SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE DIREITO "PROF. JACY DE ASSIS"

LUMA LAURA DAMASCENO GÓES

PROTEÇÃO DE DADOS PESSOAIS NO BRASIL E NO CANADÁ:

uma análise à luz do direito comparado.

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE DIREITO
Uberlândia - MG
2022

LUMA LAURA DAMASCENO GÓES

PROTEÇÃO DE DADOS PESSOAIS NO BRASIL E NO CANADÁ:
uma análise à luz do direito comparado.

Trabalho de Conclusão de Curso apresentado à Faculdade de Direito "Prof. Jacy de Assis", da Universidade Federal de Uberlândia, como requisito para a obtenção do título de Bacharel em Direito.

Orientador: Prof. Dr. *Rodrigo Vitorino Souza Alves*

Uberlândia - MG
2022

LUMA LAURA DAMASCENO GÓES

PROTEÇÃO DE DADOS PESSOAIS NO BRASIL E NO CANADÁ:
uma análise à luz do direito comparado.

Trabalho de Conclusão de Curso apresentado à Faculdade de Direito "Prof. Jacy de Assis", da Universidade Federal de Uberlândia, como requisito para a obtenção do título de Bacharel em Direito.

Orientador: Prof. Dr. *Rodrigo Vitorino Souza Alves*

Uberlândia, _____ de _____ de 2022.

_____

Professor Doutor Rodrigo Vitorino Souza Alves
Faculdade de Direito, Universidade Federal de Uberlândia
Orientador

_____

Professor Mestre João Alexandre Silva Alves Guimarães
Faculdade de Direito, Faculdade Pitágoras
Professor Convidado

Uberlândia - MG
2022

AGRADECIMENTOS

A apresentação deste trabalho marca a conclusão da minha formação como bacharel em direito junto à Universidade Federal de Uberlândia, no dia de hoje celebro a finalização de uma etapa muito importante da minha vida e que resultou de 5 anos de muito esforço e estudo. Assim, não poderia deixar de reservar este espaço para agradecer às várias pessoas que me apoiaram ao longo da minha jornada acadêmica e que, de alguma forma, colaboraram para o desenvolvimento do presente trabalho.

Inicio meus agradecimentos direcionando-os ao professor Rodrigo Vitorino, que não apenas foi o orientador da pesquisa desenvolvida no meu trabalho de conclusão de curso, mas que desde o 2º período da faculdade me inspira, pelo ilustre profissional que é, a me envolver no meio acadêmico. Tendo sido ele um dos principais responsáveis pela minha participação em projetos que marcaram a minha vida, e pelos quais tenho grande apreço. Aproveito para agradecer também ao professor João Alexandre Guimarães por aceitar o convite para compor a banca avaliadora da minha pesquisa, seus trabalhos não apenas influenciaram a escolha do presente tema, mas foram fundamentais à construção dos meus conhecimentos.

Dito isso, gostaria de registrar um agradecimento especial a minha família, aos meus pais Marcelo e Luciana, aos meus irmãos Malu, Marcelo e Luiz, e aos meus avós Gil e Namir e João e Ana, pessoas que, ao longo de toda a minha vida, me inspiraram a dar o melhor de mim e a sonhar alto. Vocês foram fonte inesgotável de apoio, confiança e amor, e, por isso, registro aqui os meus mais sinceros agradecimentos.

Por fim, agradeço aos meus amigos Bárbara Barcelos, Bárbara Lana, Carla Bonella, Carolina Barcelos, Fernanda Cunha, Júlia Aguiar, Marcela Caetano, Maria Júlia Pereira e Thobias Prado, ao meu namorado Liam Linley, aos meus caros colegas de trabalho do Escritório Schiefler Advocacia, bem como a todos aqueles que, apesar de aqui não mencionados, fizeram parte da minha história, me apoiando incondicionalmente e possibilitando que o dia de hoje se tornasse uma realidade.

PROTEÇÃO DE DADOS PESSOAIS NO BRASIL E NO CANADÁ: UMA ANÁLISE À LUZ DO DIREITO COMPARADO

Luma Laura Damasceno Góes[1]

RESUMO: O presente trabalho de conclusão de curso visa estudar, à luz do direito comparado, como o direito à proteção de dados pessoais tem se construído ao longo dos anos, em especial em meio à legislação e à jurisprudência brasileira e canadense. Para tanto, dividiu-se esta investigação em três etapas, na primeira delas analisou-se a trajetória histórica do reconhecimento do referido direito em âmbito mundial, na segunda conceituou-se e delimitou-se elementos da sociedade atual que adicionam urgência ao debate e que tornam imprescindível a aprovação de instrumentos normativos capazes de conferir adequada proteção ao dados pessoais dos internautas, em um terceiro momento, debruçou-se sobre instrumentos legais concernentes ao tema no Brasil e no Canadá, com o intuito de promover uma análise comparativa entre estes dois atores. Concluiu-se, então, que não obstante os inquestionavelmente importantes avanços já experienciados em ambos os países, o direito à proteção de dados pessoais continua em formação, no Brasil em decorrência da juvenilidade da Lei Geral de Proteção de Dados, e no Canadá, em vista a atualização normativa que está por vir.

PALAVRAS-CHAVE: Proteção de Dados Pessoais. Direito à Privacidade. Direitos Humanos. Brasil. Canadá.

[1] Discente do curso de graduação em Direito da Faculdade "Prof. Jacy de Assis", da Universidade Federal de Uberlândia (UFU). Estagiária no escritório Schiefler Advocacia. *Visiting Student Researcher* na University of Ottawa, no Canadá. Pesquisadora de iniciação científica no campo do Direito Digital e pesquisadora discente do Laboratório de Direitos Humanos e do Centro Brasileiro de Estudos em Direito e Religião (CEDIRE). No triênio 2019-2021 atuou como coordenadora do Núcleo de Traduções do CEDIRE. Contato: lumalaura@gmail.com ORCID: 0000-0002-3268-6890.

PROTECTION OF PERSONAL DATA IN BRAZIL AND IN CANADA: AN ANALYSIS BASED ON COMPARATIVE LAW

Luma Laura Damasceno Góes[2]

ABSTRACT: The present research aims to study how the right to personal data protection has been built over the years, particularly within Brazilian and Canadian legislation and case law. This investigation was conducted in three steps: first, analyzing the worldwide historical evolution and precedent regarding data protection; second conceptualizing and and examining the conditions of the so-called Information Age that require the enactment of laws which properly protect personal data; third, this study turned to Brazil and Canada and their legal frameworks regarding data protection. In conclusion, it was noticed that despite the unquestionably important advances already experienced in both countries, the right to personal data protection continues to be built, in Brazil due to the youthfulness of the Lei Geral de Proteção de Dados, and in Canada, because of the regulatory updates to come.

KEY-WORDS: Protection of Personal Data. Right to Privacy. Human Rights. Brazil. Canada.

[2] Discente do curso de graduação em Direito da Faculdade "Prof. Jacy de Assis", da Universidade Federal de Uberlândia (UFU). Estagiária no escritório Schiefler Advocacia. *Visiting Student Researcher* na University of Ottawa, no Canadá. Pesquisadora de iniciação científica no campo do Direito Digital e pesquisadora discente do Laboratório de Direitos Humanos e do Centro Brasileiro de Estudos em Direito e Religião (CEDIRE). No triênio 2019-2021 atuou como coordenadora do Núcleo de Traduções do CEDIRE. Contato: lumalaura@gmail.com ORCID: 0000-0002-3268-6890.

SUMÁRIO:

I. INTRODUÇÃO

O presente trabalho de conclusão de curso tem como objetivo analisar, à luz do direito comparado, a proteção historicamente conferida aos dados pessoais pela legislação e pela jurisprudência brasileira e canadense. A escolha do presente tema teve como propulsor a acelerada e ainda crescente expansão do uso da internet e das tecnologias de comunicação em âmbito global, pois, em decorrência dessa "nova" realidade, várias searas do mundo virtual mostraram-se carentes no quesito regulamentação.

Apesar da relativamente recente promulgação de instrumentos normativos protetivos em diversos países do mundo, a necessidade de se promover o direito à proteção de dados pessoais surgiu há tempos, desde que se tornou factível a criação de enormes bases de armazenamento de dados, cujo conteúdo ganhou considerável valor econômico. De mais a mais, é fato que o Direito não consegue se atualizar na mesma velocidade em que novas ferramentas digitais são desenvolvidas, de modo que, por mais vasta que seja a utilização do ciberespaço, sua regulamentação ainda é precária. Foram episódios de proteção deficiente à privacidade, intimidade e liberdade dos indivíduos, que levaram a conhecidos casos de excessiva relativização dos direitos humanos online.

Essa problemática se agrava quando o mundo moderno tem como uma de suas principais características a generalizada utilização da internet: o Relatório Digital Global produzido pelo *We Are Social*[3] constatou que no ano de 2012 havia 2.1 bilhões de pessoas utilizando a internet, e que passados 10 anos, no mês de janeiro de 2022, este índice alcançou a marca de 4.9 bilhões de internautas em um universo de 7.9 bilhões de pessoas.[4]

É em decorrência de quão submersa no mundo digital é a sociedade em que vivemos, que se faz imprescindível que os ordenamentos jurídicos dos mais diversos países regulamentem adequadamente as relações que nesse ambiente se formam, para evitar abusos por parte daqueles dotados de poder e controle. Assim, é forçoso que certas garantias venham a ser reconhecidas como fundamentais e merecedores de proteção ampla, a exemplo do direito à proteção de dados pessoais que, apesar de historicamente vinculado à direitos como privacidade e dignidade da pessoa humana, já conta com o *status* de direito fundamental autônomo em diversos países do mundo.

---

[3] WE ARE SOCIAL. **Digital 2022**: another year of bumper growth. 2022. Disponível em: https://wearesocial.com/uk/blog/2022/01/digital-2022-another-year-of-bumper-growth-2/. Acesso em: 01 mar. 2022.

[4] WORLDOMETER. **Current World Population**. 2022. Conforme as mais recentes estimativas das Organizações das Nações Unidas. Disponível em: http://srv1.worldometers.info/world-population/#. Acesso em: 01 mar. 2022.

Contudo, apesar dos incontestáveis avanços é possível que a aplicação dos diplomas protetivos atuais não seja ideal ou mesmo suficiente para salvaguardar o interesse dos titulares destes dados. Nicolas Suzor, por exemplo, defende que os Termos e Condições de Uso, de forma geral, reservam uma quantidade significativa e desproporcional de poder para os operadores das plataformas digitais, garantindo os interesses comerciais destes em detrimento da vontade dos titulares de tais dados, e dando-lhes autoridade quase absoluta.[5]

Em que pese a abordagem metodológica, o presente estudo se desenvolveu em três fases: i) iniciado por meio de um estudo histórico da trajetória do reconhecimento do direito à proteção de dados pessoais no mundo - o qual engloba a menção à conhecidos casos em que houvera coleta e tratamento indevido de dados pessoais, e ao surgimento dos primeiros diplomas legais protetivos; ii) procedeu-se com uma investigação doutrinária sobre a relevância de se debater a proteção de dados pessoais na sociedade da informação; e iii) conduziu-se uma análise comparativa dos instrumentos legais concernentes ao tema e que foram relevantes à construção do direito à proteção de dados pessoais no âmbito da jurisdição do Brasil e do Canadá.

Nesta senda, como um dos objetivos centrais do presente trabalho é estudar e comparar os instrumentos normativos que conferem proteção à dados pessoais nos países supramencionados, fez-se necessária a adoção, como parte do processo metodológico, de um estudo dogmático-jurídico, em vista a imprescindibilidade de se recorrer à lei, à doutrina e à jurisprudência para tratar adequadamente do tema.

II. HISTÓRICO DA PROTEÇÃO DE DADOS PESSOAIS NO MUNDO

II.1. Uma onda normativa em âmbito global

Dentre os diversos direitos sistematicamente suscetíveis de violação no mundo digital, optou-se por tratar neste trabalho do direito à proteção de dados pessoais. Tal recorte se justifica pelo fato de, recentemente, este direito ter chamado a atenção da comunidade jurídica internacional, o que se verifica pela, quase simultânea, entrada em vigor de instrumentos normativos protetivos em diversos países do mundo. São exemplos dessa "onda" normativa em favor da proteção de dados pessoais a promulgação do Regulamento Geral sobre a Proteção de Dados (RGPD)[6] na União Europeia (UE) em 2016, do *Notifiable Data Breach*

[5] SUZOR, Nicolas. Digital Constitutionalism: using the rule of law to evaluate the legitimacy of governance by platforms. **Social Media + Society**, [S.I.], v. 4, n. 3, jul. 2018. SAGE Publications.
[6] UNIÃO EUROPEIA. **Regulamento Geral sobre a Proteção de Dados - 2016/679**. Bruxelas, 27 abr 2016. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 28 fev. 2022.

Scheme[7] que, em 2018, emendou o *Privacy Act of 1988* na Austrália, do *California Consumer Privacy Act,*[8] em 2018, nos Estados Unidos, da Lei Geral de Proteção de Dados (LGPD)[9] no Brasil, também no ano de 2018, e do *Privacy Act of 2020*[10] na Nova Zelândia, em 2020.

Não obstante o Brasil e o Canadá terem sido os atores selecionados para o presente estudo quando do recorte do tema, uma análise, ainda que breve, da trajetória histórica da proteção de dados pessoais no mundo não pode se esquivar dos grandes feitos da União Europeia, dos Estados Europeus individualmente, e dos Estados Unidos da América.

Qualquer estudo aprofundado sobre a origem histórica do que hoje conhecemos como direito à proteção de dados pessoais se debruça sobre os escritos de Samuel D. Warren e Louis D. Brandeis, aquele um notável advogado norte americano, e este um futuro ministro da Suprema Corte dos Estados Unidos. Juntos, os juristas plantaram a semente do direito à proteção de dados pessoais ao debater o direito à privacidade em uma sociedade que antecedia a revolução tecnológica. Em brilhante análise sobre o desenvolvimento do Direito ao longo da história os autores consignam que: "mudanças políticas, sociais e econômicas implicam o reconhecimento de novos direitos, e o *common law,* em sua eterna juventude, evolui para satisfazer as demandas da sociedade".[11]

Warren e Brandeis, em 1890, defendiam que a evolução do Direito e o reconhecimento de novos direitos era inevitável frente às mudanças sociais, não por outro motivo os autores explicam que nos primórdios dessa ciência social aplicada garantia-se proteção apenas contra interferências físicas na vida e na propriedade dos indivíduos, anos mais tarde reconheceu-se a natureza espiritual das pessoas, seus sentimentos e intelecto, de modo que o Direito passou a não mais falar em "direito à vida", mas em "direito à aproveitar a vida" e "direito à não ser importunado", e a proteção à propriedade passou a englobar também bens intangíveis.[12]

Tendo em vista as óbvias diferenças existentes entre a sociedade do final do século XIX - da qual falam os autores -, e aquela em que hoje se vive - na qual a maioria das

---

[7] AUSTRÁLIA. **Notifiable Data Breaches - Bill 2016**. Canberra, 22 fev. 2017. Disponível em: https://www.legislation.gov.au/Details/C2017A00012. Acesso em: 28 fev. 2022.

[8] CALIFÓRNIA. **California Consumer Privacy Act - CCPA**. Sacramento, 28 jun. 2018. Disponível em: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5. Acesso em: 28 fev. 2022.

[9] BRASIL. **Lei Geral de Proteção de Dados, Lei 13.709**. Brasília, 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 07 jul. 2022.

[10] NOVA ZELÂNDIA. **Privacy Act of 2020**. Wellington, 30 jun. 2020. Disponível em: https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html#LMS23703. Acesso em 22 jun. 2022.

[11] WARREN, Samuel D.; BRANDEIS, Louis D.. The Right to Privacy. **Harvard Law Review**, Cambridge, v. 4, n. 5, p. 193-220, 15 dez. 1890. Disponível em: https://www.jstor.org/stable/1321160?seq=1. Acesso em: 23 jun. 2022.

[12] Ibid.

interações humanas é intermediada por, no mínimo, um dispositivo ou mecanismo tecnológico -, não surpreende constatar que a semente do direito à proteção de dados pessoais não se referia à dados com a mesma amplitude que atualmente goza tal termo.

Warren e Brandeis iniciaram a discussão sobre o direito à proteção de dados pessoais no escopo do direito à privacidade, e sob a ótica de juristas que reconheciam a problemática da circulação não autorizada de retratos e da abordagem invasiva de jornais em relação a questões ligadas à seara particular da vida dos indivíduos, asseverando que a estes deveria ser salvaguardado o poder de determinar até que ponto os mesmos gostariam que seus pensamentos, sentimentos e emoções fossem transmitidos para terceiros.[13]

Passados aproximadamente 60 anos, a Organização das Nações Unidas, por meio do artigo 12 da Declaração Universal dos Direitos Humanos de 1948, reconheceu o direito à privacidade como um direito fundamental a ser protegido em âmbito global,[14] o que levou o Conselho da Europa, mediante o disposto no artigo 8º da Convenção Europeia dos Direitos do Homem de 1950, a reafirmar tal garantia no escopo de jurisdição dos Estados Membros.[15]

Em 1967, entra em vigor nos Estados Unidos da América o *Freedom of Information Act*, regramento que confere a todo indivíduo o direito de solicitar acesso a arquivos e documentos armazenados por quaisquer entes governamentais, solicitação que apenas seria negada se aplicável alguma das 9 exceções da lei, dentre as quais está o dever de proteger o direito à privacidade, motivo pelo qual não era autorizada a divulgação de informação de arquivos pessoais ou médicos.[16]

Nesta senda, merece destaque o julgamento do caso Stauder vs. cidade de Ulm, pelo Tribunal de Justiça Europeu, em 12 de novembro de 1969. Apesar da presença meramente implícita do direito à proteção de dados pessoais, o caso evidencia que no imaginário do povo alemão, certas condutas - atualmente englobadas no escopo protetivo do referido direito - já não poderiam ser aceitas.

À época, existia um programa de bem-estar social que possibilitava que seus beneficiários adquirissem alimentos - no caso manteiga - por valores mais baixos do que aquele ofertado ao cidadão comum, para tanto, fazia-se necessário que o cliente estivesse em posse de um cupom que o identificasse como apto a beneficiar-se dessa condição. Ocorre que,

---

[13] WARREN, Samuel D; BRANDEIS, Louis D. Op cit.

[14] ONU. **Declaração Universal dos Direitos Humanos**. Assembleia Geral das Nações Unidas, Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 23 jun. 2022.

[15] CONSELHO DA EUROPA. **Convenção Europeia dos Direitos do Homem**. Estrasburgo, Disponível em: https://echr.coe.int/documents/convention_por.pdf. Acesso em: 23 jun. 2022.

[16] DEPARTAMENTO DE JUSTIÇA DOS ESTADOS UNIDOS. **What is FOIA?** Disponível em: https://www.foia.gov/about.html. Acesso em: 23 jun. 2022.

para fins de fiscalização, o governo alemão determinou que o nome do beneficiário constasse no voucher a ser apresentado, feito isso, no ano de 1969, o cidadão alemão Erich Stauder recorreu ao Tribunal Administrativo de Stuttgart, *Verwaltungsgericht*, contra a cidade de Ulm, localizada no estado de Baden-Württemberg, para que fosse retirada a exigência de tal dado, por entender tratar-se de violação aos artigos 1º e 3º da Constituição Alemã.[17] [18] Segundo Felix Bieker, a proteção de dados pessoais se fez presente no julgamento, ainda que de forma implícita, quando o tribunal alemão competente se mostrou preocupado com a possibilidade de a identificação de indivíduos pelo nome, para participação em um programa de assistência social, configurar violação de direitos fundamentais.[19]

O caso foi levado ao Tribunal de Justiça Europeu, e este, sem adentrar no debate sobre possível violação de direitos fundamentais, entendeu que não deveria ser exigida a identificação pelo nome, pelo simples fato de os outros países aceitarem formas variadas de verificação da qualidade de beneficiário, devendo prevalecer a interpretação mais liberal.[20]

No ano seguinte, o estado de Hesse na Alemanha, aprovou a primeira legislação específica sobre proteção de dados pessoais, iniciativa que influenciou os demais estados do país e possibilitou que, em 1978, a Alemanha contasse com o *Bundesdatenschutzgesetz*,[21] legislação de âmbito federal e que estabelecia princípios básicos para proteção de dados pessoais no país, a exemplo da obrigatoriedade da obtenção do consentimento do titular dos dados para que estes pudessem ser legalmente tratados.[22]

A Constituição da República Portuguesa (CRP) acompanhou o pioneirismo do estado de Hesse, pois, em 1976, consagrou-se como o primeiro instrumento de hierarquia constitucional a dispor sobre o direito à proteção de dados pessoais frente ao uso de novas tecnologias. Sob o artigo 35º salvaguardou-se o direito à autodeterminação informativa, conferindo aos cidadãos portugueses a prerrogativa de acessar quaisquer dados

---

[17] O artigo 1º da referida Carta Constitucional reconhece a inviolabilidade da dignidade humana, bem como que é um dever estatal protegê-la, por sua vez, o artigo 3º dispõe sobre a igualdade, consignando que todos são iguais perante à lei.

[18] EUROPA. Tribunal de Justiça Europeu. Stauder vs. Ulm. Luxemburgo, 12 nov. 1969. Disponível em: https://www.cvce.eu/content/publication/1999/1/1/fafa8ce7-544b-47c0-9cfc-cb142a4c9424/publishable_en.pdf. Acesso em: 01 jul. 2022.

[19] BIEKER, Felix. **The Right to Data Protection**: individual and structural dimensions of data protection in EU law. Berlim: Springer, 2022. p 49 - 51.

[20] Ibid.

[21] ALEMANHA. **Bundesdatenschutzgesetz**. Alemanha, Disponível em: https://www.gesetze-im-internet.de/englisch_bdsg/. Acesso em: 24 jun. 2022.

[22] STEPANOVA, Olga; JECHEL, Patricia. **The Privacy, Data Protection and Cybersecurity Law Review: Germany**. 2021. Disponível em: https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/germany#:~:text=Finally%2C%20in%20December%201983%2C%20the%20German%20Federal%20Constitutional,in%20which%20data%20processing%20has%20grown%20more%20important. Acesso em: 24 jun. 2022.

informatizados que lhes diga respeito, conhecer da coleta, uso, armazenamento e compartilhamento destes, bem como saber por quem e para qual finalidade estariam sendo tratados, "o direito previsto no art. 35.º da CRP consagra a proteção dos cidadãos perante o tratamento de dados pessoais informatizados".[23]

Anos mais tarde, em 1980, tem-se o *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data,* formulado de forma conjunta pelos países membros da Organização para a Cooperação e Desenvolvimento Econômico (OCDE). O prefácio do referido documento evidencia a preocupação já existente em relação à eventual armazenamento indevido e não consentido de dados pessoais, de modo que suas duas principais finalidades eram: i) harmonizar as normas nacionais de privacidade; e ii) facilitar o livre fluxo de informações entre os Estados Membros em respeito aos Direitos Humanos.

> O avanço do processamento automatizado de dados, que possibilita a transmissão de grandes quantidades de informação, em segundos, através de fronteiras nacionais, e mesmo continentais, faz ser necessário que se pense na proteção da privacidade em relação a dados pessoais. Leis de proteção à privacidade foram, ou serão em breve, implementadas em, aproximadamente, metade dos países membros da OCDE (Áustria, Canadá, Dinamarca, França, Alemanha, Luxemburgo, Noruega, Suécia e Estados Unidos da América já contam com leis sobre o tema, enquanto Bélgica, Islândia, Holanda, Espanha e Suíça prepararam seus projetos de lei) com o intuito de prevenir violações a direitos humanos fundamentais, a exemplo do armazenamento ilegal de dados pessoais, o armazenamento de dados pessoais inexatos, e abuso ou divulgação não autorizada de tais dados.[24]

Um ano depois surge a Convenção 108 do Conselho da Europa, o primeiro instrumento juridicamente vinculativo em âmbito internacional para a proteção contra abusos envolvendo a coleta e o tratamento de dados pessoais. A referida Convenção merece destaque por seu vanguardismo, pois no início da década de 80: i) proibia-se o tratamento de dados considerados sensíveis - etnia, política, saúde, religião, vida sexual, registo criminal, etc - caso não fosse assegurada a devida proteção legal; ii) garantia-se a todos o direito de ter conhecimento do armazenamento de quaisquer dados que lhe dissessem respeito, bem como

---

[23] GUIMARÃES, João Alexandre Silva Alves. **O Regime Jurídico do Direito ao Esquecimento (ou à Desindexação) na União Europeia e a sua Repercussão no Direito Brasileiro**. 2019. 134 f. Dissertação (Mestrado) - Curso de Direito da União Europeia, Universidade do Minho, Braga, Portugal, 2019.

[24] *The development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data. Privacy protection laws have been introduced, or will be introduced shortly, in approximately one half of OECD Member countries (Austria, Canada, Denmark, France, Germany, Luxembourg, Norway, Sweden and the United States have passed legislation. Belgium, Iceland, the Netherlands, Spain and Switzerland have prepared draft bills) to prevent what are considered to be violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorized disclosure of such data.* OCDE. **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.** Europa, Disponível em: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Acesso em: 25 jun. 2022. Tradução nossa.

de eventualmente requerer sua correção; iii) determinava-se que o excepcional não cumprimento do disposto na Convenção seria aceito apenas se mediante justificativa plausível, a exemplo da eventual necessidade de tratamento para fins de garantir a segurança nacional; e iv) previa-se que, para Estados cujas leis não conferem o mesmo nível de proteção, o fluxo transfronteiriço de dados poderia vir a ser restringido.[25]

Contudo, foi no ano de 1983 que o direito à proteção de dados pessoais foi, pela primeira vez, reconhecido e apreciado de forma expressa no âmbito de um tribunal superior.[26] A decisão do Tribunal Constitucional Federal Alemão, *Bundesverfassungsgericht*, reconhecendo o direito constitucional à autodeterminação informativa dos alemães, deve ser considerada como um divisor de águas no processo de construção do direito à proteção de dados pessoais no mundo.

O caso decorreu da resistência do povo alemão ao processamento eletrônico de dados para a realização do censo daquele ano, diligência cujo respaldo legal era a recém aprovada Lei do Censo de 1983, *Volkszählungsgesetzes von 1983,* diploma que veio a ter algumas de suas disposições declaradas inconstitucionais pelo Tribunal.[27]

Quando do julgamento, em 15 de dezembro, o Tribunal Constitucional Federal Alemão consignou que proteger os indivíduos da coleta, do armazenamento, do uso e do compartilhamento ilimitado de dados pessoais é proteger o direito à personalidade destes, conforme disposto nos artigos 2.1 e 1.1 da Constituição alemã - o artigo 2.1 da Constituição alemã determina que "toda pessoa tem direito ao livre desenvolvimento de sua personalidade, desde que não viole os direitos dos outros nem ofenda a ordem constitucional ou a lei moral", enquanto o artigo 1.1 dispõe que "a dignidade humana é inviolável. Respeitá-la e protegê-la é dever de toda autoridade estatal".[28] No entender do Tribunal, a todos os cidadãos teria sido conferido o poder de decisão sobre a divulgação e o uso de seus próprios dados pessoais, de modo que a autodeterminação informativa seria regra e não exceção:

> Limitações ao direito à "autodeterminação informativa" só são permitidas se houver um interesse público superior. Elas exigem uma base legal que deve ser constitucional e obedecer ao princípio da clareza jurídica que vigora no Estado Democrático de Direito. Além disso, o legislador deve observar o princípio da proporcionalidade. Deve também estabelecer garantias

---

[25] CONSELHO DA EUROPA. **Convenção nº 108.** Europa. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108. Acesso em: 24 jun. 2022.

[26] Quando do julgamento, em 1969, do caso Stauder vs. Ulm, pelo Tribunal de Justiça Europeu, o direito à proteção de dados pessoais estava apenas implícito no julgamento.

[27] STEPANOVA, Olga; JECHEL, Patricia. Op. cit.

[28] ALEMANHA. Tribunal Constitucional Federal Alemão. Julgamento de 15 de dezembro de 1983 - 1 BvR 209/83. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html. Acesso em: 28 jun. 2022.

> organizacionais e processuais que compensem o risco de se estar violando o direito à personalidade.[29]

Posteriormente, no âmbito do sistema universal de proteção da Organização das Nações Unidas (ONU), o direito à proteção de dados pessoais ganhou *status* de direito humano quando, em 1988, foi reconhecido como tal pelo Comitê da ONU para Direitos Humanos. Ao redigir o Comentário Geral nº 16, o Comitê expressamente indicou a proteção de dados pessoais como direito englobado no escopo de proteção do artigo 17 do Pacto Internacional de Direitos Civis e Políticos (PIDCP)[30] o qual preceitua que "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".[31]

No referido Comentário, o Comitê para Direitos Humanos tratou sobre a necessidade de haver regulamentação legal para o armazenamento de informações pessoais, ainda que por autoridades estatais, e reconheceu ser um dever dos Estados assegurar que dados concernentes à vida privada dos indivíduos não sejam tratados em desconformidade com os preceitos dispostos no Pacto.[32] Ademais, merece especial destaque as considerações do Comitê sobre direitos a serem garantidos em favor de uma proteção mais eficaz da privacidade:

> Para ter a proteção mais eficaz de sua vida privada, todo indivíduo deve ter o direito de verificar, de uma forma inteligível, quais dados pessoais são armazenados em arquivos de dados automáticos e com quais objetivos. Cada indivíduo deve também ser capaz de verificar quais autoridades públicas ou indivíduos ou órgãos privados controlam ou podem controlar seus arquivos. Se tais arquivos contiverem dados pessoais incorretos ou tiverem sido coletados ou processados de maneira contrária às disposições da lei, todo indivíduo deve ter o direito de solicitar a retificação ou a eliminação.[33]

De forma quase concomitante, diplomas nacionais que dispunham sobre proteção de dados pessoais eram promulgados em diversos países, a exemplo do *Data Protection Act of 1984* no Reino Unido[34] e da *Ley Orgánica de Protección de Datos de Carácter Personal* de 1999 na Espanha.[35] No entanto, o principal feito normativo do período data do ano de 1995, momento em que o Parlamento Europeu e o Conselho da Europa formularam a Diretiva

---

[29] ALEMANHA. Tribunal Constitucional Federal Alemão. Op cit.
[30] NÚCLEO DE ESTUDOS INTERNACIONAIS. C**omentários Gerais dos Comitês de Tratados de Direitos Humanos da ONU**. São Paulo: Núcleo de Estudos Internacionais, 2018. Disponível em: https://www.defensoria.sp.def.br/dpesp/repositorio/0/Comentários%20Gerais%20da%20ONU.pdf. Acesso em: 01 mar. 2022
[31] ONU. **Pacto Internacional de Direitos Civis e Políticos**. Assembleia Geral das Nações Unidas, Disponível em: https://www.unicef.org/brazil/pacto-internacional-sobre-direitos-civis-e-politicos. Acesso em: 30 jun. 2022.
[32] NÚCLEO DE ESTUDOS INTERNACIONAIS. Op cit.
[33] Ibid.
[34] REINO UNIDO. **Data Protection Act**. Londres, 1984. Disponível em: https://www.legislation.gov.uk/ukpga/1984/35/pdfs/ukpga_19840035_en.pdf. Acesso em: 29 jun. 2022.
[35] ESPANHA. **Ley Orgánica de Protección de Datos de Carácter Personal**. Madri, 1999. Disponível em: https://boe.es/buscar/doc.php?id=BOE-A-1999-23750. Acesso em: 29 jun. 2022.

95/46/CE, cujo dois principais objetivos eram: i) proteger o direito à proteção de dados; e ii) viabilizar seu livre fluxo dentro da União Europeia.[36]

Uma inegável consequência da entrada em vigor da Diretiva 95/46/CE foi a extensiva implementação de políticas públicas protetivas em matéria de proteção de dados pessoais em todo continente europeu, pois a União Europeia passou a exigir que seus Estados Membros dispusessem de leis nacionais sobre o tema e que qualquer empresa com sede dentro de sua jurisdição se submetesse a regras específicas no que concerne o tratamento e a transferência de dados.[37]

A Diretiva europeia contou com diversas previsões extremamente significativas e que merecem menção no presente trabalho, com sua promulgação passou-se a reconhecer, por exemplo, o direito de todo cidadão de se opor ao tratamento de seus dados pessoais, *vide* artigo 14º, e de não estar sujeito a certas consequência de decisões resultantes do tratamento automatizado de seus dados, *vide* artigo 15º, além disso, proibiu-se o tratamento de dados pessoais relativos à raça ou etnia, opiniões políticas, convicções religiosas ou filosóficas, filiação sindical, saúde e vida sexual, *vide* artigo 8º.[38]

Nos anos 2000, ao ser inserido na Carta dos Direitos Fundamentais da União Europeia, o direito à proteção de dados pessoais consagrou-se, nesta jurisdição, como um direito fundamental autônomo, pois dissociado da garantia de respeito pela vida privada e familiar - artigo 7º -, o direito a proteção de dados pessoais contava com previsão específica no artigo 8º: "todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito".[39] [40]

No mesmo ano, influenciado pelas diligências protetivas europeias, o Canadá aprovava o *Personal Information Protection and Electronic Documents Act* (PIPEDA) com o intuito de fomentar o comércio eletrônico do país, assegurando proteção a dados pessoais que viessem a ser coletados, usados e divulgados nessa atividade.[41] Avanço similar não ocorreu no Brasil, pois o país permaneceu sem uma norma especial de proteção à dados pessoais por

---

[36] GUIMARÃES, João Alexandre Silva Alves. **O Regime Jurídico do Direito ao Esquecimento (ou à Desindexação) na União Europeia e a sua Repercussão no Direito Brasileiro**. Op cit.
[37] Ibid.
[38] UNIÃO EUROPEIA. **Diretiva 95/46/CE**. Luxemburgo, 24 out. 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 29 jun. 2022.
[39] UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia**. Nice, França, 07 dez. 2000. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT. Acesso em: 29 jun. 2022.
[40] GUIMARÃES, João Alexandre Silva Alves. **O Regime Jurídico do Direito ao Esquecimento (ou à Desindexação) na União Europeia e a sua Repercussão no Direito Brasileiro**. Op cit.
[41] CANADÁ. **Personal Information Protection And Electronic Documents Act** - S.C. 2000, c. 5. Ottawa, 13 abr. 2000. Disponível em: https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/FullText.html. Acesso em: 28 fev. 2022.

mais alguns anos, apesar de sua presença em fóruns e ações concernentes à política nacional para a regulamentação no mundo digital ter aumentado.

Com o reconhecimento do direito a proteção de dados pessoais como um direito fundamental autônomo no âmbito europeu, e com a entrada em vigor da Diretiva 95/46/CE, vários casos relativos a possíveis violações do escopo desse novo direito foram apresentados ao Tribunal de Justiça Europeu ao longo dos anos, cita-se para fins didáticos o primeiro caso cujo julgamento tratava substancialmente do direito à proteção de dados pessoais: *Österreichischer Rundfunk*.

O caso *Österreichischer Rundfunk,* apresentado ao Tribunal de Justiça Europeu em 2003, contestava a legalidade, frente à Diretiva 95/46/CE e ao artigo 8º da Carta de Direitos Fundamentais da União Europeia, de uma lei austríaca que determinava a publicização dos rendimentos de todo empregado público que recebesse acima de determinado valor. Ao decidir o Tribunal de Justiça Europeu divergiu da jurisprudência do Tribunal Europeu de Direitos Humanos, entendendo por dispensável, para a aplicação dos diplomas concernentes à proteção de dados pessoais, a demonstração de nexo entre a informação divulgada e a vida privada do indivíduo exposto. Contudo, paradoxalmente, o Tribunal restringiu o escopo dos diplomas ao declarar que o mero armazenamento de dados pessoais não ocasionava interferência na vida privada e na tutela legal dos dados pessoais.[42]

No ano de 2014, ainda antes da aprovação de uma lei geral, entrava em vigor no Brasil o Marco Civil da Internet, Lei 12.965, diploma cujo objetivo principal era estabelecer princípios, garantias, direitos e deveres relativos ao uso da internet no país, mas que continha disposições concernentes também à proteção de dados pessoais. Assegurou-se, por exemplo, como um direito dos usuários "informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas", *vide* artigo 7º, inciso VIII.[43]

Além disso, em âmbito europeu, é oportuno rememorar que a Diretiva 95/46/CE foi de suma importância para a extensa regulamentação do direito à proteção de dados pessoais pelos Estados membros da União Europeia. Todavia, passados quase dez anos desde sua promulgação, atualizações tornaram-se necessárias para fortalecer o direito à privacidade e à proteção de dados pessoais, bem como para impulsionar e fomentar o mercado digital

---

[42] BIEKER, Felix. Op cit. p 51 - 54.

[43] BRASIL. **Marco Civil da Internet, Lei 12.965**. Brasília, 23 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 07 jul. 2022.

europeu,[44] pois: i) com o advento da globalização, as mudanças tecnológicas experienciadas ao longo do vigor da Diretiva e a proporção na qual cresceu o número de internautas europeus, eram fatores inimagináveis em 1995; e ii) por não ser vinculativa, a implementação da Diretiva 95/46/CE, variou para cada Estado membro, fazendo com que a conjuntura legal europeia, em matéria de proteção de dados, fosse não hegemônica.[45]

Por conseguinte, após analisar as propostas da Comissão Europeia, o Parlamento e o Conselho da Europa aprovaram, em 2016, o Regulamento Geral sobre a Proteção de Dados, (UE) 2016/679, diploma que entrou em vigor em 2018 revogando a Diretiva 95/46/EC. Uma das mais significativas mudanças decorrentes desse fato concerne o novo alcance das disposições protetivas da lei europeia, pois, diferentemente da Diretiva de 1995, o Regulamento Geral sobre a Proteção de Dados, ao dispor em seu artigo 3º sobre o âmbito de aplicação territorial de suas previsões, estabelece que as mesmas se aplicam: i) ao tratamento de dados pessoais por estabelecimento situado no território da União, ainda que o tratamento em si ocorra para além da jurisdição desta; ii) ao tratamento de dados pessoais - que diga respeito à oferta de bens ou serviços, e à controle de comportamento - de indivíduos residentes em sua jurisdição, ainda que o responsável pelo tratamento não esteja estabelecido na União Europeia; e iii) ao tratamento de dados pessoais em que o responsável não esteja estabelecido na União Europeia, mas se encontre em local em que se aplicam as leis de Estado membro do bloco.

Foi no ano de 2016, portanto, que a supramencionada "onda normativa em favor da proteção de dados pessoais" teve início. Com a aprovação do Regulamento Geral sobre Proteção de Dados, países e empresas que quisessem manter relações comerciais com Estados membros da União Europeia necessitavam de legislações tão protetivas quanto o RGPD, pois "o Estado que não possuísse lei de mesmo nível passaria a poder sofrer algum tipo de barreira econômica ou dificuldade de fazer negócios com os países da UE".[46]

Nesse momento, a proteção de dados pessoais já era reconhecida como um direito humano no âmbito do sistema de proteção universal da ONU, como um direito fundamental, na Carta de Direitos Fundamentais da União Europeia, e contava com legislações protetivas em diversos países, no entanto, faltava objetividade na definição dos critérios a serem considerados na verificação da legalidade do tratamento e do respeito à padrões mínimos de

---

[44] COMISSÃO EUROPEIA. **Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses**. 2012. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46. Acesso em: 01 jul. 2022.
[45] Ibid.
[46] PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais:** comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

segurança. Assim sendo, foi muito bem-vindo o novo diploma europeu de proteção de dados, pois padronizou-se quais seriam os atributos qualitativos de tal garantia, em cuja ausência deveria haver penalidades.[47]

O Regulamento (UE) 2016/679 serviu de inspiração para muitos dos diplomas que o sucederam, inclusive para o brasileiro, Lei Geral de Proteção de Dados, com o qual compartilha diversos princípios e garantias. À vista disso, em 2022, passados 132 anos desde que Warren e Brandeis "plantaram a semente" do direito à proteção de dados pessoais, seu escopo e importância estão bem mais delimitados, tanto normativa, quanto jurisprudencialmente. Estima-se que, atualmente, pelo menos 71% dos países do mundo já contam com leis que asseguram proteção aos dados e a privacidade de seus cidadãos, índice que chega a 80% se consideradas as nações em que tais normas estão em votação.[48]

II.2. Noções gerais quanto ao papel do Brasil e do Canadá em matéria de proteção de dados pessoais.

Uma vez analisada a trajetória histórica da construção do direito à proteção de dados pessoais no mundo, passaremos a analisar a relevância dessa evolução normativa, para posteriormente nos voltaremos às iniciativas brasileiras e canadenses sobre o tema. Em tópico próprio discorreremos de maneira pormenorizada sobre o contexto em meio ao qual os referidos países promulgaram suas primeiras legislações específicas para a proteção dos dados pessoais de seus cidadãos, sobre o escopo de tais diplomas, bem como sobre eventuais repercussões decorrentes de sua aprovação.

Por ora, nos interessa consignar que no contexto brasileiro o presente estudo terá como foco a Lei Geral de Proteção de Dados, Lei nº 13.709, diploma que, aprovado em 2018, entrou em vigor no ano de 2020, e revolucionou o ordenamento jurídico nacional, por ser o primeiro instrumento normativo pátrio específico sobre proteção de dados. Comparativamente, no concerne ao Canadá, analisar-se-á o *Privacy Act* e o *Personal Information Protection and Electronic Documents Act*, instrumentos de suma importância no sistema jurídico do país por regularem extensivamente o tratamento de dados promovido tanto por agentes públicos, quanto privados.

---

[47] PINHEIRO, Patrícia Peck. Op cit.

[48] UNCTAD, Conferência das Nações Unidas Sobre Comércio e Desenvolvimento. **Data Protection and Privacy Legislation Worldwide**. 2021. Disponível em: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide. Acesso em: 02 jul. 2022.

De antemão, adianta-se significativa diferença entre os referidos diplomas: o contexto tecnológico de seu surgimento, pois enquanto a LGPD era discutida e aprovada em 2018, o PIPEDA estava em vigor desde os anos 2000 e o *Privacy Act* desde 1983.

III. SOCIEDADE CONECTADA E O MERCADO DE DADOS PESSOAIS

III.1. Por que é relevante termos diplomas protetivos sobre dados pessoais?

Ao longo da história da humanidade diversos foram os modelos e configurações por meio dos quais esta se organizou em sociedade. Ao estudar os primórdios de nossa história, nos deparamos com a sociedade agrícola, na qual a economia era fomentada pelos produtos da agricultura. Anos mais tarde, emerge a chamada sociedade industrial, e o mundo se reorganiza ao redor da produção fabril viabilizada pela eletricidade e pela máquina a vapor. Após a Segunda Guerra Mundial tem-se o advento da sociedade pós-industrial, na qual a prestação de serviços ganha papel de destaque e as relações sociais são remoldadas à luz dessa nova lógica de mercado.[49]

Esse cenário perde espaço para uma nova forma de organização social quando a modernidade passa a ser caracterizada pela facilidade e velocidade com que se processa e transmite grande quantidade de informação. Não por outro motivo, Bruno Ricardo Bioni denomina a sociedade em que hoje se vive de "sociedade da informação", o autor defende que o papel central e adjetivante da informação se justifica por ser este o elemento estruturante que reorganiza a sociedade atual.[50]

Segundo Manuel Castells, conhecimento e informação sempre foram elementos fundamentais ao crescimento econômico, estando presentes em diferentes momentos da história, no entanto, o que hoje se testemunha é um marco de descontinuidade histórica, no qual a informação e, consequentemente, os dados dos indivíduos, deixam de ser elemento acessório do processo de produção e se tornam um produto em si mesmos:

> Com o emergir de um novo paradigma tecnológico, organizado ao redor de novas tecnologias de informação, mais poderosas e mais flexíveis, é possível que a própria informação se torne o produto do processo de produção. Para ser mais preciso: os produtos da nova indústria de tecnologia da informação são aparelhos de processamento de informação ou o processamento de informação em si mesmo.[51]

---

[49] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p 33 - 34.
[50] Ibid.
[51] CASTELLS, Manuel. **The Rise of the Network Society**. 2. ed. Oxford: Blackwell Publishing Ltd, 2010. p 77-78.

Surge, frente a esse cenário, uma economia de vigilância, que posiciona o cidadão como mero expectador do uso de suas informações, um indivíduo quase que absolutamente privado de controle, inserido em uma realidade na qual os dados pessoais "convertem-se em um fator vital para a engrenagem da economia da informação"[52] e os meios de sua captura são variados e multiplicados pela lógica da Internet das Coisas (IoT), do inglês *Internet of Things*.

Ao fazer uma digressão histórica sobre a noção de tecnologia e inovação, Eduardo Magrani vale-se da expressão IoT para descrever a realidade da sociedade atual, onde aparelhos presentes no cotidiano das pessoas, além de em constante conexão com outros dispositivos, têm a capacidade coletar informações e aspectos do mundo ao redor deles, e direcioná-los a bases de dados onde serão processados de forma inteligente. A sigla IoT refere-se, portanto, a "um mundo onde objetos e pessoas, assim como dados e ambientes virtuais, interagem uns com os outros no espaço e no tempo".[53]

Ocorre que conectividade ilimitada se traduz em potencial coleta de informações também ilimitada. Segundo o criador do termo, Kevin Ashton, na lógica do IoT é possível pensarmos no armazenamento de dados que digam respeito, inclusive, ao movimento de nossos corpos, e esses registros podem ser utilizados para fins diversos, desde economia de recursos naturais e energéticos, até facilidades pessoais e de saúde.[54] Apesar de incontestável que objetos inteligentes e interconectados proporcionam vantagens de cunho prático e solucionam problemas reais, não se pode olvidar que essa nova lógica de mercado tem alto potencial nocivo, não apenas para a proteção de dados pessoais, mas também para o direito à privacidade.

A coleta de informações é constante e massificada, bilhões de dados com conteúdo diverso são coletados diariamente, o que permite que se conheça, com extrema precisão, os hábitos, preferências e desejos dos indivíduos, para, então, lhes direcionar conteúdo de interesse. Foi nesse contexto que, percebendo o potencial lucrativo da análise desses dados, o mercado mundial passou a explorar a "personalização e customização automática de conteúdo nas plataformas digitais, inclusive capitalizando essa filtragem com publicidade direcionada por meio de rastreamento de *cookies* e processos de *retargeting* ou mídia programática (*behavioral retargeting*)".[55]

Dito isso, é oportuno ressaltar que não são apenas os dispositivos inteligentes ao nosso redor que constantemente coletam informações a nosso respeito, o mero acesso à internet

---

[52] BIONI, Bruno Ricardo. Op cit. p 39.
[53] MAGRANI, Eduardo. **A Internet das Coisas.** Rio de Janeiro: FGV Editora, 2018. p 44.
[54] Ibid. p 45.
[55] Ibid. p 49.

possibilita a coleta de diversos dados com potencial de comercialização para fins publicitários, nossas pegadas digitais são, portanto, incessantemente rastreadas. Nesse contexto, os dados dos indivíduos ganham grande valor econômico, passando a ser vistos, a todo momento, como um produto a ser negociado pelas empresas que os coletam, e a ser utilizado, como propulsor de vendas, por aquelas que os adquiriram.

No que diz respeito ao uso de dados para fins publicitários, é prudente que se esclareça que publicidade direcionada, de um modo geral, não é uma prática nova e exclusiva da sociedade da informação, não sendo sequer reservada ao mundo digital, estes são, no entanto, atributos de uma de suas espécies: a publicidade comportamental online.[56] A referida estratégia de *marketing*, por sua vez, tem intrínseca relação com a mercantilização de dados pessoais e com a lógica do *Internet of Things*, pois é viabilizada pela análise mercadológica dessa base de dados quase infinita. Sobre o tema, Bruno Ricardo Bioni explica que

> a ciência mercadológica percebeu que a Internet poderia propiciar uma abordagem publicitária mais efetiva. Por meio de diversas ferramentas tecnológicas, dentre as quais se destacam os *cookies*, tornou-se possível rastrear a navegação do usuário e, por conseguinte, inferir seus interesses para correlacioná-los aos anúncios publicitários. Por meio do registro da navegação dos usuários cria-se um rico retrato das suas preferências, personalizando-se o anúncio publicitário. A abordagem publicitária passa a ser atrelada com precisão ao perfil do potencial consumidor. Sabe-se o que ele está lendo, quais os tipos de websites acessados, enfim, tudo aquilo em que a pessoa está efetivamente interessada e, em última análise, o que ela está mais suscetível a consumir com base nesse perfil comportamental. [57]

A descrição de Bioni sobre a forma como tais dados são coletados pode gerar certa estranheza, tendo em vista, principalmente, a invasividade da conduta e o aparente desconhecimento do internauta rastreado quanto ao ocorrido. Dito isso, façamos o seguinte questionamento: "ainda que em momento anterior à entrada em vigor dos diplomas protetivos em matéria de proteção de dados pessoais, tamanho grau de vigilância já não violaria as garantias legais concernentes ao direito à privacidade?"

Tanto Paul Schiff Berman quanto Nicolas Suzor entendem que como consequência da aceitação voluntária dos termos de uso das plataformas, os internautas ficam legalmente vinculados a eles, reduzindo o peso jurídico da lei na relação internauta-plataforma.[58] [59] Berman exemplifica seu entendimento com um exemplo ligado ao contexto norte americano, ressaltando que se os operadores de determinada plataforma quisessem censurar o comentário

---

[56] BIONI, Bruno Ricardo. Op cit. p 42
[57] Ibid. p 43.
[58] BERMAN, Paul Schiff. Cyberspace and the State Action Debate: the cultural value of applying constitutional norms to private regulation. **University Of Colorado Law Review**, v. 71, p. 1263-1310, 23 mai. 2000.
[59] SUZOR, Nicolas. Op cit.

de dado usuário, poderiam fazê-lo simplesmente retirando-lhe o privilégio de acesso à plataforma, independente de o ordenamento jurídico do país resguardar a liberdade de expressão.[60] Similarmente, Suzor pontua que ao aceitar os termos de uso os internautas ficam quase sem qualquer recurso para questionar a forma como as plataformas são regidas.[61]

Contudo, a desproporcional distribuição de poder na relação internauta-plataforma assume desdobramentos ainda mais sérios quando do advento do chamado capitalismo de vigilância, uma consequência quase que natural dos demais elementos que marcam a realidade da sociedade conectada. Além disso, a dinâmica competitiva desse novo mercado faz com que a coleta de dados inclua conteúdos cada vez mais preditivo: voz, características da personalidade e emoções.[62]

Shoshana Zuboff explica que "o capitalismo de vigilância reivindica de maneira unilateral a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais".[63] É dizer, trata-se de um sistema econômico que encontra em uma sociedade hiperconectada, como a atual, terreno fértil para se desenvolver. Na sociedade da informação a comercialização de dados comportamentais, além de extremamente rentável, é facilitada pela lógica do IoT, e o capitalismo de vigilância se aproveita disso, pois por mais que parcela das informações coletadas seja direcionada ao aprimoramento de serviços em favor do próprio titular, uma porção significativa desse produto acaba sendo revertida ao mercado de dados pessoais.

O cidadão, ao se tornar espectador do processo produtivo, é privado de qualquer controle sobre o destino de seus dados, e reduzido ao papel de mera fonte inesgotável de matéria-prima. Ao ressaltar que o capitalismo de vigilância é parasítico e autorreferente, Zuboff explica que ele "revive a velha imagem que Karl Marx desenhou do capitalismo como um vampiro que se alimenta do trabalho, mas agora com uma reviravolta. Em vez do trabalho, o capitalismo de vigilância se alimenta de todo aspecto de toda a experiência humana".[64]

Em atenção aos ensinamentos desse conjunto de autores é evidente que viver na sociedade da informação traduz-se em: estar inserido na hiperconexão, onde tudo conecta todos, e onde a mais ínfimas das ações, se online ou nas proximidades de determinados objetos, ocasiona a coleta de milhares de dados; viver uma realidade essencialmente organizada sob a ótica de que a informação é o combustível que mantém a engrenagem social

---

[60] BERMAN, Paul Schiff. Op cit.
[61] SUZOR, Nicolas. Op cit.
[62] ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância**: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca Ltda, 2021. p 22.
[63] Ibid. p 23.
[64] Ibid. p 24.

em funcionamento e que alimenta a economia; e testemunhar a transformação de dados pessoais em produtos de elevado valor econômico, bem como sua comercialização em larga escala para o fomento de novos mercados, seja por meio do aprimoramento do próprio sistema IoT, seja por meio de uma maior efetividade das estratégias de *marketing*.

É evidente, portanto, que tal cenário impõe consideráveis desafios regulatórios ao arcabouço normativo mundial, em vista a imprescindibilidade de se discutir como direitos básicos humanos estão sendo resguardados nessa nova realidade. Assim sendo, existem, no mínimo, duas razões óbvias para justificar a importância de se regulamentar, extensivamente, como dados pessoais podem ser coletados e tratados. Pensando em um viés econômico, caso se considere que a *Internet of Things* é o próximo grande passo da humanidade em matéria de desenvolvimento tecnológico, é fundamental para seu crescimento que questões relacionadas à segurança, privacidade e proteção de dados estejam bem delimitadas.

Por outro lado, pensando em um viés que se preocupa com a proteção dos direitos humanos, é igualmente essencial garantir ao indivíduo maior controle sobre informações que lhe dizem respeito. Sem instrumentos normativos efetivos, viver em uma sociedade conectada é viver com o risco constante de perder o controle sobre informações pessoais eventualmente veiculadas online, sobre quem são as pessoas com acesso a esses conteúdos e sobre o alcance de tal informação. Legislar sobre proteção de dados pessoais traduz-se, portanto, em diligenciar para que um pouco desse poder retorne ao verdadeiro titular da informação.

IV. PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

Feitas tais considerações, passar-se-á à análise da construção do direito à proteção de dados pessoais no Brasil. Conforme já esclarecido, o principal diploma protetivo do país em matéria de dados pessoais é a chamada Lei Geral de Proteção de Dados, Lei 13.709 de 14 de agosto de 2018. Contudo, para tratar desse direito é necessário regressar ao ano de 1995, vez que, não obstante o atraso normativo, há anos, o Brasil se destaca por suas iniciativas concernentes à governança da Internet, fato que diretamente corroborou para a proteção atualmente conferida aos dados pessoais no país.

Em 1995, enquanto na Europa aprovava-se a Diretiva 95/46/CE e no Canadá estava-se na iminência de anunciar que o país teria uma legislação federal sobre privacidade até os anos 2000, no Brasil criava-se o Comitê Gestor da Internet no Brasil (CGI.br). Apesar de sua abrangente atuação, para além da promoção de medidas de proteção à dados pessoais, o modelo de governança multissetorial da Internet, aplicado pelo CGI.br há 27 anos, foi

essencial para a construção do direito à proteção de dados pessoais no imaginário dos brasileiros. O Comitê não apenas defendia a participação da sociedade civil na tomada de decisão concernente à implementação, administração e uso da Internet, mas também tinha como uma de suas atribuições a proposição de medidas regulatórias relativas à práticas inerentes ao meio ambiente da internet, tal qual é o tratamento de dados e a vigilância digital.[65] [66]

Um dos principais feitos do CGI.br em favor da normatização do direito à proteção de dados pessoais foi a formulação, em 2009, do Decálogo da Internet, um rol de dez princípios[67] imprescindíveis ao bom uso da internet no Brasil, documento que influenciou de maneira decisiva tanto as disposições do Marco Civil da Internet, quanto da Lei Geral de Proteção de Dados.[68] Outra iniciativa de suma importância é a promoção do Seminário de Proteção à Privacidade e aos Dados Pessoais, evento organizado anualmente pelo CBI.br desde 2010, e que, em sua primeira edição, já debatia temas como comércio eletrônico, proteção infanto juvenil, governo eletrônico e ameaças à privacidade na sociedade da informação, comparando a realidade brasileira com exemplos internacionais mais maduros, para assim fomentar o debate sobre potenciais desafios a serem enfrentados nacionalmente. Passados poucos meses do 1º Seminário, sediado na cidade de São Paulo, o Ministério da Justiça tornou público o primeiro anteprojeto do que hoje é a LGPD.[69]

Em matéria normativa, mesmo antes da entrada em vigor da Lei Geral de Proteção de Dados, já existia certa preocupação com a coleta, o armazenamento e o tratamento de dados pessoais, ainda que em menor medida e sob o escopo protetivo do direito à privacidade, contudo, com o advento da IoT e do uso generalizado da internet, problemas preexistentes agravaram-se em proporção e recorrência, tornando os poucos dispositivos legais que

---

[65] GLASER, Hartmut Richard. **Internet Governance in Brazil**: a multistakeholder approach. A multistakeholder approach. 2009. Disponível em: https://www.cgi.br/publicacao/internet-governance-in-brazil-a-multistakeholder-approach/. Acesso em: 06 jul. 2022.

[66] GLASER, Hartmut Richard. **Modelo Brasileiro de Governança da Internet**. 2013. Disponível em: https://www12.senado.leg.br/ecidadania/documentos/anexos/audiencia-cct-governanca-da-internet-20-08-2013/o-modelo-brasileiro-de-governanca-da-internet-cgi.br-hartmut-glaser. Acesso em: 06 jul. 2022.

[67] Merece especial destaque o primeiro desses dez princípios para a governança e uso da Internet no Brasil, princípio da liberdade, privacidade e direitos humanos: "O uso da Internet deve guiar-se pelos princípios de liberdade de expressão, de privacidade do indivíduo e de respeito aos direitos humanos, reconhecendo-os como fundamentais para a preservação de uma sociedade justa e democrática". CGI.BR, Comitê Gestor de Internet no Brasil. **Princípios para a Governança e Uso da Internet**. Disponível em: https://principios.cgi.br/#close. Acesso em: 07 jul. 2022.

[68] CGI.BR, Comitê Gestor de Internet no Brasil. **CBI.br 25 anos de boas práticas**: modelo pioneiro de gestão multissetorial na internet tornou-se referência mundial. São Paulo: Br, 2021. (18 ed).

[69] CGI.BR, Comitê Gestor de Internet no Brasil. **13º Seminário de Proteção à Privacidade e aos Dados Pessoais**. 2022. Disponível em: https://seminarioprivacidade.cgi.br/. Acesso em: 07 jul. 2022.

tratavam sobre proteção de dados pessoais no ordenamento brasileiro evidentemente insuficientes para regular a nova realidade da sociedade da informação.

Dito isso, esclarece-se que assim como ocorreu em âmbito internacional, o direito à proteção de dados pessoais no Brasil, em seu nascimento, esteve associado ao já consolidado direito à privacidade. Apesar de não constar do texto original da Constituição Federal de 1988, muitos autores defendiam que a proteção de dados pessoais deveria ser assegurada por estar englobada no escopo do direito à inviolabilidade da intimidade e da vida privada, disposto no artigo 5º, inciso X da Carta Constitucional. Sua tutela era justificada também pelo fato de estas informações de cunho pessoal - as quais, atualmente, estão englobadas na definição de dados pessoais - estarem intrinsecamente relacionadas aos direitos da personalidade dos internautas, e, por consequência, ao direito à dignidade humana, o qual é fundamento do próprio instituto republicano.[70]

Eduardo Magrani destaca também a previsão do inciso LXXII do artigo 5º da Constituição Federal, o qual prevê o *habeas data* como remédio constitucional apto a assegurar a proteção de informações e dados pessoais quando se objetiva "assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público", ou quando se busca a "retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo".[71]

Consequentemente, muito antes da proposição da LGPD disposições, em leis esparsas, já garantiam certa proteção aos dados pessoais. O Código de Defesa do Consumidor (CDC), Lei 8.078 de 1990, por exemplo, apesar da aplicação restrita às relações consumeristas, já continha previsões relevantes. O artigo 43 do referido diploma, ao tratar sobre o cadastro de consumidores em bancos de dados, assegura ao titular do dado cadastrado o direito de ser comunicado do cadastramento de seus dados pessoais, de acessar informações que lhe digam respeito, bem como de exigir a correção quando verificadas inexatidões.[72]

Magrani destaca que o artigo 6º, inciso II, do mesmo diploma também é previsão com importantes desdobramentos em favor da proteção de dados pessoais, pois tem grande aplicabilidade à *Internet of Things,* vez que estabelece o dever de "informar aos usuários

---

[70] MAGRANI, Eduardo. **Entre Dados e Robôs:** ética e privacidade na era da hiperconectividade. 2. ed. porto Alegre: Arquipélago Editorial, 2019. p 55 - 58.
[71] Ibid. p 86.
[72] BRASIL. **Código de Defesa do Consumidor, Lei nº 8.078.** Brasília, 11 set. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/L8078compilado.htm. Acesso em: 07 jul. 2022.

sobre os possíveis riscos que podem vir a se concretizar com o uso dos dispositivos e sobre as informações que serão coletadas com tal uso".[73]

Não obstante a relevância das disposições do Código de Defesa do Consumidor, o Marco Civil da Internet (MCI), a Lei 12.965 de 2014, tratou do tema de forma ainda mais expressiva, representando uma grande evolução em relação à realidade que imediatamente lhe antecedeu. Em vista a sua pretensão em ser a Constituição brasileira da Internet, o MCI salvaguardou diversos princípios e direitos fundamentais e expressamente tratou do direito à proteção de dados pessoais,[74] assegurando aos usuários, dentre outros:

> Art. 7º: O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: [...]
> VII – o não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
> VIII – informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação; e
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
> IX – consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;[75]

Contudo, por mais significativas que sejam as garantias dispostas no MCI, o diploma peca em certos aspectos, faltam-lhe, por exemplo, definições conceituais fundamentais para a prevenção de abusos e para a efetiva responsabilização pela coleta excessiva ou ilegal de dados. A própria definição do que se poderia entender por "dados pessoais" constou apenas no Decreto nº 8.771, que em 2016 veio regulamentar o MCI.[76]

Percebe-se, portanto, que no Brasil anterior a 2018 a proteção de dados pessoais se construiu de forma gradual e difusa, em pontuais previsões disseminadas pelos mais variados instrumentos normativos. João Alexandre Guimarães e Lecio Machado citam também "o art. 5º, II, V, VI e VII da Lei do Cadastro Positivo; o art. 4º, VII do Decreto do Comércio Eletrônico; o Capítulo IV, Seção V da Lei de Acesso à Informação, entre outras".[77] Contudo, existem questões que apenas podem ser solucionadas se exaustivamente reguladas, de modo que a carência normativa brasileira veio a ser suprida apenas em 2018, quando, após anos de

---

[73] MAGRANI, Eduardo. **Entre Dados e Robôs**. Op cit. p 63 - 64.
[74] Ibid. p 73 - 83.
[75] BRASIL. **Marco Civil da Internet, Lei 12.965**. Op cit.
[76] MAGRANI, Eduardo, **Entre Dados e Robôs**. Op cit. p 73 - 83.
[77] GUIMARÃES, João Alexandre; MACHADO, Lecio. **Comentários à lei geral de proteção de dados**: lei 13.709/2018 com alterações da MPV 869/2020. Rio de Janeiro: Lumen Juris, 2020. p 2.

tramitação e o apensamento de diversos projetos de lei, a Lei Geral de Proteção de Dados foi aprovada no Congresso Nacional.

Tendo em vista a impossibilidade fática de se esgotar o estudo do tema no presente trabalho, tecer-se-á considerações sobre as mais relevantes disposições da Lei 13.709/2018. Dito isso, é oportuno destacar que o parágrafo único do artigo 1º - acrescido pela Lei 13.853/2019 - ao afirmar que as normas contidas na LGPD seriam de interesse nacional, expressamente consigna serem de observância obrigatória pela União, Estados, Distrito Federal e Municípios. É dizer, as regras de tratamento e transmissão de dados pessoais devem também ser pelos entes públicos promovidas e respeitadas.[78]

Relativamente à abrangência territorial da LGPD, por influência de modelos internacionais, estabeleceu-se que a mesma recai sobre todo tratamento de dados realizado no território nacional, independentemente de onde estejam localizados o responsável pelo tratamento e os dados a serem tratados. Além disso, conferiu-se ao diploma brasileiro alcance extraterritorial, pois ainda que realizado fora do Brasil, aplica-se a LGPD ao tratamento em que os dados foram coletados no país ou tenham como titulares pessoas localizadas nele.[79]

De mais a mais, merece especial menção o disposto no artigo 7º, pois nos incisos do referido dispositivo se elencou as dez hipóteses legais nas quais é autorizado o tratamento de dados pessoais, são elas: i) se consentido pelo titular do dado; ii) se para o cumprimento de obrigação legal ou regulatória; iii) se para a execução de políticas públicas previstas em lei; iv) se para a realização de estudos por órgão de pesquisa; v) se necessário para a execução de um contrato; vi) se para o exercício regular de direitos; vii) se para proteger a vida ou a integridade física de alguém; viii) se em favor da tutela da saúde; ix) se, não prevalecendo direitos e liberdades do titular, para atender aos interesses legítimos do controlador ou de terceiro; e x) se para a proteção do crédito.[80]

Consequentemente, desde a entrada em vigor da LGPD, existem apenas dez fundamentos de legalidade para que dados pessoais sejam tratados no Brasil, de modo que se o tratamento de dados não decorrer do consentimento do titular, ele só será legal se necessariamente estiver "associado a uma das dimensões do princípio da proporcionalidade, pois decorre, ou do texto da lei, ou do contrato, ou da necessidade",[81] devendo, impreterivelmente, se dar de maneira proporcional aos fins que o autorizaram.

---

[78] GUIMARÃES, João Alexandre; MACHADO, Lecio. **Comentários à lei geral de proteção de dados.** Op cit. p 7 - 11.
[79] Ibid. p 17 - 19.
[80] BRASIL. **Lei Geral de Proteção de Dados, Lei 13.709**. Op cit.
[81] GUIMARÃES, João Alexandre; MACHADO, Lecio. **Comentários à lei geral de proteção de dados.** Op cit. p 43 - 51.

No que toca ao consentimento, fundamento de legalidade disposto no inciso I do artigo 7º, Bruno Bioni defende tratar-se de elemento cardeal da LGPD. Não obstante ter sido apresentado em patamar de igualdade com os demais incisos, no anteprojeto colocado sob consulta pública em 2010 o mesmo era a única base legal para o tratamento de dados pessoais, hierarquização mantida quando da consulta pública de 2015, na qual os demais incisos do atual artigo 7º foram apresentados como hipóteses em que o consentimento poderia ser dispensado. Por conseguinte, a atual estruturação do dispositivo - na qual todas as bases legais são de igual hierarquia - não é suficiente para retirar do consentimento a característica de principal vetor do tratamento de dados pessoais.[82]

Não por outro motivo, o legislador reservou todo o artigo 8º da LGPD para tratar do consentimento e o adjetivou extensivamente. Para os fins da Lei Geral de Proteção de Dados Pessoais o "consentimento deve ser uma manifestação de vontade livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento".[83] É inquestionável quão significativo foi o avanço advindo da entrada em vigor da LGPD, em especial, relativamente ao controle e à autonomia conferida aos indivíduos sobre o tratamento e a transferência de seus dados pessoais.

Esse novo cenário normativo desencadeou o debate sobre o *status* que o direito à proteção de dados pessoais teria no ordenamento nacional e levou a um dos mais importantes julgamentos da história desse direito no Brasil. Laura Schertel Mendes afirma que, em decorrência do expresso reconhecimento de que a tutela aos dados pessoais seria um direito fundamental, o julgamento do Supremo Tribunal Federal em 2020 é um marco passível de ser comparado com o julgado do Tribunal Constitucional Federal Alemão, *Bundesverfassungsgericht,* em 1983:

> Assim, não é exagero afirmar que o seu significado para o Brasil é comparável ao julgamento da Corte constitucional alemã de 1983 que, de forma pioneira, estabeleceu o conceito de autodeterminação informativa naquele país, posteriormente influenciando e moldando os debates internacionais sobre proteção de dados. Curiosamente, tanto no caso brasileiro como no alemão, debatia-se a coleta realizada por órgãos estatais para a produção de estatística oficial, destacando a necessidade da implementação de medidas concretas para a proteção de direitos

[82] BIONI, Bruno Ricardo. Op cit. p 184 - 187.
[83] GUIMARÃES, João Alexandre; MACHADO, Lecio. **Comentários à lei geral de proteção de dados.** Op cit. p 53.

> fundamentais, independentemente das boas intenções envolvidas e de sua relevante atuação.[84]

O caso, de relatoria da Ministra Rosa Weber, foi apreciado pelo Plenário do Supremo Tribunal Federal em 07 de maio de 2020, e nesta oportunidade, por maioria de 10 votos, confirmou a decisão monocrática da Ministra nas Ações Diretas de Inconstitucionalidade nº 6.387, 6.388, 6.389 e 6.390,[85] "suspendendo a eficácia da Medida Provisória nº 954, que determinava às empresas de telefonia a fornecer ao IBGE os nomes, endereços e telefones de mais de cem milhões de brasileiros".[86] Com o referido julgamento, superava-se o entendimento de que pudessem haver dados pessoais "neutros", não merecedores de tutela legal e atribuía-se ao direito à proteção de dados pessoais o *status* de direito fundamental autônomo, com âmbito de proteção distinto ao do direito à privacidade.[87] [88]

Vejamos a ementa do mencionado julgado:

> EMENTA. MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA Nº 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. FUMUS BONI JURIS. PERICULUM IN MORA. DEFERIMENTO.
>
> 1. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais.
>
> 2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados.
>
> 3. O Regulamento Sanitário Internacional (RSI 2005) adotado no âmbito da Organização Mundial de Saúde exige, quando essencial o tratamento de dados pessoais para a avaliação e o manejo de um risco para a saúde pública, a garantia de que os dados pessoais manipulados sejam "adequados,

---

[84] MENDES, Laura Schertel. **Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais.** Disponível em: https://www.jota.info/opiniao-eanalise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dadospessoais-10052020. Acesso em 20 fev 2022.
[85] Ibid.
[86] SARLET, Ingo Wolfgang. Fundamentos Constitucionais: O Direito Fundamental à proteção de dados. In: BIONI, Bruno *et al*. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. 50.
[87] MENDES, Laura Schertel. Op cit.
[88] SARLET, Ingo Wolfgang. Op cit. p 50.

relevantes e não excessivos em relação a esse propósito" e "conservados apenas pelo tempo necessário." (artigo 45, § 2º, alíneas b e d).

4. Consideradas a necessidade, a adequação e a proporcionalidade da medida, não emerge da Medida Provisória nº 954/2020, nos moldes em que editada, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia.

5. Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP nº 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF), na dimensão substantiva, por não oferecer condições de avaliação quanto à sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades.

6. Ao não apresentar mecanismo técnico ou administrativo apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados, a MP nº 954/2020 descumpre as exigências que exsurgem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros.

7. Mostra-se excessiva a conservação de dados pessoais coletados, pelo ente público, por trinta dias após a decretação do fim da situação de emergência de saúde pública, tempo manifestamente excedente ao estritamente necessário para o atendimento da sua finalidade declarada.

8. Agrava a ausência de garantias de tratamento adequado e seguro dos dados compartilhados a circunstância de que, embora aprovada, ainda não vigora a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), definidora dos critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais. O fragilizado ambiente protetivo impõe cuidadoso escrutínio sobre medidas como a implementada na MP nº 954/2020.

9. O cenário de urgência decorrente da crise sanitária deflagrada pela pandemia global da COVID-19 e a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento não podem ser invocadas como pretextos para justificar investidas visando ao enfraquecimento de direitos e atropelo de garantias fundamentais consagradas na Constituição.

10. Fumus boni juris e periculum in mora demonstrados. Deferimento da medida cautelar para suspender a eficácia da Medida Provisória nº 954/2020, a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel.

11. Medida cautelar referendada.[89]

---

[89] STF - ADI: 6387 DF 0090566-08.2020.1.00.0000, Relator: ROSA WEBER, Data de Julgamento: 07/05/2020, Tribunal Pleno, Data de Publicação: 12/11/2020. Disponível em: https://jurisprudencia.s3.amazonaws.com/STF/attachments/STF_ADI_6387_78611.pdf?AWSAccessKeyId=AKIARMMD5JEAO67SMCVA&Expires=1657389995&Signature=bAbIGAGvhgOSNUcyZt4F4gSKPsU%3D. Acesso em: 09 jul. 2022.

Passados dois anos da emblemática decisão, e do reconhecimento expresso do *status* de direito fundamental autônomo pelo Tribunal Constitucional pátrio, em 10 de fevereiro de 2022, mediante a promulgação da Emenda Constitucional nº 115, o direito à proteção de dados pessoais no Brasil passou a oficialmente compor o rol de direitos fundamentais dispostos no artigo 5º da Constituição Federal: "LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais".[90]

V. PROTEÇÃO DE DADOS PESSOAIS NO CANADÁ

No presente tópico analisar-se-á como se deu a construção do direito à proteção de dados pessoais no Canadá, dito isso, é oportuno que se esclareça que diferentemente do que ocorreu no contexto brasileiro, este estudo se debruçou, principalmente, sobre dois instrumentos normativos distintos, mas que simultaneamente regulam o tratamento de dados pessoais no país, são eles: *Privacy Act*[91] e *Personal Information Protection and Electronic Documents Act.*[92]

A razão para o estudo concomitante de ambas as legislações reside no fato de, apesar do objeto comum, o escopo da proteção conferida por cada uma dessas leis ser distinto, enquanto o *Personal Information Protection and Electronic Documents Act* regulamenta como instituições do setor privado coletam, usam e compartilham informações pessoais para fins comerciais, o *Privacy Act* de 1983 trata da coleta, uso e compartilhamento de dados pessoais pelo governo canadense, bem como assegura aos indivíduos o direito de acessar e, eventualmente, solicitar a correção de dados que estejam em posse deste.[93] Neste ponto a proteção de dados pessoais canadense destoa da brasileira, pois, como visto, o artigo 1º da Lei Geral de Proteção de Dados estende o alcance material da norma tanto para o tratamento conduzido pelo setor privado, quanto para aquele promovido pelo setor público.

No que concerne suas respectivas previsões, o *Privacy Act* de 1983 determina, por exemplo, que entes governamentais apenas poderão coletar dados pessoais se para a execução de algum programa ou atividade pública, e que, em sendo o caso de fazê-lo, além de priorizar a obtenção de tais dados diretamente junto ao seu titular, têm o dever de informar o indivíduo

---

[90] BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988.** Brasília, Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 28 fev. 2022.
[91] CANADÁ. **Privacy Act**. Ottawa, 01 jul. 1983. Disponível em: https://laws-lois.justice.gc.ca/eng/acts/P-21/. Acesso em: 09 jul. 2022.
[92] CANADÁ. **Personal Information Protection And Electronic Documents Act - S.C. 2000, c. 5** Op cit.
[93] OPC, Office of the Privacy Commissioner of Canada. **Summary of privacy laws in Canada**. 2018. Disponível em: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15#heading-0-0-1. Acesso em: 09 jul. 2022.

sobre os fins específicos para os quais suas informações estão sendo coletadas. A obrigatoriedade de tais medidas é afastada apenas se seu atendimento possibilitar que a informação coletada se torne inexata, ou se prejudicar o uso a que teria fim o tratamento. Não obstante a distância temporal de 35 anos, no *Privacy Act* de 1983, assim como na Lei Geral de Proteção de Dados Pessoais, o consentimento assume papel de destaque, tratando-se da primeira hipótese na qual dados pessoais poderiam vir a ser usados para fim diverso daquele que justificou sua coleta.[94]

No mesmo ano, 1983, foi criado o *Office of the Privacy Commissioner of Canada* (OPC), órgão responsável por controlar como agências e departamentos federais tratam dados pessoais, assegurando assim um maior grau de respeito às disposições do *Privacy Act.* Em 2001, a atuação do OPC foi ampliada para englobar também a fiscalização do tratamento de dados regulado pelo PIPEDA.[95]

De mais a mais, o *Personal Information Protection and Electronic Documents Act* também conta com certas particularidades que o diferenciam do diploma brasileiro, sendo a mais marcante o fato de sua vigência não se estender sobre todo o território do Canadá, mas apenas às províncias de Manitoba, New Brunswick, Newfoundland and Labrador, Nova Scotia, Ontario, Prince Edward Island e Saskatchewan, e aos territórios de Northwest Territories, Nunavut e Yukon. Ficando excluído o tratamento de dados pessoais realizado por empresas situadas nas províncias de Alberta, British Columbia e Quebec, salvo se tais dados estiverem cruzando fronteiras provinciais ou nacionais, caso em que aplicar-se-á o PIPEDA independentemente do local da sede do responsável pelo tratamento.[96] O motivo para a não aplicação do PIPEDA nas três províncias citadas é a existência de diplomas provinciais com garantias substancialmente similares àquelas conferidas pela lei federal: o *Personal Information Protection Act* em Alberta e British Columbia, e o *Act Respecting the Protection of Personal Information in the Private Sector* em Quebec.[97]

Pelo mesmo motivo, não obstante a aplicação do PIPEDA em sete províncias e três territórios, naqueles em que há legislação setorial de proteção de dados pessoais substancialmente similar ao PIPEDA, para as disposições concernentes ao setor em questão, aplicar-se-á a lei local. São exemplos: quanto à informações médicas ou relativas à saúde,

---

[94] CANADÁ. **Privacy Act**. Op cit.
[95] OPC, Office of the Privacy Commissioner of Canada. **Who we are**. 2022. Disponível em: https://priv.gc.ca/en/about-the-opc/who-we-are/. Acesso em: 09 jul. 2022.
[96] OPC, Office of the Privacy Commissioner of Canada. **Summary of privacy laws in Canada**. Op cit.
[97] OPC, Office of the Privacy Commissioner of Canada. **Provincial laws that may apply instead of PIPEDA**. 2018. Disponível em: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/prov-pipeda/. Acesso em: 09 jul. 2022.

diplomas protetivos das províncias de Ontario, New Brunswick, Newfoundland and Labrador e Nova Scotia, e quanto à informações empregatícias, diplomas de Alberta e British Columbia.[98] É importante ressaltar que atividades regulamentadas em nível federal também são objeto do PIPEDA, não apenas em relação à dados pessoais de clientes, mas também de funcionários, são exemplos de atividades incluídas nesse rol: o setor de transporte aéreos, de finanças, de transporte interprovincial ou internacional, de telecomunicação, etc.[99]

Não obstante a inquestionável relevância de todas as previsões do *Personal Information Protection and Electronic Documents Act,* merece especial destaque o rol de 10 princípios disposto no Anexo 1 (Schedule 1), *Fair Information Principles*, por se tratar de diretrizes de atendimento obrigatório por todas as empresas regidas pelo PIPEDA, *vide* item 5.1 da lei.[100] Os dez princípios do Código Modelo de Proteção de Informações Pessoais no Canadá traduzem regras básicas concernentes à coleta, uso, compartilhamento e concessão de acesso à informações pessoais por empresas do setor privado, e conferem certo grau de controle aos titulares da informação. Além disso, relativamente ao contexto do tratamento, o PIPEDA declara ser legítimo apenas aqueles cujos fins forem tidos como apropriados às circunstâncias, julgamento este que deve ser feito à luz do princípio da razoabilidade.[101]

De antemão e para nortear tal análise, o OPC elencou uma série de situações que, via de regra, seriam consideradas como inapropriadas pela pessoa razoável: i) coleta, uso e compartilhamento de informações pessoais com fim ilegal; ii) quando ocasionar tratamento injusto, antiético ou discriminatório, em afronta aos direitos humanos; iii) quando os fins do tratamento tiverem o condão de causar significativo dano ao indivíduo; iv) quando o objetivo da publicação da informação for a exigência de pagamento para sua remoção; v) quando envolver a requisição de senha de redes sociais para a avaliação de empregado; e vi) em se tratando de vigilância individual por meio da função de audio e vídeo de dispositivo particular.[102]

Nesta senda, são princípios norteadores da proteção de dados pessoais no Canadá:

a) Responsabilidade: ao tratar dados, toda empresa se torna responsável pelas informações sob sua custódia, sendo obrigatória a designação de uma ou

---

[98] OPC, Office of the Privacy Commissioner of Canada. **Summary of privacy laws in Canada**. Op cit.
[99] OPC, Office Of The Privacy Commissioner Of Canada. **PIPEDA in brief**. 2019. Disponível em: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/. Acesso em: 10 jul. 2022.
[100] CANADÁ. **Personal Information Protection And Electronic Documents Act S.C. 2000, C. 5**. Op cit.
[101] OPC, Office Of The Privacy Commissioner Of Canada. **PIPEDA fair information principles**. 2019. Disponível em: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/. Acesso em: 10 jul. 2022.
[102] Ibid.

mais pessoas para atuarem como responsáveis, nos termos da lei, pelo pleno atendimento das disposições do PIPEDA;

b) Identificação da Finalidade da Coleta: o propósito para o qual dados estão sendo coletados deve estar delimitado, se não antes, até o momento da coleta da informação, não podendo ser estabelecido *a posteriori*. Caso, após a coleta, pretenda-se utilizar os dados coletados para outros fins além do inicialmente identificado, é forçoso que o novo propósito seja identificado antes do tratamento dos dados, e que o titular seja contatado e consinta como o novo uso de seus dados, salvo se o fim for o cumprimento da lei;

c) Consentimento: além de obter o consentimento do titular quanto à coleta, uso e compartilhamento de suas informações, as empresas têm o dever de assegurar que os mesmos tenham pleno conhecimento dos fins para os quais seus dados serão utilizados, assim para que o consentimento tenha "valor" os objetivos do tratamento devem ser declarados de tal forma que o indivíduo possa efetivamente compreender como a informação será utilizada ou divulgada. Ademais, além de prever a possibilidade de o consentimento ser revogado, o PIPEDA expressamente tratou da legítima expectativa do titular do dado, ou seja, uso que legitimamente se espera do contexto da coleta está englobado no consentimento conferido quando desta, mas finalidades diversas não estão.

d) Limitação à Coleta: a coleta de dados não pode se dar de forma indiscriminada, sendo limitada tanto em quantidade, quanto no que concerne ao tipo de informação a ser coletada, pelo que é necessário à finalidade previamente identificada;

e) Limitação ao Uso, Compartilhamento e Retenção: informações pessoais não devem ser utilizadas ou divulgadas para fim diverso daquele identificado quando da coleta, salvo se mediante consentimento do titular ou se exigido por lei. No que tange à retenção, é necessário que se estabeleça procedimentos que indiquem os períodos mínimos e máximos em que informação pode ser armazenada, além disso, informações que não mais sejam necessárias para os fins do tratamento devem ser destruídas, apagadas, ou anonimizadas;

f) Exatidão: é importante que os dados sejam exatos, completos e atualizados, para efetivamente satisfazer à finalidade que motivou sua coleta, no entanto,

o grau de exatidão, completude e atualização varia conforme a finalidade do tratamento, tal previsão objetiva minimizar a possibilidade de informação inadequada ser utilizada na tomada de decisão sobre o indivíduo;

g) Garantias: é dever das empresas reguladas pelo PIPEDA empregar medidas de segurança suficientes para garantir a proteção de dados pessoais sob sua tutela, evitando assim perdas, roubos, e acesso, divulgação, cópia, utilização, ou modificação não autorizada da informação por estas armazenada;
h) Transparência: incumbe às empresas que tratam dados pessoais facilitar o conhecimento de indivíduos quanto aos procedimentos e políticas internas no que concerne a gestão de tal informação;
i) Acesso pelo Titular: quando requerido a todos deve ser assegurado o conhecimento sobre a existência, o uso e o compartilhamento de dados que lhes digam respeito, devendo, inclusive, ser possibilitado o acesso a estas informações, para que o titular possa questionar sua exatidão e completude, bem como requerer eventuais correções.
j) Contestação da Adequação: é necessário que indivíduos tenham meios de questionar o pleno atendimento dos princípios do PIPEDA, direcionando suas reclamações à pessoa designada pela empresa. Em havendo reclamações, é dever da empresa investigar e tomar medidas adequadas à solução de problemas.[103]

Segundo Teresa Scassa, atual *Canada Research Chair in Information Law and Policy* e ex-membro do Comitê Consultivo Externo do *Office of the Privacy Commissioner of Canada,* o diploma dos anos 2000 não foi construído para enfrentar o capitalismo de vigilância e a mercantilização de dados na sociedade da informação. A autora defende que o consentimento informado proposto pelo PIPEDA, embora comumente tido como forma de se preservar a dignidade individual e a autonomia dos titulares de dados, não mais se mostra suficiente aos desafios impostos ao direito à proteção dos dados pessoais, pois com o IoT e a lógica de vigilância em massa esse direito precisa ser visto como possuidor de uma dimensão coletiva e não mais individual. Dito isso, e ponderando que o país precisa de uma abordagem baseada nos direitos humanos, Scassa defende a necessidade de uma reforma legislativa em matéria de proteção de dados pessoais, para que o diploma federal faça mais do que apenas

[103] CANADÁ. **Personal Information Protection And Electronic Documents Act S.C. 2000, C. 5**. Op cit.

"acenar" para o direito à privacidade e aos dados pessoais, enquanto os equilibra com a necessidade de coleta e tratamento para fins comerciais.[104]

Nesta senda, em 16 de junho de 2022,[105] o Ministro da Inovação, Ciência e Indústria, senhor François-Philippe Champagne, apresentou à *House of Commons* o Bill C-27, *Digital Charter Implementation Act of 2022,* o qual, se aprovado, promulgará o *Consumer Privacy Protection Act*, o *Personal Information and Data Protection Tribunal Act* e o *Artificial Intelligence and Data Act*, bem como fará consideráveis alterações em leis já existentes, dentre as quais está o *Personal Information Protection and Electronic Documents Act,* que passará a chamar apenas *Electronic Documents Act*, uma vez que todas as disposições concernentes à proteção de dados pessoais estarão concentradas no *Consumer Privacy Protection Act*.[106]

VI. CONSIDERAÇÕES FINAIS

Em conclusão ao exposto, valiosas são as palavras de Danilo Doneda relativamente à importância de se proteger dados pessoais:

> A proteção de dados pessoais é uma maneira indireta de atingir um objetivo último, que é a proteção da pessoa. Ao estabelecer um regime de obrigações para os responsáveis pelo tratamento de dados, bem como de direitos para os titulares destes, não se está meramente regulando um objeto externo à pessoa, porém uma representação da própria pessoa. Os dados pessoais, por definição, representam algum atributo de uma pessoa identificada ou identificável e, portanto, mantêm uma ligação concreta e viva com a pessoa titular destes dados. [...] Também destas suas características específicas deriva a consideração que, hoje, diversos ordenamentos jurídicos realizam, de que a proteção de dados pessoais é um direito fundamental — uma verdadeira chave para efetivar a liberdade da pessoa nos meandros da Sociedade da Informação.[107]

Frente ao irrefreável desenvolvimento tecnológico, ao uso massificado da internet e à indissociabilidade da sistemática da *Internet of Things* da sociedade da informação, diplomas

---

[104] SCASSA, Teresa. A Human Rights-Based Approach to Data Protection in Canada. In: DUBOIS, Elizabeth; MARTIN-BARITEAU, Florian. **Citizenship in a Connected Canada**: a research and policy agenda. Ottawa: University Of Ottawa Press, 2020.

[105] Em 16 de junho de 2022, o Bill C-27 foi proposto e teve sua primeira leitura na *House of Commons*, para que venha a ser aprovado faz-se necessária a finalização do procedimento nesta casa, bem como sua remessa e apreciação pelo Senado.

[106] CANADÁ. **Bill C-27 - Digital Charter Implementation Act, 2022**. Ottawa, Projeto de Lei ainda para votação na House of Commons. Disponível em: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading. Acesso em: 10 jul. 2022.

[107] BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo:** para além da informação creditícia. Elaboração: Danilo Doneda. Brasília: SDE/DPDC, 2010. In: MAGRANI, Eduardo. **Entre Dados e Robôs:** ética e privacidade na era da hiperconectividade. 2. ed. Porto Alegre: Arquipélago Editorial, 2019. p 57.

protetivos sobre dados pessoais se tornam, cada dia mais, imprescindíveis à efetiva promoção e proteção dos direitos humanos. Além do reconhecimento expresso da relevância do direito à proteção de dados pessoais em diversos países do mundo e no âmbito do sistema universal de proteção da Organização das Nações Unidas, ambos os atores selecionados para o presente estudo apresentam peculiaridades normativas muito interessantes no que concerne à proteção de dados pessoais.

Enquanto no Brasil a proteção de dados pessoais passou a contar com instrumento normativo específico apenas em 2018, o referido direito foi rapidamente reconhecido como um direito autônomo dissociado do direito à privacidade, sendo, inclusive, adicionado ao rol de direitos fundamentais dispostos no artigo 5º da Constituição Federal, em 2022. No Canadá o direito à proteção de dados pessoais não tem previsão específica na *Canadian Charter of Rights and Freedoms* de 1982, mas conta com diplomas que datam de 1983 e dos anos 2000, e que inclusive já foram reconhecidos pelos tribunais pátrios como instrumentos de natureza quasi-constitucional,[108] assim, o país destaca-se por seu pioneirismo, mas é mais drasticamente desafiado pela reorganização social da era da informação.

Nesta senda, não obstante a relevância dos diplomas já aprovados, percebe-se que a proteção de dados pessoais continua em construção em ambos os países, no Brasil a Lei Geral de Proteção de Dados ainda é uma lei muito recente que apenas com o tempo poderá provar a efetividade de suas previsões no que concerne o grau de proteção conferido aos direitos dos indivíduos. Ao passo que no Canadá, o diploma atualmente em vigor está, possivelmente, na iminência de ser atualizado para que uma nova lei, mais protetiva e mais compatível com as necessidades sociais atuais, possa então vigorar.

[108] SCASSA, Teresa. Op cit.

REFERÊNCIAS BIBLIOGRÁFICAS

ALEMANHA. **Bundesdatenschutzgesetz**. Alemanha, Disponível em: https://www.gesetze-im-internet.de/englisch_bdsg/. Acesso em: 24 jun. 2022.

ALEMANHA. Tribunal Constitucional Federal Alemão. Julgamento de 15 de dezembro de 1983 - 1 BvR 209/83. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html. Acesso em: 28 jun. 2022.

AUSTRÁLIA. **Notifiable Data Breaches - Bill 2016**. Canberra, 22 fev. 2017. Disponível em: https://www.legislation.gov.au/Details/C2017A00012. Acesso em: 28 fev. 2022.

BERMAN, Paul Schiff. Cyberspace and the State Action Debate: the cultural value of applying constitutional norms to private regulation. **University Of Colorado Law Review**, v. 71, p. 1263-1310, 23 mai. 2000.

BIEKER, Felix. **The Right to Data Protection**: individual and structural dimensions of data protection in EU law. Berlim: Springer, 2022.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BRASIL. **Código de Defesa do Consumidor, Lei nº 8.078.** Brasília, 11 set. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/L8078compilado.htm. Acesso em: 07 jul. 2022.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 28 fev. 2022.

BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo:** para além da informação creditícia. Elaboração: Danilo Doneda. Brasília: SDE/DPDC, 2010. In: MAGRANI, Eduardo. **Entre Dados e Robôs:** ética e privacidade na era da hiperconectividade. 2. ed. Porto Alegre: Arquipélago Editorial, 2019.

BRASIL. **Lei Geral de Proteção de Dados, Lei 13.709**. Brasília, 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 07 jul. 2022.

BRASIL. **Marco Civil da Internet, Lei 12.965**. Brasília, 23 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 07 jul. 2022.

CALIFÓRNIA. **California Consumer Privacy Act - CCPA**. Sacramento, 28 jun. 2018. Disponível em: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5. Acesso em: 28 fev. 2022.

CANADÁ. **Bill C-27 - Digital Charter Implementation Act, 2022**. Ottawa, Projeto de Lei ainda para votação na House of Commons. Disponível em: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading. Acesso em: 10 jul. 2022.

CANADÁ. **Personal Information Protection And Electronic Documents Act - S.C. 2000, c. 5.** Ottawa, 13 abr. 2000. Disponível em: https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/FullText.html. Acesso em: 28 fev. 2022.

CANADÁ. **Privacy Act**. Ottawa, 01 jul. 1983. Disponível em: https://laws-lois.justice.gc.ca/eng/acts/P-21/. Acesso em: 09 jul. 2022.

CASTELLS, Manuel. **The Rise of the Network Society**. 2. ed. Oxford: Blackwell Publishing Ltd, 2010.

CGI.BR, Comitê Gestor de Internet no Brasil. **13º Seminário de Proteção à Privacidade e aos Dados Pessoais**. 2022. Disponível em: https://seminarioprivacidade.cgi.br/. Acesso em: 07 jul. 2022.

CGI.BR, Comitê Gestor de Internet no Brasil. **CBI.br 25 anos de boas práticas**: modelo pioneiro de gestão multissetorial na internet tornou-se referência mundial. São Paulo: Br, 2021. (18 ed).

CGI.BR, Comitê Gestor de Internet no Brasil. **Princípios para a Governança e Uso da Internet**. Disponível em: https://principios.cgi.br/#close. Acesso em: 07 jul. 2022.

COMISSÃO EUROPEIA. **Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses**. 2012. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46. Acesso em: 01 jul. 2022.

CONSELHO DA EUROPA. **Convenção Europeia dos Direitos do Homem**. Estrasburgo, Disponível em: https://echr.coe.int/documents/convention_por.pdf. Acesso em: 23 jun. 2022.

CONSELHO DA EUROPA. **Convenção nº 108.** Europa. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108. Acesso em: 24 jun. 2022.

DEPARTAMENTO DE JUSTIÇA DOS ESTADOS UNIDOS. **What is FOIA?** Disponível em: https://www.foia.gov/about.html. Acesso em: 23 jun. 2022.

ESPANHA. **Ley Orgánica de Protección de Datos de Carácter Personal**. Madri, 1999. Disponível em: https://boe.es/buscar/doc.php?id=BOE-A-1999-23750. Acesso em: 29 jun. 2022.

EUROPA. Tribunal de Justiça Europeu. Stauder vs. Ulm. Luxemburgo, 12 nov. 1969. Disponível em: https://www.cvce.eu/content/publication/1999/1/1/fafa8ce7-544b-47c0-9cfc-cb142a4c9424/publishable_en.pdf. Acesso em: 01 jul. 2022.

GLASER, Hartmut Richard. **Internet Governance in Brazil**: a multistakeholder approach. A multistakeholder approach. 2009. Disponível em: https://www.cgi.br/publicacao/internet-governance-in-brazil-a-multistakeholder-approach/. Acesso em: 06 jul. 2022.

GLASER, Hartmut Richard. **Modelo Brasileiro de Governança da Internet**. 2013. Disponível em: https://www12.senado.leg.br/ecidadania/documentos/anexos/audiencia-cct-governanca-da-internet-20-08-2013/o-modelo-brasileiro-de-governanca-da-internet-cgi.br-hartmut-glaser. Acesso em: 06 jul. 2022.

GUIMARÃES, João Alexandre; MACHADO, Lecio. **Comentários à lei geral de proteção de dados**: lei 13.709/2018 com alterações da MPV 869/2020. Rio de Janeiro: Lumen Juris, 2020

GUIMARÃES, João Alexandre Silva Alves. **O Regime Jurídico do Direito ao Esquecimento (ou à Desindexação) na União Europeia e a sua Repercussão no Direito Brasileiro**. 2019. 134 f. Dissertação (Mestrado) - Curso de Direito da União Europeia, Universidade do Minho, Braga, Portugal, 2019.

MAGRANI, Eduardo. **A Internet das Coisas.** Rio de Janeiro: FGV Editora, 2018.

MAGRANI, Eduardo. **Entre Dados e Robôs:** ética e privacidade na era da hiperconectividade. 2. ed. porto Alegre: Arquipélago Editorial, 2019.

MENDES, Laura Schertel. **Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais.** Disponível em: https://www.jota.info/opiniao-eanalise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dadospessoais-10052020. Acesso em 20 fev 2022.

NOVA ZELÂNDIA. **Privacy Act of 2020**. Wellington, 30 jun. 2020. Disponível em: https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html#LMS23703. Acesso em 22 jun. 2022.

NÚCLEO DE ESTUDOS INTERNACIONAIS. C**omentários Gerais dos Comitês de Tratados de Direitos Humanos da ONU**. São Paulo: Núcleo de Estudos Internacionais, 2018. Disponível em: https://www.defensoria.sp.def.br/dpesp/repositorio/0/Comentários%20Gerais%20da%20ONU.pdf. Acesso em: 01 mar. 2022

OCDE. **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.** Europa, Disponível em: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Acesso em: 25 jun. 2022.

ONU. **Declaração Universal dos Direitos Humanos**. Assembleia Geral das Nações Unidas, Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 23 jun. 2022.

ONU. **Pacto Internacional de Direitos Civis e Políticos**. Assembleia Geral das Nações Unidas, Disponível em: https://www.unicef.org/brazil/pacto-internacional-sobre-direitos-civis-e-politicos. Acesso em: 30 jun. 2022.

OPC, Office Of The Privacy Commissioner Of Canada. **PIPEDA fair information principles**. 2019. Disponível em: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/. Acesso em: 10 jul. 2022.

OPC, Office Of The Privacy Commissioner Of Canada. **PIPEDA in brief**. 2019. Disponível em: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/. Acesso em: 10 jul. 2022.

OPC, Office of the Privacy Commissioner of Canada. **Provincial laws that may apply instead of PIPEDA**. 2018. Disponível em: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/prov-pipeda/. Acesso em: 09 jul. 2022.

OPC, Office of the Privacy Commissioner of Canada. **Summary of privacy laws in Canada**. 2018. Disponível em: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15#heading-0-0-1. Acesso em: 09 jul. 2022.

OPC, Office of the Privacy Commissioner of Canada. **Who we are**. 2022. Disponível em: https://priv.gc.ca/en/about-the-opc/who-we-are/. Acesso em: 09 jul. 2022.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais:** comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

REINO UNIDO. **Data Protection Act**. Londres, 1984. Disponível em: https://www.legislation.gov.uk/ukpga/1984/35/pdfs/ukpga_19840035_en.pdf. Acesso em: 29 jun. 2022.

SARLET, Ingo Wolfgang. Fundamentos Constitucionais: O Direito Fundamental à proteção de dados. In: BIONI, Bruno *et al*. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

SCASSA, Teresa. A Human Rights-Based Approach to Data Protection in Canada. In: DUBOIS, Elizabeth; MARTIN-BARITEAU, Florian. **Citizenship in a Connected Canada**: a research and policy agenda. Ottawa: University Of Ottawa Press, 2020.

STEPANOVA, Olga; JECHEL, Patricia. **The Privacy, Data Protection and Cybersecurity Law Review: Germany**. 2021. Disponível em: https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/germany#:~:text=Finally%2C%20in%20December%201983%2C%20the%20German%20Federal%20Constitutional,in%20which%20data%20processing%20has%20grown%20more%20important.. Acesso em: 24 jun. 2022.

STF - ADI: 6387 DF 0090566-08.2020.1.00.0000, Relator: ROSA WEBER, Data de Julgamento: 07/05/2020, Tribunal Pleno, Data de Publicação: 12/11/2020. Disponível em: https://jurisprudencia.s3.amazonaws.com/STF/attachments/STF_ADI_6387_78611.pdf?AWSAccessKeyId=AKIARMMD5JEAO67SMCVA&Expires=1657389995&Signature=bAbIGAGvhgOSNUcyZt4F4gSKPsU%3D. Acesso em: 09 jul. 2022.

SUZOR, Nicolas. Digital Constitutionalism: using the rule of law to evaluate the legitimacy of governance by platforms. **Social Media + Society**, [S.I.], v. 4, n. 3, jul. 2018. SAGE Publications.

UNCTAD, Conferência das Nações Unidas Sobre Comércio e Desenvolvimento. **Data Protection and Privacy Legislation Worldwide**. 2021. Disponível em:

https://unctad.org/page/data-protection-and-privacy-legislation-worldwide. Acesso em: 02 jul. 2022.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia**. Nice, França, 07 dez. 2000. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT. Acesso em: 29 jun. 2022.

UNIÃO EUROPEIA. **Diretiva 95/46/CE**. Luxemburgo, 24 out. 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 29 jun. 2022.

UNIÃO EUROPEIA. **Regulamento Geral sobre a Proteção de Dados - 2016/679.** Bruxelas, 27 abr. 2016. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 28 fev. 2022.

WARREN, Samuel D.; BRANDEIS, Louis D.. The Right to Privacy. **Harvard Law Review**, Cambridge, v. 4, n. 5, p. 193-220, 15 dez. 1890. Disponível em: https://www.jstor.org/stable/1321160?seq=1. Acesso em: 23 jun. 2022.

WE ARE SOCIAL. **Digital 2022**: another year of bumper growth. 2022. Disponível em: https://wearesocial.com/uk/blog/2022/01/digital-2022-another-year-of-bumper-growth-2/. Acesso em: 01 mar. 2022.

WORLDOMETER. **Current World Population**. 2022. Conforme as mais recentes estimativas das Organizações das Nações Unidas. Disponível em: http://srv1.worldometers.info/world-population/#. Acesso em: 01 mar. 2022.

ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância**: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca Ltda, 2021.