e detentor do maior catálogo de referências e dados é a Google.

---

82 Cf. BBC NEWS, "*Facebook scandal 'hit 87 million users*", *in BBC News,* 2018, texto disponível em https://www.bbc.com/news/technology-43649018 [04.09.2019].

83 Cf. DAVIES, Harry et al., "*Ted Cruz campaign using firm that harvested data on millions of unwitting Facebook users*", New York, *in The Guardian*, 2015, texto disponível em https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data [04.09.2019].

84 Cf. ROSENBERG, Matthew, "*Trump Consultants Exploited the Facebook Data of Millions", in The New York Times*, 2018, texto disponível em: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html [04.09.2019].

85 Cf. CADWALLADR, Carole e GRAHAM-HARRISON, Emma, "*Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach", in The Guardian*, 2018, texto disponível em https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election [04.09.2019].

86 Cf. BBC NEWS BRASIL, "*O escândalo que fez o Facebook perder US$ 35 bilhões em horas", in BBC News Brasil*, 2018, texto disponível em https://www.bbc.com/portuguese/internacional-43466255 [04.09.2019].

A Google LLC[87], como assim é conhecida, principal subsidiária da Alphabet Inc.[88], é uma empresa multinacional estadunidense que presta serviços online e tem como finalidade colher dados de seus usuários através de seus mecanismos de buscas e comercializá-los através de publicidades pelos AdWords[89].

A Google foi fundada em 4 de setembro de 1998 como uma empresa privada por Larry Page e Sergeu Brin, enquanto os mesmos ainda eram estudantes de doutorado da Universidade de Stanford nos Estados Unidos. A oferta pública inicial da Google ocorreu em 19 de agosto de 2004 e tinha como sua principal missão "organizar a informação mundial e torná-la universalmente acessível e útil[90]". O crescimento da Google, desde seu início, aconteceu de forma muito rápida e atualmente a empresa oferece vários outros softwares, além de liderar o desenvolvimento de sistema operacional Android para smartphones e tablets.

A Google é executada em mais de um milhão de servidores ao redor do mundo[91] e trata mais de um bilhão de solicitações de buscas[92] por dia, o que gera um número ilimitado de dados através de seus buscadores, sendo classificada como o website mais visitado no mundo[93].

Ser a maior empresa do mundo em acessos e aglomerado de dados expõe a Google a criticas acerca de assuntos como direitos autorais, censura, privacidade e dados pessoais, o que não é novidade para a empresa, que já foi classificada como uma das piores empresas do mundo no que diz respeito à privacidade dos seus usuários[94], motivo que a levou a enfrentar vários processos no Brasil, sendo que o mais conhecido é "o Caso Google. A Google lê todos os seus e-mails[95]."

---

87 Cf. BERGEN, Mark, "*Alphabet Finishes Reorganization With New XXVI Company", in Bloomberg,* 2017, texto disponível em https://www.bloomberg.com/news/articles/2017-09-01/alphabet-wraps-up-reorganization-with-a-new-company-called-xxvi [28.08.2019].

88 Cf. WOMACK, Brian, "*Google Creates New Company Called Alphabet, Restructures Stock*", *in Bloomberg*, 2015, texto disponível em https://www.bloomberg.com/news/articles/2015-08-10/google-to-adopt-new-holding-structure-under-name-alphabet- [27.08.2019].

89 *"Google Ads, antes conhecido como Google AdWords, é o principal serviço de publicidade da Google e principal fonte de receita desta empresa representando 96% dos quase 37,9 Bilhões de dolares que a empresa faturou em 2011. O serviço usa o sistema de publicidade por Custo por Clique (CPC) e Custo por mil impressões (CPM) que consiste em anúncios em forma de links encontrados, principalmente, nos mecanismos de pesquisa relacionados às palavras-chave que o internauta está pesquisando."* Cf. GEDDES, David, "*How does Google make money?*", *in Revenue Infographic,* 2011, texto disponível em https://www.webanalyticsworld.net/2012/01/how-does-google-make-money-2011-revenue-infographic.html [27.08.2019].

90 *"Nossa missão é organizar as informações do mundo para que sejam universalmente acessíveis e úteis para todos."* Cf. GOOGLE, "*Google Corporate Information", in Google Inc.,* 2010, texto disponível em https://about.google/ [27.08.2019].

91 Cf. S/A, "*Google: one million servers and counting*", *in Pandia,* 2007, texto disponível em http://www.pandia.com/articles/gartner [27.08.2019].

92 Cf. KUH, Eric, "*Google unveils top political searches of 2009", in CNN,* 2009, texto disponível em http://politicalticker.blogs.cnn.com/2009/12/18/google-unveils-top-political-searches-of-2009/ [27.08.2019]

93 Cf. ALEXA, *"Alexa Traffic Rank for Google", in Alexa Internet,* 2009, texto disponível em https://www.alexa.com/siteinfo/google.com [27.08.2019].

94 Cf. BBC NEWS, "*Google ranked 'worst' on privacy", in BBC News*, 2007, texto disponível em http://news.bbc.co.uk/2/hi/technology/6740075.stm [27.08.2019].

95 Cf. GOMES, Helton Simões, *"Até R$ 9,7 milhões! Brasil quer multar Google por 'ler' emails no Gmail", São Paulo, in UOL,* 2019, texto disponível em https://www.uol.com.br/tilt/noticias/redacao/2019/02/07/ate-r-97-milhoes-brasil-quer-multar-google-por-ler-seus-emails-no-gmail.html [02.09.2019].

Como bem aponta VERONESE e CUNHA, "a rápida evolução das tecnologias de informação e comunicação aplicadas nas transações *online* não pode ignorar a necessidade de implantação de mecanismos de segurança e de criptografia cada vez mais eficazes (...). De mesmo modo, as legislações nacionais referentes às relações de consumo devem ser redesenhadas considerando o ambiente virtual em que tais operações agora ocorrem e os riscos existentes, criando obrigações de segurança para as empresas e assegurando a reparação devida às vítimas de vazamentos de dados pessoais e bancários[96]".

A surpresa em relação à matéria não chocou, como deveria ser, isso por que não era a primeira vez que fatos como esses aconteceram. MASILI, relembra que "[t]al realidade já tinha sido notada desde as revelações feitas por Edward Snowden[97], na medida em que os sistemas de vigilância utilizados pela Agência Nacional norte-americana, como o PRISM[98], não foram por ela desenvolvidos, mas criados por empresas para obter dados coletados por companhia como Microsoft, GOOGLE e Yahoo. (...) Em algumas situações, as companhias desenvolvedoras das tecnologias trabalhavam conjuntamente com a agência, ao passo que, em outros casos, era compelida judicialmente fornecer os dados ou tinham sua infraestrutura invadida pela agência[99]."

O processo judicial no Brasil, no caso Google, surgiu por meio de denúncia pela Secretaria Nacional do Consumidor (SeNaCon), do Ministério da Justiça, que já havia instaurado processo administrativo contra a Google, a fim de verificar se a empresa violava a privacidade e os dados pessoais dos consumidores. A acusação foi oferecida pelo Ministério Público Federal do Piauí (MPFPI).

No conteúdo da denúncia, as alegações eram de que a empresa fazia análise de todo o conteúdo de e-mails pessoais dos consumidores que tinham contas junto ao Gmail, com a finalidade de personalizar anúncios, fato esse que viola os Direitos à privacidade e à Proteção de Dados Pessoais

---

96 Cf. VERONESE, Alexandre e CUNHA, Marcelo, *"Desafios do comércio eletrónico no Brasil: integração vertical entre fornecedores e meios de pagamentos, proteção de dados pessoais e cooperação regulatória internacional",* Braga, UNIO - EU Law Journal, vol. 4, n°. 2, julho 2018, p 83.

97 *"O ex-técnico da CIA Edward Snowden, de 29 anos, é acusado de espionagem por vazar informações sigilosas de segurança dos Estados Unidos e revelar em detalhes alguns dos programas de vigilância que o país usa para espionar a população americana – utilizando servidores de empresas como Google, Apple e Facebook – e vários países da Europa e da América Latina, entre eles o Brasil, inclusive fazendo o monitoramento de conversas da presidente Dilma Rousseff com seus principais assessores."* Cf. G1*, "Entenda o caso de Edward Snowden, que revelou espionagem dos EUA*", São Paulo, *in G1*, 2014, texto disponível em http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html [02.09.2019].

98 *"The National Security Agency has obtained direct access to the systems of Google, Facebook, Apple and other US internet giants, according to a top secret document obtained by the Guardian. The NSA access is part of a previously undisclosed program called Prism, which allows officials to collect material including search history, the content of emails, file transfers and live chats, the document says."* Cf. BALL, James e RUSHE, Dominc, "*NSA Prism program taps in to user data of Apple, Google and others*", in The Guardian, 2013, texto disponível em https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [02.09.2019].

99 Cf. MASILI, Clarissa Menezes Vaz, *Regulação do uso de dados pessoais no Brasil: papel do usuário na defesa de um direito à tutela de dados pessoais autônomo,* Tese Doutorado, Orientadora Christiana Soares de Freitas, Universidade de Brasília, 2018, pp. 74

daqueles que utilizam o citado correio eletrônico, motivo que levou o caso a ser conhecido como "O Google, lê todos os seus e-mails".

O MPFPI usou como precedente o caso semelhante entre a Google e o governo Italiano, ocorrido em 2014. Porém, na Itália, quando da violação aos direitos mencionados, já existia figura da autoridade nacional de proteção de dados pessoais que verificou, dentre outros atos ilícitos, que a Google lia todos os e-mails para fins de escanear dados. À época, a Itália exigiu que a Google apresentasse um mecanismo próprio, para que o usuário pudesse autorizar (se assim fosse sua vontade) o escaneamento dos dados.

Na Ação Civil Pública de n.º 0025463-45.2016.4.01.4000[100], originária do inquérito civil público de n.º 1.27.000.001406/2015-03[101], a Google, em sua defesa, informou que não usava informação disponível no Gmail para a personalização de anúncios. Acrescentou ainda que seguia as legislações brasileiras sobre privacidade e Proteção de Dados Pessoais. Caso fosse condenada, a empresa poderia ser compelida a pagar multa em até 9,7 (nove vírgula sete milhões de reais).

A sentença proferida em 2018 foi favorável à Google, com os seguintes argumentos pelo magistrado do processo citado: "Concluo não restarem preenchidos os requisitos da plausibilidade jurídica e do perigo de dano. (...) Como explanado na contestação, a empresa ré não visualiza o conteúdo do e-mail, apenas identifica palavras-chave para fins de encaminhamento automatizado de propaganda direcionada[102]."

Casos como o "A Google lê todos os seus e-mails" e o "Escândalo entre o Facebook e a Cambridge Analytica" suscitam algumas dúvidas entre os usuários da internet e titulares dos dados, sendo uma delas que a esta dissertação cabe responder, estamos realmente tutelados pelas leis vigentes no que tange ao Direito à Proteção de Dados Pessoais? O que o Direito à Proteção de Dados Pessoais protege e proíbe? Essa pergunta somente poderá ser respondida após estudo hermenêutico do ordenamento jurídico brasileiro no que tange ao Direito à Proteção de Dados Pessoais, o que se passa agora a fazer.

---

100 Cf. BRASIL, Tribunal Regional Federal da 1ª Região – TRT, Ação Civil Pública, Processo n.º 0025463-45.2016.4.01.4000, 2º Vara de Teresina, Juíz Márcio Braga Magalhães, autuado em 04.11.2016, Autor: Ministério Público Federal, Réu: Google Brasil Internet Ltda, texto disponível em https://processual.trf1.jus.br/consultaProcessual/processo.php?proc=25463452016401400 0&secao=PI&nome=GOOGLE%20BRASIL%20INTERNET%20LTDA&mostrarBaixados=N [02.09.2019].

101 Cf. BRASIL, Ministério Público Federal, Inquérito Civil Público n.º 1.27.000.001406/2015-03, texto disponível em http://www.mpf.mp.br/pi/sala-de-imprensa/docs/acp-google [02.09.2019].

102 Cf. BRASIL, Tribunal Regional Federal da 1ª Região – TRT, Ação Civil Pública, Processo n.º 0025463-45.2016.4.01.4000..., op. cit.

CAPÍTULO III

DO REGIME JURÍDICO BRASILEIRO DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS

1. Do direito à proteção de dados pessoais na constituição da república federativa do brasil (CRFB) de 1988

O Direto à Proteção de Dados Pessoais não se apresenta através de uma estrutura unitária, mas sim disperso em vários instrumentos jurídicos brasileiros, como por exemplo, a própria Constituição, o Código Civil, o Código de Defesa do Consumidor, as Leis Ordinárias, como o Marco Civil da Internet e, recentemente, a Lei Geral de Proteção de Dados Pessoais, entre outros.

Na CRFB de 1988, em seu Título II, "Dos Direitos e Garantias Fundamentais" no capítulo I, "Dos Direitos e Deveres Individuais e Coletivos" é possível encontrar direitos e garantias análogos ao Direito à Proteção de Dados Pessoais, bem como ao tratamento, armazenamento e uso de dados como fonte de informação. Vejamos:

Entre eles, o Direito à Liberdade de Expressão, que se encontra respaldado no artigo 5.º, inciso IX dispondo que "é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;" inciso esse que é reforçado pelo artigo 220, também da Carta Magna, que dispõe acerca "[d]a manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição."

O mesmo reconhecimento se estende ao Direito à Informação, que também encontra apoio no artigo 5.º no inciso XIV salientando que "é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;" (...) "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;".

Há também a previsão da proteção ao Direito à inviolabilidade, bem como proibição de invasão de domicílio, o inciso XI, do mesmo artigo, que dispõe que "a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;" proteção essa que também se estende ao sigilo das correspondências, no inciso XII, já citado.

Há ainda previsão no artigo 5.º, ao Direito Fundamental à Intimidade e à Vida Privada, disposto em seu inciso X, onde o mesmo informa que, "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;" bem como, de forma mais específica ainda, há previsão de proteção contra a interceptação de comunicações telefônicas, telegráficas ou de dados, onde o inciso XII reza que "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 consagração pela CRFB de 1988, como um direito com garantia fundamental, do Direito à Intimidade e à Vida Privada a qualquer pessoa em território nacional, é reflexo do reconhecimento dos valores que constituem a personalidade garantidores da dignidade da pessoa humana. Sua inviolabilidade, independente da esfera processual, tem como finalidade evitar que individuo venha sofrer qualquer atentado a sua dignidade, bem como a uma exposição indevida.

A jurisprudência da Suprema Corte Brasileira – STF – tem solidificado entendimento no intuito de proteção ao direito fundamental à privacidade, que por sua vez, tutela a intimidade, a vida privada, a imagem das pessoas e sua honra, mesmo quando há necessidade de sobrepor esse direito em relação a outros direitos. Isso quer dizer que, mesmo quando o julgador precisar escolher entre o Estado manter sua soberania, por exemplo, ele ainda há de respeitar tais princípios constitucionais, como acontece no caso da proibição e escutas telefônicas ilícitas como prova no processo penal.

Atualmente, o Direito à Intimidade e à Vida Privada não tem tutelado – como tem de ser – as particularidades relacionadas as violações de dados pessoais, isso porque, ainda que semelhantes, são direitos distintos, razão essa que motiva o constituinte a rever o aparato jurídico nacional a fim de se ampliar o rol de direitos e garantias fundamentais para se inserir um novo Direito, sendo ele o Direito à Proteção de Dados Pessoais, tendo em vista o momento vivenciado pela sociedade em decorrência do alcance e uso da internet através das redes sociais, mercado digital e outros.

O acesso fácil às notícias, imagens e vídeos pela internet tem facilitado cada vez mais as relações interpessoais, que, dia após dia, ganham maior visibilidade dentre os meios de comunicação. Dados pessoais nunca estiveram tão expostos em toda a história da humanidade. A internet, principalmente através das redes sociais, do acesso aos e-mails, ou banco de dados na nuvem, tem captado informações que podem em algum momento serem utilizadas de forma indevida através de um tratamento, armazenamento ou uso não consentido.

A exemplo disso é que se encontram casos que envolvem exposição de fotos e vídeos íntimos, os quais tiveram maior visibilidade nacional pela exposição ter ocorrido por meio da internet, como por exemplo, o vazamento de fotos íntimas da Atriz Carolina Dieckmann, em 2012[103].

A repercussão da exposição, sem autorização, violou diretamente Direito à Intimidade e à Vida Privada, previsto na CRFB de 1988, fato esse que levou o legislador a editar a lei n.º 12.373/2012[104], mais conhecida como Lei Carolina Dieckmann, que também incluiu ao atual Código Penal Brasileiro o artigo 154-A, que passou a tipificar como crime "[i]nvadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa".

De um lado há a Carta Magna brasileira que reconhece e garante a proteção do direito à intimidade, à vida privada, porém, na prática, a jurisprudência das cortes superiores não os tratam como um direito absoluto, assim como de fato, nenhum direito é. Nesse sentido já tem se manifestado o STF[105], que, em caso de conflitos de direitos, tem firmado entendimento de sempre haver uma ponderação nos casos concretos, casos que vão além da leitura da lei, fato esse que só é possível quando se encontrar presente os princípios da proporcionalidade e da razoabilidade.

Por fim, há ainda na Carta Magna, o remédio constitucional do *habeas data* que prevê um direito genérico de acesso e retificação de dados pessoais, disposto também no artigo 5.º, em seu inciso LXXII, com a finalidade de "a) (...) assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;" e também possibilitar a " b) (...) retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;".

O *habeas data*, remédio constitucional previsto na CRFB de 1988, por muito tempo trouxe amparo a sociedade com vistas à proteção de dados pessoais, ante a ausência de uma lei específica.

---

103 Cf. POETA, Patrícia, "*Atriz Carolina Dieckmann fala sobre fotos pessoais expostas na internet*", Rio de Janeiro, *in G1*, 2012, texto disponível em http://g1.globo.com/jornal-da-globo/noticia/2012/05/atriz-carolina-dieckmann-fala-sobre-fotos-pessoais-expostas-na-internet.html [09.09.2019].

104 Cf. BRASIL, Lei nº 12.373, de 30 de novembro de 2012, *"Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências*", texto disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.html [09.09.2019].

105 Cf. SUPREMO TRIBUNAL FEDERAL – STF, Habeas Corpus nº 93250 MS, Relator: Min. Ellen Gracie, Data de Julgamento: 10/06/2008, Segunda Turma, Publicado no DJe n.º 117, divulgado em 26-06-2008, publicado em 27-06-2008, ementa VOL-02325-04, PP-00644, texto disponível em https://stf.jusbrasil.com.br/jurisprudencia/14720278/habeas-corpus-hc-93250-ms/inteiro-teor-103108730?ref=juris-tabs [09.09.2019].

Exemplo disso tem-se o julgado – importantíssimo – pelo STF[106] acerca do direito ao esquecimento, ou seja, direito de "apagar" dados pessoais inseridos em sites de maus pagadores, como SERASA, Serviço de Proteção ao Crédito (SPC) e outros.

Nesse sentido, o *habeas data* foi criado com a ideia de cada pessoa (titular dos dados) poder decidir por si, exceto, quando for de interesse restrito pelo Estado, de que forma, e quando os dados podem ser revelados ao público em geral[107]. Assim, o *habeas data* se apresenta com dois aspectos distintos, quando comparados ao direito à privacidade, pois tem força para alterar os dados que podem ser identificados e que venham a expor, de alguma forma, a vida privada de um cidadão e de impedir o acesso, divulgação dos dados pessoais que estão sob posse de algum ente público.

A doutrina brasileira[108] tem consagrado a necessidade, desde sua criação (*habeas data),* da proteção ao impetrante por se tratar de direito personalíssimo de quem dele se socorre, com a finalidade de poder ter o controle sobre seus próprios dados pessoais, que podem ser encontrados em registros públicos ou privados, bem como poder fazer retificação, complementação, explicação ou exclusão das informações que lhe convir.

---

106 Nesse sentido, importante expor o RE. n.° 22.337, sendo ele uma decisão histórica do Superior Tribunal de Justiça - STJ, onde se decidiu que "o registro de dados pessoais no SPC deve ser cancelado após cinco anos (art. 43§ 1°, Lei 8.078/90). Nesse sentido, somente para fins didáticos, cabe ainda expor, o voto do Ministro Ruy Rosado de Aguiar, que defendeu a existência na CRFB-88 de um direito à autodeterminação informativa ou direito à proteção de dados pessoais no Brasil antes de qualquer lei que regulasse sobre o tema de forma específica. Vejamos: *"A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado de diversas atividades da pessoa, nas múltiplas situações de vida, permite o conhecimento de sua conduta publica e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, publico ou privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição politica ou opressão econômica. A importância do tema cresce de ponto quando se observa o numero imenso de atos da vida humana praticados através da mídia eletrônica ou registrados nos disquetes de computador. Nos países mais adiantados, algumas providencias já foram adotadas. Na Alemanha, por exemplo, a questão está posta no nível de garantias fundamentais, com o direito de autodeterminação informacional (o cidadão tem o direito de saber quem sabe o que sobre ele), além da instituição de órgãos independentes, à semelhança do ombudsman, com poderes para fiscalizar o registro de dados informatizados, pelos órgãos públicos e privados, para garantia dos limites permitidos na legislação [...]. No Brasil, a regra do art. 5°, inc. X, da Constituição de 1988, é um avanço significativo".* Cf. SUPERIOR TRIBUNAL DE JUSTIÇA – STJ, RE.. n.° 22.337, Relator Min. Ruy Rosado de Aguiar, Quarta Turma, julgado em: 13 fev. 1995, publicado em: 20 mar. 1995, texto disponível em http://www.mpsp.mp.br/portal/page/portal/cao_consumidor/jurisprudencia/juris_diversos/Resp533625_0.doc [09.09.2019].

107 Cf. PIERINI, Alicia, et. al., *Hábeas data: derecho a la intimidad: derecho a informar, limites, censura*, Buenos Aires, Buenos Aires Universidad, 1999, p. 20.

108 Cf. MORAES, Alexandre de, "*Direito constitucional",* São Paulo, Atlas, 24. ed., 2009; Cf. FERRAZ, Sérgio Valadão, *Curso de direito constitucional: teoria, jurisprudência e questões,* Rio de Janeiro, Elsevier, 4° ed., 2008; Cf. MOURÃO NETO, Samuel Francisco, *Arquivos de consumo (cadastros e bancos de dados de consumidores) e habeas data (individual e coletivo*), In Repositório PUC, S/d, texto disponivel em http://www.pucsp.br/tutelacoletiva/download/artigo_samuel.pdf [09.09.2019].

Muito antes de qualquer discussão acerca do Direito à Proteção de Dados Pessoais no Brasil, alguns doutrinadores[109] já entendiam que o referido remédio constitucional, certamente era um instrumento processual que visava à defesa da autodeterminação informativa e dos dados pessoais.

Importante expor que a inclusão do *habeas data* na Carta Magna surgiu como resposta ao uso institucional e autoritário da informação. O crédito a tal ação é dado a José Afonso da Silva, que por sua vez foi influenciado por Firmín Morares Prats que, através de sua obra "*La tutela penal de la intimidad: "privacy" e informática",* apresentou à Comissão Provisória de Estudos Constitucionais, durante a criação do Anteprojeto da Constituição de 1988, a ideia de se reconhecer um Direito à Proteção de Dados Pessoais (artigo 17[110]); dessa forma, nascia o *habeas data* (artigo 48[111]) como remédio constitucional para fruição desse direito.

Muito embora a atual CRFB de 1988 não tenha constado o Direito à Proteção de dados pessoais, como fazia referência o artigo 17 do anteprojeto, o *habeas data* se fez presente, e acabou por servir como referência para outros ordenamentos jurídicos, tendo ainda, mais tarde, sua regulação através de Lei Ordinária de n.º 9.507, de 12 de novembro de 1997, com finalidade de regular o direito de acesso a informações e seu próprio rito processual.

De acordo com a análise realizada até aqui, percebe-se através da estrutura constitucional em relação aos direitos e garantias fundamentais elencados no artigo 5.º, que a consagração ao Direito à Proteção de Dados Pessoais, ainda que não previsto formalmente, já se encontra disposta como um direito fundamental materialmente constitucional, implícito em decorrência dos direitos à intimidade e à vida privada (artigo 5.º, inciso X), à informação (artigo 5.º, inciso XIV), ao sigilo de comunicações e dados (artigo 5.º, inciso XII) e da garantia individual ao conhecimento, correção de dados, bem como sua exclusão, pelo remédio constitucional habeas data (artigo 5.º, inciso LXXII).

Nessa ótica, desde 2008, RODOTÁ já defendia que "estamos diante da verdadeira reinvenção da proteção de dados – não somente porque ela é expressamente considerada como um direito

---

109 Cf. BAZÁN, Victor, *El habeas data e o direito à autodeterminação infor*mativa em perspectiva de direito comparado, Chile, Estudios Constitucionales (Centro de Estudios Constitucionales – Universidad de Talca), Ano 3, n.º 2, 2005, pp. 85-139; Cf. MAIA, Fernando Joaquim Ferreira, *O habeas data e a tutela da dignidade da pessoa humana na vida privada,* Vitória, Revista de Direitos e Garantias Fundamentais, n.º 12, pp. 269-303.

110 *"Art. 17 – Todos têm direito de acesso às referências e informações a seu respeito, registradas por entidades públicas ou particulares, podendo exigir a retificação de dados, com sua atualização e supressão dos incorretos, mediante procedimento judicial sigiloso. § 1º – É vedado o registro informático sobre convicções pessoais, atividades políticas ou vida privada, ressalvado o processamento de dados não identificados para fins estatísticos. § 2º – A lesão decorrente do lançamento ou da utilização de registros falsos gera a responsabilidade civil, penal e administrativa".* Cf. BRASIL, "*Anteprojeto Constitucional, elaborado pela Comissão Provisória de Estudos Constitucionais, instituída pelo Decreto nº 91.450, de 18 de julho de 1985"*, texto disponível em https://www.senado.leg.br/publicacoes/anais/constituinte/AfonsoArinos.pdf [09.09.2019].

111 *"Art. 48 – Dar-se-á habeas data ao legítimo interessado para assegurar os direitos tutelados no art. 17".* Cf. BRASIL, "*Anteprojeto Constitucional, elaborado pela Comissão Provisória de Estudos Constitucionais...* op. cit., Artigo 48.

fundamental autônomo (o autor refere-se à Carta de Direitos Fundamentais da União Europeia[112]), mas também por que se tornou uma ferramenta essencial para o livre desenvolvimento da personalidade. A proteção de dados pode ser vista como a soma de um conjunto de direitos que configuram a cidadania do novo milênio[113]".

A dimensão jusfundamental do Direito à Proteção de Dados Pessoais se da em razão de os dados serem elementos que compõem a identidade de uma pessoa, por isso, devem ser protegidos na equivalência da composição fundamental da personalidade de seu titular, que, deve ter o amparo da lei para o reconhecimento de sua dignidade.

2. Do direito à proteção de dados pessoais nos diplomas legais

2.1. Do direito à proteção de dados pessoais no código civil[114] (CC), Lei n.º 10.406, de 10 de janeiro de 2002

Um dos diplomas legais mais extensos e importantes no ordenamento jurídico brasileiro é o Código Civil (CC), que é composto por um conjunto de normas que tem como finalidade determinar direito e deveres das pessoas, quer sejam elas naturais ou coletivas, de seus bens e as suas relações no âmbito privado, tendo como base legal a CRFB de 1988. Instituído pela Lei n.º 10.406 de 10 de janeiro de 2002, o atual CC entrou em vigor em 11 de janeiro de 2003.

O Código Civil é a norma legal que disciplina e parametriza o Direito Civil, sendo esse último o ramo do direito que trata das relações de natureza civil, e que abarca desde o nascimento até a morte de um indivíduo. Nesse sentido, esse diploma legal tem como finalidade ser um ponto de equilíbrio para a manutenção da justiça e a convivência social, traz igualdade a todos e evita conflitos nas relações civis.

O Código Civil é composto por 2.046 (dois mil e quarenta e seis) artigos, que formam juntos, 8 (oito) livros, dividido em duas partes. A parte geral, disciplina acerca das Pessoas, Dos Bens e Dos Fatos Jurídicos; e a parte Especial, disciplina acerca do Direito das Obrigações, Do Direito de Empresa, Do Direito das Coisas, Do Direito de Família e Do Direito das Sucessões.

---

112 *"Artigo 8 – 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 respectiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente."* Cf. BRASIL, "*Anteprojeto Constitucional, elaborado pela Comissão Provisória de Estudos Constitucionais...* op. cit.

113 Cf. RODOTÀ, Stefano, *A vida na sociedade de vigilância: privacidade hoje*, Rio de Janeiro, Renovar, 2008, p. 14.

114 Cf. BRASIL, Lei nº 10.406, de 10 de janeiro de 2002, *"que institui...", op. cit.*

Assim como a CRFB de 1988, o Código Civil de 2002 não traz de forma unitária e clara o reconhecimento do Direito à Proteção de Dados Pessoais. Contudo, disciplina direitos análogos, que têm a mesma finalidade, qual seja, proteção do direito à personalidade humana, assim como os valores e peculiaridades que a ela estão ligados.

Logo na Parte Geral, em seu Capítulo II, o Código Civil trata "Dos Direitos da Personalidade" e nele se pode encontrar os artigos 11 ao 21. Para GONÇALVES, o reconhecimento de Direitos da Personalidade pelo legislador, reflete "o respeito à dignidade humana [que se encontra] em primeiro plano, entre os fundamentos constitucionais pelos quais se orienta o Ordenamento Jurídico Brasileiro na defesa dos direitos da personalidade na CRFB/88 no artigo 1.º, inciso III[115]."

O artigo 11 disciplina que, "[c]om exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária."

O direito à personalidade é norma de caráter subjetivo, porque são direitos inerentes à pessoa humana, e seguem sua natureza, bem como são direitos natos, tais como direito à vida, à integridade física, à honra, à imagem e à privacidade, por exemplo. Dentro do atual ordenamento jurídico não há uma descrição exauriente, perfeita e acabada de quais direitos encontram base no direito à personalidade.

Nesse sentido, ensina VENOSA que "não há que se entender que nossa lei, ou qualquer outra lei comparada, apresente um número fechado para descrever todos os direitos da personalidade. Terá essa natureza todo o direito subjetivo pessoal que apresentar as características semelhantes, ainda que não descritos perfeitamente na lei[116]".

Reafirmando a doutrina de VENOSA, o Enunciado 274[117] da IV Jornada de Direito Civil firma o entendimento de que "os direitos da personalidade, regulados de maneira não exaustiva pelo Código Civil, são expressões da cláusula geral de tutela da pessoa humana, contida no art. 1.º, III, da Constituição (princípio da dignidade da pessoa humana). Em caso de colisão entre eles, como nenhum pode sobrelevar os demais, deve-se aplicar a técnica da ponderação".

DINIZ, orienta que "o direito da personalidade é o direito da pessoa de defender o que lhe é próprio, como à vida, à identidade, à liberdade, à imagem, à privacidade, à honra etc. É o direito subjetivo,

115 Cf. GONÇALVES, Carlos Roberto, *Direito civil brasileiro, Parte Geral,* São Paulo, Saraiva, 5º ed., vol. 01, 2007, p. 19.

116 Cf. VENOSA, Silvio de Salvo, *Código Civil Interpretado*, São Paulo, Atlas, 2010, p. 21.

117 Cf. AGUIAR, Ruy Rosado de, *IV Jornada de Direito Civil. Enunciado 274,* Conselho da Justiça Federal, 2002, texto disponível em https://www.cjf.jus.br/enunciados/enunciado/219 [09.09.2019].

convém repetir, de exigir um comportamento negativo de todos, protegendo um bem próprio, valendo-se uma ação judicial[118]".

A fim de resguardar o direito à personalidade, o artigo 12 do mesmo código dispõe que aquele que tiver seu direito violado "[p]ode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei."

Mais adiante, no artigo 16 o diploma legal garante que "[t]oda pessoa tem direito ao nome, nele compreendidos o prenome e o sobrenome." O nome, tem como finalidade a identificação e a individualização de uma pessoa na sociedade. Ao mesmo tempo em que é um direito, também é um a atributo da personalidade, e certamente, faz parte do rol dos dados pessoais.

O artigo 17, também do Código Civil, prevê a proteção para aqueles que tiverem seu nome exposto na forma de desprezo em publicações públicas, fato esse ainda corroborado com o artigo 18 que reforça a violação desse direito quando a exposição for sem autorização.

Mais adiante, no artigo 20, o Diploma legal dispõe acerca do direito à exposição da imagem, direito esse ligado a personalidade. Nele diz que, "[s]alvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se destinarem a fins comerciais".

O artigo citado faz clara referência a um dado pessoal importantíssimo e de fácil identificação de uma pessoa, a imagem, que encontra proteção da norma legal. DINIZ ensina que "a imagem-retrato é a representação física da pessoa, como um todo, ou em parte separadas do corpo (nariz, olhos, sorriso etc.) desde que identificáveis, implicando o reconhecimento de seu titular, por meio de fotografia, escultura, desenho, pintura, interpretação dramática, cinematografia, televisão, sites etc., que requer autorização do retratado (CF, artigo 5.º, X). A imagem atributo é o conjunto de caracteres ou qualidades cultivadas pela pessoa, reconhecidos socialmente (CF, artigo 5.º, V), como habilidades, competência, lealdade, pontualidade etc. A imagem abrange também a reprodução, romanceada em livro, filme ou novela, da vida de pessoa de notoriedade[119]", por esse motivo merece proteção da lei, uma vez que sua exposição indevida, certamente viola outros direitos fundamentais, tais como o direito à intimidade e à privacidade, por exemplo, além do próprio Direito à Proteção de Dados Pessoais.

118 Cf. DINIZ, Maria Helena, *Curso de Direito Civil Brasileiro*, São Paulo, Saraiva, 2007, vol. I, 24. ed., p. 120.

119 Cf. DINIZ, Maria Helena. *Curso de Direito Civil Brasileiro*... op. cit., p. 129.

Oriundo do direito à personalidade, o direito à imagem também está ligado diretamente aos Dados Pessoais, e, nesse sentido, o citado artigo 20, confere essa proteção específica. Ademais, o Superior Tribunal de Justiça (STJ), por meio da súmula 403[120], consolidou o entendimento de que "[i]ndepende de prova do prejuízo a indenização pela publicação não autorizada de imagem de pessoa com fins econômicos ou comerciais", seguindo assim o entendimento do Supremo Tribunal Federal (STF)[121].

Por fim, o artigo 21, que encerra o Capítulo II do Código Civil, disciplina que "[a] vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma."

A privacidade é direito fundamental resguardado pela Carta Magna Brasileira, e é nela que o individuo guarda parte de sua vida e a mantém afastada de estranhos e do convívio público. A proteção conferida pela lei à vida privada guarda aspectos da vida íntima de uma pessoa, e garante o direito a ela de querer afastar informações pessoais que não queira dividir com outros. O mesmo fundamento se reflete na inviolabilidade de seu domicílio, no sigilo de suas correspondências, dados bancários e a outros dados pessoais.

O Código Civil ainda faz menção que os direitos da personalidade não se aplicam somente às pessoas físicas, ele também traz proteção às pessoas jurídicas, conforme dispõe seu artigo 52[122].

Importante ressaltar ainda que o Código Civil não reconhece somente os direitos da personalidade, também confere proteção processual a eles com a possibilidade de indenização pelos danos causados a pessoa quando da exposição indevida de dados que venham identificar qualquer um perante terceiro ou perante à sociedade.

Nesse sentido, encontra disposto o artigo 186, que explana que "[a]quele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito".

Não obstante o artigo 186 do Código Civil que define o que é ato ilícito, observa-se que o mesmo não disciplina o dever de indenizar, ou seja, a responsabilidade civil, matéria extremamente bem tratada

120 Cf. SUPERIOR TRIBUNAL DE JUSTIÇA – STJ, Súmula 403, texto disponível em https://ww2.stj.jus.br/docs_internet/revista/eletronica/stj-revista-sumulas-2014_38_capSumula403.pdf [09.09.2019].

121 Cf. SUPREMO TRIBUNAL FEDERAL - STF, Recurso Extraordinário n.º 215.984/RJ, Relator(a): Min. Carlos Velloso, Segunda Turma, julgado em 04/06/2002, DJe 28-06-2002, PP-00143, EMENT., VOL-02075-05, PP-00870, RTJ., VOL-00183-03, PP-01096, texto disponível em http://stf.jus.br/portal/jurisprudencia/listarJurisprudencia.asp?s1=%28RE%24%2ESCLA%2E+E+215984%2ENUME%2E%29+OU+%28RE%2EACMS%2E+ADJ2+215984%2EACMS%2E%29&base=baseAcordaos&url=http://tinyurl.com/l2n6u53 [09.09.2019].

122 *"Art. 52. Aplica-se às pessoas jurídicas, no que couber, a proteção dos direitos da personalidade".* Cf. BRASIL, Lei n.º 10.406..., *op. cit.*

no artigo 927 do mesmo Código, que assim determina: "[a]quele que, por ato ilícito (artigos 186 e 187), causar dano a outrem, fica obrigado a repará-lo."

O indivíduo é construído por um conjunto de valores que compõem o seu patrimônio e que podem ser objeto de lesões, em decorrência de atos ilícitos (já citado artigo 186, CC) que venham abalar a sua moral, dessa forma, merece reparação material.

Pelo exposto, tem-se que o Código Civil, ainda que não discipline de forma clara e reconheça um direito específico à Proteção de Dados Pessoais, esse direito encontra amparo na letra da lei, contudo, ainda há falhas, que somente uma legislação específica poderia sanar.

2.2. Do direito à proteção de dados pessoais no código de defesa do consumidor[123] (CDC), Lei n.º 8.708, de 11 de setembro de 1990

Os reflexos do Direito à Proteção de Dados Pessoais no Código de Defesa do Consumidor (CDC) são resultados da relação entre pessoas físicas e jurídicas, frente aos abusos sofridos em âmbito de igualdade fragilizada – quer seja em comparação com entes públicos ou privados –, uma vez que, as pessoas físicas, se apresentam como a parte mais fraca e vulnerável dessa relação, por isso são consideradas hipossuficientes[124] em relação às pessoas jurídicas.

Caracterizado uma relação em que haja vulnerabilidade entre as partes, a parte mais fraca deve ser agraciada com as normas atinentes na Lei n.º 8.078/90, principalmente no que tange aos direitos básicos do consumidor. Nisso a letra da lei mencionada é clara.

Devido a grande revolução informática nas últimas décadas, frente às novas tecnologias de comunicação e informação, o acesso e a veiculação de dados pessoais tem acontecido em uma escala nunca antes imaginada.

Os dados pessoais estão sendo comercializados ou pelo menos transferidos (colhidos e enviados) em todos os lugares. Exemplos disso acontecem; na compra de passagens aéreas, quando as companhias coletam e enviam dados de seus passageiros para as autoridades policiais e para o serviço de imigração e fronteiras; as operadoras telefônicas, além dos dados cadastrais em si, detêm a

123 Cf. BRASIL, Lei nº. 8.078, de 11 de setembro de 1990, *"Dispõe sobre a proteção do consumidor e dá outras providências",* texto disponível em http://www.planalto.gov.br/ccivil_03/leis/l8078.html [09.09.2019].

124 *"O CDC permite a inversão do ônus da prova em favor do consumidor, sempre que foi hipossuficiente ou verossímil sua alegação. Trata-se de aplicação do princípio constitucional da isonomia, pois o consumidor, como parte reconhecidamente mais fraca e vulnerável na relação de consumo (CDC 4º, I), tem de ser tratado de forma diferente, a fim de que seja alcançada a igualdade real entre os partícipes da relação de consumo. O inciso comentado amolda-se perfeitamente ao princípio constitucional da isonomia, na medida em que trata desigualmente os desiguais, desigualdade essa reconhecida pela própria Lei."* Cf. JÚNIOR, Nelson Nery, et al., *Código de Processo Civil Comentado.*, São Paulo, Revista dos Tribunais, 4ª ed., 1999, nota 13, p. 1805.

informação das ligações efetuadas e recebidas, número do IP de acessos à internet, da mesma forma que os provedores de internet tem a capacidade de armazenamento e rastreio de sites acessados.

Outro ponto de coletas de dados pessoais (imagem) em meio público, que também pode ser realizado por empresas privadas, são as câmeras de segurança, que ficam localizadas em pontos estratégicos e que coletam milhões de imagens de pessoas ao redor do mundo vinte e quatro horas por dia.

Em todas as relações comerciais o uso de dados pessoais se faz presente, motivo pelo qual mereceu atenção do CDC para sua proteção, código esse que foi publicado em 11 de setembro de 1990.

No que diz respeito a proteção específica de dados pessoais, o CDC, inicialmente, teve como preocupação principal a proteção dos consumidores ante o grande repositório de informações relativas a negativação de crédito.

Apenas a título de informação, há de se expor que, banco de dados – "coleção de dados inter-relacionados, representando informações sobre um domínio específico[125]"–, ou seja, informações em massa, já existem no Brasil desde o fim da década de 60, e desde então, têm se intensificado dia após dia com volume de contratos firmados, principalmente pela influência da internet na facilidade de contratar.

Muito antes da promulgação da CRFB de 1988, a violação de dados pessoais já era uma realidade vivenciada pelos brasileiros, ou seja, acontecia na prática, porém, os consumidores que sofriam com as violações de seus direitos não tinham a seu favor nenhum instrumento jurídico que lhes possibilitassem recorrer ao judiciário ante o problema dos repositórios de dados, principalmente por que não havia previsão legal acerca do assunto.

Quando da sua entrada em vigor, o CDC veio introduzir alguns dos princípios fundamentais constitucionais visando à proteção de dados pessoais. Teve como referência as principais leis de proteção de dados do mundo, o que refletiu no reconhecimento e proteção de uma série de direitos novos, bem como deveres para os gestores de bancos de dados.

O princípio fundamental constante no CDC se refere ao direito do consumidor "ter conhecimento", ou seja, saber de fato sobre todas informações que venham reger a relação de consumo, inclusive, por analogia, saber ainda quem detém informações a seu respeito, independente de sua vontade ou aprovação (aqui se refere a autorização por parte de quem tiver domínio dos dados do consumidor).

125 Cf. KORTH, Henry F. e SILBERSCHATZ, Abraham, *Sistemas de Bancos de Dados*, Makron Books, 2ª ed. revisada, 1994, p. 12.

O referido princípio se encontra disposto no artigo 6.º[126], corroborado ainda no § 2.º do artigo 43 que assim dispõe: "[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. (...) § 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."

Outro princípio igualmente importante se encontra disposto no § 3.º do artigo 42, que assim baliza: "[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."

O direito de retificação dos dados, inclusive naqueles já arquivados, demonstra claramente a possibilidade de controle dos dados pessoais daqueles que tenham conhecimento de que suas informações se encontram dispostas em um determinado banco de dados. Segundo o parágrafo do artigo citado, o consumidor pode, isto é, tem o direito de, a qualquer momento, requisitar informações e exigir a retificação ao gestor do banco de dados sobre seus dados pessoais.

Da mesma forma que o CDC trouxe direitos aos consumidores sobre seus dados, também ocasionou deveres aos gestores de banco de dados, como por exemplo no que tange ao armazenamento de dados pessoais que estão sob sua posse. Nesse sentido, o § 5.º, do artigo 43 dispõe que: "[c]onsumada 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."

A prescrição que se refere o parágrafo citado é regida por outro diploma legal, o Código Civil, que, traz no bojo do inciso I, do § 5.º no artigo 206, a seguinte disposição: "Art. 206. Prescreve: (...) §

126 "*Art. 6° São direitos básicos do consumidor: I - a proteção da vida, saúde e segurança contra os riscos provocados por práticas no fornecimento de produtos e serviços considerados perigosos ou nocivos; II - a educação e divulgação sobre o consumo adequado dos produtos e serviços, asseguradas a liberdade de escolha e a igualdade nas contratações; III - a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem; (Redação dada pela Lei n° 12.741, de 2012) Vigência; IV - a proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, bem como contra práticas e cláusulas abusivas ou impostas no fornecimento de produtos e serviços; V - a modificação das cláusulas contratuais que estabeleçam prestações desproporcionais ou sua revisão em razão de fatos supervenientes que as tornem excessivamente onerosas; VI - a efetiva prevenção e reparação de danos patrimoniais e morais, individuais, coletivos e difusos; VII - o acesso aos órgãos judiciários e administrativos com vistas à prevenção ou reparação de danos patrimoniais e morais, individuais, coletivos ou difusos, assegurada a proteção Jurídica, administrativa e técnica aos necessitados; 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; IX - (Vetado); X - a adequada e eficaz prestação dos serviços públicos em geral. Parágrafo único. A informação de que trata o inciso III do caput deste artigo deve ser acessível à pessoa com deficiência, observado o disposto em regulamento".* Cf. BRASIL, Lei n.° 8.078, de 11 de setembro de 1990, *Dispõe sobre a proteção do consumidor... op. cit.*

5.º Em cinco anos: I - a pretensão de cobrança de dívidas líquidas constantes de instrumento público ou particular; (...)."

Nesse sentido, tem-se que qualquer informação relativa aos dados pessoais, tais como nome, sobrenome, endereço, débitos vencidos, dados da empresa credora, data de vencimento, dentre outros, deverão ser excluídos da base de dados (sites de maus pagadores, como SPC, SERASA e outros) quando alcançar a prescrição, que suspenderá o "direito de exposição[127]" de dados específicos, autorizados por lei.

Outro ponto que também merece atenção no mencionado diploma legal, se encontra disposto no capítulo II, intitulado como "Das Ações Coletivas Para a Defesa de Interesses Individuais Homogêneos", bem como no capítulo III, intitulado como "Das Ações de Responsabilidade do Fornecedor de Produtos e Serviços" que apresentam os artigos 91 a 100.

Em relação a possibilidade de reclamação de direitos violados, VERONESE e CUNHA, defendem que "que o sistema jurídico brasileiro [de acordo com o CDC, à época] <previa> 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[128]".

Muito embora o CDC tenha artigos esparsos sobre o tema, e que, de alguma forma, incorpore alguns princípios visando o Direito à Proteção de Dados Pessoais, e ainda, levando em consideração a época da sua promulgação (1990), verifica-se que a proteção que ele oferece não satisfaz completamente a necessidade de proteção e anseio do consumidor/titular frente às violações de seus direitos. A título de exemplo, deve-se levar em consideração que, a internet somente se popularizou na década de 90 e as redes sociais vieram a ter importância num plano global somente no século XXI.

Nesse plano, em específico no mundo virtual – na internet –, a questão legal e também problemática envolve em grande parte o tratamento de dados pessoais, situação essa que extrapola a

---

127 *"RESPONSABILIDADE CIVIL. DANO MORAL NÃO CONFIGURADO. INSCRIÇÃO DEVIDA EM CADASTRO RESTRITIVO DE CRÉDITO. EXERCÍCIO REGULAR DE DIREITO. I - Caso em que a inscrição no cadastro de restrição ao crédito originou-se da inadimplência decorrente da insuficiência de fundos na conta corrente da mutuaria, na qual eram debitados os valores para o adimplemento das prestações do contrato de financiamento habitacional celebrado com a Caixa Econômica Federal. Nesse cenário, a insuficiência de provisão de fundos revelada pelos documentos juntados aos autos, prejudica o desconto da mensalidade, constitui o devedor em mora e enseja a inscrição de seu nome em cadastros de inadimplentes. II - Demonstrada a inadimplência da mutuaria em relação ao pagamento das prestações do financiamento habitacional, a inscrição nos cadastros restritivos de crédito revela-se exercício regular de direito por parte do agente financeiro. Precedente do STJ. III - Apelação da Autora a que se nega provimento".* Cf. Tribunal Regional Federal da 1° Região – TRF1 - AC: 3724320124013304, Relator: Juíza Federal Hind Ghassan Kayath (CONV.), Data de Julgamento: 21/07/2014, SEXTA TURMA, Data de Publicação: 06/08/2014, texto disponível em https://trf-1.jusbrasil.com.br/jurisprudencia/162022523/apelacao-civel-ac-3724320124013304?ref=serp [09/09/2019].

128 Cf. VERONESE, Alexandre e CUNHA, Marcelo, *"Desafios do comércio...", op. cit.*, p 84.

figura de consumo amparada pelo CDC e que somente uma legislação específica tem a capacidade de resguardar direito específico e regular as relações existentes na web.

3. Da legislação especifica visando à proteção de dados pessoais

3.1. Das leis ordinárias

Conforme exposto, restou claro que a Constituição da República Federativa do Brasil de 1988 e os diplomas legais, como o Código Civil e o Código de Defesa do Consumidor não conseguiram resguardar a efetiva proteção aos dados pessoais, isso porque não disciplinaram, de forma específica, sobre o tema, ou seja, não há a positivação deste direito.

Muito embora já houvesse leis em outros países, à época da promulgação da CRFB de 1988, que positivaram o direito à proteção de dados pessoais, o momento histórico e político do Brasil, até então, impediu que se avançasse na busca de preservação de direitos como esse.

Vale ressaltar que na época da promulgação da CRFB de 1988, e da entrada em vigor do CDC em 1990 e do atual CC em 2002, o acesso à internet não era uma realidade para a maioria dos brasileiros, na verdade, esse "benefício" se estendia apenas a uma minoria privilegiada.

Até o ano de 2010, o único diploma legal que disciplinava de forma específica a respeito dos dados pessoais era o CDC, contudo, não disciplinava expressamente sobre o tratamento das informações, ou seja, dos dados pessoais, junto à sites de cadastros de proteção ao crédito.

Uma vez que o CDC cuidava apenas das relações de consumo, o tratamento de dados em sites e cadastros de proteção se encontravam desprotegidos em relação à proteção de dados pessoais. A lacuna na lei permitia então que, a concessão de crédito aos consumidores fosse baseada nas informações negativas que existiam a respeito dos compromissos não cumpridos junto às outras instituições, quer sejam privadas ou públicas (como no caso de empresa fornecedora de energia elétrica ou de água).

Desse modo, as relações para concessão de crédito eram apenas de duas formas: ou o consumidor não tinham informações a seu respeito junto às outras instituições e a ele, o crédito lhe era concedido com base na renda e na possibilidade de pagamento ou por não ter cumprido regularmente com os compromissos, ou seja, por estar inadimplente, seu crédito era negado. As informações relativas à inadimplência eram de acesso público e se apresentavam como negativas em sites de cadastro de proteção ao crédito.

Da mesma forma que ao consumidor inadimplente os dados expostos não lhe favoreciam, ao consumidor adimplente não havia nenhum benefício, como por exemplo a figura de bom pagador, para que com isso lhe fosse concedido condições especiais de créditos, como juros e taxas diferenciadas.

Por sua vez, as empresas que ofereciam bens ou serviços não tinham a possibilidade de conhecer o quão bom aquele consumidor era, ou conhecer qual o nível do seu endividamento. Na verdade, este benefício existia apenas para as instituições financeiras, uma vez que, através do Banco Central, tinham acesso ao Serviço de Informações de Crédito (SCR), informações estas que até os dias atuais se encontram disponíveis apenas às instituições financeiras.

Em 31 de dezembro de 2010, essa situação mudava, e por meio da Medida Provisória n.º 518/2010, "nasceu" a Lei Ordinária n.º 12.414, publicada em 10 de junho de 2011 com o objetivo de "[d]isciplinar a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito".

Dessa forma, a legislação brasileira passou a ter uma lei ordinária que permitisse o registro de dados positivos junto aos órgãos de proteção de créditos, ou seja, criou-se um banco de dados a respeito do histórico de compromissos assumidos e pagos pelos consumidores, que acabou por constituir um verdadeiro cadastro positivo.

A lei regulava, pela primeira vez no Brasil, através do inciso I do artigo 2.º, a figura do banco de dados, sendo ele o "conjunto de dados relativo à pessoa natural ou jurídica armazenados com a finalidade de subsidiar a concessão de crédito, a realização de venda a prazo ou de outras transações comerciais e empresariais que impliquem risco financeiro".

Mais adiante, no inciso VII do mesmo artigo, a lei passou a disciplinar de que forma seria composto o histórico de crédito, sendo ele o "conjunto de dados financeiros e de pagamentos, relativos às operações de crédito e obrigações de pagamento adimplidas ou em andamento por pessoa natural ou jurídica".

A saber, podem ser consideradas informações positivas para os cadastros de proteção de crédito, empréstimos ou financiamentos contratados, prazos, valor das parcelas, pagamentos efetuados, saldo a pagar, dentre outros.

Outro benefício que a Lei n.º 12.414/2011 trouxe foi a possibilidade de tratamento desigual em relação ao consumidor adimplente (bom pagador) e o consumidor inadimplente (mau pagador), princípio previsto no artigo 5.º da CRFB de 1988, uma vez que, o tratamento desigual permitiu atender ambos, na medida de suas desigualdades. Isso significa dizer que o consumidor adimplente, acabava por ter

preferência em relação ao consumidor inadimplente, bem como, ao bom pagador, eram apresentas condições especiais para fechar negócios.

Outro ponto positivo em relação a lei mencionada que se pode destacar é a informação relativa ao endividamento do consumidor. A indicação da possibilidade de superendividamento previne a concessão de crédito desregrada. A Lei n.º 12.414/2011 veio equiparar o Brasil a outros países desenvolvidos que se utilizam da mesma informação para cadastro de informações positivas e negativas.

A Lei ao preservar direito do titular de suas informações, possibilitou ainda a condição de optar por participar ou não do Cadastro Positivo. O direito de escolha da exposição de seus dados pessoais é possível por força do artigo 5.º, que dispõe acerca dos direitos dos cadastrados, de poder, conforme inciso I "obter o cancelamento ou a reabertura do cadastro, quando solicitado;" além de ainda, conforme inciso VII, poder contar com a proteção da lei para "ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados".

Interessante ressaltar que, em relação às informações negativas, a lei não concede o mesmo direito quando comparado com as informações positivas, e isso acontece devido à sobreposição do interesse social, que, nesse caso, aparece com a finalidade de manter a proteção ao crédito. Entretanto, o registro das informações negativas em relação aos consumidores não pode violar os requisitos legais previstos no artigo 43 do CDC.

Nesse prisma, pode-se notar que o Cadastro Positivo se encontra alinhado ao disposto nos artigos 1º, inciso III[129], e artigo 5.º, caput e inciso X[130] da CRFB de 1988, bem como, aos artigos 11 a 21 do CC, já citados neste capítulo.

Imperioso é destacar que, as informações relativas ao Cadastro Positivo não são públicas. Conforme disciplina o artigo 7.º da Lei n.º 12.414/2011, "[a]s informações disponibilizadas nos bancos de dados somente poderão ser utilizadas para: I - realização de análise de risco de crédito do cadastrado; ou II - subsidiar a concessão ou extensão de crédito e a realização de venda a prazo ou outras transações comerciais e empresariais que impliquem risco financeiro ao consulente".

Desse modo, as informações relativas ao cadastro positivo somente poderão ser acessadas: "I – pelo detentor dos dados pessoais, ou seja, pelo próprio consumidor; II – pelas instituições cadastradas e autorizadas por lei, bem como o Poder Judiciário, Ministério Público e Defensoria Pública; III – e os

129 *"Art. 1.º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos: (...) III - a dignidade da pessoa humana;"*

130 *"Art. 5.º 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: (...) X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;"*

gestores do banco de dados. Ademais, as instituições somente poderão valer da consulta quando as vendas versarem sobre condição a prazo, ou em transações que impliquem em risco financeiro".

Certamente a primeira lei editada no Brasil que disciplinou acerca de dados pessoais trouxe benefícios na relação consumerista, bem como ao panorama financeiro do país para evitar o endividamento, porém, não previa proteção nas relações extra consumeristas.

Ainda no ano de 2011, promulgava-se outra Lei Federal que também disciplinou acerca da proteção de dados pessoais. Cinco meses após a promulgação da Lei n.º 12.414, em 18 de novembro de 2011, era promulgada a Lei Federal n.º 12.527[131], a chamada Lei de Acesso à Informação (LAI), que veio regular "o acesso às informações conforme previsto no inciso XXXIII do art. 5º, no inciso II do § 3.º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei n.º 8.112, de 11 de dezembro de 1990; revoga a Lei n.º 11.111, de 5 de maio de 2005, e dispositivos da Lei n.º 8.159, de 8 de janeiro de 1991; e dá outras providências."

A Lei de Acesso à Informação regulamentou dispositivos da CRFB que já tratavam acerca do direito de acesso a informações e suas restrições.

Em comparação com a Lei n.º 12.414/2011, ela é relativamente extensa, conta com 47 artigos, porém, em alguns deles, abre lacunas para que os direitos ali tratados venham ser tutelados por uma legislação infralegal.

Apesar de se tratar de uma lei federal, a aplicabilidade dela alcança toda a administração pública, fato esse tratado na doutrina como Lei Nacional[132]. Isso acontece por força do artigo 1.º, que assim preconiza: "[e]sta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5.º , no inciso II do § 3.º do art. 37 e no § 2.º do art. 216 da Constituição Federal. Parágrafo único. Subordinam-se ao regime desta Lei: I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público; II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios."

---

131 Cf. BRASIL, Lei n.º 12.527, de 18 de novembro de 2011, *"Regula o acesso a informações previsto no inciso XXXIII do art. 5.º, no inciso II do § 3.º do art. 37 e no § 2.º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei n.º 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências*", texto disponível em http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.html [09.09.2019].

132 Em linhas gerais, uma lei nacional se aplica a todo o território nacional. Em outras palavras, uma lei nacional é aplicada a todos os entes da federação: União, Estados, Distrito Federal e Municípios. Como exemplos de leis nacionais: Consolidação das Leis do Trabalho, Lei de Licitações (Lei nº. 8.666/90), Código Penal etc. Por sua vez, uma lei federal é aplicada apenas à União. Como exemplos, podemos citar a Lei n.º 8.112/90, que trata do Estatuto dos Servidores Públicos Civis da União, suas Autarquias e Fundações Públicas.

Importante ainda ressaltar que a LAI também se aplica a outras entidades além das citadas, como por exemplo, a entidades privadas sem fins lucrativos, mas, que recebam recursos públicos. Porém, o artigo 2.º, § único[133], o qual disciplina acerca da aplicabilidade por exceção a outras entidades, explana que só haverá obrigação da lei apenas em relação aos recursos públicos recebidos. Em relação aos demais recursos não há obrigação da publicidade.

A publicidade dos atos satisfaz uma obrigação de prestação de contas da entidade para com a sociedade, sendo tal ato conhecido como Transparência Pública, requisito esse, essencial para o Estado Democrático de Direito.

Países vizinhos ao Brasil à época, já possuíam leis que disciplinavam sobre o tema antes mesmo da promulgação da lei em 2011. No Peru foi adotada em 2003, a Ley n.º 27.806[134], Ley de Transparencia y Acceso a la Información Pública. No Chile, foi editada, em 2008, a Ley n.º 20.285[135] sobre transparencia y acceso a la información pública. Ainda em 2008, o Uruguai promulgou a Ley n.º 18.381[136], sobre Derecho de Acceso a la Información Pública.

O movimento em prol da normatização através de leis que instituíram a transparência dos atos públicos faz parte das orientações da ONU, e tem sido, mesmo antes do Brasil, acatado pelos países da América do Sul.

Muito embora a transparência seja reflexo do direito fundamental à informação, disciplinado pela própria CRFB de 1988, há de se ressaltar que a publicidade dos atos não é regra. A exceção encontra respaldo legal na Lei n.º 12.527/2011, através dos artigos 3.º, incisos I e III; 6.º, inciso III e artigo 23[137]

---

133 *"Art. 2º Aplicam-se as disposições desta Lei, no que couber, às entidades privadas sem fins lucrativos que recebam, para realização de ações de interesse público, recursos públicos diretamente do orçamento ou mediante subvenções sociais, contrato de gestão, termo de parceria, convênios, acordo, ajustes ou outros instrumentos congêneres. Parágrafo único. A publicidade a que estão submetidas as entidades citadas no caput refere-se à parcela dos recursos públicos recebidos e à sua destinação, sem prejuízo das prestações de contas a que estejam legalmente obrigadas".*

134 Cf. PERU, Ley n.º 27.806, de 13 de julio de 2002, texto disponível em https://www.mef.gob.pe/es/normas-legales/298-portal-de-transparencia-economica/normas-legales/830-ley-nd-2780 [13.09.2019].

135 Cf. CHILE, Ley n.º 20.285, de 05 de julio de 2016, texto disponível em https://www.leychile.cl/Navegar?idNorma=276363 [13.09.2019].

136 Cf. URUGUAY, Ley n.º 18.381, de 17 de octubre de 2008, texto disponível em https://legislativo.parlamento.gub.uy/temporales/leytemp9616241.html [13.09.2019].

137 *"Art. 23. São consideradas imprescindíveis à segurança da sociedade ou do Estado e, portanto, passíveis de classificação as informações cuja divulgação ou acesso irrestrito possam: I - pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional; II - prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País, ou as que tenham sido fornecidas em caráter sigiloso por outros Estados e organismos internacionais; III - pôr em risco a vida, a segurança ou a saúde da população; IV - oferecer elevado risco à estabilidade financeira, econômica ou monetária do País; V - prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas; VI - prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional; VII - pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares; ou VIII - comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações".*

e seguintes. Da mesma forma que a transparência é reflexo do direito fundamental à informação, o sigilo também é reflexo do direito fundamental à intimidade e à vida privada.

A LAI trouxe ainda outra obrigação para com as entidades públicas e as privadas (dentro da exceção), como por exemplo, a de manter um Serviço de Informação ao Cidadão (SIC), serviço esse disciplinado pelo artigo 8.º[138] da lei. Em relação aos SICs, de acordo com o artigo 45 da LAI, compete ainda aos Municípios, Estados e o Distrito Federal, regulamentar através de lei própria a sua execução na prática.

Um ponto que merece muita importância na LAI se encontra disposto em seu artigo 31, que assim baliza: "O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. § 1.º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem: (...) II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem. § 2.º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido".

A LAI, primeira lei no Brasil que disciplinou acerca do tratamento de dados pessoais para exposição na internet, reforçou a ideia de que o uso indevido de dados quando publicados, viola direitos fundamentais e deve ser visto como ato ilícito e, portanto, merecem, indenização aquele que foi lesado.

---

138 "Art. 8º É dever dos órgãos e entidades públicas promover, independentemente de requerimentos, a divulgação em local de fácil acesso, no âmbito de suas competências, de informações de interesse coletivo ou geral por eles produzidas ou custodiadas. § 1º Na divulgação das informações a que se refere o caput, deverão constar, no mínimo: I - registro das competências e estrutura organizacional, endereços e telefones das respectivas unidades e horários de atendimento ao público; II - registros de quaisquer repasses ou transferências de recursos financeiros; III - registros das despesas; IV - informações concernentes a procedimentos licitatórios, inclusive os respectivos editais e resultados, bem como a todos os contratos celebrados; V - dados gerais para o acompanhamento de programas, ações, projetos e obras de órgãos e entidades; e VI - respostas a perguntas mais frequentes da sociedade. § 2º Para cumprimento do disposto no caput, os órgãos e entidades públicas deverão utilizar todos os meios e instrumentos legítimos de que dispuserem, sendo obrigatória a divulgação em sítios oficiais da rede mundial de computadores (internet). § 3º Os sítios de que trata o § 2º deverão, na forma de regulamento, atender, entre outros, aos seguintes requisitos: I - conter ferramenta de pesquisa de conteúdo que permita o acesso à informação de forma objetiva, transparente, clara e em linguagem de fácil compreensão; II - possibilitar a gravação de relatórios em diversos formatos eletrônicos, inclusive abertos e não proprietários, tais como planilhas e texto, de modo a facilitar a análise das informações; III - possibilitar o acesso automatizado por sistemas externos em formatos abertos, estruturados e legíveis por máquina; IV - divulgar em detalhes os formatos utilizados para estruturação da informação; V - garantir a autenticidade e a integridade das informações disponíveis para acesso; VI - manter atualizadas as informações disponíveis para acesso; VII - indicar local e instruções que permitam ao interessado comunicar-se, por via eletrônica ou telefônica, com o órgão ou entidade detentora do sítio; e VIII - adotar as medidas necessárias para garantir a acessibilidade de conteúdo para pessoas com deficiência, nos termos do art. 17 da Lei nº 10.098, de 19 de dezembro de 2000, e do art. 9º da Convenção sobre os Direitos das Pessoas com Deficiência, aprovada pelo Decreto Legislativo nº 186, de 9 de julho de 2008. § 4º Os Municípios com população de até 10.000 (dez mil) habitantes ficam dispensados da divulgação obrigatória na internet a que se refere o § 2º , mantida a obrigatoriedade de divulgação, em tempo real, de informações relativas à execução orçamentária e financeira, nos critérios e prazos previstos no art. 73-B da Lei Complementar nº 101, de 4 de maio de 2000 (Lei de Responsabilidade Fiscal)".

Nesse sentido, há de se expor que os reflexos da LAI reforçam a ideia de reconhecimento de um direito fundamental materialmente constitucional em relação ao Direito à Proteção de Dados Pessoais, uma vez que o trata como tal.

Ainda no mesmo artigo, em seu § 3.º, a LAI também disciplina as situações em que não será necessário o consentimento para a exposição dos dados pessoais. Vejamos:

> "O consentimento referido no inciso II do § 1.º não será exigido quando as informações forem necessárias: I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico; II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem; III - ao cumprimento de ordem judicial; IV - à defesa de direitos humanos; ou V - à proteção do interesse público e geral preponderante".

Nesses casos, não será considerado ato ilícito, bem como não haverá reconhecimento de violação à direitos fundamentais.

Como visto, a LAI regulamentou matéria que até então não encontrava disposição legal, sendo ela o Direito à Proteção de Dados Pessoais no tratamento de dados e na publicação em SICs. É inegável que foi um grande avanço em relação às leis vigentes até o ano de 2011, mas esse era somente um começo.

3.2. Dos projetos legislativos sobre o direito à proteção de dados pessoais

Como dito alhures, não havia até o momento uma lei específica que disciplinasse acerca do tratamento de dados pessoais, bem como à proteção dos mesmos. Muito embora a LAI tenha tratado de assunto muito semelhante ao direito exposto e defendido por essa dissertação, e que serviu como base legal para garantir a proteção dos dados, não previa de fato todas as possibilidades de violação, para só então ter uma garantia de efetiva proteção.

Nesse sentido, o Deputado Federal Milton Monti (PR-SP) propôs para apreciação em plenário do Congresso Nacional o Projeto de Lei n.º 4.060[139], em 13 de junho de 2012, o qual que tinha como objetivo dispor "sobre o tratamento de dados pessoais".

139 Cf. BRASIL, Congresso Nacional, Projeto de Lei nº 4.060 de 13 de junho de 2012, *"Dispõe sobre o tratamento de dados pessoais, e dá outras providências*", texto disponível em https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066 [09.09.2019].

A proposta de uma lei específica para o tratamento de dados com vistas à proteção de dados pessoais certamente veio ao encontro com o anseio da sociedade e se igualaria a outros países que há tempo já disciplinavam sobre o tema.

Porém, a linguagem do texto não acompanhava as discussões mais relevantes dos últimos anos sobre o assunto, isso porque não assegurava a proteção mínima necessária para os titulares de dados pessoais, e, desse modo, se distanciava das referências internacionais sobre o reconhecimento desse direito.

Logo no artigo 1.º é apresentada a finalidade do projeto de lei, que passava a dispor que, "[e]sta lei tem por objetivo garantir e proteger, no âmbito do tratamento de dados pessoais, a dignidade e os direitos fundamentais da pessoa natural, particularmente em relação a sua liberdade, privacidade, intimidade, honra e imagem." Nesse ponto é de todo oportuno destacar que, desde o início, o legislador brasileiro encontrava grande dificuldade em apresentar o direito à proteção de dados pessoais como um direito autônomo e não implícito em decorrência de outros direitos, como o direito à intimidade, à privacidade e outros.

O artigo 2º – incontroverso quando comparado com o artigo 1º –, teve grande importância nesse Projeto de Lei (PL), porque passava a reconhecer a proteção de dados pessoais como um direito autônomo, sem ligação a outros direitos, e, por esse motivo, merecia a devida proteção, assim como já era para os direitos fundamentais já mencionados.

Certamente o artigo 2.º do PL n.º 4.060/2012 deve ser considerado um marco histórico no ordenamento jurídico brasileiro, isso porque, foi a primeira vez que se disciplinou, de forma clara e objetiva, acerca do Direito à Proteção de Dados Pessoais.

No artigo 3.º[140], o PL busca conexão com outros diplomas legais que também asseguram de alguma forma, direito análogo aos dados pessoais, inclusive a CRFB de 1988.

Todavia, em nenhum artigo, o PL discorreu expressamente o direito à liberdade de expressão, mesmo quando citou, em regime de exceção a não aplicabilidade do PL aos jornalistas (artigo 6.º), sendo esse direito importante para qualquer discussão acerca da privacidade. O PL também não fez menção à LAI, apesar desta ter importância ímpar no ordenamento jurídico brasileiro, uma vez que estabelecia o tratamento de dados por instituições públicas e privadas.

140 *"Artigo 3º - A proteção aos direitos e garantias mencionados no artigo primeiro desta lei deverá ser promovida com observância dos princípios constitucionais da Defesa do Consumidor, Livre iniciativa, Liberdade de Comunicação e Ordem Econômica, nos termos dos artigos 1º, IV, 5º, inc. IX, XXXII, 170 e 220 da Constituição Federal".*

A aplicação da obrigatoriedade sobre o tratamento de dados, descrito no artigo 4.º do PL, se dava em todo território nacional, bem como em território estrangeiro, nos seguintes termos:

> "A presente lei aplica-se aos tratamentos de dados pessoais realizados em território nacional, por pessoa física ou jurídica, de direito público ou privado, ainda que o correspondente banco de dados, representado por arquivos, registros ou quaisquer outras bases de processamento, esteja, permanente ou provisoriamente, armazenado em território estrangeiro".

Reconhecendo que à Proteção de Dados Pessoais merecia atenção da lei, no artigo 5.º, o PL apresentou qual meio jurídico, ou seja, qual caminho processual deveria se valer o lesado para buscar a reparação pela violação de seu direito, que poderia se dar através do CDC, bem como pela Ação Civil Pública, regida pela Lei n.º 7.347[141], de 24 de julho de 1985.

Em regime de exceção, o artigo 6.º[142] fez o necessário afastamento das obrigações relativas ao cumprimento do PL da atividade jornalística. A não aplicação do PL aos agentes dos incisos do artigo citado tinha como respaldo a preservação das garantias à liberdade de imprensa e de expressão, garantidas pela CRFB de 1988. A essa classe, em especial aos jornalistas, a aplicabilidade como um dever, privaria atividades do meio, tais como, jornalismo investigativo, dentre outros.

Muito embora o artigo 6.º esteja em consonância com o disposto na CRFB de 1988 no que diz respeito à preservação de direitos fundamentais, um ponto que merece destaque, no sentido negativo, diz respeito aos incisos III e IV, isso, devido o fato de o PL não se aplicar aos dados que estejam sob domínio público, principalmente àqueles dados em que se encontram em bancos de dados sem o consentimento do seu titular, ou seja, foram colhidos de forma ilegal, logo, viola direitos fundamentais à intimidade e à vida privada, assim como o próprio direito à proteção de dados pessoais. Nesse sentido, o PL deveria ter tratado acerca do consentimento do titular.

Ademais, a exclusão das atividades de investigação criminal ou inteligência, oferecia um sério risco aos direitos individuais dos titulares dos dados pessoais e favoreceria situação como a do programa PRISM[143], exposta no ano de 2013.

---

141 Cf. BRASIL, Lei n.º 7.347, de 24 de julho 1985, *"Disciplina a ação civil pública de responsabilidade por danos causados ao meio-ambiente, ao consumidor, a bens e direitos de valor artístico, estético, histórico, turístico e paisagístico (VETADO) e dá outras providências",* texto disponível em http://www.planalto.gov.br/ccivil_03/leis/L7347orig.html [14.09.2019].

142 *"Art. 6º. Esta lei não se aplica: I – aos bancos de dados utilizados para o exercício regular da atividade jornalística; II – aos dados relativos a pessoas físicas, quando se referirem, exclusivamente, a informações relativas às suas atividades profissionais e/ou comerciais; III - aos bancos de dados utilizados para a pesquisa histórica, científica ou estatística, de administração pública, investigação criminal ou inteligência; IV – ao tratamento de dados pessoais de informações de domínio público".*

143 Cf. BALL, James e RUSHE, Domin, "*NSA Prism program taps in to user data of Apple...", op. cit.*

O artigo 7.º, de grande importância também, trouxe um rol explicativo dos termos que são encontrados no PL, bem como os conceitua. Ele apresenta conceitos relativos ao que se entende por: "I – dado pessoal; II – tratamento de dados; III – banco de dados; IV – dados sensíveis; V – responsável; VI – interconexão; VII – bloqueio."

No capítulo II, o PL tratou "dos requisitos para o tratamento de dados pessoais", os quais se encontraram dispostos nos artigos 9.º ao 18. Em relação ao primeiro artigo desse capítulo, o artigo 9.º limitou-se apenas em dispor que "os dados pessoais serão tratados com lealdade e boa-fé, de modo a atender aos legítimos interesses dos seus titulares".

Outro ponto negativo do PL n.º 4.060/2012 se encontra no artigo 10, que trouxe a ideia de que "o tratamento de dados pessoais tem como objetivos fundamentais a proteção dos direitos básicos do consumidor", ou seja, limitou-se a dizer que a lei que disciplinaria sobre "o tratamento de dados pessoais e a sua proteção", abrangeria somente a relação consumerista, deixando assim lacuna nas relações que não se enquadrassem como relações de consumo. Neste ponto, não haveria avanços com o PL, uma vez que, havia matéria sobre o tema disciplinada pelo CDC, por exemplo.

Ademais, o artigo era restrito e limitador no que tange à proteção de dados pessoais, uma vez que não foram inclusos os direitos fundamentais, em especial, os direitos à privacidade e à liberdade de expressão. Tampouco sugeriu um rol de direitos objetivos fundamentais ligados à proteção de dados pessoais.

Outro ponto também negativo, encontra-se disposto no artigo 11. O PL faz apenas duas citações ao tratamento de dados sensíveis. A primeira citação encontra-se no parágrafo único do artigo 11, que reconhece a necessidade de adoção de medidas tecnológicas "proporcionais ao atual estado da tecnologia, à natureza dos dados e às características específicas do tratamento, em particular no caso do tratamento de dados sensíveis".

Quando comparado a outras legislações internacionais sobre o tema, percebe-se que há uma preocupação no que diz respeito à definição mais profunda do que se entende por dados de caráter sensíveis, bem como, as especificidades de tratamento para esses tipos de dados, que, deve ser diferente dos dados comuns.

A segunda citação é encontrada no artigo 12, que dispõe "[o] início do tratamento de dados pessoais sensíveis, quando não solicitado pelo titular, somente ocorrerá mediante autorização deste, por qualquer meio que permita a manifestação de sua vontade, ou na hipótese de imposição legal".

A realidade fatídica das relações que o PL previa abarcar – como por exemplo sobre o consentimento para o tratamento de dados de caráter sensíveis –, provavelmente seria através de

contratos longos e complexos, o que dificultaria o entendimento dos titulares desses dados, que automaticamente limitaria à proteção no tratamento dos dados sensíveis.

Pela leitura do PL, percebe-se que o texto não possui um artigo que lida especificamente com a segurança dos dados, principalmente em relação aos dados sensíveis, situação essa que distanciou o PL das demais leis vigentes no âmbito internacional, as quais foram usadas como referência para a elaboração de leis sobre o tema no Brasil.

O próprio PL traz indícios de possibilidade de violação ou pelo menos limitação do direito sobre os dados pessoais através do consentimento. No artigo 14, o PL assegurava que "os responsáveis pelo tratamento de dados poderão compartilhá-los, inclusive para fins de comunicação comercial, com empresas integrantes de um mesmo grupo econômico, parceiros comerciais ou terceiros que direta ou indiretamente contribuam para a realização do tratamento de dados pessoais".

Nesse sentido, a intenção de legislador era de permitir aos gestores dos bancos de dados o compartilhamento dos dados pessoais com terceiros, apenas com o consentimento ao agente de tratamento dos dados. Na prática, o titular dos dados poderia perder o controle do acesso aos seus dados pelo simples fato da terceirização desse tratamento e da circulação de seus dados. Ainda que o artigo 13 outorgasse previsão aos titulares dos dados o bloqueio do registro para tratamento ou interconexão, na prática, haveria dificuldade para controle desse tratamento.

O PL também não previu proteção ao tratamento de dados, bem como a sua transferência no âmbito internacional. Desse modo, entende-se, por analogia, que o tratamento e compartilhamento internacional seriam abordados nos mesmos moldes do tratamento nacional e não levariam em consideração os acordos entre os países ou a preocupação se tutelavam ou não o Direito à Proteção de Dados Pessoais.

O capítulo III do PL n.º 4.060/2012 tratou acerca "dos direitos do titular", sessão esta composta apenas pelos artigos 19 e 20. Por tratar-se da possibilidade de reconhecimento de um direito novo, ou seja, o reconhecimento ao direito "à proteção de dados pessoais", revelou-se insuficiente aos termos que realmente assegurem direitos aos titulares dos dados. Os artigos citados não previam direitos novos, pelo contrário, disciplinavam direitos já existentes no ordenamento jurídico brasileiro, através do CC e do CDC.

No título II do PL n.º 4.060/2012 foi disciplinado acerca "da tutela fiscalizatória e sancionatória". Nesse título se encontravam dispostos os artigos 21, 22 e 23. Logo no artigo 21, havia uma observação especial em relação ao CDC, sujeitando a lei à dependência deste diploma legal, enfatizando que o PL estaria adstrito somente às relações de caráter econômico por não se tratar de direito relacionado aos

direitos humanos. O artigo 23, menciona que há a necessidade de autorregulação dos pontos não tratados pela lei, por meio de Conselhos, mas não faz alusão de quais órgãos públicos seriam responsáveis por essa regulamentação.

Desse modo, o PL n.º 4.060/2012 revelou-se falho em vários termos, isso por que apresentou omissões em relação a real proteção de dados pessoais, de modo que acabou por não merecer a atenção devida naquele ano junto ao plenário da câmara, porém, mais tarde foi reaproveitado conforme será disposto mais adiante.

Tendo em vista o fracasso do PL n.º 4.060/2012, em 13 de setembro de 2013, foi protocolado junto ao plenário do Senado Federal o Projeto de Lei do Senado (PLS) n.º 330/2013[144], que "Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências." A mesma finalidade do PL n.º 4.060/2012.

O PLS n.º 330/2013 foi encabeçado pelo Senador Antônio Carlos Valadares (PSB – SE), e apresentado ao Plenário do Senado Federal para apreciação pela Comissão de Constituição, Justiça e Cidadania, com vista a assegurar direitos no processo de tratamento de dados pessoais a todos os brasileiros.

Em seu primeiro capítulo o PLS n.º 330/2013, trata sobre o seu "objeto e âmbito de aplicação". Comparado ao PL n.º 4.060/2012, o artigo 1.º do PLS n.º 330/2013, apresenta uma estrutura diferente. A sua finalidade encontra-se bem-disposta e de forma mais clara. O artigo dispõe que "[e]sta Lei regula a proteção, o tratamento e o uso de dados das pessoas naturais e jurídicas de direito público ou privado."

No parágrafo único do mesmo artigo, encontra disposto à aplicabilidade da lei, que assim diz: "Reger-se-á por esta Lei todo tratamento de dados pessoais, qualquer que seja o mecanismo empregado, quando sua coleta, armazenamento ou utilização ocorrer em território nacional ou em local onde seja aplicável a lei brasileira, por força de tratado ou convenção".

O parágrafo citado apresenta o campo de aplicabilidade do PLS a todo o território nacional, bem como, onde a lei brasileira pudesse ser aplicada.

Ao capítulo II foi reservada a parte conceitual constituído pelo extenso artigo 3.º, o PLS apresentou de forma clara e específica o que se entendia por: "I – dado pessoal; II – banco de dados; III – tratamento de dados pessoais; IV – gestor de banco de dados; V – gestor aparente; VI – proprietário

144 Cf. BRASIL, *Projeto de Lei do Senado Federal n.º 330/2013, "Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências"*, texto disponível em https://legis.senado.leg.br/sdleg-getter/documento?dm=2931559&ts=1567533189697&disposition=inline [14.09.2019].

do banco de dados; VII – titular de dados pessoais; VIII – usuário de banco de dados; IX – dados sensíveis; X – interconexão de dados; (sic) XII – dissociação;".

Contava ainda com 6 parágrafos que auxiliavam na explicação da finalidade de cada figura e termo jurídico, bem como a sua aplicabilidade na prática.

O PLS apresentou à proteção de dados pessoais como um direito autônomo e não como um direito ligado a outros direitos, como por exemplo à liberdade de expressão, à intimidade ou à vida privada.

O capítulo III foi reservado ao "Tratamento de Dados Pessoais", e é composto pelos artigos 4.º, 5.º e 6.º. O artigo 4.º apresenta os princípios pelos quais deve reger o tratamento de dados pessoais. Insta destacar que no inciso V, há previsão de que para o tratamento de dados deve-se constar o consentimento livre, específico, inequívoco e informado pelo titular dos dados pessoais.

O artigo 5.º dispõe acerca do tratamento aos dados de caráter sensível, estabelecendo em seus incisos a obrigatoriedade do consentimento. Vejamos:

> "I – com o expresso, específico e inequívoco consentimento de seu titular ou representante legal; II – para fins meramente estatísticos, históricos ou científicos, vedada a identificação do titular; III – por força de decisão judicial; IV – por expressa disposição legal; V – por relevante interesse público, na forma do regulamento desta Lei; VI – com o objetivo de preservar o direito à vida do titular de dados."

Em relação ao consentimento, SILVEIRA e MARQUES, explicam que "[o] caráter explícito da declaração de consentimento obriga a uma ação (declaração ou ato positivo inequívoco) do titular dos dados que demonstre esse consentimento, sendo inadmissível a obtenção do consentimento por meio de presunções ou omissões[145]".

O artigo 6.º, balizou acerca do tratamento de dados pessoais para fins de segurança pública, estabelecendo ainda que o tratamento somente poderá ser realizado "por órgão da administração pública direta ou pessoa jurídica de direito público, limitando-se às seguintes hipóteses: I – exercício de competência prevista em lei; II – prevenção ou repressão de infração penal, administrativa ou tributária; III – compartilhamento de informações para fins de segurança do Estado e da sociedade; IV –

145 Cf. SILVEIRA, Alessandra e MARQUES João, *"Do Direito a estar Só ao Direito ao Esquecimento. Considerações sobre a Proteção de Dados Pessoais Informatizados no Direito da União Europeia: Sentido, Evolução e Reforma Legislativa",* Curitiba, Revista da Faculdade de Direito – UFPR, vol. 61, n.º 3, 2016, p. 112.

atendimento dos termos de acordo, tratado ou convenção internacional de que o Estado brasileiro seja parte".

Diferentemente de todas as leis vigentes até então sobre o tema, bem como os projetos de leis, a disposição de um artigo dedicado ao tratamento de dados pela administração pública, e um rol taxativo sobre as hipóteses em que não há necessidade do consentimento do titular dos dados, visa princípio constitucional da segurança pública frente ao interesse da sociedade, ou seja, o interesse coletivo, princípio resguardado pela CRFB de 1988.

Em seu capítulo IV, o PLS trata "Dos Direitos Básicos do Titular de Dados", e apresenta, através do artigo 7.º, direitos considerados como básicos aos titulares de dados, sendo eles:

> "Inviolabilidade de consciência e de crença e à proteção da vida privada, intimidade, honra e imagem; II – o acesso à origem e ao conteúdo de dados pessoais coletados e tratados em banco de dados; III – a ciência prévia, e por escrito, como requisito à inclusão de informações pessoais em banco de dados; IV – a retificação, a título gratuito, de dados pessoais inexatos, incompletos, omissos, inverídicos ou desatualizados; V – o consentimento prévio como requisito à coleta e ao tratamento de dados pessoais sensíveis, bem como à interconexão internacional de dados realizada por banco de dados privado (art. 10); VI – o cancelamento, a título gratuito, de dados que deixarem de ser necessários à consecução da finalidade para a qual foram coletados; VII – a oposição, a título gratuito, à inclusão, cessão ou transmissão de informações pessoais que tenham por finalidade a publicidade ou divulgação comercial; VIII – a exclusão ou a dissociação gratuitas de dados pessoais sensíveis inseridos em banco de dados, se manifesto o interesse; IX – a exclusão automática, após o prazo de cinco anos, a contar da inscrição, de dados pessoais capazes de gerar restrições à obtenção de crédito; X – a facilitação da defesa de seus direitos em processos judiciais ou administrativos, admitida a inversão do ônus da prova, quando, a critério do juiz, for verossímil a alegação".

A importância de um artigo que exponha claramente direitos considerados como básicos aos titulares dos dados pessoais, reforça a ideia de sua proteção, bem como limita seu direito frente às violações causadas pelas instituições públicas ou privadas, isto é, expõe de forma clara o que o PLS visava proteger e proibir.

Nesse sentido, em comparação com ao PL n.º 4.060/2012, o PLS se apresentava mais preparado para uma aprovação pelo Senado Federal, uma vez que, conseguia preencher a lacuna jurídica sobre o tema. A considerar o ano do protocolo do PLS, ou seja, em 2013, bem como por ainda não existir referência no ordenamento jurídico brasileiro, esse se apresentava inovador e em consonância com as leis internacionais que disciplinam o tratamento de dados pessoas e à sua proteção.

No capítulo V o PLS trata dos deveres dos "Proprietários e dos Gestores do Banco de Dados." Esse capítulo é composto pelo artigo 8.º, e nele encontra-se disciplinado acerca dos deveres para com a justiça e para com os titulares dos dados.

Percebe-se que o legislador, buscou, de forma clara e precisa, apresentar que, tanto a coleta, quanto o tratamento e o armazenamento dos dados, devem estar de acordo com os incisos do artigo 8º, que assim balizam:

> "I – informar aos titulares de dados pessoais: a) a inclusão e o tratamento de suas informações; b) a extensão de seus direitos; c) a finalidade da coleta; d) as categorias de usuários da informação; e) a identidade do proprietário e do gestor do banco de dados; II – não utilizar os dados para finalidades incompatíveis com aquelas para as quais foram coletados; III – não proceder a tratamento de dados por meios fraudulentos, desleais ou ilícitos; IV – não utilizar os dados com a finalidade exclusiva de revelar a terceiros a origem racial ou étnica, crença religiosa, filosófica, política ou ideológica, atuação partidária ou sindical, estado de saúde, informações genéticas ou orientação sexual da pessoa natural do titular dos dados; V – oferecer proteção e segurança aos dados coletados, observada a natureza destes e os riscos a que estejam expostos, a fim de impedir sua perda, destruição, alteração, tratamento, cópia, difusão ou acesso não autorizado; VI – não inserir dados oriundos de fontes acessíveis ao público sem que prévia ciência seja conferida ao titular dos dados; VII – não inserir dados pessoais sensíveis sem o consentimento prévio e expresso do titular dos dados; VIII – apreciar, no prazo máximo de dez dias, a contar da solicitação, pedido de retificação, oposição, cancelamento e exclusão de dados; IX – retificar, independentemente de provocação do titular, dados inexatos, incompletos, inverídicos ou desatualizados; X – cancelar, independentemente de provocação do titular,

dados que deixarem de ser necessários à consecução da finalidade para a qual foram coletados;".

Pelo exposto, nota-se que a intenção do legislador foi a de realmente criar normas que trouxessem efetiva proteção para os direitos do titular dos dados e impor deveres palpáveis aos proprietários e gestores dos bancos de dados.

Ainda quanto à efetiva proteção no tratamento dos dados pessoais, o inciso XI do artigo citado, disciplinou acerca da possibilidade de indenização pela violação dos direitos e deveres constantes no PLS, assegurando assim o dever de "indenizar, por danos morais e materiais, os titulares de dados coletados, tratados ou utilizados em desacordo com as prescrições legais, sem prejuízo da responsabilidade administrativa ou penal que lhes possa ser imputada".

Corrobora ainda com tal, o inciso XI, estendia a obrigação de indenizar contida no parágrafo único, trazendo a obrigação para os proprietários ou aos gestores dos bancos de dados, o dever de sigilo, mesmo após a extinção da relação jurídica que possibilitou a coleta dos dados.

Nos capítulos VI e VII o PLS tratou acerca das "Disposições Especiais Aplicáveis aos Bancos de Dados Públicos e aos Bancos de Dados Privados". Em relação aos Bancos de Dados Públicos, colhe-se o § 1.º do artigo 9.º, que assim dispõe: "Ao banco de dados público que tenha por objeto tratamento de dados com vistas a auxiliar atividade de segurança nacional ou pública, investigação administrativa, tributária, criminal ou instrução processual penal, não se aplica o disposto nos incisos II, III, IV, V, VI e VIII do caput do artigo 7.º e nos incisos I, VI, VII e VIII do art. 8.º, sem prejuízo da responsabilidade civil ou penal que ao titular ou gestor possa ser imputada por desvio de finalidade no uso das informações tratadas".

Em relação aos Bancos de Dados Privados, o artigo 10, nos § 1.º e 3.º, tratava de forma mais específica as obrigações do que em relação ao § 1.º do artigo 9.º, isso porque a esses não se aplicava a possibilidade da utilização sem consentimento como argumento de segurança nacional, uma vez que, para essas informações, as instituições da inteligência do governo têm autonomia para tratar esses dados, bem como amparo legal.

Em relação aos dados sensíveis, o § 1.º passava e prever que: "Ao banco de dados privado que tenha por objeto tratar dados necessários à salvaguarda de interesse vital do titular não se aplica, quanto aos dados pessoais sensíveis sobre o estado de saúde, o disposto na primeira parte do inciso V do caput do artigo 7.º e no inciso VII do artigo 8.º, sem prejuízo da responsabilidade civil ou penal que ao titular ou gestor possa ser imputada por desvio de finalidade no uso dos dados."

O § 3.º passava a expor situações em que os proprietários ou gestores dos bancos de dados poderão "utilizar os dados tratados, excetuados os dados sensíveis, para fins de publicidade ou divulgação comercial, mediante consentimento prévio conferido ao titular, o qual poderá exercer direito de oposição, nos termos do inciso VII do caput do artigo 7.º".

O PLS reserva ainda um capítulo para a "Segurança dos Dados", o capítulo VIII, que, no artigo 11 impõe a obrigação e cuidados para o tratamento e armazenamento dos dados pessoais coletados. Em relação aos dados de caráter sensível, o paragrafo único instituía que "[n]ão se registrarão dados sensíveis em bancos de dados que não reúnam condições mínimas de segurança, conforme definido no regulamento desta Lei." Nesse ponto, se percebe mais uma vez a preocupação do legislador na proteção especial aos dados de caráter sensível.

No capítulo IX, o PLS trata "Da Interconexão de Dados", ou seja, do envio de dados de um banco de dados para outro banco de dados. O artigo 12, menciona sobre quais os requisitos mínimos que devem atender a interconexão dos dados dentro do território nacional. Em relação à interconexão entre banco de dados nacional público a banco de dados internacional, o § 1.º regulamenta em que termos isso poderá ocorrer, sendo que "somente será permitida se houver tratado ou acordo internacional autorizativo de que seja parte a República da Federativa do Brasil, ou promessa de reciprocidade, e tiver por objetivo coibir crime organizado transnacional, tráfico de seres humanos, crime de corrupção, terrorismo, financiamento ao terrorismo, narcotráfico, lavagem de dinheiro, extorsão mediante sequestro ou crimes contra o sistema financeiro nacional", desde que, atendido as condições expressas em seus incisos I, II e III.

No tocante à interconexão de dados entre banco de dados privados e banco de dados internacional, o § 2.º expõe que somente acontecerá se atender os requisitos, explanados em seus incisos, mediante "I – prévio consentimento do titular das informações, atendidas as disposições desta Lei, que poderá ser dispensado na hipótese de dados transmitidos em razão de transferências bancárias ou de operações realizadas em bolsa de valores;" desde que haja a "II – intermediação do Estado brasileiro, para interconexão de dados sensíveis".

O Capítulo X, do PLS, discorria acerca do direito "Da Retificação e do Cancelamento de Dados". O artigo 13 resguardava o direito do titular dos dados para exata retificação dos seus dados, ou o cancelamento desses, quando não mais satisfazer seus interesses.

Importante expor que o PLS tratava de forma satisfatória a respeito do direito de ser indenizado pela violação à proteção de dados pessoais. Conforme demonstrado na leitura e comentários ao artigo

6.º, inciso XI, traz ainda o Capítulo XI, que tem como título específico "Da Responsabilidade Civil", que trata da possibilidade de reparação do dano causado ao titular dos dados.

Através do artigo 14, que merece ser exposto em sua integralidade, se prevê que a "[q]ualquer pessoa que sofra prejuízo decorrente do tratamento irregular ou ilícito de dados possui direito à reparação dos danos, materiais e morais".

Na ultima seção, ou seja, no capítulo XII, o PLS trata "Das Sanções Administrativas" através dos artigos 15 a 17, sendo essas sanções relativas a infrações às normas dispostas no PLS. Insta salientar que as medidas previstas nos artigos 15, 16 e 17, se aplicam apenas na esfera administrativa pelas autoridades competentes, que deverão ser apresentadas por normas regulamentares e independem de ações de natureza civil e criminal.

Conforme visto, o Projeto de Lei do Senado de n.º 330/2013, se apresentou de forma satisfatória se comparado ao Projeto de Lei n.º 4.060/2012, e ainda, por considerar a realidade vivenciada pela sociedade brasileira. Contudo, até o ano de 2014, quando, efetivamente, fora sancionada lei específica, o ordenamento jurídico não se beneficiou do seu texto legal.

Somente 25 (vinte e cinco) anos após a promulgação da Constituição da República Federativa do Brasil de 1988, em 23 de abril de 2014, fora sancionada lei que tratava de forma direta sobre o tema. A Lei n.º 12.965, que "Estabelece(u) princípios, garantias, direitos e deveres para o uso da Internet no Brasil", lei essa que ficou conhecida como "O Marco Civil da Internet".

3.3. Do marco civil da internet

3.3.1. Do projeto de lei n.º 2.126, de 24 de agosto de 2011

Oriundo do Projeto de Lei n.º 2.126/2011[146] que fora apresentado ao Plenário do Congresso Nacional, em 24 de agosto de 2011, e encaminhado em 26 de março de 2014 ao Senado Federal sob Projeto de Lei da Câmara n.º 21/2014[147], em 23 de abril de 2014 era publicada a Lei Ordinária n.º 12.925, nacionalmente conhecida como Marco Civil da Internet, sendo a primeira Lei Federal que disciplinou acerca do uso da internet no Brasil.

146 Cf. BRASIL, Projeto de Lei n.º 2.126, de 24 de agosto de 2011, *"Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil"*, texto disponível em https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=912989&filename=PL+2126/2011 [17.09.2019].

147 Cf. BRASIL, Projeto de Lei da Câmara n.º 21/2014, de 26 de março de 2014, *"Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil"*, texto disponível https://legis.senado.leg.br/sdleg-getter/documento?dm=3846743&ts=1567526304766&disposition=inline [17.09.2019].

As discussões a respeito da necessidade de se existir uma lei própria, que disciplinasse atos na internet iniciou através de um artigo[148] publicado em 22 de maio de 2007, no qual Ronaldo LEMOS discutia a respeito do projeto de lei de crimes virtuais, e salientava que "caminho natural de regulamentação da rede, seguido por todos os países desenvolvidos, é primeiramente estabelecer um marco regulatório civil, que defina claramente as regras e responsabilidades com relação a usuários, empresas e demais instituições acessando a rede, para a partir daí definir uma regras criminais".

A inconformidade com um projeto de lei penal, antes de uma lei civil se justificou, segundo LEMOS pelo fato de que "o projeto em questão afeta a vida da maioria dos brasileiros, sejam aqueles que possuem telefones celulares, sejam aqueles que acessam a Internet por computadores, ou aqueles que serão futuros espectadores da televisão digital. Por essa razão, é inconcebível que um projeto como esse não seja debatido de forma mais ampla com a sociedade civil e com os representantes dos interesses diretamente afetados. O rol destes é grande e inclui: provedores de acesso, empresas de tecnologia de modo geral, consumidores, universidades, organizações não-governamentais, empresas de telecomunicação, apenas para elencar alguns".

Por fim, ele chama a atenção da sociedade ao argumentar que "todo o esforço de debate público em torno de um tal projeto de lei, que tem por objetivo regulamentar a Internet do ponto de vista criminal, deveria se voltar à regulamentação civil da rede, definindo claramente o seu marco regulatório e privilegiando a inovação, tal qual foi nos países desenvolvidos. Privilegiar a regulamentação criminal da Internet antes de sua regulamentação civil tem como consequência o aumento de custos públicos e privados, o desincentivo à inovação e sobretudo, a ineficácia".

Os argumentos foram suficientes para gerar uma onda de manifestações a cerca da importância de uma lei civil que regesse os atos na internet. No ano de 2009, entre o período de 29 de outubro a 17 de dezembro, iniciou a primeira fase dos debates.

O resultado dos debates públicos foi proveitoso e como reflexo fora elaborada a minuta do anteprojeto da Lei, que voltou a ser confrontando em uma segunda fase de debates, desta vez, com a contribuição de toda a sociedade. Os debates ocorreram no ano de 2010, entre as datas de 8 de abril a 30 de maio.

148 Cf. LEMOS, Ronaldo, *"Internet brasileira precisa de marco regulatório civil"*, Rio de Janeiro, *in UOL*, 2007, texto disponível em https://tecnologia.uol.com.br/ultnot/2007/05/22/ult4213u98.jhtm [17.09.2019].

E como resultado desses dois grandes debates públicos e com auxilio da sociedade nascia o primeiro projeto de lei, escrito a mão por Luiz Paulo Barreto, então Ministro da Justiça, e que ficou conhecido como "A Constituição da Internet[149]".

O projeto de Lei n.º 2.126/2011, concluso em 24 de agosto de 2011, fora enviado pela então Presidente da República Dilma Rousseff[150] à Câmara, em 12 de abril de 2012, o mesmo fora apensado ao PL n.º 5.403/2001[151] (que mais tarde acabou sendo arquivado) e desapensado. À época, mais de 38 (trinta e oito) projetos já haviam sido rejeitados pela Câmara dos Deputados, pelo Poder Executivo e pelo Senado Federal, contudo, o PL n.º 2.126/2011 fora declarado constitucional de modo que acabou sendo aprovado.

Em 8 de julho de 2013, após noticias[152] veiculadas acerca das violações das comunicações pelo governo dos Estados Unidos da América (EUA), o governo brasileiro entendeu a gravidade da ausência de uma lei que disciplinasse sobre a proteção de dados pessoais, momento em que a então Presidente Dilma Rousseff requereu urgência no julgamento do PL. A intenção da aprovação rápida do Marco Civil da Internet era a de aumentar as garantias legais de direitos digitais fundamentais, que até então simplesmente não existiam.

Em 11 de setembro de 2013 foi publicado no Diário Oficial da União[153] (DOU) a carta de urgência emitida pela Presidente Dilma Rousseff. Após a publicação do ato de urgência, iniciou o prazo de 45 (quarenta e cinco dias) para apreciação do PL pela Câmara dos deputados, porém até a data de 29 de outubro de 2013 não houve o cumprimento do pedido de urgência fato esse que trancou a pauta de julgamento.

Em posse do Senado Federal, o PL n.º 2.126/2011 passou a tramitar sob o número PLC n.º 21/2014. Apreciado pelas Comissões de Ciência, Tecnologia, Inovação, Comunicação e Informática; de Constituição, Justiça e Cidadania; Meio Ambiente, Defesa do Consumidor e Fiscalização e Controle, o

149 Cf. AGÊNCIA ESTADO, "*Barreto defende criação de 'Constituição' da Internet'", in G1*, 2010, texto disponível em http://g1.globo.com/brasil/noticia/2010/05/barreto-defende-criacao-de-constituicao-da-internet.html [17.09.2019].

150 Cf. JINKINGS, Daniella, "*Governo apresenta proposta do Marco Civil da Internet ao Congresso Nacional", in Agência Brasil,* 2011, texto disponível em http://memoria.ebc.com.br/agenciabrasil/noticia/2011-08-24/governo-apresenta-proposta-do-marco-civil-da-internet-ao-congresso-nacional [17.09.2019].

151 Cf. BRASIL, Projeto de Lei n.º 5.403/2001, *"Dispõe sobre o acesso a informações da Internet, e dá outras providências",* texto disponível em https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=34462&ord=1 [17.09.2019].

152 Cf. AQUINO, Yara, "*Após denúncias de espionagem, governo pedirá agilidade na votação do Marco Civil da Internet*", *in Agência Brasil,* 2013, texto disponível em http://memoria.ebc.com.br/agenciabrasil/noticia/2013-07-08/apos-denuncias-de-espionagem-governo-pedira-agilidade-na-votacao-do-marco-civil-da-internet [17.09.2019].

153 Cf. BRASIL, Diário Oficial da União, - DOU, N.º 176, de 11 de setembro de 2013, texto disponível em http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=11/09/2013&jornal=1&pagina=3 [17.09.2019].

projeto recebeu três emendas e em razão de seu caráter de urgência foi votado e aprovado pelo Senado Federal e aprovado em 23 de abril de 2014. O PL foi sancionado e aprovado pela Presidente sra. Dilma Rousseff na forma de Lei Ordinária sob n.º 12.965/2014.

3.3.2. Da lei n.º 12.965, de 23 de abril de 2014 – marco civil da internet

A Lei do Marco Civil da Internet foi construída sob 3 (três) pilares importantes, sendo eles: a neutralidade da Rede; a Liberdade de Expressão; e a Privacidade dos internautas. A "Constituição da Internet", como assim também ficou conhecida, abordou pontos que até então não tinham previsão legal, como por exemplo, a proteção de dados pessoais – porém toda a matéria não fora regulamentada.

A Lei do Marco Civil da Internet é composta por 32 (trinta e dois) artigos, divididos em 5 (cinco) capítulos: "Disposições preliminares; Dos direitos e garantias dos usuários; Da provisão de conexão e aplicações da Internet; Da atuação do poder público; e Disposições Finais".

No capítulo I, "Disposições preliminares", logo no artigo 1.º, a lei apresenta sua finalidade e estabelece "princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria".

O objetivo principal da lei é a de "garantir a segurança dos usuários da internet e proteger seus dados pessoais contra possíveis violações". Além do ponto ligado à proteção, a lei ainda disciplina acerca da qualidade e estabilidade da conexão.

O artigo 2.º disciplina o uso da internet no Brasil e estabelece fundamentos, como por exemplo, "o respeito à liberdade de expressão; I - o reconhecimento da escala mundial da rede; II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais; III - a pluralidade e a diversidade; IV - a abertura e a colaboração; V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VI - a finalidade social da rede".

O referido artigo reconhece a internet como um conjunto de meios de transmissão, transferência, roteamento e comunicação, estruturados em escala mundial que pode ser acessado em qualquer lugar do mundo a qualquer momento. Distingue ainda que independente do direito disciplinado, seja no mundo virtual ou real, os atos devem estar sob proteção dos direitos humanos.

Em seu artigo 3.º a lei traz os princípios pelos quais se rege o uso da internet no Brasil, sendo eles:

> "I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei; IV - preservação e garantia da neutralidade de rede; V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei; VII - preservação da natureza participativa da rede; VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei".

Um dos principais objetivos da lei, como dito, é o de garantir a privacidade dos dados na internet e estabelecer um sistema de segurança para o acesso das informações utilizadas, principalmente, em *sites* de compras *online*.

Ademais, a lei ainda prevê, como se percebe pelo inciso V, a boa qualidade do serviço de internet oferecido pelas empresas fornecedoras, proibindo a sua interrupção bem como a sua instabilidade, inclusive em horários de pico.

Nesse sentido, a proteção de direitos, a boa qualidade na prestação do serviço e a proteção de dados pessoais visam combater o seu mau uso. Segue assim a mesma linha legal de tratados internacionais, como por exemplo a Convenção de Budapeste[154] que regulou o Cibercrime, sendo este o primeiro tratado internacional ratificado pelo Brasil sobre o tema.

O artigo 4.º vê o uso da internet na intenção de promover o "I - do direito de acesso à internet a todos; II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos; III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e IV - da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados".

---

154 *"Convictos de que a presente Convenção é necessária para impedir os actos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta de desses sistemas, redes e dados, assegurando a incriminação desses comportamentos tal como descritos na presente Convenção, e da adopção de poderes suficientes para combater eficazmente essas infracções, facilitando a detecção, a investigação e o procedimento criminal relativamente às referidas infracções, tanto ao nível nacional como internacional, e estabelecendo disposições materiais com vista a uma cooperação internacional rápida e fiável (...)".* Cf. CONSELHO DA EUROPA, *Convenção sobre o Cibercrime – Convenção de Budapeste,* Budapeste, 2001, texto disponível em http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf [16.09.2019].

O artigo citado e os seus incisos visam o exercício dos direitos constitucionais, direitos estes disponíveis a todos os cidadãos brasileiros, da mesma forma que impõe deveres em relação ao uso consciente da internet.

O artigo 5.º apresenta-se como um artigo conceitual, demonstrando o que a lei entende por "I - internet; II - terminal; III - endereço de protocolo de internet (endereço IP); IV - administrador de sistema autônomo; V - conexão à internet; VI - registro de conexão; VII - aplicações de internet; e VIII - registros de acesso a aplicações de internet".

O artigo 6.º reforça que a interpretação da lei em relação a vida prática deve acontecer dentro dos moldes populares e dos costumes, isso porque, desde o início, a internet se se popularizou a tal ponto que constituí ambiente próprio de vivência.

No capítulo II trata "Dos Direitos e Garantia dos Usuários" e é composto pelos artigos 7.º e 8.º. No artigo 7.º, a lei ressalta que "o acesso a internet é essencial ao exercício da cidadania" e por esse motivo assegura os direitos relativos a:

> "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; IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização; V - manutenção da qualidade contratada da conexão à internet; VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade; 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, (...); 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; XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet; XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet."

O artigo 7.º é visto como um dos mais importantes, haja vista que ele trata diretamente acerca do direito à privacidade dos dados pessoais na internet. Menciona ainda que, qualquer violação a esse direito é passível de indenização. Ademais, a guarda desses dados deve estar sobre estrita observância da lei com vistas à proteção da intimidade.

Outro ponto que merece destaque no artigo 7.º se encontra no inciso V, quando a lei trata da obrigatoriedade da manutenção da qualidade da conexão à internet, sendo que a velocidade oferecida não pode ser menor do que 80%[155] (oitenta por cento) do plano contratado. Além da garantia da velocidade, o artigo ainda impõe que o consumidor deve ser informado de forma simples, clara e objetiva a respeito do contratado com a prestadora do serviço, em respeito, inclusive, ao CDC.

Ademais, a lei institui a obrigatoriedade da ciência do usuário a respeito da guarda de seus dados pessoais pelos provedores, ou seja, o consentimento do usuário deverá ser expresso e não pode ser tácito ou verbal, além de constar em cláusula específica no contrato da prestação de serviços, de modo que possa ser encontrado facilmente.

O artigo 8.º da lei trouxe também grande mudança em relação às situações já existentes no serviço de prestação de internet, isso porque haverá respaldo para a anulação dos contratos, sempre que eles: "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."

Nesse ponto, VERONESE e CUNHA entendem "que o Marco Civil da Internet aprofundou as obrigações que fornecedores de produtos e serviços na Internet devem atender na preservação do sigilo dos dados pessoais que detêm, independentemente da existência de relação de consumo e de a pessoa jurídica (coletiva) estar ou não sediada no Brasil, desde que ofereça seus serviços no país. Criou ainda

---

155 *"Limites mínimos de velocidade da banda larga ficam mais rigorosos 31 de outubro de 2014. Pelos novos limites que entram em vigor amanhã, 1º de novembro, as prestadoras deverão garantir mensalmente, em média, 80% da velocidade contratada pelos usuários".* Cf. ANATEL, *"Limites mínimos de velocidade da banda larga ficam mais rigorosos",* in ANATEL.GOV, 2014, texto disponível em https://www.anatel.gov.br/Portal/exibirPortalPaginaEspecialPesquisa.do?acao=&tipoConteudoHtml=1&codNoticia=35544 [16.09.2019].

sistema próprio de sanção que pode ser aplicado cumulativamente com as penalidades do Código de Defesa do Consumidor e das responsabilizações cíveis e criminais aplicáveis[156]".

O descumprimento de qualquer um dos deveres dos artigos citados será punido pelas sanções previstas no artigo 12 da mesma lei, sem obstar a implicação dos demais diplomas legais que disciplinem sobre o assunto.

No capítulo III, que tem por título "Da Provisão de Conexão e de aplicações de Internet", Seção I "Da Neutralidade de Rede", mais especificamente artigo 9.º, a lei buscou proibir que os provedores de internet induzam os consumidores a ter acesso a aplicações específicas que favoreçam minoria e gere lucro direcionado. A fim de evitar tal prática, a lei estabelece ainda que os provedores/operadores devem fornecer somente pacotes de dados e valores livres, isto é, sem limite de acessos e velocidade, esta última deve ser vinculada na contratação.

Além disso, a lei ainda prevê que os danos causados pelo não cumprimento por parte do provedor/operadora gerará o direito de indenizar aqueles que foram lesados, conforme fundamentação jurídica do artigo 927 do CC.

Na seção II do mesmo capítulo, a lei trata acerca da "Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas". Nessa sessão encontra-se disposto os artigos 10, 11 e 12.

O artigo 10 reforça direitos fundamentais reconhecidos pela CRFB de 1988, pois entende que a "guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, 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".

Nesse sentido, a letra da lei assevera que à proteção de dados pessoais, é reflexo da preservação de direitos como à intimidade, à vida privada, à honra e imagem, o que reforça a ideia de que os dados pessoais são uma subdivisão desses direitos e não um direito autônomo, o que acabava por ser um retrocesso para o ordenamento jurídico brasileiro.

A previsão legal a respeito da obrigatoriedade no armazenamento e a disponibilização dos rastros de conexão a sites ou a aplicações, bem como demais dados pessoais, não poderão ser disponibilizados sem a clara e expressa autorização do titular dos dados, exceto quando o requerimento das informações se der por determinação judicial.

Outro artigo que demonstra a soberania brasileira em relação às legislações extraterritoriais encontra-se no artigo 11. Esse artigo reforça o poder do Estado quando determina a obrigação de se

156 Cf. VERONESE, Alexandre e CUNHA, Marcelo, *"Desafios do comércio...", op. cit.*, p. 85.

submeter qualquer ato de coleta, armazenamento, guarda e tratamento de registros, dados pessoais ou comunicações ao ordenamento jurídico brasileiro.

Não é a primeira lei nacional que possui essas especificidades, outras como a Lei n.º 9.296[157], de 24 de julho 1996, que trata a respeito das interceptações de comunicações telefônicas e a LAI, já mencionada, também disciplinam sobre o tema. Importante salientar que a lei se aplica somente aos dados pessoais coletados em território brasileiro.

O artigo 12, aborda a respeito das infrações relativas aos artigos 10 e 11. As punições previstas não têm escopo penal, contudo não exime os responsáveis pelas violações nas esferas civil, penal e administrativa, uma vez que essas são dotadas de autonomia, assim pode então o violador, pelo mesmo ato, responder nas 3 (três) esferas conjuntamente.

Entretanto, imperioso se faz explanar que haverá somente duas exceções em que a absolvição na seara criminal vinculará as searas civil e administrativas, sendo elas caso comprovadas a inexistência do fato (o fato não ocorreu) ou a negativa de autoria (não foi aquela pessoa que praticou o ato).

Às empresas estrangeiras, que de alguma forma violem os direitos constantes na lei do Marco Civil da Internet, independente de haver sede ou estabelecimento em solo brasileiro serão responsabilizadas pelo pagamento de multa e pode ainda ser processadas perante as cortes internacionais.

Na Subseção I, que apresenta "Da Guarda de Registros de Conexão", se encontra disposto o artigo 13. No referido artigo, o Marco Civil da Internet trata a respeito da obrigatoriedade de guarda sobre os registros de conexão, impondo a obrigação com lapso temporal de 01 (um) ano, estendendo ainda a mesma obrigação as empresas estrangeiras que operam ou que venham operar no país.

Caso haja o descumprimento da obrigação, a empresa poderá sofrer multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil, além de demais sanções como: suspensão temporária do fornecimento dos serviços e até mesmo a proibição do exercício de suas atividades em território brasileiro.

Um ponto que se deve destacar no artigo é a obrigação *propter-rem*, isso porque, como a guarda se torna obrigatória por período mínimo, além da guarda as empresas deverão garantir ainda a inviolabilidade dos dados pessoais, com vistas a garantir a segurança dos usuários.

---

157 Cf. BRASIL, Lei n.° 9.296, de 24 de julho de 1996, *"Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal"*, Texto disponível em http://www.planalto.gov.br/ccivil_03/leis/l9296.html [16.09.2019].

Na Subseção II, que trata "Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Conexão", encontra disposto o artigo 14.

Nesse artigo, o legislador buscou vedar de forma expressa o provedor de conexão na guarda – sob sigilo – dos registros de acesso a aplicações na internet. Para o cumprimento dessa obrigação, deverá ainda o provedor de aplicações constituir pessoa jurídica que regule e guarde os dados pelo prazo de 06 (seis) meses – obrigação também estendida aos provedores de aplicações –, conforme ordena o artigo 15, disposto na Subseção III, que trata "Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Aplicações".

A exemplo de provedores de aplicações, têm-se o Facebook, Twitter, Skype, Google+ e outros. A exemplo de provedores de internet – no Brasil –, têm-se Oi, Algar, Vivo, GVT, NET e outros.

No artigo 16, a lei versa em seus dois incisos que a guarda só será vedada quando: "I - os registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no artigo 7.º; ou II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular."

Contudo, o artigo 17 – autoexplicativo –, dispõe que "[r]essalvadas as hipóteses previstas nesta Lei, a opção por não guardar os registros de acesso a aplicações de internet não implica responsabilidade sobre danos decorrentes do uso desses serviços por terceiros". Nesse sentido, o provedor não será obrigado a indenizar aquele que venha ser lesado pela não guarda dos registros.

Na Seção III, a lei trata "Da Responsabilidade por Danos Decorrentes de conteúdo Gerado por Terceiros", onde encontram-se dispostos os artigos 18, 19, 20 e 21.

A responsabilidade civil e criminal tratada na Lei do Marco Civil da Internet envolve tanto o usuário, quanto os provedores. No que tange ao direito de indenizar por violação de conteúdo, merece atenção o artigo 18, que assim diz: "O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros."

O artigo citado reforça direito constitucional[158] acerca da punibilidade, ou seja, indica que a pena não poderá passar da pessoa do infrator. Desse modo, provedores de internet não responderão pelos conteúdos publicados pelos usuários de aplicativos, quando esses conteúdos violarem direitos de outrem.

158 *"Nos termos do art. 5º, XLV, da CF, nenhuma pena passará da pessoa do condenado, podendo a obrigação de reparar o dano e a decretação do perdimento de bens ser, nos termos da lei, estendidas aos sucessores e contra eles executadas, até o limite do valor do patrimônio transferido. Esse princípio tem total correção com o princípio da responsabilidade pessoal, que proíbe a imposição de pena por fato de outrem, ninguém pode ser punido por fato alheio. O filho não responde pelo delito do pai, a esposa não responde pelo delito do marido etc".* Cf. GOMES, Luiz Flávio, *Direito penal: introdução e princípios fundamentais*, São Paulo, Editora Revista dos Tribunais, vol. 01., 2ª ed., 2009, p. 403.

Contudo, faz se necessário explanar que a responsabilidade poderá ser transferida ao provedor quando este for acionado pela justiça para tornar o conteúdo indisponível e mesmo assim não o fizer, passa então a responder também pela violação ante a sua responsabilidade. A mesma responsabilidade se estende aos provedores de aplicativos.

Nesse sentido o artigo 19 disciplina que: "Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário".

No artigo 20, a lei trata da obrigação dos provedores, quando da "retirada" do conteúdo do "ar", em notificar o usuário sobre o motivo, ou seja, da violação, de modo que possa permitir ainda possibilitar "o contraditório e a ampla defesa em juízo, salvo expressa previsão legal ou expressa determinação judicial fundamentada em contrário".

Conforme citado no artigo 19, sobre a isenção da responsabilidade pelos provedores, a exceção ao caso, encontra-se disposta no artigo 21, que os responsabilizam solidariamente pela disponibilização de conteúdo sem autorização dos usuários.

Quando da elaboração do artigo o legislador visou – além da proibição e a criminalização de conteúdo produzido ilicitamente e disponibilizado por terceiro –, a punição para o provedor que, mesmo depois de notificado extrajudicialmente pelo usuário violado manteve-se inerte e não retirou o conteúdo de sua plataforma.

Na Seção IV, que trata "Da Requisição Judicial de Registros", se encontram dispostos os artigos 22 e 23, que versam sobre o requerimento pela justiça para o acesso de dados pessoais disponibilizados pelos provedores.

Nesse sentido, o legislador, através do artigo 22, teve a intenção de reduzir os pedidos de obtenção de dados pessoais dos usuários sem um motivo plausível, o que evita a divulgação desnecessária.

Os pedidos que tenham como objeto o acesso a dados pessoais que estejam sob posse dos provedores serão regidos pela Lei Federal n.º 9.296/1996, lei essa que disciplina acerca das interceptações das comunicações. A lei disciplina que, o acesso aos dados somente será deferido quando estiverem ligados a casos de investigação em processos de natureza criminal e quando comprovadamente existir fatos que torne o pedido plausível.

Visando ainda a proteção da intimidade do acusado/investigado, o artigo 23 da lei concede aos juízes e às partes, o direito de requerer que o processo venha tramitar sob sigilo, ou seja, em segredo de justiça, ato esse reconhecido e autorizado por lei e em conformidade com direitos fundamentais como à intimidade e à vida privada, bem como o direito à proteção de dados pessoais.

No Capítulo IV, que trata "Da Atuação do Poder Público", se encontram dispostos os artigos 24, 25, 26, 27 e 28.

O artigo 24 vem estabelecer "diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios no desenvolvimento da internet no Brasil". Nesse sentindo, apresentam as diretrizes em seus incisos. Vejamos:

> "I - estabelecimento de mecanismos de governança multiparticipativa, transparente, colaborativa e democrática, com a participação do governo, do setor empresarial, da sociedade civil e da comunidade acadêmica; II - promoção da racionalização da gestão, expansão e uso da internet, com participação do Comitê Gestor da internet no Brasil[159]; III - promoção da racionalização e da interoperabilidade tecnológica dos serviços de governo eletrônico, entre os diferentes Poderes e âmbitos da Federação, para permitir o intercâmbio de informações e a celeridade de procedimentos; IV - promoção da interoperabilidade entre sistemas e terminais diversos, inclusive entre os diferentes âmbitos federativos e diversos setores da sociedade; V - adoção preferencial de tecnologias, padrões e formatos abertos e livres; VI - publicidade e disseminação de dados e informações públicos, de forma aberta e estruturada; VII - otimização da infraestrutura das redes e estímulo à implantação de centros de armazenamento, gerenciamento e disseminação de dados no País, promovendo a qualidade técnica, a inovação e a difusão das aplicações de internet, sem prejuízo à abertura, à neutralidade e à natureza participativa; VIII - desenvolvimento de ações e programas de capacitação para uso da internet; IX - promoção da cultura e da cidadania; e X - prestação de serviços públicos de atendimento ao cidadão de forma integrada, eficiente, simplificada e por múltiplos canais de acesso, inclusive remotos".

159 Cf. BRASIL, Decreto n.º 4.829, de 3 de setembro de 2003, *"Dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGIbr, sobre o modelo de governança da Internet no Brasil, e dá outras providências"*, texto disponível em http://www.planalto.gov.br/ccivil_03/decreto/2003/d4829.html [17.09.2019].

De acordo com o artigo citado, percebe-se que a lei disciplina a obrigação de haver um envolvimento entre todos os setores do governo brasileiro, com a finalidade de contribuir com o desenvolvimento da Internet para atender o bem comum. Desse modo, o governo, através da interoperabilidade, deverá envolver seus três níveis federativos para criar e manter um programa que possibilite o acesso, e a troca de dados sobre seus cidadãos.

A lei ainda disciplina acerca da utilização da internet com o intuito de promover a cultura e cidadania, de forma que todos possam ter acesso a ela e através dela poder conhecer de informações úteis, além de colaborar para a promoção de eventos em que haja a participação da população.

O artigo 25, aventa a respeito das aplicações de internet que sejam desenvolvidas pelos entes do poder público. Para tanto, os entes devem buscar:

> "(...) II - acessibilidade a todos os interessados, independentemente de suas capacidades físico-motoras, perceptivas, sensoriais, intelectuais, mentais, culturais e sociais, resguardados os aspectos de sigilo e restrições administrativas e legais; III - compatibilidade tanto com a leitura humana quanto com o tratamento automatizado das informações; IV - facilidade de uso dos serviços de governo eletrônico; e V - fortalecimento da participação social nas políticas públicas."

Muito embora a lei tenha previsto a respeito das aplicações desenvolvidas pelos entes do poder público, na prática isso só acontecerá quando houver a compatibilidade da tecnologia de suporte das informações para que realmente haja o seu entrelaçamento.

Ademais, ainda é de responsabilidade do governo, segundo a lei, desenvolver tecnologias para facilitar o acesso à Internet a todos os cidadãos brasileiros, inclusive os que tenham algum tipo de limitação (as minorias), como, por exemplo, os indígenas, isso no intuito da promoção da universalização do acesso à Internet.

No artigo 26 a lei visa a inclusão digital na educação, atribuindo responsabilidade ao governo para a capacitação integrada ainda a outras práticas educacionais, com vistas ao uso consciente e seguro da internet, e apresentar o uso da mesma como uma ferramenta para o exercício da cidadania.

Corroborado pelo artigo 26, o artigo 27, trata acerca das "iniciativas públicas de fomento à cultura digital e de promoção da internet como ferramenta social devem: I - promover a inclusão digital; II - buscar reduzir as desigualdades, sobretudo entre as diferentes regiões do País, no acesso às tecnologias da informação e comunicação e no seu uso; e III - fomentar a produção e circulação de conteúdo nacional." A lei, além de promover a importância da proteção dos dados dos usuários, aborda

também sobre a inclusão digital, ou seja, da facilitação (obrigação do governo) para o acesso da internet pela população.

Nesse prisma, o artigo 28 impõe obrigação ao próprio Estado para se manter atualizado, bem como apresentar estratégias para atingir as metas de inclusão digital e social com vistas à promoção e o desenvolvimento social.

No capítulo V, a lei trata das "Disposições Finais", e este é composto pelos artigos 29, 30, 31 e 32. Dentre os artigos elencados neste capítulo, vale ressaltar o disposto no artigo 30 que assim diz: "A defesa dos interesses e dos direitos estabelecidos nesta Lei poderá ser exercida em juízo, individual ou coletivamente, na forma da lei".

Nesse sentido, qualquer pessoa que se sinta lesada por alguma infração relativa à violação de direitos previstos no Marco Civil da Internet, poderá acionar a justiça para propor ação individual ou coletiva, na busca da preservação de seus direitos.

A Lei n.º 12.926/2014 foi publicada em 23 de abril de 2014, e por força do artigo 32, passou a vigorar em 23 de junho de 2014, ou seja, 60 (sessenta) dias após sua publicação.

Há de se destacar que a criação de lei específica sobre o tratamento de dados pessoais no ordenamento jurídico brasileiro, com vistas a reconhecer um direito à proteção de dados pessoais, é um divisor de águas, isso por que, foi o pontapé inicial para se explorar a necessidade e possibilidade de normatização no mundo da internet.

Contudo, percebe-se que o Marco Civil da Internet, tratou a respeito do Direito à Proteção de Dados Pessoais com um viés mais civilista do que constitucional, ou seja, mais como o dever de se regulamentar um direito civil – relativo ao acesso a internet de qualidade e em decorrência disso, resguardar direitos ao titular dos dados – do que se reconhecer a jusfundamentalidade desse direito.

3.3.3. Dos decretos n.º 8.771 e n.º 8.777, de 11 de maio de 2016

A Lei do Marco Civil da Internet veio estabelecer princípios, garantias, direitos e deveres relativos ao uso da internet. Suas normas, basicamente, contemplam o dever de os provedores promoverem a neutralidade da rede, bem como garantir a liberdade de expressão e a privacidade dos usuários. Algumas das normas elencadas na lei eram tratadas em outros instrumentos jurídicos, tais como CRFB de 1988, CC, CDC, LAI e outros. No entanto, mesmo sendo a primeira lei nacional específica sobre o tema, a lei necessitava de regulamentação relativa a alguns pontos, como os dispostos nos seus artigos: 9.º, § 1.º; 10, § 4.º; 11, § 3.º e 4º; 13; 15, e outros.

A carência dos artigos que necessitavam de regulamentação foi suprida pela publicação do Decreto n.º 8.771[160] em 11 de maio de 2016, que entrou em vigor em 11 de junho de 2016. O Decreto teve por objetivo regulamentar "a Lei n.º 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações".

A Lei do Marco Civil da Internet dispõe, em seu artigo 9.º, § 1.º, acerca da neutralidade como regra, apresentando ainda que, a exceção, somente deveria ocorrer em duas situações, as quais são tratadas nos seus incisos I (requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações) e II (priorização de serviços de emergência).

O Decreto regulamenta tal assunto nos artigos 4.º a 10. Em síntese, definiu que:

> "Os requisitos técnicos indispensáveis à prestação adequada de serviços e aplicações devem ser observados pelo responsável de atividades de transmissão, de comutação ou de roteamento, no âmbito de sua respectiva rede, e têm como objetivo manter sua estabilidade, segurança, integridade e funcionalidade". (artigo 5.º)

Nesse prisma, não houve inovação no que diz respeito ao princípio da neutralidade, uma vez que manteve a determinação da obrigação daquele que for responsável para se atentar aos requisitos técnicos que autorizem a discriminação ou a limitação do tráfego dos dados. Os requisitos (§ 1.º) apresentados são: "tratamento de questões de segurança de redes, tais como restrição ao envio de mensagens em massa (spam) e controle de ataques de negação de serviço e para o tratamento de situações excepcionais de congestionamento de redes, tais como rotas alternativas em casos de interrupções da rota principal e em situações de emergência (incisos I e II)".

O § 2.º do mesmo artigo 5.º dispõe que ficará a cargo da Agência Nacional de Telecomunicações (ANATEL), para atuar na "fiscalização e na apuração de infrações quanto aos requisitos técnicos elencados neste artigo, consideradas as diretrizes estabelecidas pelo Comitê Gestor da Internet – CGIbr".

---

160 Cf. BRASIL, Decreto nº 8.771, de 11 de maio de 2016, *"Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações",* texto disponível em http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2016/Decreto/D8771.html [17.09.2019].

O artigo 6.º, estabelece acerca da permissão de gerenciamento de redes com a finalidade de manter a estabilidade, segurança e funcionalidade, desde que haja técnicas compatíveis com os padrões internacionais para o bom e regular funcionamento da internet e que sejam observados os parâmetros publicados pela ANATEL e seguidos as diretrizes do CGI.

O artigo 7.º baliza a respeito da transparência dos provedores para com os consumidores, devendo, como por exemplo, discriminar as informações a respeito do tráfego, bem como que os contratos sejam de simples e fácil compreensão.

Para tanto, o artigo 8.º expõe as situações que poderão haver a discriminação, assim como degradação, quando houver situações de emergência nas "comunicações destinadas aos prestadores dos serviços de emergência, ou comunicação entre eles, conforme previsto na regulamentação da Agência Nacional de Telecomunicações – Anatel (inciso I)"; ou nas "comunicações necessárias para informar a população em situações de risco de desastre, de emergência ou de estado de calamidade pública (inciso II)", apresentando ainda que, nesses casos a transmissão se dará de forma gratuita (§ único).

O artigo 9.º impede que os provedores de aplicações "comprometam o caráter público e irrestrito do acesso à internet e os fundamentos, os princípios e os objetivos do uso da internet no País (inciso I); priorizem pacotes de dados em razão de arranjos comerciais (inciso II); ou privilegiem aplicações ofertadas pelo próprio responsável pela transmissão, pela comutação ou pelo roteamento ou por empresas integrantes de seu grupo econômico (inciso III)".

O artigo 10.º determina que "[a]s ofertas comerciais e os modelos de cobrança de acesso à internet devem preservar uma internet única, de natureza aberta, plural e diversa, compreendida como um meio para a promoção do desenvolvimento humano, econômico, social e cultural (...)".

No capítulo III, intitulado "Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas" encontram-se dispostos os artigos 11, 12, 13, 14, 15 e 16. A Seção I, trata "Da Requisição de Dados Cadastrais", onde o artigo 11 determina que as autoridades administrativas que tenham competência para a requisição dos dados pessoais deverão, em suas requisições, informar expressamente o dispositivo legal que assegura tal direito, bem como especificar em quais dados tem interesse.

Ainda na Seção I, o artigo 12 regulamenta que deverá a "autoridade máxima de cada órgão da administração pública federal publicará anualmente em seu sítio na internet relatórios estatísticos de requisição de dados cadastrais: I - o número de pedidos realizados; II - a listagem dos provedores de conexão ou de acesso a aplicações aos quais os dados foram requeridos; III - o número de pedidos

deferidos e indeferidos pelos provedores de conexão e de acesso a aplicações; e IV - o número de usuários afetados por tais solicitações".

A Seção II, que regula os "Padrões de segurança e sigilo dos registros, dados pessoais e comunicações privadas", encontra-se disposto o artigo 13, que apresenta as "diretrizes sobre os padrões de segurança", e estabelece ainda que deve ser levado em consideração o porte do provedor recebedor, especificando os tratamentos que a eles serão conferidos, de acordo com as indicações do CGI.

O artigo 14 regulamenta o conceito de dado pessoal, sendo ele um "dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa (inciso I)". Regulamentou ainda o conceito de tratamento de dados pessoais, sendo "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 (inciso II)".

O artigo 15 determina que os dados pessoais, regulamentados no artigo anterior, bem como os mencionados no artigo 11 do Marco Civil da Internet, devem ser mantidos "em formato interoperável e estruturado, para facilitar o acesso decorrente de decisão judicial ou determinação legal (...)".

O artigo 16 finaliza a Seção II do capítulo III e estabelece que "[a]s informações sobre os padrões de segurança adotados pelos provedores de aplicação e provedores de conexão devem ser divulgadas de forma clara e acessível a qualquer interessado, preferencialmente por meio de seus sítios na internet, respeitado o direito de confidencialidade quanto aos segredos empresariais".

No último Capítulo de n.º IV, o Decreto trata "Da Fiscalização e Da Transparência", e nele encontram-se dispostos os artigos finais, sendo eles o 17, 18, 19, 20, 21 e 22. Nos artigos 17 a 19, o Decreto vem regulamentar a responsabilidade da ANATEL, impondo-a o dever de regulamentar e fiscalizar a apuração das infrações de acordo com a Lei n.º 9.472/97[161]; a responsabilidade de fiscalizar e apurar as infrações nos termos do CDC será da Secretaria Nacional do Consumidor; e por fim, as apurações de infrações à ordem econômica recairão sobre o Sistema Brasileiro de Defesa da Concorrência, de acordo com o disposto na Lei n.º 12.529/2011[162].

161 Cf. BRASIL, Lei nº 9.472, de 16 de julho 1997, *"Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº. 8, de 1995*, texto disponível em http://www.planalto.gov.br/ccivil_03/LEIS/L9472.html [17.09.2019].

162 Cf. BRASIL, Lei n.º 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; altera a Lei nº 8.137, de 27 de dezembro de 1990, o Decreto-Lei nº 3.689, de 3 de outubro de 1941 - Código de Processo Penal, e a Lei nº 7.347, de 24 de julho de 1985; revoga dispositivos da Lei nº 8.884, de 11 de junho de 1994, e a Lei nº 9.781, de 19*

O Decreto n.º 8.771/2016 teve como finalidade regulamentar a Lei n.º 12.965/2014, para que essa realmente pudesse alcançar sua finalidade, que é a de proteger o uso da internet no país. Porém, algumas matérias ainda careciam de regulamentação, que foram supridas através do Decreto n.º 8.777, publicado em 11 de maio de 2016, momento em que, de imediato, começou a vigorar (artigo 11).

A fim de regulamentar a questão da Política Nacional de Dados Abertos, não tratada na Lei n.º 12.965/2014, em 11 de maio de 2016, foi publicado o Decreto n.º 8.777[163] que instituiu Política de Dados Abertos do Poder Executivo federal.

A Política Nacional de Dados Abertos teve como finalidade contribuir para a evolução na qualidade da transparência do governo, que apresentou melhores possibilidades de controle social frente às ações governamentais.

Nesse sentido, a Transparência não teve como finalidade apenas combater a corrupção e controlar os gastos públicos ao expô-los, mas também como fonte de obtenção de informações relativas às politicas públicas para a sociedade.

Os objetivos do Decreto estão elencados logo no artigo 1.º. Vejamos:

> "I - promover a publicação de dados contidos em bases de dados de órgãos e entidades da administração pública federal direta, autárquica e fundacional sob a forma de dados abertos; II - aprimorar a cultura de transparência pública; III - franquear aos cidadãos o acesso, de forma aberta, aos dados produzidos ou acumulados pelo Poder Executivo federal, sobre os quais não recaia vedação expressa de acesso; IV - facilitar o intercâmbio de dados entre órgãos e entidades da administração pública federal e as diferentes esferas da federação; V - fomentar o controle social e o desenvolvimento de novas tecnologias destinadas à construção de ambiente de gestão pública participativa e democrática e à melhor oferta de serviços públicos para o cidadão; VI - fomentar a pesquisa científica de base empírica sobre a gestão pública; VII - promover o desenvolvimento tecnológico e a inovação nos setores público e privado e fomentar novos negócios; VIII - promover o compartilhamento de recursos de tecnologia da informação, de maneira a evitar a duplicidade de ações e o desperdício de recursos na

de janeiro de 1999; e dá outras providências", texto disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/Lei/L12529.html [17.09.2019].

163 Cf. BRASIL, Decreto nº 8.777, de 11 de maio de 2016, *"Institui a Política de Dados Abertos do Poder Executivo federal",* texto disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8777.html [19.09.2019].

disseminação de dados e informações; e IX - promover a oferta de serviços públicos digitais de forma integrada".

No artigo 3.º o Decreto regulamenta em seus incisos conceitos, tais como:

> "I - dado - sequência de símbolos ou valores, representados em qualquer meio, produzidos como resultado de um processo natural ou artificial; II - dado acessível ao público - qualquer dado gerado ou acumulado pelo Governo que não esteja sob sigilo ou sob restrição de acesso nos termos da Lei n.º 12.527, de 18 de novembro de 2011 ; III - dados abertos - dados acessíveis ao público, representados em meio digital, estruturados em formato aberto, processáveis por máquina, referenciados na internet e disponibilizados sob licença aberta que permita sua livre utilização, consumo ou cruzamento, limitando-se a creditar a autoria ou a fonte; IV - formato aberto - formato de arquivo não proprietário, cuja especificação esteja documentada publicamente e seja de livre conhecimento e implementação, livre de patentes ou qualquer outra restrição legal quanto à sua utilização; e V - Plano de Dados Abertos - documento orientador para as ações de implementação e promoção de abertura de dados de cada órgão ou entidade da administração pública federal, obedecidos os padrões mínimos de qualidade, de forma a facilitar o entendimento e a reutilização das informações".

Os princípios e diretrizes do Decreto foram disciplinados através do artigo 3º, que assim dispõe:

> "I - observância da publicidade das bases de dados como preceito geral e do sigilo como exceção; II - garantia de acesso irrestrito às bases de dados, as quais devem ser legíveis por máquina e estar disponíveis em formato aberto; III - descrição das bases de dados, com informação suficiente para a compreensão de eventuais ressalvas quanto à sua qualidade e integridade; IV - permissão irrestrita de reuso das bases de dados publicadas em formato aberto; V - completude e interoperabilidade das bases de dados, as quais devem ser disponibilizadas em sua forma primária, com o maior grau de granularidade possível, ou referenciar as bases primárias, quando disponibilizadas de forma agregada; VI - atualização periódica, de forma a garantir a perenidade dos dados, a padronização de estruturas de informação e o valor dos dados à sociedade e atender às necessidades de seus usuários;

> e VII - designação clara de responsável pela publicação, atualização, evolução e manutenção de cada base de dado aberta, incluída a prestação de assistência quanto ao uso de dados".

Em relação à Gestão, o Decreto trata no Capítulo III – que tem por título "Da Governança", mais especificamente no artigo 5.º – sobre a gestão da Política, e regulamenta que o órgão responsável pela coordenação das ações, inicialmente seria o Ministério do Planejamento, Orçamento e Gestão, entidade essa que foi substituída pela Controladoria-Geral da União, através do Decreto n.º 9.903[164], de 08 de julho de 2019, por meio da Infraestrutura Nacional de Dados Abertos (INDA).

Quanto à "implementação da Política de Dados Abertos, essa ocorrerá por meio da execução de Plano de Dados Abertos no âmbito de cada órgão ou entidade da administração pública federal, direta, autárquica e fundacional (...)". (§ 2.º, artigo 5.º)

Ademais, a "INDA poderá estabelecer normas complementares relacionadas com a elaboração do Plano de Dados Abertos, bem como relacionadas à proteção de informações pessoais na publicação de bases de dados abertos" (§ 3.º, artigo 5.º).

A respeito da possibilidade de solicitar a "abertura de bases de dados da administração pública federal aplicam-se os prazos e os procedimentos previstos para o processamento de pedidos de acesso à informação, nos termos da Lei n.º 12.527, de 2011, e do Decreto n.º 7.724[165], de 16 de maio de 2012".

Portanto, após análise hermenêutica minuciosa sobre a primeira lei nacional que visou à proteção de direitos, bem como uso da internet, restou claro que a mesma não garante suficientemente direitos como à privacidade, bem como a efetiva Proteção de Dados Pessoais de forma ampla, completa e estruturada.

Percebeu-se ainda que nem todas as disposições visavam o reconhecimento de um Direito à Proteção de Dados Pessoais, de modo que, a Lei do Marco Civil da Internet acabou por não ser uma lei que instituía um Direito à Proteção de Dados Pessoais no âmbito da internet.

Contudo, imperioso é reconhecer que o Marco Civil foi um importante avanço da luta pela disponibilização de uma internet de qualidade, justa, protegida e democrática no Brasil, tendo sido,

---

164 Cf. BRASIL, Decreto n.º 9.903, de 8 de julho de 2019, *"Altera o Decreto n.º 8.777, de 11 de maio de 2016, que institui a Política de Dados Abertos do Poder Executivo federal, para dispor sobre a gestão e os direitos de uso de dados abertos*", texto disponível em http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9903.htm#art1 [17.9.2019].

165 Cf. BRASIL, Decreto n.º 7.724, de 16 de maio de 2012, *"Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição*", texto disponível em http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2012/Decreto/D7724.html [17.09.2019].

inclusive referência para outros países; porém, em pontos como a Proteção de Dados Pessoais a eficácia não foi garantida, motivo esse que levou à discussão do Projeto de Lei n.º 5.276/2016.

3.4. Da lei geral de proteção de dados pessoais

3.4.1. Do projeto de lei n.º 5.276, de 13 de maio de 2016

Devido à falsa sensação de proteção ao titular sobre seus dados pessoais pela Lei n.º 12.925/2014, mesmo após a regulamentação dos Decretos de n.º 8.771 e 8.777 de 2016, ainda havia a necessidade da criação de outra lei específica que reparasse a falha em relação à Proteção de Dados Pessoais, no que toca ao tratamento dos mesmos.

Nesse sentido, surge o Projeto de Lei n.º 5.276[166] de 29 de abril de 2016. O PL surgiu a partir resultado de grande debate[167] promovido pelo Ministério da Justiça, o qual abriu espaço para a sociedade se manifestar acerca dos anseios sobre o tema. A votação, à época, recebeu mais de 1.100 (um mil e cem) contribuições, com mais de 50 (cinquenta) mil acessos ao site de votação.

A preocupação da sociedade indicou que os ditames ajustados pelo Marco Civil da Internet necessitavam de um complemento, além dos decretos em vigor, motivo esse que levou o legislador a pensar no PL n.º 5.276/2016.

O PL foi apresentado ao Plenário do Congresso Nacional pelo Poder Executivo em 15 de maio de 2016, com caráter de urgência, a pedido da então Presidente Dilma Rousseff. O mesmo foi apensado ao PL n.º 4.060/2012, em 14 de julho de 2016, por se tratarem e matérias correlatas.

Enquanto o Marco Civil da Internet trouxe ao mundo virtual garantias constitucionais, como por exemplo, à liberdade de expressão e de informação, o PL apresentou um rol de direitos mais específicos relacionados ao Direito à Proteção de Dados Pessoais, bem como a forma de tratamento desses no tocante ao armazenamento, independente se poderiam ser por entidades públicas ou privadas. O PL apresentou um escopo de disposições que vão além do mundo virtual. A regulamentação disciplinava acerca do tratamento de dados extra internet, ou seja, em qualquer meio.

O PL era composto por 56 artigos, distribuídos em 9 (nove) capítulos, a saber:

166 Cf. BRASIL, Câmara do Deputados, Projeto de Lei nº 5.276/2016, *"dispõe sobre o tratamento de dados pessoais..."*, *op. cit.*

167 Cf. SOUZA, Murilo, "*Projeto abrange operações de tratamento de dados realizados tanto no Brasil como no exterior, mas cuja coleta tenha ocorrido em território nacional", in Câmara dos Deputados,* 2016, texto disponível em https://www.camara.leg.br/noticias/493890-projeto-regulamenta-acesso-a-dados-pessoais-no-brasil/ [17.09.2019].

> "Disposições Preliminares; Requisitos para o Tratamento de Dados Pessoais (Seção I – Requisitos para o Tratamento; Seção II – Término do Tratamento); Dos Direitos do Titular; Do tratamento de Dados Pessoais pelo Poder Público (Seção I – Tratamento de Dados Pessoais pelo Poder Público; Seção II – Responsabilidade); Da Transferência Internacional de Dados; Dos Agentes do Tratamento de Dados Pessoais (Seção I – Responsável e Operador; Seção II – Encarregado pelo Tratamento de Dados Pessoais; Seção III – Responsabilidade e Ressarcimento de Danos); Segurança e das Boas Práticas (Seção I – Segurança e Sigilo de Dados; Seção II – Boas Práticas); Da Fiscalização (Seção I – Sanções Administrativas; Seção II – Órgão Competente e Conselho Nacional de Proteção de Dados e da Privacidade); Disposições Finais e Transitórias".

Importante ressaltar que não será feita uma análise hermenêutica do PL – assim como foi feito sobre a Lei n.º 12.965/2014 –, isso porque, no próximo tópico, será apresentado conteúdo idêntico, uma vez que, o conteúdo do PL n.º 5.276/2016 é refletido na Lei n.º 13.709/2018.

Todavia serão abordados os aspectos mais relevantes tratados pelo PL, que se apresentou como um conteúdo inédito quando comparado com o Marco Civil da Internet.

O principal ponto que merece destaque é o que diz respeito à definição de dados sensíveis, bem como a sua transferência (repasse e venda) entre empresas, como, por exemplo, dados relativos a menores (crianças e adolescentes), a informações financeiras e de créditos, e, por fim, a respeito da criação de uma autoridade específica para a proteção de dados pessoais.

O artigo 5.º trata da parte conceitual dos direitos que a Lei deve assegurar, e no inciso III trata sobre dos Dados Sensíveis que são "dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos".

O conceito de dados sensíveis apresentado pelo PL, no artigo 5.º, inciso III, segue a mesma linha de definição apresentada pela Convenção do Conselho da Europa 108, que tratou da "Protecção das Pessoas Relativamente ao Tratamento Automatizado de Dados De Carácter Pessoal". No artigo 6.º, a Convenção dispôs que a categoria de dados especiais incluem os "[o]s dados de carácter pessoal que revelem a origem racial, as opiniões políticas, as convicções religiosas ou outras, bem como os dados de carácter pessoal relativos à saúde ou à vida sexual, só poderão ser objecto de tratamento

automatizado desde que o direito interno preveja garantias adequadas. O mesmo vale para os dados de carácter pessoal relativos a condenações penais".

Os dados sensíveis se apresentam mais frágeis em relação aos dados comuns. Assim, o PL apresenta no artigo 11, inciso I, que, para que ocorra o tratamento, deverá haver o "consentimento livre, inequívoco, informado, expresso e específico pelo titular", diferente do que trata o artigo 7.º, inciso I, em relação ao tratamento de dados comuns, que poderá ocorrer sempre quando o consentimento for "livre, informado e inequívoco".

Contudo, é valido ressalvar que o mesmo artigo 11 prevê situações em que os dados sensíveis sofrerão tratamento sem a necessidade de consentimento do seu titular, mesmo que esses dados não se apresentem anonimizados, como por exemplo, no caso de pesquisas comerciais. Outro fato que vale a pena ressaltar acontece em relação aos dados de condenações criminais, ou seja, registros policias, haja vista que o PL não os trata como dados sensíveis, diferentemente da legislação estrangeira.

Em que pese a legislação considerar como dados sensíveis os dados relativos a condenações criminais, mesmo sobrepesando uma possível violação a direitos fundamentais, a possibilidade de acessos a esses dados em específico pelo Estado acaba por se tornar mais relevante para a sociedade por contribuir para a segurança pública, bem como para tomada de decisões judiciais para a aplicação de penas mais justas.

Em relação ao tratamento aos dados sensíveis, o PL brasileiro apresentou semelhanças ao disposto na Diretiva Europeia 95/46/CE de 24 de outubro de 1995, que, em seu artigo 8.º, n.º 1, dispôs que:

> "1. Os Estados-membros proibirão o tratamento de dados que revelem a origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual. 2. O parágrafo 1 não se aplica quando: (a) o titular dos dados deu consentimento explícito ao tratamento desses dados, salvo se a legislação do Estado-Membro estabelecer que a proibição referida no parágrafo 1 não pode ser retirada por consentimento da pessoa em causa".

Outro ponto que merece destaque no PL, considerado como um ponto negativo, diz respeito à transferência nacional e interconexão de dados, pois, o projeto não oferecia garantias especiais para a transferência nacional ou a interconexão de dados entre entidades privadas para fins comerciais. Além disso, de acordo com o disposto no PL, não haveria necessidade de consentimento para esses tipos de transações, o que acabava por ferir direito dos titulares dos dados.

Desse modo, os usuários titulares dos dados poderiam sofrer possíveis violações por ter seus dados comercializados ou somente repassados entre empresas privadas sem o devido consentimento expresso para essa finalidade.

Merece ainda devida atenção o artigo 14, que assim dispõe: "O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado no seu melhor interesse, nos termos da legislação pertinente". Em relação ao tratamento de dados de menores – crianças e adolescentes –, o PL apresentava dispositivos genéricos e evitava dar a importância devida ao assunto.

Por analogia de leis congêneres, a exemplo de países como os EUA, onde vigora a Lei COOPA[168] – "Children's Online Privacy Protection Act" (disposta no Código Americano, no Título 15, Capítulo 91, parágrafos 6501 a 6506) que dispõe a respeito do tratamento dos dados pessoais de crianças na internet e caracteriza como regra geral, ilícito, em relação a menores de 13 anos sem o devido consentimento dos pais –, o PL se apresentou falho, pois não demonstrou preocupação na preservação de direitos desse grupo específico de titulares de dados. Portanto, sem consonância com o Estatuto da Criança e do Adolescente (ECA)[169], o código brasileiro de referência para proteção e garantias para crianças e adolescentes.

Merece destaque também a Seção II, do Capítulo VIII, do PL que trata sobre o "Órgão competente e Conselho Nacional de Proteção de Dados e da Privacidade". Nos artigos 53, 54 e 55, foram apresentadas as atribuições do Órgão competente, a composição do Conselho Nacional de Proteção de Dados Pessoais e a sua competência.

O PL previu que as atribuições do Órgão competente pela implementação e fiscalização da "lei", seriam:

> "I – zelar pela proteção dos dados pessoais, nos termos da legislação; II – elaborar diretrizes para uma Política Nacional de Proteção de Dados Pessoais e Privacidade; III – realizar auditoria nos tratamentos de dados pessoais e processos envolvidos com dados pessoais visando garantir a sua conformidade aos princípios desta lei; IV – promover entre a população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e medidas de segurança; V – promover estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; VI –

168 Cf. UNITED STATES OF AMERICA, *Code of Federal Regulations, Title 16, Chapter I, Subchapter C, Part 312 - Children's Online Privacy Protection Rule,* texto disponível em https://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5 [18.09.2019].

169 Cf. BRASIL, Lei n.° 8.069, de 13 de julho de 1990, *"Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências"*, texto disponível em http://www.planalto.gov.br/ccivil_03/leis/l8069.html [18.09.2019].

> estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais; VII – promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional e transacional; VIII – dispor sobre as formas pelas quais se dará a publicidade das operações de tratamento; IX – solicitar, a qualquer momento, às entidades do Poder Publico que realizem operações de tratamento de dados pessoais, informe específico sobre o âmbito, natureza dos dados e demais detalhes do tratamento realizado, podendo emitir parecer técnico complementar para garantir o cumprimento de dados pessoais; X – estabelecer normas complementares para as atividades de comunicação de dados pessoais; XI – elaborar relatórios anuais acerca de suas atividades; XII – editar normas sobre proteção de dados pessoais e privacidade; e XIII – realizar demais ações dentro de sua esfera de competência, inclusive as previstas nesta Lei e em legislação específica".

Além de um órgão competente para fiscalizar a lei, o artigo 54 determinava a criação de um "Conselho Nacional de Proteção de Dados Pessoais e da Privacidade", que seria composto por quinze representantes titulares e seus respectivos suplentes, indicados pelo Ministério da Justiça, seguindo os seguintes critérios: 7 (sete) representantes do Poder Executivo, 1 (um) do Congresso Nacional, 1 (um) do CNJ, 1 (um) do Ministério Público, 1 (um) do CGI, 1 (um) da sociedade civil, 1 (um) da academia e 2 (dois) do setor privado.

A fim de implantar uma cultura de valorização da informação sobre o tema, de acordo com o artigo 55, o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade deveria "disseminar o conhecimento sobre a proteção de dados pessoais e privacidade à população em geral, uma vez que, através da educação, uma cultura pode ser mudada". (inciso V)

Conforme visto, o Projeto de Lei apresentava uma arquitetura de dispositivos legais que assegurariam a efetiva Proteção de Dados Pessoais, oferecendo ainda uma série de dispositivos que, com vistas a proteção, à intimidade, à privacidade e o desenvolvimento da personalidade das pessoas, trataria da coleta e do tratamento de dados pessoais por parte das entidades públicas e das privadas.

Inicialmente o Projeto de Lei n.º 5.276/2016 foi visto como uma complementação à Lei do Marco Civil da Internet, uma vez que se apresentou em consonância com a ocasião legal nacional e internacional. O Projeto também era extremamente detalhado no que diz respeito às atividades que deveriam ser desenvolvidas pela administração pública quando do tratamento de dados, além de garantir

uma maior transparência aos titulares sobre seus dados coletados. De outro norte, o projeto previu ainda a exploração dos dados pessoais e apontava para uma nova seara de negócios as empresas privadas.

Muito embora tenha trazido inovações sobre o tema, o Projeto de Lei n.º 5.276/2016 foi arquivado em 29 de maio de 2018, e, consequentemente, desapensado do Projeto de Lei n.º 4.060/2012, sendo este último, em 14 de agosto de 2018 transformado na Lei Ordinária n.º 13.709, a "Lei Geral de Proteção de Dados Pessoais (LGPD)", que passou a dispor sobre o Direito à Proteção de Dados Pessoais e o seu tratamento, além de dar outras providências.

3.4.2. Da lei federal n.º 13.709, de 14 de agosto de 2018 – lei geral de proteção de dados pessoais (LGPD)

Depois de mais de 8 (oito) anos de debates[170] sobre o tema de tratamento e proteção de dados pessoais – no intento de traçar uma linha histórica (nacional) legal, desde a Lei n.º 12.414/2011; Lei n.º 12.527/2011; Projeto de Lei n.º 4.060/2012, Projeto de Lei do Senado n.º 330/2013; Lei n.º 12.925/2014; Decretos n.º 8.771 e 8.777 de 2016; e, por fim o Projeto de Lei n.º 5.276/2016, tendo ainda em consideração as influências da Diretiva Europeia 95/46/CE, de 24 de outubro de 1995, bem como o "General Data Protection Regulation" (GDPR), Regulamento Geral sobre a Proteção de Dados da União Europeia, Regulamento (UE) 2016/679, de 27 de abril de 2016 –, foi sancionada em 14 de agosto de 2018 a Lei Federal n.º 13.709[171], lei essa que "[d]ispõe sobre a proteção de dados pessoais e altera a Lei n.º 12.965, de 23 de abril de 2014 (Marco Civil da Internet)".

Qual a importância de uma regulamentação específica versando a respeito da necessidade à proteção de dados pessoais? Qual a importância de o titular ter efetivamente tutelado a proteção na circulação de seus dados, mediante seu consentimento? SILVEIRA e FROUFRE, alertam que, "[s]e não for devidamente regulada, essa escolha civilizacional implicará na perda daquilo que é mais genuíno na humanidade, pois as experiências humanas seriam reduzidas a padrões de dados. Tínhamos que as experiências aconteciam dentro de nós e era aí onde procurávamos a razão de tudo aquilo que nos

170 Cf. JINKING, Daniella, "*Governo vai debater criação de marco legal para proteção de dados pessoais no Brasil.* Brasília", *in Rede Brasil Atual*, 2010, texto disponível em https://www.redebrasilatual.com.br/cidadania/2010/12/governo-vai-debater-criacao-de-marco-legal-para-protecao-de-dados-pessoais-no-brasil/ [18.09.2019].

171 Cf. BRASIL, Lei nº 13.709, de 14 de agosto de 2018, *"Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Redação original, antes da alteração da Lei nº 13.853/2019",* texto disponível em https://legis.senado.leg.br/norma/27457334/publicacao/27457731 [18.09.2019].

acontece". Em tom de crítica, acrescentam ainda que "valor já não [mais] reside nas experiências quotidianas e sim na capacidade de as transformarmos em dados que circulam livremente[172]".

Inicialmente, a Lei n.º 13.709/2018 foi composta por 65 artigos, os quais foram distribuídos em 10 (dez) capítulos, sendo eles:

> "Capítulo I – Disposições Preliminares; Capítulo II – Do Tratamento de Dados Pessoais, Seção I – Dos Requisitos para o Tratamento de Dados Pessoais, Seção II – Do Tratamento de Dados Pessoais Sensíveis, Seção III – Do Tratamento de Dados Pessoais de Crianças e de Adolescentes, Seção IV – Do Término do Tratamento de Dados; Capítulo III – Dos Direitos do Titular; Capítulo IV – Do Tratamento de Dados Pessoais pelo Poder Público, Seção I – Das Regras, Seção II – Da Responsabilidade; Capítulo V – Da Transferência Internacional de Dados; Capítulo VI – Dos Agentes de Tratamento de Dados Pessoais, Seção I – Do Controlador e do Operador, Seção II – Do Encarregado pelo Tratamento de Dados Pessoais, Seção III – Da Responsabilidade e do Ressarcimento de Danos; Capítulo VII – Da Segurança e das boas práticas, Seção I – Da Segurança e do Sigilo de Dados, Seção II – Das Boas Práticas e da Governança; Capítulo VIII – Da Fiscalização, Seção I – Das Sanções Administrativas; Capítulo IX – Da Autoridade Nacional de Proteção de Dados (ANPD) E Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, SEÇÃO I – Da Autoridade Nacional de Proteção de Dados (ANPD), SEÇÃO II – Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; Capítulo X – Disposições Finais e Transitórias".

Antes ainda de entrar em vigor, a referida lei sofreu vetos[173] em relação aos artigos 23, inciso II; 26, § 1.º, inciso II; 28; 52, § 1.º, incisos VII, VIII e IX; 55; 56; 57; 58 e 59, e foi decretada pelo Congresso Nacional e sancionada pelo então Presidente da República sr. Michel Temer[174], em 14 de agosto de 2018,

172 Cf. SILVEIRA, Alessandra e FROUFRE, Pedro, *"Do mercado interno...", op. cit.*, p. 15.

173 Cf. DE PAULA, Felipe, e NAEGELE, Vitor Rabelo, "*Há vício de iniciativa na criação da Autoridade Nacional de Proteção de Dados?*", in JOTA, 2018, texto disponível em https://www.jota.info/paywall?redirect_to=//www.jota.info/tributos-e-empresas/regulacao/ha-vicio-de-iniciativa-na-criacao-da-autoridade-nacional-de-protecao-de-dados-26072018 [19.09.2019].

174 Cf. MAZUI, Guilherme, e CASTILHOS, Roniara, "*Temer sanciona com vetos lei de proteção de dados pessoais",* Brasília, *in G1*, 2018, texto disponível em https://g1.globo.com/politica/noticia/2018/08/14/temer-sanciona-lei-de-protecao-de-dados-pessoais.ghtml [19.09.2019].

sendo publicada no Diário Oficial da União em 15 de agosto de 2018[175], mas que, por força de seu artigo 65 passará a vigorar em sua totalidade somente em 14 agosto de 2020.

Logo no artigo 1.º, a lei apresenta sua finalidade legal, qual seja, a de dispor "sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural".

Nesse sentido, percebe-se que a lei tem aplicação a todos os brasileiros (pessoas naturais) e as empresas (pessoas jurídicas), independente se essas últimas são de direito público ou privado, desde que realizem o tratamento de dados pessoais, tanto em plataforma online quanto off-line.

Assim, se vislumbra que a lei tem aplicação ampla e abrangente, incluindo assim quase que a totalidade dos projetos e atividades inerentes à classe empresarial, principalmente por levar em consideração a facilidade, para não dizer, obrigatoriedade, do uso da internet, para firmar negócios em todo o território nacional, bem como em relações extraterritoriais (internacionais) sob um nível de proteção legal aos dados pessoais.

Em relação a importância da criação de uma lei com aplicação extraterritorial, SILVEIRA e FROUFRE afirmam que tem "de ser assim porque a Internet não conhece limites territoriais – e a proteção de dados só resulta se for exercida de forma tendencialmente universal[176]".

A Lei trata de forma clara e objetiva, a respeito da necessidade da proteção aos dados pessoais. Reforça essa ideia o artigo 2.º, que disciplina sobre os seguintes fundamentos:

> "I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais".

A partir da leitura do inciso IV do artigo mencionado, a figura do Direito à Proteção de Dados Pessoais – que até então era tido por boa parte da doutrina e jurisprudência como um subdireito, ligado ao Direito à Intimidade e à Vida Privada –, passou a ser reconhecido na forma de um direito autônomo,

175 Cf. BRASIL, Diário Oficial da União – DOU, Seção 1, Edição Extra, 15 de agosto de 2018, texto disponível http://www.in.gov.br/leiturajornal?data=15-08-2018&secao=DO1E [19.09.2019].

176 Cf. SILVEIRA, Alessandra e FROUFRE, Pedro, *"Do mercado interno...", op. cit.*, p. 18.

ou seja, independente, contudo se articulando aos direitos à inviolabilidade da intimidade, da imagem, da honra dentre outros.

Nota-se que pela redação do artigo 3.º a aplicabilidade da lei ocorrerá, além de todo o território nacional, também em território internacional, desde que "I - a operação de tratamento seja realizada no território nacional; II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional. § 1.º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta".

A exceção está na competência de atuação, conforme preceitua o § 2.º, do artigo 3.º, que dispõe "[e]xcetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4.º desta Lei". Portanto, a lei abrangerá todo o tratamento de dados pessoais, quer sejam eles em meio *online* ou *offline*, físico ou virtual, sempre que envolver dados relativos à pessoa física, jurídica de direito público ou privado. Deste modo, o Direito à Proteção de Dados Pessoais será resguardado pela lei e trará proteção para todos os titulares de dados que estiverem no Brasil, quer sejam eles brasileiros natos ou naturalizados ou estrangeiros.

A exceção da aplicação dessa lei encontra-se disposta no artigo 4.º, que assim baliza:

> "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) jornalísticos 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".

O disposto no artigo 4.º encontra-se em consonância com os projetos leis, que foram objetos de debates junto à Câmara dos Deputados, bem como no Senado Federal – aliás, é oriundo da análise dos projetos de leis n.º 4.060/2012 e 5.276/2016.

Um ponto específico no artigo 4.º – foi tratado nos § 1.º, 2.º, 3.º e 4.º, o qual teve como base o inciso III –, diz respeito à exceção do tratamento para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado. Vejamos como o artigo se apresenta:

> "§ 1.º 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. § 2.º 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 § 4.º deste artigo. § 3.º 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. § 4.º 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".

Em linhas gerais, durante a coleta, bem como todo o tratamento de dados, os titulares poderão se beneficiar por ter um maior controle sobre seus dados, uma vez que, para ocorrer o processamento, além do consentimento que será discorrido mais adiante, há previsão de obrigações para os controladores (a quem competem as decisões sobre o tratamento dos dados), bem como aos operadores (aqueles que tratam os dados de acordo com o estipulado pelos controladores).

A parte conceitual da lei encontra-se disposta no artigo 5.º, que expõe, de forma clara e objetiva, o que se entende por:

> "I - dado pessoal; II - dado pessoal sensível; III - dado anonimizado; IV - banco de dados; V - titular; VI - controlador; VII - operador; VIII - encarregado; IX - agentes de tratamento; X - tratamento; XI - anonimização; XII - consentimento; XIII - bloqueio; XIV - eliminação; XV - transferência internacional de dados; XVI - uso compartilhado de dados; XVII - relatório de impacto à proteção de dados pessoais; XVIII - órgão de pesquisa; XIX - autoridade nacional".

Diferentemente do artigo 3.º da Lei n.º 12.925/2014 – "O Marco Civil da Internet" –, a lei em comento (neste subcapítulo) trouxe um rol explicativo sobre os termos utilizados e abarcados por ela, o que acaba por facilitar, ao julgador e aos titulares dos dados, o conhecimento da extensão da Proteção de seus Dados Pessoais. Ainda, numa comparação com a primeira lei nacional que disciplinou sobre o tema de proteção de dados e o uso da internet, a Lei n.º 13.709/2018 inovou ao regulamentar em seu próprio corpo o conceito relativo aos dados pessoais, aos dados de caráter sensível e aos dados anônimos.

Em relação à atividade de tratamento de dados, o artigo 6.º discorre sobre os princípios que regerão o ato, sendo eles a "I - finalidade; II - adequação; III - necessidade; IV - livre acesso; V - qualidade dos dados; VI - transparência; VII - segurança; VIII - prevenção; IX - não discriminação; X - responsabilização e prestação de contas". Um dos princípios mais importantes disposto no artigo 6.º é o da finalidade (inciso I), haja vista que ele rege os demais, uma vez que os dados pessoais deverão ser utilizados somente para sua finalidade específica (inciso II), ou seja, o que motiva a sua coleta, sendo ainda necessário informar aos seus titulares qual será a sua destinação (inciso IV e VI).

Para cumprir com a finalidade, a coleta respeitará o princípio da minimização (inciso III), ou seja, somente a quantidade necessária de dados deverá ser coletada, isto é, o suficiente apenas para atingir a sua finalidade. Deve ainda ter, sua retenção ser mínima, sendo que, após a utilização, os dados deverão ser excluídos.

O capítulo II dispõe a respeito "Do Tratamento de Dados Pessoais". Em sua Seção I – "Dos requisitos para o Tratamento dos Dados Pessoais", encontram-se dispostos os artigos 7.º, 8.º, 9.º e 10.

De acordo com o artigo 7.º, o tratamento de dados somente poderá acontecer quando houver o consentimento pelo titular (inciso I), que será reconhecido através de sua manifestação livre, ou seja, sem impedimento.

Deve ainda ser informado a finalidade da coleta, em documento, através do qual, se o titular concordar, autorizará o tratamento. Se houver o consentimento, a coleta deverá cumprir com sua obrigação legal pelo controlador dos dados (inciso II), que também poderá ser coletado pela Administração Pública, quando os utilizar para a execução de suas políticas públicas (inciso III).

O tratamento ainda poderá acontecer para realização de estudos e pesquisa (inciso IV) ou para a execução de um contrato, no qual uma das partes seja o titular dos dados (inciso V). Pode também ser autorizado quando for necessária a coleta para o exercício regular de direitos em um processo, quer seja judicial, administrativo ou arbitral (inciso VI), ou quando assim fizer necessária (a coleta) para a proteção da vida ou da incolumidade física do titular ou de outro (inciso VII).

Nesse sentido ainda, relacionado às situações que versem sobre o bem indisponível vida, poderá haver o tratamento de dados para a tutela da saúde, por meio de profissionais da área da saúde ou entidades sanitárias (inciso VIII).

O tratamento de dados pessoais também poderá acontecer com a finalidade de atender aos interesses legítimos do controlador (inciso IX), exceto, quando prevalecer direitos e liberdades fundamentais que necessitem da proteção desses dados.

Ressalta-se que o tratamento de dados também poderá ocorrer para promover a proteção de crédito (inciso X) com vistas à estabilidade econômica e financeira do país.

Em relação ao consentimento pelo titular para o tratamento de dados, o artigo 8.º disciplina que "deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular".

Nesse prisma, SILVEIRA e FROUFRE esclarecem que "[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[177]".

Importante salientar o que dispõe o § 5.º do artigo mencionado em relação ao consentimento. De acordo com o parágrafo em comento, o "consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação".

O artigo 9.º enfatiza que o titular passa a ter total direito às informações relativas ao tratamento de seus dados, tais como "I - finalidade específica do tratamento; II - forma e duração do tratamento, observados os segredos comercial e industrial; III - identificação do controlador; IV - informações de contato do controlador; V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VI - responsabilidades dos agentes que realizarão o tratamento; e VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei".

A acerca do legitimo interesse do controlador, disposto no inciso IX do artigo 7.º, o artigo 10 considera como legítimas, as seguintes situações: "I - apoio e promoção de atividades do controlador; e II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei".

177 Cf. SILVEIRA, Alessandra e FROUFRE, Pedro, *"Do mercado interno...", op. cit.*, p. 19.

Na Seção II, que dispõe sobre o "Tratamento de Dados Sensíveis", encontram-se os artigos 11, 12 e 13. O artigo 11 discorre a respeito do tratamento dos dados considerados sensíveis. Segundo esse artigo, somente poderá haver o tratamento de dados de caráter sensível:

> "I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei n.º 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais".

O artigo 12 trata a respeito dos dados anonimizados, sendo eles aqueles dados que eram tidos como dados pessoais e passaram por um processo de anonimização, de modo que, quando isso ocorrer deixarão de ser considerados "dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido".

Segundo a Lei, também são considerados como dados sensíveis aqueles "referentes à saúde ou à vida sexual, dado genético ou biométrico (inciso II, artigo 5º)", e como tal, por força do artigo 13, podem passar por tratamento quando forem utilizados com a finalidade de:

> "[r]ealização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro,

> conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas".

Ainda, a respeito do tratamento de dados, a lei reserva a Seção III para o "Tratamento de Dados Pessoais de Crianças e de Adolescentes", onde se encontra disposto o artigo 14.

Reservada em apartado, o tratamento de dados de Crianças e de Adolescentes encontra limitação quando comparados aos dados dos demais titulares, isso porque, quando se trata de preservação dos melhores interesses, a lei, independente de qual for, deverá estar em consonância com a Lei Federal n.º 8.069/1990, que disciplina sobre o Estatuto da Criança e do Adolescente (ECA).

Percebe-se que neste caso, o legislador, atento a preservação de direitos em relação à Criança e ao Adolescente, quando da elaboração do artigo 14 da Lei Federal n.º 13.709/2018 previu que a esses titulares, o "§ 1.º O tratamento de dados pessoais (...) deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. § 2.º No tratamento de dados de que trata o § 1.º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei".

Para esse grupo de titulares em específico, como regra geral, o tratamento somente poderá acontecer com o consentimento dos seus responsáveis (ou de apenas um deles) apresentado pelo § 1º. Entretanto, como exceção a regra, o tratamento de dados poderá ser coletado "sem o consentimento a que se refere o § 1.º deste artigo, quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1.º deste artigo (§ 3.º, artigo 14)". Nesse caso, a ressalva preserva outros interesses que, dado o momento, são superiores à proteção de dados pessoais. Contudo, deverão ser excluídos assim que alcançarem sua finalidade.

Na Seção IV, do Capítulo II, que trata "Do Termino do Tratamento de Dados", o artigo 15, explica quando findará o tratamento.

> "O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses: I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; II - fim do período de tratamento; III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme

> disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei".

Finalizado o tratamento e cumprida a sua finalidade, por força do artigo 16, "[o]s dados pessoais serão eliminados (...)". Porém, a guarda deles poderá ser realizada quando cumprir 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".

A Lei n.º 13.709/2018 reserva um capítulo inteiro (Capítulo III) para disciplinar sobre os "Direitos dos Titulares". Neste capítulo encontram-se dispostos os artigos 17, 18, 19, 20, 21 e 22.

O artigo 17 menciona que "[t]oda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade". Nesse aspecto, tem-se que toda pessoa física/titular de dados, dentro do território nacional, será agraciada com à proteção de seus dados, nos termos da lei.

Através do artigo 18, se apresenta os direitos que são conferidos pela lei aos titulares para obter dos controladores a qualquer momento, mediante requisição, ou seja, pedido escrito (administrativamente). Vejamos:

> "I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador; VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei".

Importante salientar que, quando da negativa do controlador em ceder as informações requisitadas pelo titular dos dados, por força do § 1.º, o titular poderá "peticionar em relação aos seus dados contra o controlador perante a autoridade nacional".

A lei garante ainda, que os direitos elencados no artigo 18, poderão ser "exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento (§ 3.º)". O requerimento que assegura a lei será realizado de forma gratuita, ou seja, "sem custos para o titular, nos prazos e nos termos previstos em regulamento (§ 5.º)", e, além da Autoridade Nacional, poderá ainda o Titular reclamar seus direitos junto aos organismos de Defesa do Consumidor, como por exemplo o Programa de Proteção e Defesa do Consumidor (PROCON)[178].

A requisição de dados – que trata os § 1.º e 3.º do artigo 18 –, após apresentada deverá ser respondida, conforme dispõe o artigo 19, "I - em formato simplificado, imediatamente; ou II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular".

Caso o requerimento administrativo, disposto nos artigos anteriores, tiver resposta negativa ou insatisfatória, poderá o titular reclamar o seu direito de acordo com o que baliza o artigo 20, ou seja, "ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva".

O Capítulo IV baliza acerca "Do Tratamento de Dados Pessoais Pelo Poder Público" e está disposto em duas seções (I e II), sendo ele composto pelos artigos 23, 24, 25, 26, 27, 28, 29, 30, 31 e 32.

Na primeira seção, que trata a respeito "Das Regras", os artigos de 23 a 30 disciplina a respeito da forma que o tratamento de dados poderá se desenrolar pelo Poder Público. No artigo 23, de forma específica, a lei dispõe que o "tratamento de dados pessoais pelas pessoas jurídicas de direito público, referidas no parágrafo único do artigo 1.º da Lei n.º 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

178 *"Trata-se de um órgão administrativo de poder executivo municipal e/ou estadual destinado à proteção e defesa dos direitos e interesses dos consumidores. A função do Procon é a orientação dos consumidores, mas também é a mediação de conflitos nas relações de consumo e fiscalização dessas relações de consumo. O Procon tem a missão de fazer cumprir as leis de proteção ao consumidor que proíbem práticas comerciais desleais, fraudulentas e enganosas, a fim de garantir um mercado justo para consumidores e empresas. As atividades do órgão incluem coletar denúncias/reclamações, investigação, resolução de reclamações, fornecer informações sobre direitos, educação, defesa e divulgação a fim de educar consumidores e empresas sobre seus direitos e responsabilidades".* Cf. PROCON, *"O que é o PROCON", in Procon online,* S/d, texto disponível em https://www.procononline.com.br/o-que-e-o-procon/ [19.09.2019].

interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público".

O mesmo artigo ainda dispõe a respeito do direito do titular em relação aos seus dados perante a administração pública, informando que "[o]s prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei n.º 9.507, de 12 de novembro de 1997 (Lei do Habeas Data), da Lei n.º 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo), e da Lei n.º 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação)".

O artigo 24 estende a possibilidade de tratamento diferenciado para as empresas públicas e as sociedades de economia mista, tendo assim o mesmo tratamento em relação às pessoas jurídicas de direito privado no tratamento de dados pessoais.

O artigo 25, trouxe uma obrigação em relação ao tratamento de dados pelo poder público, que é manter os dados "em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral". Neste sentido, a interoperabilidade terá o dever de "atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6.º desta Lei" (artigo 26).

Deste modo, a Autoridade Nacional deverá zelar pela proteção de dados pessoais e segredos comerciais e industriais e poderá "solicitar, a qualquer momento, às entidades do Poder Público, a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados e demais detalhes do tratamento realizado e poderá emitir parecer técnico complementar (...)" (artigo 29). Pode ainda "estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais". (artigo 30).

Na última Seção do Capítulo IV, os artigos 31 e 32 tratam da responsabilização aos órgãos públicos pela violação da lei. Segundo ao artigo 31, "Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação". Além disso, a Autoridade Nacional "poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público" (artigo 32).

O Capítulo V da Lei regulamenta a respeito "Da Transferência Internacional de Dados", através dos artigos 33, 34, 35 e 36. O primeiro artigo deste capítulo, o 33, apresenta em quais casos a transferência internacional de dados será permitida. Vejamos:

> "I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado 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; 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".

Em suma, a transferência citada no inciso I do artigo mencionado somente será permitida se o país recebedor assegurar o grau mínimo à Proteção de Dados Pessoais. Por grau mínimo entende-se as leis equivalentes a Lei tratada aqui (Lei n.º 13.709/2018), com respaldo do artigo 34, que apresenta os requisitos mínimos.

Além das funções descritas, caberá ainda à Autoridade Nacional a responsabilidade de "verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do caput do art. 33 desta Lei (artigo 35)", quando houver a transferência internacional de dados.

As garantias contratuais dispostas nos artigos 33, 34 e 35 da lei, quando alteradas deverão ser imediatamente comunicadas à Autoridade Nacional, porque podem violar os direitos já firmados pela lei (artigo 36).

No capítulo VI, a lei trata sobre a figura "Dos Agentes de Tratamento de Dados Pessoais". A Seção I reserva espaço para disciplinar a respeito "Do controlador e do Operador".

A lei disciplina através do seu artigo 37 que o Controlador e o Operador serão agentes responsáveis pelo tratamento dos dados pessoais, sendo eles os encarregados para manter o registro de todas as operações relativas ao tratamento de dados que realizarem, principalmente quando essas acontecerem em seu legítimo interesse.

Na hierarquia apresentada pela lei, o artigo 39 disciplina que será de competência do operador a realização do tratamento de todos os dados, sempre que houver instruções fornecidas pelo controlador.

Os artigos 38 e 40 disciplinam acerca da atuação da Autoridade Nacional em relação ao Controlador e ao Operador, que pode, inclusive, "determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial (artigo 38)", bem como "dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência" (artigo 40).

Na Seção II, do Capítulo VI, a lei trata sobre a figura "Do Encarregado pelo Tratamento de Dados Pessoais". O Artigo 41 disciplina a respeito da figura do Encarregado. O encarregado será a pessoa indicada pelo controlador que ficará responsável pelo tratamento dos dados pessoais. A Lei institui que o encarregado deverá ser pessoa natural e atuará, além da responsabilidade pelo tratamento dos dados, como o elo entre o controlador, a Autoridade Nacional e os Titulares dos dados pessoais.

A identidade e as informações para o contato do encarregado devem ser claras, objetivas e divulgadas publicamente, de preferência em site do controlador (§ 1.º, artigo 41). Será de responsabilidade do encarregado o recebimento de reclamações e comunicações dos titulares, devendo ainda prestar esclarecimentos e adotar providência para resolução dos litígios. Será o responsável por receber as comunicações das autoridades competentes e atuará como um orientador dos funcionários e contratados do operador sobre as práticas a serem adotadas para que a proteção de dados pessoais se torne efetiva. Pode ainda ter outras atribuições que sejam estabelecidas pelas autoridades competentes (§ 2.º, artigo 41).

A Seção III, do Capítulo VI trata "Da Responsabilidade e do Ressarcimento de Danos". Nesta seção, a lei disciplinou sobre a possibilidade de responsabilização do controlador ou do operador pelos danos causados ao titular dos dados. Em seu artigo 42, a lei obriga os agentes (controlador e operador)

a reparar os danos que causarem, quer sejam eles de caráter patrimonial, moral, individual ou coletivo, em decorrência da violação de algum dos termos da Lei n.º 13.709/2018.

Nesse prisma, quando não observado, por exemplo, o princípio da segurança (inciso VII, artigo 6.º) e causar danos ao titular, assumem esses (operador e controlador) a obrigação pela responsabilidade civil e criminal, de forma solidária para a reparação dos danos, independente da aplicação de sanções administrativas (§ 1.º, incisos I e II, artigo 42).

A exceção em relação ao dever de indenizar é apresentada pelo artigo 43, que assim dispõe: "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".

Ainda em relação ao dever de indenizar, o artigo 44, deixa claro em quais situações poderá o titular de dados ser indenizado em decorrência do tratamento de dados. São considerados circunstâncias relevantes e fato gerador do dever de indenizar: "I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado".

No que tange às violações em relações de consumo, segundo o artigo 45, essas continuarão sob o amparo do Código de Defesa do Consumidor (CDC).

O Capítulo VII trata "Da Segurança e das Boas Práticas", e nele encontra-se a Seção I que dispõe acerca "Da Segurança e do Sigilo de Dados". Nesta seção, o artigo 46 baliza a respeito das medidas de seguranças que deverão ser adotadas pelos agentes de tratamento, desde a coleta dos dados até a finalização do serviço. As medidas de segurança deverão ser aptas para proteger os dados pessoais de acessos não autorizados ou de situações alheias à natureza do ato e até mesmo de atos ilícitos de destruição, perda, alteração, comunicação ou qualquer outra situação decorrente do tratamento irregular ou ilícito. Os padrões técnicos de segurança podem ser definidos também pela autoridade competente (§ 1.º, artigo 46).

Segundo o artigo 47, tanto os agentes, quanto qualquer outra pessoa que intervenha em algumas das fases do tratamento de dados, tem a obrigação de manter a segurança prevista na lei.

Caso ocorra algum incidente em relação ao tratamento de dados, segundo o artigo 48, "[o] controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo: I - a descrição da

natureza dos dados pessoais afetados; II - as informações sobre os titulares envolvidos; III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; IV - os riscos relacionados ao incidente; V - os motivos da demora, no caso de a comunicação não ter sido imediata; e VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo".

Após comprovado o incidente em alguma das fases do tratamento dos dados, segundo o § 2.º do artigo 48, será avaliado a situação pela Autoridade Nacional e, caso seja necessário, a fim de resguardar direito dos titulares, determinará ao controlador que adote medidas como "I - ampla divulgação do fato em meios de comunicação; e II - medidas para reverter ou mitigar os efeitos do incidente".

No intuito de evitar as situações descritas, os sistemas utilizados para o tratamento de dados deverão ser estruturados de forma que possam atender perfeitamente os requisitos de segurança, bem como aos padrões mínimos de boas práticas e de governança (artigo 49), e ainda os princípios gerais elencados no artigo 6.º e seus incisos.

Na Seção II, que trata "Das Boas Práticas e da Governança", encontram-se dispostos os artigos 50 e 51. De acordo com o artigo 50, poderão os agentes de tratamento (controlador e operador), de modo individual ou por meio de associações, formular regras de boas práticas e de governança, bem como padrões técnicos, obrigações específicas, normas de segurança, mecanismos de supervisão e intervenção para minimização dos riscos em relação ao tratamento de dados.

Segundo o artigo 51, caberá à Autoridade Nacional aplicar padrões técnicos para facilitar o controle dos titulares sobre seus dados pessoais.

O Capítulo VIII, que trata "Da Fiscalização", também elenca na Seção I, a parte relativa "Das Sanções Administrativas". Em relação às penalidades, como sanções administrativas aplicadas em decorrência das violações, essas por força do artigo 52, se apresentam bem rigorosas.

De acordo com o artigo 52, as sanções poderão se dar através de: "I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II; IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração; VII - suspensão parcial ou total do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis)

meses, prorrogável por igual período até a regularização da atividade de tratamento pelo controlador; VIII - 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; IX - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados".

Importante clarificar que as sanções somente serão aplicadas após exercido o direito da ampla defesa e do contraditório de acordo com o instituído pela CRFB de 1988 (§ 1.º, artigo 52).

Ademais, as penalidades não substituem a aplicação das sanções administrativas, indenizações civis, ou sua responsabilização criminal (§ 2.º, artigo 52).

De acordo com o artigo 53 ficará a cargo da Autoridade Nacional regulamentar "sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa".

Para a aplicação da sanção de multa que trata o inciso II do artigo 52, deverá ser levado em consideração a obrigação violada, sua gravidade e a extensão do dano ou prejuízo sofrido pelo titular dos dados, sanção essa que deverá ser fundamentada pela Autoridade Nacional, conforme disposto no artigo 54.

Um ponto importante deve ser exposto em relação ao Capítulo IX, que abarcava os artigos 55 a 59, o qual tinha por título "Autoridade Nacional de Proteção de Dados (ANPD) e Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade", e que tratava nas Seções I e II, "Da Autoridade Nacional de Proteção de Dados (ANPD)" e "Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade".

Inicialmente, a lei trazia em seu corpo os artigos 55, 56, 57, 58 e 59, porém, antes de sua publicação, sofreram vetos sob o argumento de que "[o]s dispositivos incorrem em inconstitucionalidade do processo legislativo, por afronta ao artigo 61, § 1.º, II, 'e', cumulado com o artigo 37, XIX da Constituição[179]".

O ultimo Capítulo, o X, trata das "Disposições Finais e Transitórias", e nele encontram-se dispostos os artigos 60, 61, 62, 63, 64 e 65.

A Lei, além de disciplinar matérias novas, e em obediência ao artigo 60, também veio alterar os artigos 7.º, inciso X, e artigo 16, inciso II, do Marco Civil da Internet, Lei n.º 12.965 de 23 de abril de 2014. No artigo 61 a lei fez constar obrigações em relação às empresas estrangeiras sobre os atos relativos a esta lei.

179 Cf. BRASIL, Lei nº 13.709, de 14 de agosto de 2018, *"Vetos,"* texto disponível em https://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-veto-156214-pl.html [19.09.2019].

O artigo 62 outorga obrigação à "Autoridade Nacional e o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep), no âmbito de suas competências," para editar "regulamentos específicos para o acesso a dados tratados pela União para o cumprimento do disposto no § 2.º do art. 9º da Lei n.º 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional), e aos referentes ao Sistema Nacional de Avaliação da Educação Superior (Sinaes), de que trata a Lei n.º 10.861, de 14 de abril de 2004".

Não há duvidas que a Lei n.º 13.709/2018 inovou ao tratar sobre o Direito à Proteção de Dados Pessoais na internet. Para o Brasil, a lei funciona como o Regulamento (UE) 2016/679, o Regulamento Geral sobre a Proteção de Dados (RGPD), para os países da União Europeia.

A Lei, além de reconhecer o Direito à Proteção de Dados Pessoais como um direito autônomo, também o nivela como um direito fundamental, quando o valora, assemelha e o equipara com os Direitos fundamentais à Intimidade e à Vida Privada.

A Lei adotou a perspectiva da ideia de que a privacidade deve ser respeitada acima de qualquer outro fato durante as fases do tratamento dos dados, pois, somente assim, trará efetivamente proteção para o titular para com seus dados. Porém, conforme demonstrado, antes mesmo de sua publicação os vetos a deixaram-na incompleta. Assim, certos aspectos ainda precisavam ser debatidos, como por exemplo a criação da Autoridade Nacional de Proteção de Dados, item vetado.

Nesse sentido, a fim de preencher a lacuna na Lei, surgiu a Medida Provisória n.º 869, de 27 de dezembro de 2018, que foi convertida, em 8 de julho de 2019, na Lei n.º 13.853.

3.4.3. Das alterações à lei n.º 13.709/2018 – Da medida provisória n.º 869, de 28 de dezembro de 2018 e da lei n.º 13.853, de 08 de julho de 2019

Após os vetos aos artigos 55, 56, 57, 58 e 59 da Lei n.º 13.709/2018, artigos esses relacionados à criação da Autoridade Nacional de Proteção de Dados (ANPD) e à criação do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, o então Presidente Michel Temer editou Medida Provisória de n.º 869[180], em 27 de dezembro de 2018, para alterar "a Lei n.º 13.709, de 14 de agosto de 2018," e "para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados".

180 Cf. BRASIL, Medida Provisória N.º 869, de 27 de dezembro de 2018, *"Altera a Lei nº 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"*, texto disponível em http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=28/12/2018&jornal=515&pagina=8&totalArquivos=540 [19.09.2019].

A MP n.º 869/2018 alterou o conteúdo normativo da Lei n.º 13.709/2018 com a finalidade de "(i) excepcionar, condicionar ou adequar sua aplicação em situações específicas, como a pesquisa acadêmica, a formulação de políticas públicas ou a prestação de serviços por órgãos estatais ou por seus prepostos; e (ii) instituir a Autoridade Nacional de Proteção de Dados (ANPD), órgão competente para regulamentar, interpretar e fiscalizar o cumprimento da referida lei, bem como, eventualmente, sancionar agentes responsáveis por seu descumprimento[181]".

Antes mesmo de sua aprovação pelo Congresso Nacional, a MP sofreu várias alterações, de acordo com o Projeto de Lei de Conversão de n.º 7[182], de 7 de maio de 2019, que alterou "a Lei n.º 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 (...)".

Pouco mais de dois meses, a MP n.º 869/2019 e o PLC n.º 7/2019 foram convertidos na Lei n.º 13.853[183], em 8 de julho de 2019, que veio alterar a "Lei n.º 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". A Lei n.º 13.853/2019 é composta por 4 (quatro) artigos, e a sua finalidade é a de preencher lacunas encontradas na LGPD, em decorrência dos vetos, quando da sua publicação em 2018.

A Lei n.º 13.853/2019, logo no artigo 1.º, altera a ementa de citação da Lei n.º 13.709/2018, que passou a vigorar com a seguinte ementa: "Lei Geral de Proteção de Dados Pessoais (LGPD)."

No artigo 2.º, a lei modifica a letra da Lei n.º 13.709/2018 em relação aos artigos 1.º, § ún.; 3.º, inciso II; 4.º, § 4.º; 5.º, incisos VIII, XVIII, XIX; 7.º, inciso VIII, § 1.º e 2.º, § 7.º; 11, inciso II, alínea f, § 4.º, incisos I e II, § 5.º; 18, inciso V, § 6.º; 20, § 3.º; 23, incisos III e IV; 26, § 1.º, incisos IV e V; 27, § ún.; 29; 41, § 4.º; 52, incisos X, XI e XII, § 2.º, 3.º, 5.º, 6.º e 7.º; 55-A, § 1º, 2º e § 3º; 55-B; Art. 55-C, incisos I, II, III, IV, V e VI; 55-D; § 1º, 2º, 3º, 4º e 5º; 55-E, § 1.º e 2.º; 55-F; 55-G, § 1.º e 2.º; 55-H; 55-I; 55-J, incisos I, II, III, IV, V, VI, VII, VIII, IX, X, XI, XII, XIII, XIV, XV, XVI, XVII, XVIII, XIX, XX, XXI, XXII, XXIII e XXIV, § 1º, 2º, 3º, 4.º, 5.º e 6.º ; Art. 55-K; Art. 55-L, incisos I, II, III, IV, V, VI e VII; 58-A, incisos

181 Cf. FREITAS, Igor Vilas Boas de, *"Sumário Executivo de Medida Provisória, Resumo das Disposições",* texto disponível em https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/135062 [19.09.2019].

182 Cf. BRASIL, Lei de Conversão de n.º 7, de 07 de maio de 2019, *"Altera a Lei nº 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",* texto disponível em https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2201766 [19.09.2019].

183 Cf. BRASIL, Lei n.º 13.853, em 08 de julho de 2019, "*Altera a Lei nº 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"*, texto disponível em http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1 [19.09.2019].

I, II, III, IV, V, VI, VII, VIII, IX, X e XI; § 1.º, 2.º e 3.º; incisos I, II e III, § 4.º; 58-B, incisos I, II, III, IV e V; 65, incisos I e II".

O artigo 3.º, revoga os § 1.º e 2.º, do artigo 7.º, da Lei n.º 13.709/2018. Pelo zelo à determinação do artigo 4.º, a lei entrou em vigência logo após sua publicação.

Em suma, a Lei criou a Autoridade Nacional de Proteção de Dados (ANPD) e atribuiu a ela a natureza transitória de órgão da Administração Pública Federal, vinculada diretamente à Presidência da República, que pode vir, a critério do Poder executivo, após dois anos, ser transformada em autarquia.

Nesse ponto, o legislador pareceu ser tendencioso no que diz respeito a uma dependência direta de decisões advindas da Presidência da República, totalmente em desconformidade quando comparada com outras agências ou entidades que visam a fiscalização de direitos. A vinculação direta à Presidência da República demonstra claramente a possibilidade de manipulação de decisões e controle de poder sobre a ANPD, o que acaba por tirar a sua independência apresentando-a com uma falsa autonomia.

A organização interna da ANPD, está disposta da seguinte forma: 01 (um) Conselho Diretor (órgão máximo de direção); 01 (um) Um Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; 01 (uma) Corregedoria; 01 (uma) Ouvidoria; 01 (um) Órgão de assessoramento jurídico próprio; 01 (uma) Unidade administrativas e especializadas necessárias à aplicação do disposto na lei.

Em relação à gestão da ANPD, esta será integrada por Diretores escolhidos pelo Presidente da República (sujeito à aprovação pelo Senado Federal), que ocuparão o cargo no Conselho Diretor, com mandatos fixos.

Além das competências já dispostas na Lei n.º 13.709/2018, compete ainda à ANPD, zelar pela proteção dos dados pessoais, elaborar diretrizes relativas à Política Nacional de Proteção de Dados Pessoais e da Privacidade, fiscalizar e aplicar sanções em situações que, comprovadamente, haja violação a lei. Deverá ainda promover o acesso à informação das normas através de políticas públicas sobre a proteção de Dados Pessoais e de medidas de seguranças que deverão ser tomadas.

Por fim, será de responsabilidade também da ANPD editar regulamentos e procedimentos sobre à Proteção de Dados Pessoais, bem como à privacidade dos titulares, realizando auditorias e celebrando compromissos para a eliminação das irregularidades que possam ser encontradas.

Diante de todo exposto, é cristalino que a Lei Geral de Proteção de Dados Pessoais, Lei n.º 13.709/2018 mudou o foco do Direito à Proteção de Dados Pessoais o apresentando como um direito autônomo e não mais como um do direito fundamental dependente dos direitos à intimidade ou à privacidade.

Assim que entrar em vigor, o Brasil passará a contar com uma lei exclusiva sobre o tema, a qual está em consonância com o Regulamento Geral sobre a Proteção de Dados, Regulamento EU 2016/679 de 27 de abril de 2016, que é a Lei internacional de referência sobre o Direito à Proteção de Dados Pessoais.

Contudo, o reconhecimento do Direito à Proteção de Dados Pessoais conferido pela Lei n.º 13.709/2018 (LGPD) não tem o poder para consagra-lo como um direito com garantia fundamental, isso porque uma Lei Federal não tem competência legislativa para alterar a Constituição brasileira, haja vista que este processo somente é feito por meio de Propostas de Emendas à Constituição (PEC).

CAPÍTULO IV
NOVOS DESENVOLVIMENTOS DA PROTEÇÃO DE DADOS PESSOAIS EM MEIO A PÂNDEMIA DO COVID–19

1. O Direito à Proteção de dados Pessoais em tempos de COVID-19

Em 30 de janeiro de 2020, a Organização Mundial de Saúde (OMS) declarou ao mundo a gravidade em relação ao surto da doença causada pelo novo corona vírus (COVID-19)[184], que passou a ser tratada com o mais alto nível de alerta da organização, ou seja, como uma Emergência de Saúde Pública de Importância Internacional. Devido ao alto risco de contágio e mesmo em continentes distantes já se ter notifica de infectados, em 11 de março de 2020, a COVID-19 foi caracterizada OMS como uma pandemia.

Inevitavelmente, a crise desenfreada do COVID-19 veio impactar diretamente a forma como o Estado deve atuar para manter as políticas de saúde pública, sendo uma delas (a que nos importa tratar aqui) a utilização de dados pessoais para exposição de informações relativas ao número de pessoas infectadas, recuperadas, hospitalizadas, óbitos, dados genéticos para anticorpos, sexo do paciente, comorbidades – ou seja, preexistência de outras doenças –, dados esses para se criar um perfil de grupo de risco que podem desenvolver a doença em sua forma mais grave.

Importante salientar que os dados ora mencionados são caracterizados pela legislação atual como dados de caráter sensível e justo por esse motivo merecem mais atenção da lei se comparado com outros tipos de dados. Além da utilização desses dados para fins de estatísticas, estudo para desenvolvimento de vacinas e outros relacionados a saúde de pacientes, o Estado tem demonstrado o interesse em utiliza-los como fim de conter aglomerações, como por exemplo rastreamento de dados[185] de acesso e geolocalização por meio de smartphones.

---

184 *"O que é COVID-19? A COVID-19 é uma doença causada pelo coronavírus SARS-CoV-2, que apresenta um quadro clínico que varia de infecções assintomáticas a quadros respiratórios graves. De acordo com a Organização Mundial de Saúde (OMS), a maioria dos pacientes com COVID-19 (cerca de 80%) podem ser assintomáticos e cerca de 20% dos casos podem requerer atendimento hospitalar por apresentarem dificuldade respiratória e desses casos aproximadamente 5% podem necessitar de suporte para o tratamento de insuficiência respiratória (suporte ventilatório). (...) Coronavírus é uma família de vírus que causam infecções respiratórias. O novo agente do coronavírus foi descoberto em 31/12/19 após casos registrados na China. Provoca a doença chamada de coronavírus (COVID-19)."* Cf. MINISTÉRIO DA SAÚDE, *"Sobre a doença", in Ministério da Saúde,* Brasil, 2020, texto disponível em https://coronavirus.saude.gov.br/sobre-a-doenca#o-que-e-covid [23.06.2020].

185 Cf. BBC News, *"Coronavírus: governo brasileiro vai monitorar celulares para conter pandemia",* Londres, *in BBC Brasil em Londres*, 2020, texto disponível em https://www.bbc.com/portuguese/brasil-52154128 [23.06.2020].

Contudo, é em meio a esse turbulento período de pandemia que o legislador deve se atentar entre o conflito de direitos fundamentais e sobrepesar até quando o Estado poderá ter legitimidade sobre o que outrora é considerado como violação de direitos considerados como indisponíveis para a dignidade da pessoa humana. Sendo essencial neste momento uma análise crítica quanto ao tratamento dos dados pessoais relativos ao COVID-19.

A exemplo disso, o Ministério Público do Distrito Federal e Territórios (MPDFT) fez recomendações à Secretária de Saúde (SES) "que expeça ato normativo para proibir as unidades de saúde de divulgar aos veículos de comunicação os dados pessoais das vítimas fatais da Covid-19. Após a orientação, o governo local informou que não fornecerá dados pessoais como nome, filiação, endereço, profissão ou qualquer outro que permita a identificação de seus titulares à imprensa. (...) É permitida a divulgação de dados objetivos, como causa da morte, gênero, idade e comorbidades prévias[186]".

Nota-se então que a proteção de dados se encontra em destaque no momento atual, apresentando-se como momento oportuno para se discutir a sua relevância como um direito com garantia fundamental frente a sua fragilidade.

É público e notório a utilização de dados pessoais para fins humanitários em situações de emergência como a do COVID-19. Vários países, mesmo aqueles em que já existe um regulamento próprio e vigente que versa sobre a proteção de dados pessoais, têm utilizado os dados pessoais como objeto de monitoramento de pessoas, a exemplo disso temos Israel[187], Singapura[188] e China[189].

Várias autoridades de proteção de dados já se pronunciaram a respeito da utilização de dados pessoais para fins relacionados a saúde. Nesse caso em específico, devido a pandemia do COVID-19, a Global Privacy Assembly[190] ressaltou que as normas de proteção de dados pessoais não obstam a luta contra a COVID-19 e a utilização atípica dos dados pessoais se faz necessário como modo de cooperação

186 Cf. MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS - MPDFT, "*Unidades de saúde devem resguardar identidade de vítimas fatais da Covid-19",* Distrito Federal, *in MPDFT*, 2020, texto disponível em https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2020/noticias-covid/11801-unidades-de-saude-devem-resguardar-identidade-de-vitimas-fatais-da-covid-19 [23.06.2020].

187 Cf. HAARETZ, *"Israeli Coronavirus Surveillance Explained: Who's Tracking You and What Happens With the Data"* , Israel, *in Haaretz.com*, 2020, texto disponível em https://www.haaretz.com/amp/israel-news/.premium-israeli-coronavirus-surveillance-who-s-tracking-you-and-what-happens-with-the-data-1.8685383 [23.06.2020].

188 Cf. NATURE, *"Coronavirus contact-tracing apps: can they slow the spread of COVID-19?",* Singapure, In Nature.com, 2020, texto disponível em: https://www.nature.com/articles/d41586-020-01514-2 [23.06.2020].

189 Cf. THE GUARDIAN, *"'The new normal': China's excessive coronavirus public monitoring could be here to stay", in The Guardian,* 2020, texto disponível em https://www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay [23.06.2020].

190 Cf. GLOBAL PRIVACY ASSEMBLY - GPA, *"Statement by the GPA Executive Committee on the Coronavirus (COVID-19) pandemic"*, Nova Zelândia, in GlobalPrivacyAssembly.org, 2020, texto disponível em https://globalprivacyassembly.org/gpaexco-covid19/ [23.06.2020].

para conter o vírus. Nessa mesma ótica, o Comitê Europeu de Proteção de Dados (EPDB)[191] destacou a necessidade de que a utilização dos dados pessoais, neste momento de contenção do vírus, bem como e a restrição a direitos, contudo, devendo ser limitadas ao período de emergência.

1.1. Os efeitos do COVID-19 sobre a lei geral de proteção de dados pessoais – A medida provisória n.º 959[192] de 2020 e a lei ordinária n.º 14.010[193] de 10 de junho de 2020.

Pouco tempo antes da LGPD entrar em vigor, o Brasil iniciou o enfrentamento do COVID-19 e isso veio atingir diretamente os rumos da proteção de dados pessoais prevista pela Lei Geral da Proteção de Dados, isso porque, por meio de medida provisória e lei ordinária, visando a contenção de gastos a nível nacional durante a pandemia, foi postergado a sua entrada em vigor que antes, aconteceria em 14 de agosto de 2020.

Na verdade, o interesse em postergar a entrada em vigor da Lei n.º 13.709/2018 não é recente e nem teve como pontapé inicial a pandemia instalada mundialmente. É de todo oportuno salientar que vários outros projetos de lei já foram analisados nas duas casas legislativas com esse mesmo objeto, como por exemplo do PL n.º 5.762/2019, de autoria do Deputado Carlos Bezerra (MDB/MT), que propõe a prorrogação para 15 de agosto de 2022; o PL n.º 1.027/2020, do Senador Otto Alencar (PSD/BA) que adia a LGPD para 16 de fevereiro de 2022, assim como, o PL n.º 1.179/2020, de autoria do Senador Antônio Anastasia (PSD/MG), já aprovado no Senado Federal e agora em trâmite na Câmara dos Deputados – pronto para pauta no plenário – que prorroga a entrada em vigor da LGPD para 1º de janeiro de 2021, e as sanções dispostas nos arts. 52 a 54, seriam aplicáveis somente a partir de 1º de agosto de 2021.

Contudo, a entrada em vigor de fato da LGPD, que antes aconteceria em 14 de agosto de 2020, se dará somente em 03 de maio de 2021 por força da Medida Provisória n.º 959 publicada em 29 de abril de 2020, que veio estabelecer "a operacionalização do pagamento do Benefício Emergencial de

---

191 Cf. EUROPEAN DATA PROTECTION BOARD - EDPB, *"Statement on the processing of personal data in the context of the COVID-19 outbreak"*, de 19 de março de 2020, texto disponível em https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf [23.06.2020].

192 Cf. MEDIDA PROVISÓRIA n.º 959/2020, *"Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, e prorroga a vacatio legis da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais – LGPD"*, texto disponível em http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Mpv/mpv959.htm#art4 [23.06.2020].

193 Cf. BRASIL, Lei n.º 14.010/2020 de 10 de junho de 2020, *"Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19)"*, texto disponível em http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Lei/L14010.htm [23.06.2020].

Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, e prorroga a *vacatio legis* da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais – LGPD".

O artigo 4º da MP n.º 959/2020 veio dispor uma nova redação ao artigo 65 da LGPD que assim veio balizar: "Art. 4º - A Lei nº 13.709, de 14 de agosto de 2018, passa a vigorar com as seguintes alterações: "Art. 65. (...) II - em 3 de maio de 2021, quanto aos demais artigos." Dessa forma, a LGPD que antes entraria em vigor em 14 de agosto de 2020, passará a vigorar em relação aos artigos citados em seu artigo 65, inciso II, somente a partir de 3 de maio de 2021.

Um dos principais motivos para a prorrogação da *vacatio legis* da LGPD, apontado pelo Ministro de Estado da Economia em relação a MP n.º 959/2020, se dá "em consequência de uma possível incapacidade de parcela da sociedade em razão dos impactos econômicos e sociais da crise provocada pela pandemia do Coronavírus[194]". Portanto, o adiamento é medida que se impõe levando em consideração os custos a serem incorridos na adequação às diretrizes da LGPD por todos aqueles, pessoas jurídicas, principalmente para as médias e pequenas empresas, ou as pessoas naturais, que venham fazer o tratamento de dados pessoais de terceiros, exceto se para as finalidades descritas no art. 4º da LGPD.

Não só a MP citada veio fazer alterações na LGPD. O PL n.º 1.179/2020, em 10 de junho de 2020, foi aprovado nas duas casas legislativas e foi convertido na Lei Ordinária n.º 14.010, passando a dispor "sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19)".

No que diz respeito a LGPD, o artigo 20 da Lei Ordinária n.º 14.010/2020 veio acrescentar a seguinte redação: "O caput do art. 65 da Lei nº 13.709, de 14 de agosto de 2018, passa a vigorar acrescido do seguinte inciso I-A: Art. 65. (...) I-A – dia 1º de agosto de 2021, quanto aos arts. 52, 53 e 54;", artigos esses que tratam justamente das sansões administrativas aplicáveis como resultado da fiscalização dos direitos elencados na LGPD.

As razões que assistiram a aprovação da MP n.º 959 e da Lei Ordinária 14.010, ambas de 2020, seguem a realidade fatídica dos impactos do COVID-19 em relação ao prejuízo financeiro sentido por todos os brasileiros e empresas instaladas no território nacional, entretanto, a prorrogação da lei também traz grandes prejuízos a todos, principalmente no que diz respeito a segurança jurídica e transparência nas atividades de tratamento de dados pessoais durante a pandemia.

194 Cf. PLANALTO, *"Justificativas da MP n.º 959/2020, EM. nº 00168/2020 ME",* Brasília, *in Planalto.gov,* 2020, texto disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Exm/Exm-MP-959-20.pdf [23.06.2020].

Ademais, distancia o Brasil da possibilidade de reconhecimento como um país adequado às diretrizes da União Europeia, que atualmente é referência mundial em legislar acerca do Direito à Proteção de Dados Pessoais. Desse modo, constata-se que, infelizmente, a legislação em vigor não é capaz de fornecer a segurança esperada pelas empresas e pela sociedade no que tange a proteção dos dados pessoais no seu tratamento.

Outro ponto que merece destaque ainda é a dificuldade política em nomear a Autoridade Nacional de Proteção de Dados, que, de fato, deverá ser imparcial e fundamental para a orientação e fiscalização da proteção de dados pessoais no Brasil.

Levando ainda em consideração a "nova realidade" vivenciada pela quarenta obrigatória de vários Estados e municípios, bem como a implementação de *Lockdown*[195] já recomendada em varias localidades, o trabalho via *homeoffice* tem-se tornado essencial para movimentação, ainda que mínima, da economia nacional, modelo de trabalho esse que se utiliza de plataformas tecnológicas com controle de dados pessoais, que consequentemente aumenta ainda mais o tratamento de dados pessoais sem nenhuma segurança para o titular de dados.

2. Da possível consagração do direito à proteção de dados pessoais como um direito fundamental pela constituição da república federativa do brasil de 1988 – A proposta de emenda à constituição (PEC) n.º 17/2019, de 03 de julho de 2019

Em 12 de março de 2019 foi apresentado ao Plenário do Senado Federal a Proposta de Emenda à Constituição (PEC), de n.º 17/2019[196] que visa acrescentar "o inciso XII-A, ao art. 5.º, 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".

Aprovada em 2 de julho de 2019, em dois turnos, pelo Senado Federal, a Proposta de Emenda à Constituição de n.º 17/2019 (caso seja aprovada pela Câmara dos Deputados) poderá incluir o Direito

195 "*Lockdown é a versão mais rígida do distanciamento social e quando a recomendação se torna obrigatória. É uma imposição do Estado que significa bloqueio total. No cenário pandêmico, essa medida é a mais rigorosa a ser tomada e serve para desacelerar a propagação do novo Coronavírus, quando as medidas de isolamento social e de quarentena não são suficientes e os casos aumentam diariamente."* Cf. DASA, *"Lockdown durante a pandemia do Coronavírus: o que é e quais países adotaram", in Dasa,* 2020, texto disponível em https://dasa.com.br/blog-coronavirus/lockdown-coronavirus-significado [23.06.2020].

196 Cf. BRASIL, Proposta de Emenda à Constituição – PEC de n.º 17/2019, *"Acrescenta o inciso XII-A, ao art. 5.º, 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",* texto disponível em https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1773684&filename=PEC+17/2019 [19.09.2019].

à Proteção de Dados Pessoais – direito reconhecido pela Lei Geral da Proteção de Dados Pessoais, Lei n.º 13.709/2018, no inciso I, do artigo 5.º – no rol de direitos e garantias fundamentais da Constituição da República Federativa do Brasil de 1988.

A PEC n.º 17/2019 fora aprovada em primeiro turno com 65 (sessenta e cinco) votos favoráveis, e em segundo turno com 62 (sessenta e dois) votos favoráveis. Nos dois turnos não houve votos contrários e nem abstenções. No dia 3 de julho de 2019, a PEC n.º 17/2019 fora encaminhada para votação na Câmara dos Deputados, e até então esta sem data para julgamento. A proposta fora apresentada pelo Senador Eduardo Gomes (MDB-TO), sob a alegação de que a proteção aos dados pessoais segue como uma continuação da proteção à intimidade e à privacidade. A consagração do Direito à Proteção de Dados Pessoais como um direito fundamental, formalmente constitucional, terá força para resguardar a inviolabilidade das informações dos brasileiros na internet.

Atualmente, tanto a doutrina quanto a jurisprudência têm pacificado entendimento no sentido de que o direito à proteção de dados pessoais segue além da proteção a vida privada do indivíduo. Algumas leis infraconstitucionais – como por exemplo a lei do Marco civil da Internet – que apresentam suporte para o reconhecimento do Direito à Proteção de Dados Pessoais como um direito fundamental, materialmente constitucional, uma vez que está essencialmente ligado à dignidade da pessoa humana.

Para a Senadora Relatora Simone TEBET (MDB-MS), "[n]ão basta mais termos normas infraconstitucionais, precisamos agora constitucionalizar esse direito[197]". Caso seja aprovado na Câmara dos Deputados, a PEC n.º 17/2019, alterará "a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais", nos termos: "Art. 1.º O inciso XII do art. 5.º da Constituição Federal passa a vigorar com a seguinte redação: Art. 5.º (...) 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, bem como é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais; (...). Art. 2.º O caput do art. 22 da Constituição Federal passa a vigorar acrescido do seguinte inciso XXX: "Art. 22 (...) XXX – proteção e tratamento de dados pessoais".

197 Cf. SENADO FEDERAL, *"Proteção de dados pessoais deverá ser direito fundamental na Constituição", in Senado Federal,* 2019, texto disponível em https://www12.senado.leg.br/noticias/materias/2019/07/02/protecao-de-dados-pessoais-devera-entrar-na-constituicao-como-direito-fundamental [19.09.2019].

Portanto, resta-nos aguardar o julgamento junto da Câmara dos Deputados para que, caso seja aprovada, a Proposta de Ementa à Constituição n.º 17/2019 venha a alterar os artigos 5.º e 22, da CRFB de 1988, para incluir o Direito à Proteção de Dados Pessoais no rol de direitos e garantias fundamentais, um direito que já encontra eficácia no ordenamento jurídico brasileiro como um direito fundamental materialmente constitucional.

3. O reconhecimento pelo Supremo Tribunal Federal (STF) do direito fundamental à proteção de dados pessoais

Em importantíssimo julgamento de cinco Ações Direitas de Inconstitucionalidade[198] (ADIn), que certamente marcará para sempre a história do Direito à Proteção de Dados Pessoais no Brasil, o Supremo Tribunal Federal (STF), nas datas de 06 e 07 de maio de 2020, por decisão da maioria dos votos, referendou a liminar anteriormente deferida pela Relatora das ações, Ministra Rosa Weber e suspendeu a eficácia da Medida Provisória n.º 954[199] de 17 de abril de 2020, que dispõe "sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020."

As Ações Diretas de Inconstitucionalidade foram ajuizadas por partidos políticos e pela própria Ordem dos Advogados do Brasil (OAB), com a finalidade de questionar dispositivos da MP n.º 954/2020, que vinha autorizar o compartilhamento de dados pessoais por empresas de telefonias com o IBGE. O objeto da MP tinha como finalidade justificar a produção oficial de estatísticas durante toda a situação de emergência pública instaurada em decorrência da pandemia do COVID-19.

Contudo, o STF acabou entendendo que a MP n.º 954/2020 poderia trazer mais riscos a direitos fundamentais como à intimidade, à privacidade, e à proteção de dados pessoais, do que benefícios a sociedade e ao Estado. Os riscos suscitados estariam ligados ao tratamento, uma vez que

198 ADIns n.º 6387, 6388, 6389, 6393, 6390.

199 Cf. BRASIL, Medida Provisória n.º 954 de 17 de abril de 2020, *"Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus* ***(covid-19)****, de que trata a Lei nº 13.979, de 6 de fevereiro de 2020.",* texto disponível em http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm [23.06.2020].

a MP não previa mecanismos e procedimentos para proteção das informações pessoais contra vazamentos, acessos não autorizados ou indevidos, tampouco assegura a higidez, o sigilo e o anonimato dos dados.

Para SCHERTEL, três aspectos centrais facilitam a compreensão do peso e a importância da decisão proferida pelo STF no âmbito da proteção de dados pessoais, sendo eles:

> "I - O julgamento representa a superação da ideia de que existiriam dados neutros ou insignificantes, os quais não seriam objeto de tutela, e afirma a proteção constitucional ao dado pessoal;
>
> II - Houve a afirmação da existência de um direito fundamental autônomo à proteção de dados, o que implica em um duplo dever do Estado. Em sua faceta negativa, o Estado teria o dever de não interferir indevidamente nesse direito fundamental e, na positiva, de adotar medidas para assegurar esse direito; e
>
> III - A prorrogação do início da vigência da Lei Geral de Proteção de Dados (LGPD) para maio de 2021, determinada pela Medida Provisória n. 959/2020, e a ausência de criação da Autoridade Nacional de Proteção de Dados (ANPD) pelo governo demonstram que há, no Brasil, um fraco arcabouço institucional protetivo aos dados pessoais. Com o reconhecimento da proteção de dados como um direito fundamental autônomo pelo STF, conclui-se que essa estrutura institucional débil é antagônica a preceitos constitucionais[200]."

A decisão da relatora, bem como do Plenário, não está adstrita à suspensão da MP, alias, não é por esse ponto que merece ser lembrada. Na verdade, o julgamento se tornou um divisor de águas para a história do Direito à Proteção de Dados Pessoais, porque o STF veio afirmar a dimensão da proteção de dados pessoais como um direito fundamental autônomo, matéria essa que foi pela primeira vez debatida de forma tão clara pela suprema corte brasileira.

200 Cf. MENDES, Laura Schertel, *"Decisão histórica do STF reconhece o direito fundamental à proteção de dados pessoais"*, in JOTA, 2020, texto disponível em https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020 [23.06.2020].

CONCLUSÕES

O crescente acesso as tecnologias de informação e de comunicação, quer seja através de um computador, smartphone, tablet ou outro, tem ganhado mais espaço e importância na sociedade, inclusive, tem-se tornado essencial para a realização das mais variadas tarefas do cotidiano. Inevitavelmente, dia após dia, as atividades humanas têm-se ligado cada vez mais à internet, tanto nas relações empresariais com a finalidade de firmar novos contratos, conhecer melhor seus clientes para potencializar seus lucros oferecendo serviços ou produtos específicos, quanto em afazeres domésticos, como no caso dos carros inteligentes, Smart-Tvs, Smart-Phones e até mesmo das Smart-Homes.

O uso de itens que se demonstram como facilitadores para uma vida agitada, sem tempo e estressante, muitas vezes, acaba por camuflar os riscos que o uso da tecnologia oferece. A principal vítima das violações nesse meio é titular/consumidor/usuário da internet, ou seja, qualquer pessoa singular (conhecida também como pessoa física), que, para ter acesso a essas tecnologias, precisam "ensiná-las" como quer que suas atividades sejam realizadas, ou inserir seus informações para encontrar as respostas daquilo que procuram nas redes sociais ou nas páginas de buscas da internet.

VERONESE e CUNHA bem apresentam que "[a] evolução tecnológica, ao tempo em que possibilita a inclusão social por meio das tecnologias de informação e comunicação, também traz novos desafios, tanto para empresas como para os Estados e as sociedades[201]".

Para melhor eficiência do uso da internet e das tecnologias disponíveis atualmente, o titular/consumidor/usuário da internet deve inserir e permitir a coleta de seus dados pessoais – que serão organizados pelo *algoritmo de aprendizagem –,* para que tenha acesso a aquilo que busca ou deseja. É justamente neste meio, entre a coleta e o alcance da finalidade do uso do dado, que consiste o ponto principal da discussão desta dissertação, qual seja, existe no ordenamento jurídico brasileiro um direito que, efetivamente, vem proteger o titular de violações pelo tratamento e uso indevido de seus dados pessoais?

As violações pelo uso ou compartilhamento não consentido dos dados pessoais são reais e acontecem em proporções gigantescas no mundo virtual, e isso acontece, principalmente, pela falta de regulamentação específica de um Direito com garantia fundamental que vise à Proteção de Dados Pessoais.

Através do consentimento do titular, é que ocorre o tratamento de seus dados pessoais, desde a coleta, o repasse ou compartilhamento, quer seja para fins comerciais ou pessoais, até ao alcance da

201 Cf. VERONESE, Alexandre e CUNHA, Marcelo, *"Desafios do comércio...", op. cit.*, p. 86.

sua finalidade. O consentimento do titular não traz o privilégio da segurança em relação à proteção de seus dados.

Nesse sentido, desde as grandes guerras mundiais, as entidades visionarias de paz mundial e diversos países têm regulamentado através de tratados, leis, decretos e outros, direitos com a finalidade de solidificar entendimento quanto à necessidade de proteção de um rol de direitos fundamentais universais que viesse garantir a proteção da vida privada e o que ela venha abranger. Aliás, um dos motivos para a proclamação da Declaração Universal dos Direitos Humanos (DUDH), em 1948, documento esse elaborado pela Organização das Nações Unidas (ONU), que através de uma carta, veio reconhecer o Direitos Fundamentais à vida privada, direito esse que foi legalmente universalizado através do Pacto Internacional de Direitos Civis e Políticos (PIDCP) em 1966. Foi esse o ponto precursor do direito à vida privada.

Desde a década de 50, a União Europeia tem-se demonstrado muito preocupada em regulamentar e proteger direitos fundamentais relacionados a privacidade de seus cidadãos. Como reflexo desse movimento, o direito à vida privada e familiar, desde 1950 é considerado como um direito fundamental pela Convenção Europeia dos Direitos do Homem (CEDH). A partir de então, esse direito tem evoluído chegando ao tema principal desta dissertação, o direito à proteção de dados pessoais.

O reconhecimento de um Direito à Proteção de Dados Pessoais reflete, além da valorização do individuo como ser humano dotado de direitos e deveres, a preocupação do legislador em evitar danos ao titular dos dados que lhe digam respeito, assim como já fez em relação à intimidade, à vida privada, à honra e à imagem do cidadão.

Neste prisma, a Europa é pioneira em legislar sobre à proteção de um direito autônomo à proteção de dados; que, desde a Convenção n.º 108, de 1958, do Conselho da Europa, corroborado ainda pela Diretiva 45/94/CE, de 1994, até o atual Regulamento Geral sobre a Proteção de Dados, Regulamento (EU) 2016/679 de 2016, tem sido efetiva.

Ademais, tem sido referência por consagrar os Dados Pessoais como um direito fundamental (artigo 8, n.º 1) desde a Carta de Direitos Fundamentais da União Europeia[202], ainda no ano 2000, e que foi reafirmado pelo Tratado sobre o Funcionamento da União Europeia (TFUE) de 2009 (artigo 16, n.º 1).

SILVEIRA e MARQUES expõem que "[o] modelo de proteção dos direitos fundamentais da UE baseia-se no seu reconhecimento como princípios gerais do direito da União e no apelo a normas

202 Cf. CONSELHO DA EUROPA, *Carta dos Direitos Fundamentais da União Europeia,* texto disponível em https://www.cnpd.pt/bin/legis/internacional/CARTAFUNDAMENTAL.pdf [26.09.2019].

jusfundamentais de distintas fontes: normas de proveniência europeia (constantes dos Tratados constitutivos, e especialmente a CDFUE), normas de proveniência nacional (constantes das Constituições dos Estados-Membros e correspondentes às suas tradições constitucionais comuns) e normas de proveniência internacional relativas à proteção dos direitos humanos (sobretudo a CEDH que funciona, desde a década de 1970, como quadro de referência para a proteção dos direitos fundamentais na UE)[203]".

No Brasil, a atual carta de Direitos Fundamentais encontra-se disposta no Título II da Constituição da República, promulgada em 05 de outubro de 1988. No rol de direitos fundamentais é possível encontrar a consagração a direitos relacionados à intimidade, à vida privada, à honra, à imagem, porém, não há nada relativo à proteção de dados pessoais.

Os avanços são recentes, quando comparado com as legislações internacionais sobre o tema, pois, conta apenas com a lei que instituiu o Marco Civil na Internet, Lei n.º 12.935/2014 e seus Decretos n.º 8.771, 8.777 de 2016, e a Lei Geral de Proteção de Dados Pessoais, Lei n.º 13.709/2018 e suas alterações, sendo essa última, a única lei específica, que veio apresentar os dados pessoais como um direito autônomo e que destaca a sua devida proteção, mas que entrará em vigor somente em 03 de maio de 2021 e que poderá aplicar as sanções previstas na lei somente a partir de 1º de agosto de 2021.

Nesse sentido, até a entrada em vigor da Lei Geral de Proteção de Dados Pessoais, o Brasil vivencia o período de *Vacatio Legis* em relação ao Direito à Proteção de Dados Pessoais, contando apenas com a Lei do Marco Civil da Internet, em vigor, para assegurar a proteção ao titular dos dados, lei essa que, de fato, não assegura esse direito dentro dos parâmetros mínimos, quando comparada com as leis internacionais que versam sobre o tema.

Importante salientar que no ordenamento jurídico brasileiro, a Lei Federal em comento (LGPD) não terá eficácia *ex tunc*[204], ou seja, não haverá a retroatividade de seus efeitos. Sua eficácia será *ex nunc*, ou seja, terá força vinculativa apenas a partir do momento da sua entrada em vigor.

De outro modo, conforme dito, o Brasil não consagra formalmente o Direito da Proteção de Dados Pessoais como um Direito Fundamental pela Constituição Federal, contudo, há em trâmite junto à Câmara dos Deputados, a Proposta de Emenda à Constituição (PEC) n.º 17/2019, que já fora aprovada

203 Cf. SILVEIRA, Alessandra e MARQUES João, "*Do Direito a estar Só ao Direito ao Esquecimento. Considerações sobre a Proteção de Dados Pessoais Informatizados no Direito da União Europeia: Sentido, Evolução e Reforma Legislativa",* Curitiba, Revista da Faculdade de Direito – UFPR, vol. 61, n.º 3, 2016, p. 94.

204 Os termos ex tunc e ex nunc tratam-se de expressões utilizados no meio jurídico e se originam no latim. São usados para indicar se certa decisão ou lei terá seus efeitos "desde então" (do fato, momento passado) ou "a partir de agora" (após a decisão), respectivamente.

pelo Senado Federal e, se aprovada (pela Câmara dos Deputados), alterará o artigo 5º, para incluir no inciso XI, à proteção de Dados Pessoais como um Direito Fundamental, bem como alterar o artigo 22, para incluir no inciso XXX, o direito à proteção e tratamento dos dados pessoais.

Todavia, tanto o Supremo Tribunal Federal, em julgamento inédito, quanto a doutrina e algumas jurisprudências recentes dos tribunais brasileiros têm firmado entendimento de que há sim a consagração de forma implícita na CRFB de 1988, à Proteção de Dados Pessoais como um Direito subjetivo Fundamental, ainda que materialmente constitucional, ou seja, como um Direito Fundamental Autônomo e não mais relacionado aos Direitos Fundamentais à intimidade e à vida privada.

SILVEIRA e FROUFRE defendem ainda que "a importância e a atenção concedidas à efetividade do direito fundamental à proteção de dados pessoais não se deve justificar, apenas pela pressão dos tempos tecnológicos que vivemos e pela emergência progressiva de um *homo digitalis*[205][206]", mas sim pela importância que os dados representam para o cidadão.

A Proteção de Dados Pessoais como um direito com dimensão fundamental representa a evolução da extensão da dignidade da pessoa humana frente a constante mudança no panorama mundial de estilo de vida (a internetizacão[207] das coisas), bem como a padronização da proteção deste direito como um direito fundamental universal, sendo assim, uma medida que se faz necessária.

Portanto, finalizamos a presente dissertação afirmando que existe o jusfundamentalidade[208] da Proteção de Dados Pessoais no Brasil, resposta essa demonstrada de forma clara pela Suprema Corte brasileira, ou seja, há o reconhecimento materialmente constitucional do Direito à Proteção de Dados Pessoais.

Ademais, por força da Lei n.º 13.709/2018 (LGPD), o direito à proteção de dados pessoais passará a ser reconhecido como um direito autônomo e independente, que também tem como objetivo garantir a dignidade da pessoa humana, a fim de assegurar proteção a cada cidadão brasileiro e estrangeiro (dentro do território nacional) contra os perigos que resultam das estruturas do poder do Estado e das empresas públicas e privadas, tanto território brasileiro quanto internacional (por empresas

---

205 "The expression has already begun to be used regularly, as a synonym for literacy / knowledge and dependence in relation to the New Information Technology that, more and more, we have in our daily lives". Cf. SAXBERG, Natasha Friis, *"Homo Digitalis. How the Human Needs Support Digital Behavior For People, Organizations and Societies",* Danish, Friis & Saxberg, 2015.

206 Cf. SILVEIRA, Alessandra e FROUFRE, Pedro, *"Do mercado interno...", op. cit.*, p. 8.

207 Cf. MALOFF, Joel, *"A Internet e o valor da "internetização",* Brasilia, *in SciElo*, vol. 26, n.º 3, 1997, ISSN 0100-1965, texto disponível em http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-19651997000300004&lng=en&nrm=iso [01.10.2019].

208 Cf. BIELSCHOWSKY, Raoni Macedo, "*Notas sobre a jusfundamentaldade ou apontamentos sobre o problema de todo direito ser considerado fundamental",* Brasília, *in Senado Federal,* Ano 54, n.º 208, 2015, pp. 81-100, texto disponível em https://www12.senado.leg.br/ril/edicoes/52/208/ril_v52_n208_p81.pdf [01.10.2019].

que façam a coleta dos dados no Brasil, mas que o tratamento aconteça no exterior), diante do assustador aumento do tratamento e uso de Dados Pessoais, bem como a conexão (com e sem consentimento) desregrada desses com empresas internacionais.

BIBLIOGRAFIA

AGÊNCIA ESTADO, "*Barreto defende criação de 'Constituição' da Internet'", in G1*, 2010, texto disponível em http://g1.globo.com/brasil/noticia/2010/05/barreto-defende-criacao-de-constituicao-da-internet.html [17.09.2019].

AGUIAR, Ruy Rosado de, *IV Jornada de Direito Civil. Enunciado 274,* Conselho da Justiça Federal, 2002, texto disponível em https://www.cjf.jus.br/enunciados/enunciado/219 [09.09.2019].

ALEXA, *"Alexa Traffic Rank for Google", in Alexa Internet,* 2009, texto disponível em https://www.alexa.com/siteinfo/google.com [27.08.2019].

ANATEL, *"Limites mínimos de velocidade da banda larga ficam mais rigorosos",* in ANATEL.GOV, 2014, texto disponível em https://www.anatel.gov.br/Portal/exibirPortalPaginaEspecialPesquisa.do?acao=&tipoConteudoHtml=1&codNoticia=35544 [16.09.2019].

AQUINO, Yara, "*Após denúncias de espionagem, governo pedirá agilidade na votação do Marco Civil da Internet", in Agência Brasil,* 2013, texto disponível em http://memoria.ebc.com.br/agenciabrasil/noticia/2013-07-08/apos-denuncias-de-espionagem-governo-pedira-agilidade-na-votacao-do-marco-civil-da-internet [17.09.2019].

ASADI, Arash, et al., "*A Survey on Device-to-Device Communication in Cellular Networks", in IEEE Communications Surveys & Tutorials*, v. 16, Issue 4, 2014, texto disponível em https://ieeexplore.ieee.org/document/6805125/references#references [27.08.2019].

BALL, James e RUSHE, Dominc, "*NSA Prism program taps in to user data of Apple, Google and others*", in The Guardian, 2013, texto disponível em https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [02.09.2019].

BAZÁN, Victor, *El habeas data e o direito à autodeterminação infor*mativa em perspectiva de direito comparado, Chile, Estudios Constitucionales (Centro de Estudios Constitucionales – Universidad de Talca), Ano 3, n.° 02, 2005.

BBC NEWS, "*Facebook scandal 'hit 87 million users*", *in BBC News,* 2018, texto disponível em https://www.bbc.com/news/technology-43649018 [04.09.2019].

–, "*Google ranked 'worst' on privacy", in BBC News*, 2007, texto disponível em http://news.bbc.co.uk/2/hi/technology/6740075.stm [27.08.2019].

–, *"Coronavírus: governo brasileiro vai monitorar celulares para conter pandemia",* Londres, *in BBC Brasil em Londres*, 2020, texto disponível em https://www.bbc.com/portuguese/brasil-52154128 [23.06.2020].

–, "*Google ranked 'worst' on privacy",* In BBC News, 2007, Disponível em http://news.bbc.co.uk/2/hi/technology/6740075.stm [27.08.2019].

BBC NEWS BRASIL, "*O escândalo que fez o Facebook perder US$ 35 bilhões em horas", in BBC News Brasil*, 2018, texto disponível em https://www.bbc.com/portuguese/internacional-43466255 [04.09.2019].

BERGEN, Mark, "*Alphabet Finishes Reorganization With New XXVI Company", in Bloomberg,* 2017, texto disponível em https://www.bloomberg.com/news/articles/2017-09-01/alphabet-wraps-up-reorganization-with-a-new-company-called-xxvi [28.08.2019].

BIELSCHOWSKY, Raoni Macedo, "*Notas sobre a jusfundamentaldade ou apontamentos sobre o problema de todo direito ser considerado fundamental",* Brasília, *in Senado Federal,* Ano 54, n.º 208, 2015, texto disponível em https://www12.senado.leg.br/ril/edicoes/52/208/ril_v52_n208_p81.pdf [01.10.2019].

CADWALLADR, Carole e GRAHAM-HARRISON, Emma, "*Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach", in The Guardian*, 2018, texto disponível em https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election [04.09.2019].

CARLSON, Nicholas, "*At last - the full story of how Facebook was founded*", In Business Insider, 2010, texto disponível em https://www.businessinsider.com/how-facebook-was-founded-2010-3 [04.09.2019].

CLEMENT, James, "*Most famous social network sites worldwide as of July 2019, ranked by number of active users (in millions)", in Statista*, 2019, texto disponível em https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ [04.09.2019].

COMISSÃO EUROPEIA, *"Comunicação da Comissão Europeia sobre a revisão intercalar relativa à aplicação da Estratégia para o Mercado Único Digital - Um Mercado Único Digital conectado para todos [COM(2017) 228 final]* de 10 de maio de 2017", Bruxelas, 2017, texto disponível em http://eur-lex.europa.eu/legal-content/PT/TXT/ HTML/?uri=CELEX:52017DC0228&from=PT [29.11.2019].

CONCEITO, "*Conceito de rede de dados*", *in Conceito.de,* 2014, texto disponível em https://conceito.de/rede-de-dados [14.01.2019].

COSTA JÚNIOR, Paulo José da, *O direito de estar só: tutela penal da intimidade,* São Paulo, Revista dos Tribunais, 1995.

DASA, *"Lockdown durante a pandemia do Coronavírus: o que é e quais países adotaram", in Dasa,* 2020, texto disponível em https://dasa.com.br/blog-coronavirus/lockdown-coronavirus-significado [23.06.2020].

DAVIES, Harry et al., "*Ted Cruz campaign using firm that harvested data on millions of unwitting Facebook users*", New York, *in The Guardian*, 2015, texto disponível em https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data [04.09.2019].

DE PAULA, Felipe, e NAEGELE, Vitor Rabelo, "*Há vício de iniciativa na criação da Autoridade Nacional de Proteção de Dados?*", in JOTA, 2018, texto disponível em

https://www.jota.info/paywall?redirect_to=//www.jota.info/tributos-e-empresas/regulacao/ha-vicio-de-iniciativa-na-criacao-da-autoridade-nacional-de-protecao-de-dados-26072018 [19.09.2019].

DINIZ, Maria Helena, *Curso de Direito Civil Brasileiro*, São Paulo, Saraiva, 2007, vol. I, ed. 24.

DOMINGOS, Pedro, *O Algoritmo Mestre: Como a busca pelo algoritmo de machine learning definitivo recriará nosso mundo*, São Paulo, Novatec, 2017.

DOTTI, René Ariel, *Proteção da Vida Privada e Liberdade de Informação*, São Paulo, Revista dos Tribunais, 1980.

FERRAZ, Sérgio Valadão, *Curso de direito constitucional: teoria, jurisprudência e questões,* Rio de Janeiro, Elsevier, ed. 4º, 2008.

FERREIRA, Rubem E, "*Linux: Guia do Administrador do Sistema*", São Paulo, Novatec, 2ª ed., 2013.

FREITAS, Igor Vilas Boas de, *"Sumário Executivo de Medida Provisória, Resumo das Disposições",* texto disponível em https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/135062 [19.09.2019].

GEDDES, David, "*How does Google make money?*", *in Revenue Infographic,* 2011, texto disponível em https://www.webanalyticsworld.net/2012/01/how-does-google-make-money-2011-revenue-infographic.html [27.08.2019].

GLANCY, Dorothy J., "*The Invention of the Right to Privacy*", Arizona Law Review, 1979, v. 21, nº. 21, pp. 1–39, texto disponível em https://web.archive.org/web/20100722230541/http://law.scu.edu/site/dorothy-glancy/File/Privacy.pdf [25.09.2019]

GLOBAL PRIVACY ASSEMBLY - GPA, *"Statement by the GPA Executive Committee on the Coronavirus (COVID-19) pandemic"*, Nova Zelândia, in GlobalPrivacyAssembly.org, 2020, texto disponível em https://globalprivacyassembly.org/gpaexco-covid19/ [23.06.2020].

GOMES, Luiz Flávio, *Direito penal: introdução e princípios fundamentais*, São Paulo, Editora Revista dos Tribunais, vol. 01., ed. 2ª, 2009.

GOMES, Helton Simões, *"Até R$ 9,7 milhões! Brasil quer multar Google por 'ler' emails no Gmail", São Paulo, in UOL,* 2019, texto disponível em https://www.uol.com.br/tilt/noticias/redacao/2019/02/07/ate-r-97-milhoes-brasil-quer-multar-google-por-ler-seus-emails-no-gmail.html [02.09.2019].

GONÇALVES, Carlos Roberto, *Direito civil brasileiro, Parte Geral,* São Paulo, Saraiva, 5º ed., vol. 01, 2007.

GOOGLE, *"Glass Enterprise Edition 2", in Google*, texto disponível em https://www.google.com/glass/tech-specs/ [27.08.2019].

–, "*Google Corporate Information", in Google Inc.,* 2010, texto disponível em https://about.google/ [27.08.2019].

G1*, "Entenda o caso de Edward Snowden, que revelou espionagem dos EUA*", São Paulo, *in G1*, 2014, texto disponível em http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html [02.09.2019].

–, "*Facebook atinge os 2 bilhões de usuários*", in G1, 2017, texto disponível em https://g1.globo.com/tecnologia/noticia/facebook-atinge-os-2-bilhoes-de-usuarios.ghtml [04.09.2019].

HAARETZ, *"Israeli Coronavirus Surveillance Explained: Who's Tracking You and What Happens With the Data"* , Israel, *in Haaretz.com*, 2020, texto disponível em https://www.haaretz.com/amp/israel-news/.premium-israeli-coronavirus-surveillance-who-s-tracking-you-and-what-happens-with-the-data-1.8685383 [23.06.2020].

HIGUERAS, Manuel Heredero, *La Directiva Comunitaria de Protección de los datos de carater personal,* Madrid, Aranzadi Editorial, 1997.

IBGE, *O que é o IBGE?,* in IBGE.GOV, S/d, texto disponível em https://www.ibge.gov.br/institucional/o-ibge.html [26.08.2019].

JINKINGS, Daniella, "*Governo apresenta proposta do Marco Civil da Internet ao Congresso Nacional", in Agência Brasil,* 2011, texto disponível em http://memoria.ebc.com.br/agenciabrasil/noticia/2011-08-24/governo-apresenta-proposta-do-marco-civil-da-internet-ao-congresso-nacional [17.09.2019].

–, Daniella, "*Governo vai debater criação de marco legal para proteção de dados pessoais no Brasil",* Brasília, In Rede Brasil Atual, 2010, Disponível em https://www.redebrasilatual.com.br/cidadania/2010/12/governo-vai-debater-criacao-de-marco-legal-para-protecao-de-dados-pessoais-no-brasil/ [18.09.2019].

JÚNIOR, Nelson Nery, et al., *Código de Processo Civil Comentado.*, São Paulo, Revista dos Tribunais, 4ª ed., 1999, nota 13.

KORTH, Henry F. e SILBERSCHATZ, Abraham, *Sistemas de Bancos de Dados*, Makron Books, 2ª ed. revisada, 1994.

KUH, Eric, "*Google unveils top political searches of 2009", in CNN,* 2009, texto disponível em http://politicalticker.blogs.cnn.com/2009/12/18/google-unveils-top-political-searches-of-2009/ [27.08.2019]

LACOMBE, Francisco José Masset et al., *Administração Princípios e Tendências*, São Paulo, Saraiva, 2003.

LEMOS, Ronaldo, *"Internet brasileira precisa de marco regulatório civil",* Rio de Janeiro, *in UOL*, 2007, texto disponível em https://tecnologia.uol.com.br/ultnot/2007/05/22/ult4213u98.jhtm [17.09.2019].

LÉVY, Pierre, *Cibercultura,* Tradução de Carlos Irineu da Costa, São Paulo, Editora 34, 2008.

LUIGGI, Mirella, *"Vale a pena investir em uma geladeira inteligente?",* São Paulo, *in UOL*, 2017, texto disponível em https://www.uol.com.br/tilt/noticias/redacao/2018/06/23/vale-a-pena-investir-em-uma-geladeira-inteligente-conheca-os-recursos.html [26.08.2019].

MAIA, Fernando Joaquim Ferreira, *O habeas data e a tutela da dignidade da pessoa humana na vida privada,* Vitória, Revista de Direitos e Garantias Fundamentais, n.º 12.

MALOFF, Joel, *"A Internet e o valor da "internetização",* Brasilia, *in SciElo*, vol. 26, n.º 3, 1997, ISSN 0100-1965, texto disponível em http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-19651997000300004&lng=en&nrm=iso [01.10.2019].

MANCINI, Mônica, *"Internet das Coisas: História, Conceitos, Aplicações e Desafios"*, São Paulo, *in Research Gate*, 2017, texto disponível em https://www.researchgate.net/publication/326065859_Internet_das_Coisas_Historia_Conceitos_Aplicacoes_e_Desafios [23.08.2019].

MARINONI, Luis Guilherme, et al., *Curso de Direito Constitucional,* São Paulo, Revista dos Tribunais, 2014.

MASILI, Clarissa Menezes Vaz, *Regulação do uso de dados pessoais no Brasil: papel do usuário na defesa de um direito à tutela de dados pessoais autônomo,* Tese Doutorado, Orientadora Christiana Soares de Freitas, Universidade de Brasília, 2018.

MAZUI, Guilherme, e CASTILHOS, Roniara, "*Temer sanciona com vetos lei de proteção de dados pessoais",* Brasília, *in G1*, 2018, texto disponível em https://g1.globo.com/politica/noticia/2018/08/14/temer-sanciona-lei-de-protecao-de-dados-pessoais.ghtml [19.09.2019].

MENDES, Laura Schertel, *"Decisão histórica do STF reconhece o direito fundamental à proteção de dados pessoais",* in JOTA, 2020, texto disponível em https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020 [23.06.2020].

MINISTÉRIO DA SAÚDE, *"Sobre a doença", in Ministério da Saúde,* Brasil, 2020, texto disponível em https://coronavirus.saude.gov.br/sobre-a-doenca#o-que-e-covid [23.06.2020].

MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS - MPDFT, "*Unidades de saúde devem resguardar identidade de vítimas fatais da Covid-19",* Distrito Federal, *in MPDFT*, 2020, texto disponível em https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2020/noticias-covid/11801-unidades-de-saude-devem-resguardar-identidade-de-vitimas-fatais-da-covid-19 [23.06.2020].

MORAES, Alexandre de, "*Direito constitucional",* São Paulo, Atlas, 24. ed., 2009.

MOURÃO NETO, Samuel Francisco, *Arquivos de consumo (cadastros e bancos de dados de consumidores) e habeas data (individual e coletivo*), In Repositório PUC, S/d, texto disponivel em http://www.pucsp.br/tutelacoletiva/download/artigo_samuel.pdf [09.09.2019].

NAÇÕES UNIDAS DO BRASIL, *"Declaração Universal dos Direitos Humanos está disponível em mais de 500 idiomas",* in Nações Unidas Brasil, 2016, texto disponível em https://nacoesunidas.org/declaracao-universal-dos-direitos-humanos-esta-disponivel-em-mais-de-500-idiomas/ [25.09.2019]

NATURE, *"Coronavirus contact-tracing apps: can they slow the spread of COVID-19?",* Singapure, In Nature.com, 2020, texto disponível em: https://www.nature.com/articles/d41586-020-01514-2 [23.06.2020].

PANDIA, "*Google: one million servers and counting*", *in Pandia,* 2007, texto disponível em http://www.pandia.com/articles/gartner [27.08.2019].

PIERINI, Alicia, et al., *Hábeas data: derecho a la intimidad: derecho a informar, limites, censura*, Buenos Aires, Buenos Aires Universidad, 1999.

PLANALTO, *"Justificativas da MP n.º 959/2020, EM. nº 00168/2020 ME",* Brasília, *in Planalto.gov,* 2020, texto disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Exm/Exm-MP-959-20.pdf [23.06.2020].

POETA, Patrícia, "*Atriz Carolina Dieckmann fala sobre fotos pessoais expostas na internet*", Rio de Janeiro, *in G1*, 2012, texto disponível em http://g1.globo.com/jornal-da-globo/noticia/2012/05/atriz-carolina-dieckmann-fala-sobre-fotos-pessoais-expostas-na-internet.html [09.09.2019].

PROCON, *"O que é o PROCON", in Procon online,* S/d, texto disponível em https://www.procononline.com.br/o-que-e-o-procon/ [19.09.2019].

RODOTÀ, Stefano, *A vida na sociedade de vigilância: privacidade hoje*, Rio de Janeiro, Renovar, 2008.

ROSENBERG, Matthew, "*Trump Consultants Exploited the Facebook Data of Millions", in The New York Times*, 2018, texto disponível em: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html [04.09.2019].

R7, "*Brasil é o 3º país com o maior número de usuários do Facebook*", *in R7*, 2019, texto disponível em https://noticias.r7.com/tecnologia-e-ciencia/brasil-e-o-3-pais-com-o-maior-numero-de-usuarios-do-facebook-02032019 [04.09.2019].

SARDETO, Patrícia Eliane da Rosa, "A proteção de dados pessoais em debate no Brasil", 2011, *in Âmbito Jurídico*, Florianópolis, texto disponível em http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=9455 [13.02.2019].

SAXBERG, Natasha Friis, *"Homo Digitalis. How the Human Needs Support Digital Behavior For People, Organizations and Societies",* Danish, Friis & Saxberg, 2015.

SENADO FEDERAL, *"Proteção de dados pessoais deverá ser direito fundamental na Constituição", in Senado Federal,* 2019, texto disponível em https://www12.senado.leg.br/noticias/materias/2019/07/02/protecao-de-dados-pessoais-devera-entrar-na-constituicao-como-direito-fundamental [19.09.2019].

–, "*Cláusula pétrea",* Agência Senado, texto disponível em https://www12.senado.leg.br/noticias/glossario-legislativo/clausula-petrea [10.02.2019].

SERPRO, *"O que são dados sensíveis, de acordo com a LGPD"*, *in serpro.gov*, S/d, texto disponível em https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-sensiveis-lgpd [25.09.2019].

SILVA, Camila, *"O mercado de dados no Brasil", in E-commerce Brasil*, 2014, texto disponível em https://www.ecommercebrasil.com.br/artigos/o-mercado-de-dados-brasil/ [07.11.2019].

SILVA, Daniel Neves, *Ditadura Militar*, Brasil Escola, S/d, texto disponível em https://brasilescola.uol.com.br/historiab/ditadura-militar.html [07.08.2019].

SILVA, José Afonso da, *Curso de Direito Constitucional Positivo,* São Paulo, Editora Malheiros, ed. 38, 2014.

SILVEIRA, Alessandra e MARQUES João, *"Do Direito a estar Só ao Direito ao Esquecimento. Considerações sobre a Proteção de Dados Pessoais Informatizados no Direito da União Europeia: Sentido, Evolução e Reforma Legislativa",* Curitiba, Revista da Faculdade de Direito – UFPR, vol. 61, n.º 3, 2016.

SILVEIRA, Alessandra e FROUFRE, Pedro, *"Do mercado interno à cidadania de direitos: a proteção de dados pessoais como a questão Jusfundamental identitaria dos nossos tempos"*, Braga, UNIO - EU Law Journal, Vol. 4, N.º 2, 2018.

SOLON, Olivia, "*Facebook says Cambridge Analytica may have gained 37m more users' data*", *in The Guardian*, 2018, texto disponível em https://www.theguardian.com/technology/2018/apr/04/facebook-cambridge-analytica-user-data-latest-more-than-thought [04.09.2019].

SOUZA, Murilo, "*Projeto abrange operações de tratamento de dados realizados tanto no Brasil como no exterior, mas cuja coleta tenha ocorrido em território nacional", in Câmara dos Deputados,* 2016, texto disponível em https://www.camara.leg.br/noticias/493890-projeto-regulamenta-acesso-a-dados-pessoais-no-brasil/ [17.09.2019].

SRISHTI Deoras, "*Primeiro dispositivo IoT - "The Internet Toaster"*, in ldapwiki.com, 2018, texto disponível https://ldapwiki.com/wiki/Internet%20Toaster [23.08.2019].

TEIXEIRA, Tarcísio. *"Aspectos atuais do e-commerce",* São Paulo, *in Jornal Carta Forense*, 2014, texto disponível em http://www.cartaforense.com.br/conteudo/entrevistas/aspectos-atuais-do-e-commerce/14650 [10.02.2019].

THE GUARDIAN, *"'The new normal': China's excessive coronavirus public monitoring could be here to stay", in The Guardian,* 2020, texto disponível em https://www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay [23.06.2020].

THE ECONOMIST, *"Regulating the internet giants. The world's most valuable resource is no longer oil, but data", in The Economist,* ed. 06 de maio de 2017*,* texto disponível em

https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data [12.11.2019].

UDHR50, National Coordinating Committee for, "*Didn't Nazi tyranny end all hope for protecting human rights in the modern world? ",* Franklin and Eleanor Roosevelt Institute, 1998, texto disponível em https://archive.is/20120919000037/http://www.udhr.org/history/overview.htm#selection-553.0-553.43 [25.09.2019]

VEALE, Kate, "*Como Esconder Seu IP – 4 Formas Rápidas e Fáceis",* in vpnMentor, S/d, texto disponível em https://pt.vpnmentor.com/blog/4-formas-faceis-de-ocultar-seu-endereco-ip/ [25.09.2019].

VENOSA, Silvio de Salvo, *Código Civil Interpretado*, São Paulo, Atlas, 2010.

VERONESE, Alexandre e CUNHA, Marcelo, *"Desafios do comércio eletrónico no Brasil: integração vertical entre fornecedores e meios de pagamentos, proteção de dados pessoais e cooperação regulatória internacional",* Braga, UNIO - EU Law Journal, vol. 4, nº. 2, 2018.

VIEIRA, João Estróia, *"The Great Hack: uma visão sobre o escândalo da Cambridge Analytica", In Comunidade Cultura e Arte*, 2019, texto disponível em https://www.comunidadeculturaearte.com/the-great-hack-uma-visao-sobre-o-escandalo-da-cambridge-analytica/ [04.09.2019].

VOLTILINI, Ramon, "*Brasil é o segundo país com mais contas registradas no Facebook", in Tecmundo,* 2013, texto disponível em https://www.tecmundo.com.br/facebook/38693-brasil-e-o-segundo-pais-com-mais-contas-registradas-no-facebook.html [04.09.2019].

WOMACK, Brian, "*Google Creates New Company Called Alphabet, Restructures Stock*", *in Bloomberg*, 2015, texto disponível em https://www.bloomberg.com/news/articles/2015-08-10/google-to-adopt-new-holding-structure-under-name-alphabet- [27.08.2019].

WORLD HEALTH ORGANIZATION, "*Coronavirus Disease (COVID-19) Dashboard*", in OMS, S/d, texto disponível em https://covid19.who.int/ [22.06.2020].

BIBLIOGRAFIA NORMATIVA E JURISPRUDÊNCIAL

BRASIL, "*Anteprojeto Constitucional, elaborado pela Comissão Provisória de Estudos Constitucionais, instituída pelo Decreto n.º 91.450, de 18 de julho de 1985"*, texto disponível em https://www.senado.leg.br/publicacoes/anais/constituinte/AfonsoArinos.pdf [09.09.2019].

–, Câmara dos Deputados, Projeto de Lei da Câmara n.º 21/2014, de 26 de março de 2014, *"Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil",* texto disponível https://legis.senado.leg.br/sdleg-getter/documento?dm=3846743&ts=1567526304766&disposition=inline [17.09.2019].

–, Câmara dos Deputados, Projeto de Lei n.º 5.276/2016, de 29 de abril de 2016, *"dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural",* texto disponível em https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=E0C5C0C9CEB5C726CC764F3E7AAB0B62.proposicoesWebExterno1?codteor=1457459&filename=PL+5276/2016 [26.08.2019].

–, Congresso Nacional, Projeto de Lei n.º 4.060, de 13 de junho de 2012, *"Dispõe sobre o tratamento de dados pessoais, e dá outras providências*", texto disponível em https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066 [09.09.2019].

–, Constituição da República Federativa do Brasil, de 05 de outubro de 1988, texto disponível em http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm [13.02.2019].

–, Decreto n.º 4.829, de 3 de setembro de 2003, *"Dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGIbr, sobre o modelo de governança da Internet no Brasil, e dá outras providências",* texto disponível em http://www.planalto.gov.br/ccivil_03/decreto/2003/d4829.html [17.09.2019].

–, Decreto n.º 7.724, de 16 de maio de 2012, *"Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição",* texto disponível em http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2012/Decreto/D7724.html [17.09.2019].

–, Decreto n.º 8.771, de 11 de maio de 2016, *"Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações",* texto disponível em http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2016/Decreto/D8771.html [17.09.2019].

–, Decreto n.º 8.777, de 11 de maio de 2016, *"Institui a Política de Dados Abertos do Poder Executivo federal",* texto disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8777.html [19.09.2019].

–, Decreto n.º 9.903, de 8 de julho de 2019, *"Altera o Decreto n.º 8.777, de 11 de maio de 2016, que institui a Política de Dados Abertos do Poder Executivo federal, para dispor sobre a gestão e os direitos*

de uso de dados abertos", texto disponível em http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9903.htm#art1 [17.9.2019].

–, Decreto Legislativo n.º 226, 12 de dezembro de 1991, *"Aprova os textos do Pacto Internacional sobre Direitos Civis e Políticos e do Pacto Internacional sobre Direitos Econômicos, Sociais e Culturais, ambos aprovados, junto com o Protocolo Facultativo relativo a esse último pacto, na XXI Sessão (1966) da Assembléia-Geral das Nações Unidas",* texto disponível em https://www2.camara.leg.br/legin/fed/decleg/1991/decretolegislativo-226-12-dezembro-1991-358251-exposicaodemotivos-146136-pl.html [25.09.2019].

–, Diário Oficial da União – DOU, n.º 176, de 11 de setembro de 2013, texto disponível em http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=11/09/2013&jornal=1&pagina=3 [17.09.2019].

–, Diário Oficial da União – DOU, Seção 1, Edição Extra, 15 de agosto de 2018, texto disponível http://www.in.gov.br/leiturajornal?data=15-08-2018&secao=DO1E [19.09.2019].

–, Lei n.º 7.347, de 24 de julho 1985, *"Disciplina a ação civil pública de responsabilidade por danos causados ao meio-ambiente, ao consumidor, a bens e direitos de valor artístico, estético, histórico, turístico e paisagístico (VETADO) e dá outras providências",* texto disponível em http://www.planalto.gov.br/ccivil_03/leis/L7347orig.html [14.09.2019].

–, Lei n.º 8.069, de 13 de julho de 1990, *"Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências"*, texto disponível em http://www.planalto.gov.br/ccivil_03/leis/l8069.html [18.09.2019].

–, Lei n.º 8.078, de 11 de setembro de 1990, *"Dispõe sobre a proteção do consumidor e dá outras providências",* texto disponível em http://www.planalto.gov.br/ccivil_03/leis/l8078.html [09.09.2019].

–, Lei n.º 9.296, de 24 de julho de 1996, *"Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal",* Texto disponível em http://www.planalto.gov.br/ccivil_03/leis/l9296.html [16.09.2019].

–, Lei n.º 9.472, de 16 de julho 1997, *"Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº. 8, de 1995"*, texto disponível em http://www.planalto.gov.br/ccivil_03/LEIS/L9472.html [17.09.2019].

–, Lei n.º 10.406, de 10 de janeiro de 2002, *"Institui o Código Civil",* Disponível em http://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406.htm [25.09.2019]

–, Lei n.º 12.373, de 30 de novembro de 2012, *"Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências*", texto disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.html [09.09.2019].

–, Lei n.º 12.527, de 18 de novembro de 2011, *"Regula o acesso a informações previsto no inciso XXXIII do art. 5.º, no inciso II do § 3.º do art. 37 e no § 2.º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei n.º 11.111, de 5 de maio de 2005, e dispositivos da*

Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências", texto disponível em http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.html [09.09.2019].

–, Lei n.º 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; altera a Lei nº 8.137, de 27 de dezembro de 1990, o Decreto-Lei nº 3.689, de 3 de outubro de 1941 - Código de Processo Penal, e a Lei nº 7.347, de 24 de julho de 1985; revoga dispositivos da Lei nº 8.884, de 11 de junho de 1994, e a Lei nº 9.781, de 19 de janeiro de 1999; e dá outras providências",* texto disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/Lei/L12529.html [17.09.2019].

–, Lei n.º 12.965, de 23 de abril de 2014, *"Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil",* 2014, Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.html [14.01.2019].

–, Lei n.º 13.709, de 14 de agosto de 2018, *"Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Redação original, antes da alteração da Lei nº 13.853/2019",* texto disponível em https://legis.senado.leg.br/norma/27457334/publicacao/27457731 [18.09.2019].

–, Lei n.º 13.709, de 14 de agosto de 2018, *"Vetos,"* texto disponível em https://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-veto-156214-pl.html [19.09.2019].

–, Lei n.º 13.853, em 08 de julho de 2019, "*Altera a Lei nº 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"*, texto disponível em http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1 [19.09.2019].

–, Lei n.º 14.010, de 10 de junho de 2020, *"Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19)",* texto disponível em http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Lei/L14010.htm [23.06.2020].

–, Lei de Conversão de n.º 7, de 07 de maio de 2019, *"Altera a Lei nº 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",* texto disponível em https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2201766 [19.09.2019].

–, Medida Provisória n.º 869, de 27 de dezembro de 2018, *"Altera a Lei nº 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*", texto disponível em http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=28/12/2018&jornal=515&pagina=8&totalArquivos=540 [19.09.2019].

–, Medida Provisória n.º 954, de 17 de abril de 2020, *"Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional*

*decorrente do coronavírus (**covid-19**), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020.",* texto disponível em http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm [23.06.2020].

–, Medida Provisória n.º 959/2020, de 29 de abril de 2020, *"Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, e prorroga a vacatio legis da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais – LGPD",* texto disponível em http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Mpv/mpv959.htm#art4 [23.06.2020].

–, Ministério Público Federal, Inquérito Civil Público n.º 1.27.000.001406/2015-03, texto disponível em http://www.mpf.mp.br/pi/sala-de-imprensa/docs/acp-google [02.09.2019].

–, Projeto de Lei n.º 2.126, de 24 de agosto de 2011, *"Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil",* texto disponível em https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=912989&filename=PL+2126/2011 [17.09.2019].

–, Projeto de Lei n.º 5.403/2001, *"Dispõe sobre o acesso a informações da Internet, e dá outras providências",* texto disponível em https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=34462&ord=1 [17.09.2019].

–, Projeto de Lei do Senado Federal n.º 330/2013, *"Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências",* texto disponível em https://legis.senado.leg.br/sdleg-getter/documento?dm=2931559&ts=1567533189697&disposition=inline [14.09.2019].

–, Proposta de Emenda à Constituição – PEC de n.º 17/2019, *"Acrescenta o inciso XII-A, ao art. 5.º, 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",* texto disponível em https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1773684&filename=PEC+17/2019 [19.09.2019].

–, Tribunal Regional Federal da 1ª Região – TRF1, Ação Civil Pública n.º 3724320124013304, Relator: Juíza Federal Hind Ghassan Kayath (CONV.), Data de Julgamento: 21/07/2014, SEXTA TURMA, Data de Publicação: 06/08/2014, texto disponível em https://trf-1.jusbrasil.com.br/jurisprudencia/162022523/apelacao-civel-ac-3724320124013304?ref=serp [09/09/2019].

–, Tribunal Regional Federal da 1ª Região – TRF1, Ação Civil Pública, Processo n.º 0025463-45.2016.4.01.4000, 2º Vara de Teresina, Juiz Márcio Braga Magalhães, autuado em 04.11.2016, Autor: Ministério Público Federal, Réu: Google Brasil Internet Ltda., texto disponível em https://processual.trf1.jus.br/consultaProcessual/processo.php?proc=25463452016401400 0&secao=PI&nome=GOOGLE%20BRASIL%20INTERNET%20LTDA&mostrarBaixados=N [02.09.2019].

CHILE, Ley n.º 20.285, de 05 de julio de 2016, texto disponível em https://www.leychile.cl/Navegar?idNorma=276363 [13.09.2019].

CONSELHO DA EUROPA, Convenção 108, de 28 de janeiro de 1981, "*para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal"*, texto disponível em https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm [25.09.2019]

–, Carta dos Direitos Fundamentais da União Europeia, de 18 de dezembro de 2000, texto disponível em https://www.cnpd.pt/bin/legis/internacional/CARTAFUNDAMENTAL.pdf [26.09.2019].

–, Convenção sobre o Cibercrime, *Convenção de Budapeste,* Budapeste, 2001, texto disponível em http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf [16.09.2019].

ESTADOS UNIDOS DA AMÉRICA, Carta dos Direitos dos Estados Unidos de 1789, *"A Carta de Direitos é formada pelas dez primeiras Emendas à Constituição dos Estados Unidos da América. Foi redigida pelo Congresso dos EUA em 1789 e ratificada pelos estados em 15 de dezembro de 1791",* 1789, texto disponível em http://www.dhnet.org.br/direitos/anthist/marcos/carta_direitos_eua_1789.htm[25.09.2019].

EUROPEAN DATA PROTECTION BOARD - EDPB, *"Statement on the processing of personal data in the context of the COVID-19 outbreak"*, de 19 de março de 2020, texto disponível em https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf [23.06.2020].

FRANÇA, "*Declaração dos Direitos do Homem e do Cidadão de 1789, (...) o esquecimento ou o desprezo dos direitos do homem são as únicas causas dos males públicos e da corrupção dos Governos, resolveram declarar solenemente os direitos naturais, inalienáveis e sagrados do homem, a fim de que esta declaração, sempre presente em todos os membros do corpo social, lhes lembre permanentemente seus direitos e seus deveres; a fim de que os atos do Poder Legislativo e do Poder Executivo, podendo ser a qualquer momento comparados com a finalidade de toda a instituição política, sejam por isso mais respeitados (...)*", 1789, declaração disponível em http://www.direitoshumanos.usp.br/index.php/Documentos-anteriores-%C3%A0-cria%C3%A7%C3%A3o-da-Sociedade-das-Na%C3%A7%C3%B5es-at%C3%A9-1919/declaracao-de-direitos-do-homem-e-do-cidadao-1789.html [25.09.2019].

ORGANIZAÇÃO DAS NAÇÕES UNIDAS – ONU, *Carta Das Nações Unidas*, 1945, texto disponível em https://nacoesunidas.org/wp-content/uploads/2017/11/A-Carta-das-Na%C3%A7%C3%B5es-Unidas.pdf [25.09.2019]

–, *Declaração Universal dos Direitos Humanos*, Paris, 1948, texto disponível em http://www.onu.org.br/img/2014/09/DUDH.pdf [13.02.2019].

–, "*Pacto Internacional dos Direitos Civis e Políticos – PIDCP, de 16 de dezembro de 1966, (...) Reconhecendo que estes direitos derivam da dignidade inerente à pessoa humana; Reconhecendo que, de acordo com a Declaração Universal dos Direitos do Homem, não se pode realizar o ideal do ser humano livre, gozando das liberdades civis e políticas, libertos do terror e da miséria, a menos que se criem condições que permitam a cada pessoa gozar dos seus direitos civis e políticos, assim como dos*

seus direitos económicos, sociais e culturais, (...)", texto disponível em http://www.cne.pt/content/onu-pacto-internacional-sobre-os-direitos-civis-e-politicos [25.09.2019].

PERU, Ley n.º 27.806, de 13 de julio de 2002, texto disponível em https://www.mef.gob.pe/es/normas-legales/298-portal-de-transparencia-economica/normas-legales/830-ley-nd-2780 [13.09.2019].

REINO UNIDO, "*Declaração de Direitos de 1689, considerando que o falecido Rei Jaime II, com a ajuda de diversos maus conselheiros juízes e ministros empregados por ele, empenhou-se em destruir e extirpar a religião protestante, e as leis e liberdades deste reino",* 1689, declaração disponível em http://www.direitoshumanos.usp.br/index.php/Documentos-anteriores-%C3%A0-cria%C3%A7%C3%A3o-da-Sociedade-das-Na%C3%A7%C3%B5es-at%C3%A9-1919/a-declaracao-inglesa-de-direitos-1689.html [25.09.2019].

SUPERIOR TRIBUNAL DE JUSTIÇA – STJ, Recurso Especial n.º 306.570/SP, Rel. Ministra Eliana Calmon, Segunda Turma, julgado em 18/10/2001, DJe 18/02/2002, p. 340, texto disponível em https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=IMG&sequencial=30922&num_registro=200100235255&data=20020218&formato=PDF [22.08.2019].

–, Recurso Especial n.º 22.337, Relator Min. Ruy Rosado de Aguiar, Quarta Turma, julgado em: 13 fev. 1995, publicado em: 20 mar. 1995, texto disponível em http://www.mpsp.mp.br/portal/page/portal/cao_consumidor/jurisprudencia/juris_diversos/Resp533625_0.doc [09.09.2019].

–, Habeas Corpus n.º 444.024/PR, Rel. Ministro Rogerio Schietti Cruz, Sexta Turma, julgado em 02/04/2019, DJe 02/08/2019, texto disponível em https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1769509&num_registro=201800782456&data=20190802&formato=PDF [22.08.2019].

–, Súmula n.º 403, texto disponível em https://ww2.stj.jus.br/docs_internet/revista/eletronica/stj-revista-sumulas-2014_38_capSumula403.pdf [09.09.2019].

SUPREMO TRIBUNAL FEDERAL – STF, Recurso Extraordinário n.º 215.984/RJ, Relator(a): Min. Carlos Velloso, Segunda Turma, julgado em 04/06/2002, DJe 28-06-2002, PP-00143, EMENT., VOL-02075-05, PP-00870, RTJ., VOL-00183-03, PP-01096, texto disponível em http://stf.jus.br/portal/jurisprudencia/listarJurisprudencia.asp?s1=%28RE%24%2ESCLA%2E+E+215984%2ENUME%2E%29+OU+%28RE%2EACMS%2E+ADJ2+215984%2EACMS%2E%29&base=baseAcordaos&url=http://tinyurl.com/l2n6u53 [09.09.2019].

–, Mandado de Segurança n.º 23452 RJ, Relator: Celso de Mello, Data de Julgamento 16/09/1999, Tribunal Pleno, Data de Publicação: Dj 12-05-2000, PP-00020 Ement. Vol-01990-01 PP-00086, texto disponível em https://stf.jusbrasil.com.br/jurisprudencia/738746/mandado-de-seguranca-ms-23452-rj [25.09.2019].

–, Ação Direta de Inconstitucionalidade n.º 1.790 MC, Relatora: Min. Sepúlveda Pertence, Tribunal Pleno, julgado em 23/04/1998, DJe 08-09-2000, PP-00004, EMENT VOL-02003-01, PP-00199, texto disponível em http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=347269 [22.08.2019].

–, Habeas Corpus n.º 93250 MS, Relator: Min. Ellen Gracie, Data de Julgamento: 10/06/2008, Segunda Turma, Publicado no DJe n.º 117, divulgado em 26-06-2008, publicado em 27-06-2008, ementa VOL-02325-04, PP-00644, texto disponível em https://stf.jusbrasil.com.br/jurisprudencia/14720278/habeas-corpus-hc-93250-ms/inteiro-teor-103108730?ref=juris-tabs [09.09.2019].

UNITED STATES OF AMERICA, Code of Federal Regulations, Title 16, Chapter I, Subchapter C, Part 312, *Children's Online Privacy Protection Rule,* texto disponível em https://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5 [18.09.2019].

UNIÃO EUROPEIA, "*Directiva 95/46/CE do Parlamento Europeu e do Conselho da União Europeia, 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"*, diretiva disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT [07.11.2019].

–, "*Regulamento (UE) 2016/679 Do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)",* 2016, regulamento disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN [03.08.2019]

URUGUAY, Ley n.º 18.381, de 17 de octubre de 2008, texto disponível em https://legislativo.parlamento.gub.uy/temporales/leytemp9616241.html [13.09.2019].