



UNIVERSIDADE FEDERAL DO CEARÁ
FACULDADE DE DIREITO
DEPARTAMENTO DE DIREITO PÚBLICO
CURSO DE GRADUAÇÃO EM DIREITO

FRANZ MICHEL DE MENESES AGUIAR

**A PROTEÇÃO DE DADOS PESSOAIS NO DIREITO BRASILEIRO: ENTRE
DIREITOS HUMANOS E DIREITOS FUNDAMENTAIS**

FORTALEZA

2023

FRANZ MICHEL DE MENESES AGUIAR

A PROTEÇÃO DE DADOS PESSOAIS NO DIREITO BRASILEIRO: ENTRE
DIREITOS HUMANOS E DIREITOS FUNDAMENTAIS

Monografia apresentada ao Curso de Graduação em Direito da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Bacharel em Direito.

Orientadora: Prof^ª. Dra. Lígia Maria Silva Melo de Casimiro.

FORTALEZA

2023

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

A229p Aguiar, Franz Michel de Meneses.
A proteção de dados pessoais no direito brasileiro : entre direitos humanos e direitos fundamentais /
Franz Michel de Meneses Aguiar. – 2023.
63 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Faculdade de Direito,
Curso de Direito, Fortaleza, 2023.
Orientação: Profa. Dra. Lígia Maria Silva Melo de Casimiro.

1. LGPD. 2. privacidade. 3. proteção de dados pessoais. 4. direitos humanos. 5. direitos fundamentais. I.
Título.

CDD 340

FRANZ MICHEL DE MENESES AGUIAR

A PROTEÇÃO DE DADOS PESSOAIS NO DIREITO BRASILEIRO: ENTRE
DIREITOS HUMANOS E DIREITOS FUNDAMENTAIS

Monografia apresentada ao Curso de
Graduação em Direito da Universidade
Federal do Ceará, como requisito parcial à
obtenção do título de Bacharel em Direito.

Aprovada em: 11/07/2023

BANCA EXAMINADORA

Prof.^a Dra. Lígia Maria Silva Melo de Casimiro.(Orientadora)
Universidade Federal do Ceará (UFC)

Prof.^a Dra. Cynara Monteiro Mariano
Universidade Federal do Ceará (UFC)

Glauber Isaias Pinheiro Dantas
Mestrando em Direito (UFC)

A Deus, minha rocha e fortaleza.

Aos meus pais, pelo apoio amoroso nas
decisões difíceis.

À professora Lígia, por acreditar em mim
quando até eu duvidei.

AGRADECIMENTOS

Aos meus pais, pelo apoio incondicional e pela confiança tal qual a dos marujos de Ulisses ao navegar comigo pelos mares revoltos da vida no cenário pandêmico, rumo ao infinito e além.

À Faculdade de Direito da Universidade Federal do Ceará, por me acolher, propiciar a aquisição do conhecimento e o debate sadio.

À Prof^ª. Dr^ª. Lígia Maria Silva Melo de Casimiro, pela orientação, humanidade e compreensão nos momentos de turbulência, bem como na infinita paciência durante o prolongado tempo de elaboração deste trabalho.

Aos participantes da banca examinadora, Prof^ª. Dr^ª. Cynara Monteiro Mariano e o mestrando Glauber Isaias Pinheiro Dantas pelo tempo, pelas valiosas colaborações e sugestões.

Aos meus amigos e demais entes queridos, por fazer as perguntas que deviam ser feitas, por não fazer as perguntas que não deviam ser feitas, bem como pela renúncia aos momentos e lembranças felizes que poderíamos ter vivido (outros virão, melhores e mais felizes!).

We're an information economy. They teach you that in school. What they don't tell you is that it's impossible to move, to live, to operate at any level without leaving traces, bits, seemingly meaningless fragments of personal information. Fragments that can be retrieved, amplified... (GIBSON, William, *Johnny Mnemonic*, 1981, p. 57)

RESUMO

O presente estudo busca reconstituir a evolução do direito à privacidade e do direito à proteção de dados no direito brasileiro através das principais contribuições acadêmicas, jurisprudenciais e normativas sobre este tema multidisciplinar que envolve normas de direito internacional, princípios e teorias relativas aos direitos humanos e direitos fundamentais, bem como normas previstas nos diplomas constitucionais e infraconstitucionais do Brasil. A pesquisa aqui desenvolvida possui natureza qualitativa, de cunho bibliográfico e documental, examinando literatura acadêmica, documentos públicos como leis, sentenças, acórdãos, recomendações, relatórios de auditoria e notas técnicas, sejam nacionais ou internacionais. Valendo-se deste alicerce, buscamos fazer conexões e concatená-las de modo a estabelecer um fio condutor que auxiliará a compreensão da formação e gradual reconhecimento dos direitos à privacidade e à proteção de dados dentro de um recorte abrangendo direito internacional, direitos humanos e direito constitucional. O propósito deste trabalho é cobrir e desvelar um referencial teórico com o intuito de subsidiar a elaboração de trabalhos futuros sobre tópicos ainda controversos na Lei Geral de Proteção de Dados (LGPD). Ao final do trabalho são sugeridas algumas dentre tais questões pendentes de solução, para alicerçar pesquisas futuras deste ou de outros pesquisadores, concluindo-se pela imprescindibilidade do conhecimento do processo formativo dos direitos aqui estudados de forma a saber de onde partiram e como estão se acomodando na conjuntura social contemporânea.

Palavras-chave: LGPD; privacidade; proteção de dados pessoais; direitos humanos; direitos fundamentais.

ABSTRACT

The present study aims to reconstitute the evolution of the right of privacy and the right of data protection in Brazilian Law through the main academic, jurisprudential and normative contributions about this multidisciplinary theme which involves norms of international law, principles and theories regarding human rights and fundamental rights, as well as the norms prescribed in the Brazilian constitutional and infraconstitutional legislation. The research developed here has qualitative, bibliographic and documental nature, examining academic literature, judicial sentences, court rulings, guidelines, audit reports and technical notes, either national or international. Making use of this foundation, we tried to make connections and put them together in a way to establish a driving force which will help to understand the gradual formation and acknowledgement of the rights of privacy and data protection inside a profile encompassing international legislation, human rights and constitutional law. The purpose of this study is to cover and to reveal a theoretical framework in order to subsidize the elaboration of future works about yet controversial topics regarding Brazilian General Data Protection Law (LGPD). At the end of this work a few of those questions of pending solution are suggested in order to lay the groundwork for future research, from this author or other researchers, concluding about the indispensability of the knowledge regarding the formative process of the rights hereby studied in order to know whence they originated and how they are accommodating in the contemporary social conjuncture.

Keywords: LGPD; privacy; personal data protection; human rights; fundamental rights.

LISTA DE ILUSTRAÇÕES

Figura 1 – Mapa da Legislação sobre Privacidade e Proteção de Dados ao redor do	22
Mundo	

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ADI	Ação Direta de Inconstitucionalidade
ANATEL	Agência Nacional de Telecomunicações
ANPD	Autoridade Nacional de Proteção de Dados
APPI	<i>Act on the Protection of Personal Information</i> (Lei sobre a Proteção de Informações Pessoais do Japão)
CDC	Código de Defesa do Consumidor (Lei n.º. 8.078/1990)
CF 1988	Constituição da República Federativa do Brasil de 1988
CGI.br	Comitê Gestor da Internet no Brasil
CNJ	Conselho Nacional de Justiça
CNMP	Conselho Nacional do Ministério Público
DPO	<i>Data Protection Officer</i>
DUDH	Declaração Universal dos Direitos Humanos
ECA	Estatuto da Criança e do Adolescente (Lei n.º. 8.069/1990)
EDPB	<i>European Data Protection Board</i> (Comitê Europeu para a Proteção de Dados)
ENCCLA	Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro
EUA	Estados Unidos da América (do Norte)
FBI	<i>Federal Bureau of Investigation</i> (Departamento Federal de Investigação dos Estados Unidos)
FEBRABAN	Federação Brasileira de Bancos
GDPR	<i>General Data Protection Regulation</i> (Regulamento Geral de Proteção de Dados Pessoais da União Europeia)
IBGE	Instituto Brasileiro de Geografia e Estatística

IP	<i>Internet Protocol address</i> (endereço do Protocolo de Internet)
LAI	Lei de Acesso à Informação (Lei n°. 12.527/2011)
LGPD	Lei Geral de Proteção de Dados Pessoais (Lei n°. 13.709/2018)
MCI	Marco Civil da Internet (Lei n°. 12.965/2014)
MP	Medida Provisória
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
ONU	Organização das Nações Unidas
PIPEDA	<i>Personal Information Protection and Electronic Documents Act</i> (Lei de Documentos Eletrônicos e Proteção de Informações Pessoais do Canadá)
PL	Projeto de Lei
POPIA	<i>Protection of Personal Information Act</i> (Lei de Proteção de Informações Pessoais da África do Sul)
UNCTAD	<i>United Nations Conference on Trade and Development</i> (Conferência das Nações Unidas sobre o Comércio e o Desenvolvimento)
SAC	Serviço de Atendimento ao Consumidor
SAFARI	<i>Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus</i> (Sistema Automatizado para os Arquivos Administrativos e o Repertório de Indivíduos)
SENACON	Secretaria Nacional do Consumidor
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
TCU	Tribunal de Contas da União
TICs	Tecnologias de Informação e Comunicação

SUMÁRIO

1	INTRODUÇÃO	14
2	LINHAS GERAIS SOBRE O DESENVOLVIMENTO DO DIREITO À PRIVACIDADE NO ÂMBITO INTERNACIONAL	18
3	O DIREITO À PRIVACIDADE NA PERSPECTIVA DOS DIREITOS HUMANOS	27
4	A EVOLUÇÃO DO DIREITO À PROTEÇÃO DE DADOS NO ORDENAMENTO JURÍDICO BRASILEIRO	35
4.1	Elementos afeitos à privacidade na Constituição Federal de 1988 e a proteção de dados como direito fundamental	35
4.2	Previsões correlatas no ordenamento infraconstitucional	38
5	CONSIDERAÇÕES FINAIS	53
	REFERÊNCIAS	56

1 INTRODUÇÃO

A despeito da ênfase que hoje temos no mundo hiperconectado da sociedade da informação e percorrendo uma trajetória rumo à globalização, com o advento de novas tecnologias e expressões como *banco de dados*, *big data*, datificação (ou dataficação), *machine learning* e outras tantas, a relação do ser humano com os dados não é recente e, se é verdade que esta tenha se intensificado com o volume cada vez maior de dados que trafegam pelas redes, também é verdadeiro que esta se estabelece antes mesmo do nascimento, tendo em vista que estamos inseridos em um mundo que nos antecede, no qual há troca de informações desde o ventre materno e que nosso próprio código genético é dotado de carga informacional¹.

Diante desse cenário, a frase célebre atribuída ao matemático e cientista de dados Clive Humby em 2006 de que os dados seriam o novo petróleo² poderia atualmente ser risível, considerando a onipresença do fluxo de dados nas relações entre usuários, empresas e governos; seu potencial incomensurável que beira a infinitude (ao contrário do petróleo, um recurso finito e escasso) e o valor agregado pelos dados em uma economia pautada na informação, como demonstra o fato de que, em 2022, o pódio das companhias mais valiosas do mundo era liderado por gigantes da tecnologia como Apple, Google, Amazon, entre outras³.

Da importância de que estes dados se revestem deflui a necessidade de que sua proteção e a privacidade dos titulares a quem dizem respeito mereçam proteção não apenas no quesito técnico, no sentido de medidas e tecnologias adotadas para tal fim – as quais são imprescindíveis -, mas também que gozem de proteção legal e tutela jurisdicional contra o tratamento de dados ilegítimo e os danos provocados, intencionais ou não, que este tratamento, possa acarretar.

Todavia, o despertar de uma nova consciência sobre a importância de se resguardar a privacidade e a proteção dos dados da pessoa natural (muitas vezes, parte hipossuficiente em uma relação desigual) foi fruto de décadas de debates, formulações teóricas e legislações tanto

-
- 1 CARDOSO, Carlos. **Armazenagem de dados em DNA atinge densidade teórica de 215 petabytes por grama**. Disponível em: <<https://meiobit.com/387476/armazenagem-de-dados-em-dna-atinge-densidade-teorica-de-215-petabytes-por-grama/>>. Acesso em: 01 jul, 2023.
 - 2 KERSHNER, Michael. **Data isn't the new oil - Time is**. Disponível em: <<https://www.forbes.com/sites/theyec/2021/07/15/data-isnt-the-new-oil--time-is/?sh=230cd84d35bb>>. Acesso em: 01 jul, 2023.
 - 3 LARGHI, Natália. **Veja o ranking das empresas mais valiosas do mundo (e saiba quem é a única latino-americana)**. Disponível em: <<https://valorinveste.globo.com/mercados/renda-variavel/empresas/noticia/2022/06/15/veja-o-ranking-das-empresas-mais-valiosas-do-mundo-e-saiba-quem-e-a-unica-latino-americana.ghml>>. Acesso em: 01 jul, 2023.

no âmbito internacional como nacional, de modo que se torna difícil saber onde a questão começa e onde termina.

Uma estipulação categórica do marco inicial do tema seria impossível, visto que possivelmente as primeiras preocupações quanto à privacidade se originem de épocas que antecedem a ciência ou até mesmo o advento da escrita, fazendo com que o estudo recaia em especulações vazias.

Ainda, trata-se de tema multidisciplinar com uma infinidade de cruzamentos entre conjunturas ideológicas, períodos históricos e (im)possibilidades técnicas, tema este em constante desenvolvimento, rápido como as mudanças trazidas pela tecnologia, com a qual hoje se encontra inevitavelmente associado.

Longe de se pretender exaustivo ou definitivo, este estudo pretende tão somente divisar e ressaltar os contornos da formação e gradual reconhecimento dos direitos à privacidade e à proteção de dados da pessoa natural, estabelecendo conexões e concatenando-as de modo a buscar um fio condutor, uma espinha dorsal a partir da qual estes direitos possam ser melhor compreendidos, partindo-se de um recorte delimitado pela legislação e jurisprudência internacional, pela doutrina dos direitos humanos e pelo que estabelece o ordenamento jurídico brasileiro acerca do tema, o qual se enquadra na intersecção entre os campos dos direitos da personalidade, direitos humanos, direitos do consumidor, dos direitos dos particulares perante a Administração Pública e dos direitos da pessoa natural no uso da Internet.

A escolha do tema encontra seu fundamento no fato de que, no Brasil, a matéria atinente à disciplina da privacidade e da proteção de dados pessoais é recente e, apesar da promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD) no ano de 2018, ainda no ano de 2021 pouco se conhecia a respeito⁴, como relatado em pesquisa da Federação Brasileira de Bancos (FEBRABAN) no portal tecnológico Olhar Digital.

Vivemos em um país marcado por desigualdades, que ainda não solucionou problemas como analfabetismo, analfabetismo funcional, exclusão digital e analfabetismo digital. Em que pese o aumento nos índices de acessibilidade à Internet reportado por pesquisa do IBGE no ano passado (logo, referente ao ano de 2021)⁵, muito em decorrência da pandemia do

4 SORRENTINO, Eduardo. **Poucos brasileiros sabem o que é LGPD, aponta pesquisa**. Disponível em: <<https://olhardigital.com.br/2021/08/10/videos/poucos-brasileiros-sabem-o-que-e-lgpd-aponta-pesquisa/>>. Acesso em: 01 jul, 2023.

5 INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. **Internet já é acessível em 90,0% dos domicílios do país em 2021**. Disponível em: <<https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/34954-internet-ja-e-acessivel-em-90-0-dos-domicilios-do-pais-em-2021>>. Acesso em: 01 jul, 2023.

coronavírus, pesquisas mais recentes⁶ como a promovida pelo Comitê Gestor da Internet no Brasil (CGI.br), durante junho a outubro de 2022 com a inclusão de 23.292 domicílios e 20.688 usuários, apontam para um retrocesso (ou, antes, uma reacomodação diante da suspensão das medidas de distanciamento social após a superação da crise pandêmica) desse marcador.

Ainda, referido estudo também traz outras informações relevantes, como a prevalência do uso exclusivo da internet através do celular pelas classes sociais D e E (84%); a baixa adoção de medidas de segurança por parte dos usuários de internet exclusivamente através do celular (33%); a não alteração das configurações de privacidade dos dispositivos, contas e aplicativos de modo a limitar o compartilhamento de dados pessoais (23%). Dos 36 milhões de brasileiros que sequer acessam a Internet, fração significativa possui baixo grau de instrução, são pretos e pardos, pertencem às classes D e E e possuem 60 anos ou mais.

Nesse cenário se evidencia, portanto, que privacidade e proteção de dados não apenas são direitos os quais parte não desprezível da população do Brasil não compreende bem, como muitos sequer possuem conhecimento de sua existência, de modo que se afiguram vulneráveis numa sociedade pautada pela economia da informação.

Mesmo que desconsideremos o fator de vulnerabilidade social a que esses estratos estão expostos, por reputá-los minoritários, de todo modo o cenário de insegurança e ausência de tutela jurídica efetiva persiste, visto que pesquisa recente feita pela agência de consultoria Daryus indica que 80% das empresas no Brasil não estão completamente adequadas à LGPD, 35% estão parcialmente adequadas e 24% em fase de adequação⁷.

Tal conjuntura de insegurança jurídica e inadequação não é exclusiva da iniciativa privada: em junho de 2022, o plenário do Tribunal de Contas da União proferiu o Acórdão TCU n.º 1384/2022, no qual 382 organizações públicas federais, incluindo o próprio Conselho Nacional de Justiça (CNJ) e o Conselho Nacional do Ministério Público (CNMP) foram auditadas no tocante aos requisitos de segurança da informação e adequação à LGPD.

No acórdão constatou-se que à época da auditoria apenas 45% das organizações havia iniciado a identificação e planejamento de medidas necessárias à adequação; 77% ainda não havia identificado as categorias de titulares de dados com os quais mantinha relacionamento; 17% identificaram os processos de negócio nos quais havia atividade de tratamento de dados

6 COMITÊ GESTOR DA INTERNET NO BRASIL. **92 milhões de brasileiros acessam a Internet apenas pelo telefone celular, aponta TIC Domicílios 2022**. Disponível em: <<https://www.cgi.br/noticia/releases/92-milhoes-de-brasileiros-acessam-a-internet- apenas-pelo-telefone-celular-aponta-tic-domicilios-2022/>>. Acesso em: 01 jul, 2023.

7 FEDERAÇÃO BRASILEIRA DE BANCOS. **LGPD está fora da realidade de 80% das empresas no Brasil, diz estudo**. Disponível em: <<https://febrabantech.febraban.org.br/blog/lgpd-esta-fora-da-realidade-de-80-das-empresas-no-brasil-diz-estudo>>. Acesso em: 01 jul, 2023.

personais; 14% identificaram todos os dados pessoais que tratam; 27% identificaram os locais onde os dados eram hospedados (informação importante para avaliar se há tratamento de dados internacional); e apenas 33% das organizações auditadas fizeram a análise de riscos do tratamento dos dados pessoais sob sua guarda.

Desta feita, considerando o enquadramento exposto, reputa-se necessário um maior amadurecimento do debate sobre as questões envolvendo os direitos à privacidade e à proteção de dados, questões as quais buscaremos expandir nas linhas a seguir.

2 LINHAS GERAIS SOBRE O DESENVOLVIMENTO DO DIREITO À PRIVACIDADE NO ÂMBITO INTERNACIONAL

A preocupação com a privacidade e a proteção dos dados pessoais dos indivíduos não se deu de modo súbito e intensivo como decorrência do *General Data Protection Regulation* (GDPR), regulamento europeu que eventualmente inspirou de modo decisivo a edição da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil; antes derivou, acima de tudo, de uma construção histórica que remonta ao ano de 1890, perpassada por discussões jurisprudenciais, inovações legislativas e a influência de fatores econômicos e tecnológicos no tocante ao tema.

Poder-se-ia dizer que o desejo de não se submeter ao escrutínio alheio originou-se desde ou até antes que a linguagem do ser humano houvesse evoluído como uma forma de fofoca e adquirisse um papel relevante para a formação e manutenção de redes de cooperação em grande número (HARARI, 2018, pp. 31-32), atuando como elemento fundante da sociedade como hoje a conhecemos.

Algumas previsões vagas sobre o tema vieram depois em sociedades antigas como a da Grécia e da China, bem como em tribos hebraicas e sociedades iletradas (MOORE JR., 1984, *apud* DONEDA, 2021, p. 113). Em 1361, seria editado o *Justices of the Peace Act*, que configurou um marco concreto do início da proteção da *privacy* no Reino Unido, de acordo com Doneda (2021, p. 113).

No entanto, a problematização das questões afeitas à privacidade, bem como a formulação de seu próprio conceito, veio muito depois, tendo como alguns de seus precursores os escritos de Samuel Warren e Louis Brandeis, notadamente o artigo *The Right to Privacy* (O Direito à Privacidade), publicado nos Estados Unidos em 1890 pela revista *Harvard Law Review*, ao tratar sobre “*the right to be left alone*” (o direito de estar só/ser deixado em paz) no contexto dos impactos causados pelos avanços tecnológicos e a invenção da câmera fotográfica.

A proposição de Warren e Brandeis que descortinava a existência de um princípio geral no *common law*, não expressamente mencionado na Constituição e fundamentado no direito à vida, teve um impacto considerável na produção doutrinária e na jurisprudência americana, porém suas repercussões não se deram de modo imediato e, tampouco, sem resistência ou modificações ao longo das décadas seguintes. Como ilustração de tais modificações, podemos citar, por exemplo, os sucessivos deslocamentos dos fundamentos do *right to privacy*, ora com escólio no direito à vida, ora como parte do direito à propriedade, com base na responsabilidade civil (*tort*) ou, finalmente, passando a ser abordado como

direito pessoal (ZANINI, 2015).

Dentre os casos emblemáticos da época que sedimentaram o arcabouço proposto por Warren e Brandeis, podemos citar o caso *Pavesich v. New England Life Ins Co.* em 1905, no qual Paolo Pavesich teve reconhecida a violação ao seu direito à privacidade, materializada na conduta da *New England Life Insurance Company* em utilizar uma foto de Pavesich, sem o seu consentimento, colocando-o lado a lado com a foto de um homem vestido em andrajos, para promover uma campanha publicitária no ramo de seguros.

A decisão proferida pela Suprema Corte da Geórgia corroborou o entendimento de Warren e Brandeis e passou a ser aplicada como precedente por tribunais de vários outros estados americanos, de tal forma que a oposição ao *right of privacy* se encerrou em meados de 1950 (KAMLAH, 1969, pp. 59-60 *apud* ZANINI, 2015).

Vale mencionar o advento da Declaração Universal dos Direitos Humanos em 1948, que também traz disposições afeitas ao tema, estas constituindo objeto do próximo tópico deste trabalho.

A partir de então, até a década de 1950, as decisões seguintes apenas confirmaram a construção argumentativa de Warren e Brandeis. Com a ausência de conflitos, ocorreu uma estagnação do *right of privacy*, de modo que a falta de provocação acarretou o fato de que o direito não acompanhou os avanços tecnológicos do período (ZANINI, 2015).

Nos anos seguintes, a controvérsia foi retomada com o caso *Olmstead v. United States* acerca de escutas telefônicas feitas sem mandado judicial pelo *Federal Bureau of Investigation* (FBI) contra Roy Olmstead e outros.

No caso em comento, prevaleceu em votação apertada a tese da Suprema Corte dos Estados Unidos no sentido de que não houve violação da Quarta Emenda da Constituição (inviolabilidade da pessoa, da casa, dos documentos e bens contra buscas e apreensões ilegítimas), porquanto a escuta por meios eletrônicos não teria se dado mediante invasão física nem ocorrera a apreensão de objetos tangíveis, razão pela qual não violaria o espírito da Constituição dos Estados Unidos.

Embora no caso *Olmstead v. United States* não figure o reconhecimento de uma interpretação liberal do *right of privacy*, ele é importante na medida em que, em seu voto de dissidência, Louis Brandeis propugnou que a Constituição protegeria os cidadãos “contra qualquer violação injustificada ao *privacy*”, bem como a tutela constitucional não se restringiria apenas ao aspecto material, porém compreenderia também “as crenças, os pensamentos, as emoções e as sensações” (MCWIRTHER, Darien A.; BIBLE, Jon D., 1992, p. 93 *apud* ZANINI, 2015).

A partir daí, os juízes americanos passaram a aplicar o posicionamento de Brandeis quanto ao *right of privacy*, em que pese a Suprema Corte manter ressalvas quanto ao seu *status* constitucional e sua aplicação no contexto de admissão de provas no processo criminal. As discussões posteriores se concentraram na aplicação do *right of privacy* para fins de direitos de imagem em anúncios publicitários, de modo que o sistema de *common law* adotou um modelo dualista de proteção da imagem, composto pelo *right of privacy* e pelo *right of publicity*.

Em 1966, um artigo publicado por Harry Kalven Jr. (1966, p. 02) questionou o enquadramento do *right of privacy* no âmbito da responsabilidade civil (*tort*) do *common law*, valendo-se das contribuições de Warren e Brandeis para defender que a tutela do *right of privacy* por meio do referido instituto seria um equívoco.

Junto com Bloustein (1964, *apud* ZANINI, 2015), buscou-se apontar a confusão feita por aplicadores da legislação de *torts*, acusando-os de vincular o direito à privacidade às antigas instituições jurídicas, contrariando o pensamento de Warren e Brandeis, que propunham no *privacy* uma figura jurídica nova e unitária, fundada na tutela da dignidade e da individualidade humana.

Foi a partir do caso *Griswold v. Connecticut* em 1965, porém, que o direito à privacidade na concepção proposta por Warren e Brandeis passou a ser expressamente reconhecido pela Suprema Corte dos Estados Unidos como portador de feições constitucionais.

O caso dizia respeito a um processo criminal instaurado contra um médico e o diretor do hospital (o senhor Griswold) por violação de lei que declarava ilegal a prescrição ou o aconselhamento referente a medicamentos contraceptivos, sendo o contexto da lide afeito a situação envolvendo o planejamento familiar de um casal. A decisão do tribunal foi no sentido de declarar a lei inconstitucional por violar uma zona de privacidade “criada por diversas garantias constitucionais fundamentais” (SUPREME, 1965).

Os casos seguintes julgados pela Suprema Corte dos Estados Unidos sedimentaram o entendimento de que o *right of privacy* era um direito que encontrava guarida constitucional, seja com fundamento exposto na Quarta Emenda, seja nas “penumbras” de emendas outras (ex. primeira, terceira, quarta, quinta e nona), como assevera Zanini (2015).

Na Europa, as contribuições de Warren e Brandeis inspiraram a Declaração Universal dos Direitos Humanos em 1948 e a Convenção Europeia de Direitos Humanos em 1950, coincidindo o avanço das telecomunicações a partir da década de 70 com a formação da União Europeia em 1993 através do Tratado de Maastricht.

Em 1980, em razão do avanço tecnológico e do aumento das operações de tratamento internacional de dados, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) publicou o documento *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Diretrizes sobre a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais), que visava consolidar a proteção da privacidade, bem como harmonizar a legislação dos estados-membros sobre o tema de modo a não obstruir o livre fluxo de dados através das fronteiras.

Referido documento foi recepcionado e passou a ter o cumprimento exigido pelo Conselho Europeu na Europa após a *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Convenção para a Proteção de Indivíduos acerca do Tratamento Automático de Dados Pessoais), em 1981, então conhecida como *Treaty of Strasbourg* (Tratado de Estrasburgo) e, a partir da entrada em vigor do GDPR em 2018, adotando o nome de Convenção 108+ (FACHINETTI; CAMARGO, 2021).

À medida que o comércio internacional se expandia, a tecnologia se desenvolvia e a necessidade de proteção dos indivíduos aumentava, um novo esforço de harmonização da legislação europeia sobre o tema da privacidade e da proteção de dados pessoais se fez necessário, acarretando a formação da Diretiva 95/46/CE.

Na diretiva destacam-se os Considerandos n.º 07⁸, 08⁹ e 10¹⁰, que tratam da proteção dos direitos e liberdades fundamentais referentes ao tratamento de dados (notadamente o direito à privacidade) e ao livre fluxo de dados entre os Estados-Membros da União Europeia.

A Diretiva 95/46/CE estabelecia, ainda, no seu Considerando n.º 65 e no Artigo 29, a criação de um grupo de trabalho independente com função de aconselhamento e contribuição para a uniformidade da aplicação das regras nacionais dos Estados-Membros referente às disposições da diretiva, grupo este que recebeu o nome de *Article 29 Working Party*.

No entanto, o esforço não logrou pleno êxito, pois um problema surgiu a partir da formulação dos Considerandos n.º 22, 23 e 30, que outorgavam aos Estados-Membros os poderes para editar legislações locais e específicas acerca do tema, de modo que, embora baseadas na diretiva suprarreferida, tais legislações locais traziam disposições diferentes e, por vezes, conflitantes, dificultando portanto o comércio exterior e o fluxo livre de dados entre os Estados-Membros.

8 (7) *Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data [...]*

9 (8) *Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data [...]*

10 (10) *Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy [...]*

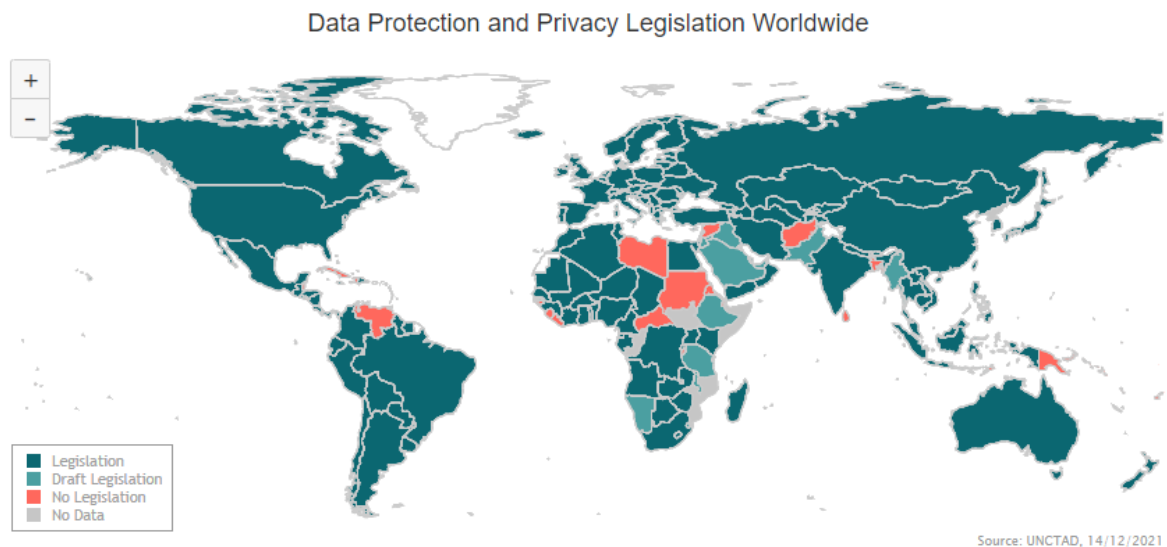
Eventualmente, após anos de negociações para contornar a questão, foi publicado em 25 de maio de 2016 o *General Data Protection Regulation* (GDPR), que se aplicava de modo uniforme a todos os países integrantes do Espaço Econômico Europeu. Com a entrada em vigor do GDPR dois anos depois, em 25 de maio de 2018, a Diretiva 95/46/CE deixou de produzir efeitos, embora o texto da diretiva inspirasse o GDPR. Além disto, o *Article 29 Working Party* também deixou de existir, sendo substituído pelo *European Data Protection Board* (EDPB). No entanto, as orientações produzidas pelo *Article 29 Working Party* permaneceriam sendo consideradas como referências válidas pelo EDPB.

Em que pese a relevância dos Estados Unidos e da União Europeia na construção e no desenvolvimento do direito à privacidade, no tocante à legislação codificada, eles não foram os únicos a editarem leis abordando o tema, podendo ser citados a título de exemplo:

- Canadá: com o *Privacy Act* (1985), acerca do tratamento de informações pessoais pelo governo federal, e o *Personal Information Protection and Electronic Documents Act - PIPEDA* (2000), sobre a proteção das informações pessoais e promoção do comércio eletrônico no âmbito das empresas privadas.
- Japão: com o *Act on the Protection of Personal Information - APPI* (*Act N.º. 57 of 2003*).
- Na América Latina, Argentina, México e Colômbia promulgaram suas leis sobre o tema antes mesmo do regulamento europeu; embora, no caso da Argentina, a legislação datada do ano 2000 necessite de atualizações.
- África do Sul: com o *Protection of Personal Information Act - POPIA* (*Act n.º 04 of 2013*).
- Brasil: com a Lei Geral de Proteção de Dados (LGPD), promulgada em agosto de 2018 e em vigor a partir de 18 de setembro de 2020, notavelmente inspirada pelas disposições contidas no GDPR europeu.

A partir desta construção histórica, doutrinária, jurisprudencial e regulatória, outros países ao redor do globo editaram suas normas relativas à privacidade e proteção dos dados pessoais, de modo que a maioria deles possui legislação própria, consoante figura 01, onde consta o mapa da *United Nations Conference on Trade and Development* (Conferência das Nações Unidas sobre o Comércio e o Desenvolvimento) – UNCTAD:

Figura 01 - Mapa da Legislação sobre Privacidade e Proteção de Dados ao redor do Mundo



Fonte: United Nations Conference on Trade and Development (2021). Disponível em: <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>. Acesso em: 06 jul, 2023.¹¹

No Brasil, um país vinculado à tradição jurídica da *civil law*, os primeiros esboços da noção de privacidade - ainda que não expressamente referida sob este termo - como um valor jurídico a ser protegido partiram de uma interpenetração entre: a) o pensamento liberal, individualista e elitista cujas raízes se inspiraram no constitucionalismo medieval de Locke (COLOMBO, 2017, p. 01) que culminou na abordagem refratária à intervenção estatal orientadora do *right of privacy* norte-americano; e b) o desenvolvimento da doutrina dos direitos da personalidade que se seguiu a partir das contribuições de Otto Von Gierke no fim do século XIX, com fundamento na teoria da personalidade de Immanuel Kant (LUZ SEGUNDO, 2020).

Assim, como decorrência desta influência, verifica-se que a ideia de privacidade ainda não se encontrava desvinculada por completo do direito de ser deixado em paz (*the right to be left alone*), como, por exemplo, se depreende do texto constitucional do Brasil Imperial em 1824, onde o direito à privacidade essencialmente se restringia às garantias de inviolabilidade do domicílio (art. 179, inciso VII) e do sigilo de correspondência (art. 179, inciso XXVII).

Esta tendência persistiu nas constituições brasileiras de 1891 (art. 72, §§ 11 e 18) e no Código Civil de 1916, este marcado por uma forte tendência patrimonialista onde o ser humano é apenas visto como indivíduo e não havia qualquer referência à vida privada, intimidade ou mesmo um capítulo reservado aos direitos de personalidade, como observa

¹¹ UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT. **Data Protection and Privacy Legislation Worldwide**. Disponível em: <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>. Acesso em: 06 jul, 2023.

Colombo (2017, p. 02). Quando muito, o diploma civil de 1916 dispunha sobre a possibilidade de não depor de fatos a que se esteja obrigado a guardar segredo por força de estado ou profissão (art. 144), a prerrogativa de se recorrer ao segredo de justiça em questões de afinidade resultante de relação espúria (art. 184), direito de vizinhança e limitações ao direito de construir (arts. 573, 576 e 577).

A Constituição de 1934 também partiu do mesmo viés em relação às garantias de inviolabilidade do domicílio e o sigilo de correspondência (art. 113, alíneas 8 e 16); porém, para Colombo (2017, p. 03), a carta constitucional se configura como uma síntese do pensamento individual liberalista com o constitucionalismo social pós-Constituição de Weimar e a ascensão de uma corrente em tom corporativo e autoritário no tocante à representação de classes profissionais.

Desta síntese deriva uma maior sofisticação nas questões relacionadas à privacidade, como quando a Constituição de 1934 trata da competência da União para realização do recenseamento geral da população (art. 5º, XVII), da produção de estatísticas de interesse coletivo (art. 5º, alínea 'c'), do estabelecimento de acordos entre a União e os Estados para permuta de informações (art. 9º, caput) e da suspensão das garantias de inviolabilidade do domicílio e correspondência na vigência do estado de sítio (art. 175, alíneas 'c' e 'e'). O diploma constitucional de 1934 também traz controverso dispositivo que incumbe os entes federativos de promover a educação eugênica e a luta contra os venenos sociais (art. 138, alíneas 'b' e 'g'), o que num contexto de intercâmbio de informações entre os entes federativos, suscita problemáticas envolvendo dados sensíveis (saúde, vida sexual, filiação política, credo religioso etc.) e tratamento discriminatório de grupos.

Na Constituição de 1937, durante o período autoritário do Estado Novo, verificou-se um retrocesso, na medida em que os direitos afeitos à privacidade que haviam sido recepcionados nas constituições anteriores, a saber, inviolabilidade do domicílio e da correspondência, foram suprimidos do texto constitucional de 1937, via decreto, no ano de 1942.

Retomando a via democrática, a Constituição de 1946 restabeleceu as garantias fundamentais da inviolabilidade do domicílio (art. 141, §15) e do sigilo da correspondência (art. 141, §6º). Aproximadamente na mesma época, em 1955, a doutrina dos direitos da personalidade ganhou impulso adicional por meio das lições de Pontes de Miranda, que propugnavam pelo reconhecimento de direitos correlatos como a própria personalidade, o direito ao nome, à honra e à identidade pessoal, consubstanciada nos meios para sua identificação, como fichas datiloscópicas, retratos e outros meios, cuja evolução viriam

futuramente a ser as imagens, o correio eletrônico e registros de bancos de dados no mundo virtual (MIRANDA *apud* COLOMBO, 2017, pp. 03-04).

Três anos depois da instauração do Regime Militar de 1964, a Constituição de 1967 manteve, no seu art. 150, §§9º e 10, as garantias de inviolabilidade do domicílio e de sigilo das correspondências, com a inovação de que o parágrafo nono também tratou de incluir o sigilo das comunicações telegráficas e telefônicas.

Posteriormente, a carta constitucional de 1967 foi sucessivamente alterada por 17 atos institucionais, dos quais se destaca o Ato Institucional nº. 5 (AI-5), de 13 de dezembro de 1968, que, dentre outras medidas, suspendeu as garantias de inviolabilidade do domicílio e do sigilo de correspondências e comunicações - medidas tais que se afeiçoam a um estado de polícia e vigilância, em violação frontal à privacidade dos cidadãos.

Seguindo o espírito do período de redemocratização, a inspiração humanista do pós-Segunda Guerra Mundial e as bases do Estado Social, a Constituição Federal de 1988 representou um marco importante em termos de direitos e garantias fundamentais fundados na dignidade da pessoa humana, incluindo a privacidade e a proteção de dados, em cujo exame específico nos debruçaremos em tópico apartado.

Em que pese este avanço, o tema atinente à privacidade ainda não encontrava aceitação na doutrina e na jurisprudência em razão da carência de uma definição quanto ao que se entende por privacidade, uma vez que os países de *common law* e *civil law* percorreram caminhos diferentes antes que se verificasse uma tendência recente de unificação do conteúdo da expressão, como aduz Danilo Doneda (2021, p. 101).

A despeito da acepção tomada nos primórdios, fato é que a privacidade se distanciou do seu formato individualista como manifestação do dever estatal de abstenção do escrutínio do indivíduo e passou a assumir feições coletivas que se revelam na conotação política do controle sobre o indivíduo, a autodeterminação informativa dos cidadãos, o imperativo da não-discriminação de minorias e, de modo mais contundente, pela interdependência da tutela da privacidade com o livre desenvolvimento da personalidade, da cidadania e o princípio da dignidade da pessoa humana (DONEDA, 2021, p. 46).

Nessa toada, arremata o autor que a definição de privacidade já não importa tanto quanto o que dela se espera:

Mas o problema reside menos na definição em si do que em determinar o que se espera dessa definição. O contexto em que se tenta definir a privacidade não raro é reduzido a uma perspectiva epistemológica eminentemente conceitual, que visa (por vezes sem a consciência disso), em primeiro lugar, à coesão do sistema, operando precisamente através de um processo de generalização do qual a individuação de um

conceito dogmático é seu ápice. Vale o alerta de Pietro Perlingieri, de que ‘o perigo é grave: a ciência do direito elaborada sobre o geral torna-se abstrata; o jurista não vai mais ao particular da vida e da experiência, e seus livros nascem predominantemente a partir da reflexão sobre outros livros’. (DONEDA, 2021, p. 102)

Acrescente-se a esta problemática acerca da difícil consolidação de um conceito para privacidade o fato de que se trata de um conceito mutável, em dependência estrita e direta do nível tecnológico de uma determinada sociedade, como bem assevera Rony Vainzof (*apud* MALDONADO; BLUM, 2019, p. 25).

Para Marcel Leonardi, valendo-se da definição de Alan Westin, o caráter essencial da privacidade está na autodeterminação informativa, isto é, “a capacidade de o indivíduo controlar a circulação de informações a seu respeito” (LEONARDI *apud* MALDONADO; BLUM, 2019, p. 26). Citando as contribuições de Marcel Leonardi, Pascoal (2017) aduz que a privacidade se reveste de um conjunto de conceitos unitários (direito a ser deixado só, resguardo contra interferências alheias, segredo ou sigilo e autodeterminação informativa) que constituem facetas de um mesmo prisma, demandando um conceito plural de privacidade, que já vem sendo aceito pela doutrina e jurisprudência.

Cumprindo observar, porém, que a despeito desta expansão do conceito de privacidade e sua abordagem ao longo das constituições e normas infraconstitucionais, o vocábulo privacidade só veio a ser expressamente referido no art. 2º, inciso VIII, da Lei n.º 7.232, de 29 de outubro de 1984, bem como no art. 3º, inciso II, da Lei 12.965, de 23 de abril de 2014, esta última também conhecida como Marco Civil da Internet (MCI).

O MCI também expressamente reconheceu o correlato direito à proteção dos dados pessoais, que passou a constituir disciplina própria derivada da noção de privacidade, de significado mais restrito, intuitivo e menos controverso, além de requisito essencial para a tutela da privacidade, na medida em que esta não existe se os dados pessoais não forem tidos como merecedores de proteção, seja técnica ou jurídica.

Dentre os casos emblemáticos que alçaram a proteção de dados à categoria de direito individual correlato ao direito à privacidade, além da própria referência constante no Marco Civil da Internet, Doneda (2021, pp. 163-176) cita os casos da central de informações *National Data Center* nos EUA, do sistema *SAFARI* na França e da lei do censo alemão em 1982, que fortaleceram as bandeiras da dignidade, da proteção à personalidade, da autodeterminação informativa e da liberdade informática, que continuam a “raiz do pensamento que veio posteriormente a despontar no instituto brasileiro do Habeas Data” (DONEDA, 2021, p. 174).

3. O DIREITO À PRIVACIDADE NA PERSPECTIVA DOS DIREITOS HUMANOS

É cediço que, com a superação dos modelos de Estado absolutista e liberal e os horrores vivenciados no período da Segunda Guerra Mundial, um novo capítulo foi inaugurado no direito, com a ascensão do Estado Social, a revalorização das Constituições como ponto basilar de todo o ordenamento e um resgate do valor intrínseco da pessoa humana, que passou a ocupar uma posição central nos principais ordenamentos jurídicos ao redor do mundo.

Longe de significar um retorno às correntes jusnaturalistas, o resgate valorativo da dignidade da pessoa humana ocorrido no período pós-guerra reformulou as bases do positivismo tradicional através da incorporação de valores e princípios a orientarem o direito positivo, assentados em uma posição superior na hierarquia das normas, até mesmo acima da lei positivada e do poder estatal.

Com o pós-positivismo, os valores e princípios passaram a constituir o alicerce dos novos sistemas constitucionais, sendo alçados ao status de normas jurídicas dotadas de eficácia, a despeito de seu conteúdo abstrato que, não obstante, reclamam como fundamentação o tratamento de todos os seres humanos com igual consideração, respeito e dignidade (MARMELSTEIN, 2011, pp. 11-12), irrigando e orientando todo o ordenamento jurídico, constitucional e infraconstitucional.

A primazia da dignidade da pessoa humana, com base no pensamento kantiano, ao estabelecer que todo ser humano deve ser visto como um fim em si mesmo, além de tratar da igualdade essencial de todas as pessoas, implica aos particulares o dever recíproco de favorecer, na medida do possível, o fim de outrem como se fosse os de si mesmo (COMPARATO, 2008, pp. 22-23); e, ao Estado, a proibição de utilizar-se das pessoas como simples meio para o alcance de certos propósitos, além da obrigação de sempre buscar o bem comum e fornecer condições para o livre e digno desenvolvimento da personalidade e da cidadania (GUERRA, 2020, p. 428). A igualdade meramente formal e abstrata proposta pelo Estado liberal já não era capaz de satisfazer a fome das sociedades por igualdade substancial, por respeito e condições dignas de vida para participação na cidadania. Nas palavras de Paulo Bonavides (2013, p. 392), a “igualdade material faz livres aqueles que a liberdade do Estado de Direito da burguesia fizera paradoxalmente súditos”.

A experiência da guerra e as barbaridades cometidas por Estados autoritários e totalitários ao redor do globo revelaram a insuficiência da tutela da pessoa humana meramente no âmbito do direito interno, ensejando um fenômeno de internacionalização dos direitos

humanos, a fundação da Organização das Nações Unidas (ONU) em 1945 e a aprovação da Declaração Universal dos Direitos Humanos (DUDH) em 10 de dezembro de 1948, que remetia ao ideário tripartite (liberdade, igualdade e fraternidade) da Revolução Francesa e, segundo Fábio Comparato (2008, p. 57), configurou-se marco da internacionalização dos direitos humanos, consagrando não apenas os direitos individuais, civis, políticos, econômicos e sociais, mas também afirmando os direitos dos povos e os direitos das humanidades.

No tocante aos temas da privacidade e da proteção de dados pessoais, o texto da Declaração Universal dos Direitos Humanos expressa, no seu art. 12, os direitos humanos à inviolabilidade de intromissões arbitrárias na vida privada e na família, ao sigilo de correspondência e à proteção contra ataques à honra e à reputação. Do exame do referido artigo, é possível traçar considerações acerca da influência, do objeto e do alcance temporal de suas disposições.

Quanto às influências, seu núcleo epistemológico estava associado à teoria dos círculos concêntricos de Heinrich Hubmann e Heinrich Henkel (porém veio posteriormente a transcendê-la) para distinguir a esfera pública da esfera privada do indivíduo.

Até este ponto, a noção de privacidade estava mais alinhada com o direito de ser deixado em paz ou o *right of privacy* de Warren e Brandeis, ainda impregnada com resquícios do viés individualista da burguesia liberal.

As implicações do direito à privacidade e à proteção dos dados pessoais a nível coletivo e no desenvolvimento da cidadania só viriam a ser percebidas posteriormente, com o crescimento vertiginoso da tecnologia e a transição do modelo econômico industrial para o modelo fundado na economia da informação.

Em relação ao objeto, na mesma esteira do raciocínio supra, o caráter inicialmente individualista do direito à privacidade denotava, a princípio, uma preocupação muito maior com a limitação do poder estatal, ou seja, dizia respeito principalmente a uma abstenção (liberdade negativa) do Estado, contrapondo-se aos direitos sociais ou direitos humanos de segunda geração na medida em que estes demandam uma prestação (liberdade positiva). No entanto, até mesmo em razão do nível tecnológico da época, não se cogitava de que entidades privadas viessem, futuramente, a se tornar tão capazes de violar a privacidade e outros direitos fundamentais dos cidadãos como qualquer governo, perplexidade tal externada por Canotilho (2008, pp. 85-86).

Segundo Doneda (2021, p. 35) o descompasso entre o volume de informações (e dados pessoais, por via de consequência) processados pelo Estado e aquele por entes privados devia-se principalmente em virtude do fato de que, considerando os altos custos, tal atividade

não se apresentava interessante às empresas.

A situação só se modificou quando os custos de aquisição de tecnologia baratearam de modo a torná-la acessível e a tecnologia proporcionou uma vasta gama de novas possibilidades de uso das informações e de auferimento de lucro jamais imaginadas.

Sobre o alcance temporal do disposto no art. 12 da DUDH, verifica-se portanto que, no que toca à privacidade e à proteção dos dados pessoais, a tutela conferida à privacidade da pessoa humana no referido diploma padece de um anacronismo, na medida em que a ideia de privacidade ali estabelecida remetia ao paradigma burguês, liberal e individualista do passado; além do que, a própria noção de privacidade se transmudou a partir dali. É que os direitos fundamentais não são imutáveis nem podem ser compreendidos de forma estanque, senão através da dinâmica social ao longo do tempo, estando “sujeitos a saltos evolutivos e tropeções históricos, já que acompanham a evolução cultural da própria sociedade” (MARMELSTEIN, 2011, p. 41).

Um exemplo deste anacronismo é o que sucedeu com o sigilo de correspondência, que não compreendia -pelo menos expressamente- o sigilo das telecomunicações, a despeito de o telefone ter sido inventado há quase meio século. A despeito disso, o sigilo de correspondência não só estava associado à privacidade do ponto de vista do desenvolvimento da personalidade e da proteção da esfera íntima, mas também viria a ser um dos núcleos essenciais da autodeterminação comunicativa (CANOTILHO, 2008, p. 162). Tal autodeterminação comunicativa viria a ser precursora da novel autodeterminação informativa e mesmo da proteção de dados, ambas atualmente tão em voga com o advento da sociedade da informação.

Não obstante tal anacronismo, a guinada axiológica em prol dos valores humanistas decorrente do período pós-guerra, ao lançar as bases de um Estado de bem-estar social (*welfare state*), promoveu uma mudança no relacionamento entre cidadãos e Estado e um aumento na demanda por direitos sociais e trabalhistas, gradativamente operando uma “juridificação da vida cotidiana” que, mais tarde, com o crescimento do fluxo informacional e da importância da informação para o indivíduo, para os negócios e para a cidadania, representou uma fâsca para um despertar de consciência em relação ao direito à privacidade:

“Praticamente não havia lugar para a tutela jurídica da privacidade em sociedades nas quais as condutas humanas estavam condicionadas a outra ordem de mecanismos - fosse uma rígida hierarquia social ou então uma determinada arquitetura de espaços públicos e privados; fosse porque eventuais pretensões a esse respeito fossem neutralizadas por um ordenamento jurídico de caráter corporativo e patrimonialista; fosse, então, em determinadas sociedades nas quais a privacidade representasse não mais que um sentimento subjetivo que não poderia nem deveria

ser tutelado. O despertar do direito para a privacidade ocorreu justamente num período em que muda a percepção da pessoa humana pelo ordenamento e ao qual se seguiu a juridificação de vários aspectos de sua vida cotidiana.” (DONEDA, 2021, p. 30)

Este prenúncio na mudança do escopo da privacidade não se deu da noite para o dia, contudo, perfazendo um longo e inacabado percurso de expansão do seu conceito, aos poucos atravessando as múltiplas dimensões dos direitos humanos até assumir as feições hodiernas.

Durante esse percurso, a Convenção para a proteção dos Direitos do Homem e das Liberdades Fundamentais, também conhecida como Convenção Europeia de Direitos Humanos, foi assinada em 04 de novembro de 1953 e se tornou o primeiro instrumento a dar efetividade a certos direitos constantes na Declaração Universal de Direitos Humanos e torná-los vinculantes no âmbito dos países constituintes da comunidade europeia. No tocante aos temas da privacidade e da proteção de dados, porém, pouco contribuiu, limitando-se a reafirmar, no seu art. 8º, o respeito à vida privada e familiar, a inviolabilidade do domicílio e o sigilo de correspondência, presentes no art. 12 da DUDH.

Um hiato de quase vinte anos se seguiu a partir da Declaração Universal de Direitos Humanos, conforme relata André de Carvalho Ramos (2021, p. 410), em virtude da Guerra Fria. Para o autor, a DUDH consistia em um instrumento preliminar que visava a formação de um tratado internacional de direitos humanos, de modo a vincular todos os países signatários. No entanto, o intento foi postergado para o ano de 1966, em virtude de desacordo de agenda entre os países que integravam os blocos capitalista e comunista (além de países africanos), onde os primeiros insistiam em reconhecer apenas as liberdades individuais clássicas de cunho liberal e os últimos enfatizavam os direitos sociais e econômicos com políticas de apoio a grupos desfavorecidos, deixando um pouco de lado as liberdades individuais (COMPARATO, 2008, p. 280).

Assim, em 1966, foram aprovados dois pactos internacionais, sendo o primeiro referente aos direitos civis e políticos e o segundo acerca dos direitos sociais, econômicos e culturais. Em matéria de privacidade, o Pacto Internacional sobre Direitos Civis e Políticos de igual modo não trazia muito que não fosse a reafirmação dos direitos contidos no art. 12 da Declaração Universal de Direitos Humanos e no art. 8º da Convenção Europeia de Direitos Humanos, insculpida em seu art. 17, tendo caráter vinculante para os países signatários, dos quais o Brasil faz parte. Cabe observar que o Brasil só aprovou o diploma em 12 de dezembro de 1991, portanto, depois da instauração do regime militar e do processo de redemocratização que culminou na promulgação da Constituição de 1988. Eventualmente, o referido pacto foi incorporado às normas de direito interno brasileiro por força do Decreto nº 592, de 6 de julho

de 1992.

No âmbito das Américas, tivemos a Convenção Americana de Direitos Humanos ou Pacto de São José da Costa Rica, aprovada em 22 de novembro de 1969 com a reprodução de maior parte das declarações de direitos no Pacto Internacional sobre Direitos Civis e Políticos de 1966, a princípio deixando de fora o Pacto sobre Direitos Sociais, Econômicos e Culturais, a fim de se obter a adesão dos EUA (COMPARATO, 2008, p. 367). Quanto à questão da privacidade, a Convenção Americana de Direitos Humanos teve essencialmente o conteúdo do Pacto Internacional sobre Direitos Civis e Políticos de 1966, limitando-se a dispor sobre a proteção à vida privada e familiar, à inviolabilidade do domicílio e ao sigilo de correspondência, constante no art. 11, inciso II. Além disto, no artigo 14, continha previsão acerca do direito de resposta e retificação de informações inexatas divulgadas ao público. À semelhança do que ocorreu com o pacto sobre direitos civis e políticos, o diploma só foi recepcionado no Brasil em novembro de 1992, através do Decreto n.º. 678/1992, portanto, após o regime militar e a redemocratização do país. Em que pese o tardar, os direitos humanos constantes no Pacto de São José da Costa Rica, uma vez recepcionados no ordenamento jurídico brasileiro, possuem sua efetividade assegurada “graças a uma sentença internacional irrecorrível, que deve ser implementada pelo Estado brasileiro”, nos termos do art. 68.1 do Pacto (RAMOS, 2021, p.122).

Com a consolidação do Estado de bem-estar social, o poder público passou a necessitar de mais e mais dados pessoais dos cidadãos de forma a promover uma administração racional de recursos e políticas públicas.

No entanto, soluções tecnocratas aplicadas ao planejamento administrativo por vezes atropelavam - ainda que com boas intenções, em alguns casos - a privacidade dos cidadãos, fortalecendo mais e mais a consciência de que a privacidade possuía uma dimensão coletiva, que não vinha sendo tutelada a contento pelo paradigma individualista de outrora e que demandava uma proteção diferenciada.

O clamor e a repercussão de casos como o do *National Data Center*, ocorrido nos EUA em 1965 e do projeto *SAFARI*, na França de 1974, ressaltaram a inadequação do conceito clássico de privacidade perante o aumento exponencial do tráfego de informações pessoais, levando a uma sofisticação deste direito e fazendo surgir a demanda por um direito à proteção de dados pessoais, consectário da privacidade e menos vago que ela, motivando na década de 70 o surgimento da primeira geração de legislações de proteção de dados pessoais, como a Lei do *Land* alemão de Hesse, em 1970; o *Datalag* sueco de 1973 e o *Privacy Act* norte-americano de 1974, que logo vieram a ser ultrapassadas em razão da falta de

experiência com as tecnologias, da proliferação de centros de processamentos de dados e da rápida evolução tecnológica (DONEDA, 2021, p. 179-181), além de gerar uma fragmentação normativa que só tenderia à uniformização em tempos recentes.

Em 1980, o estreitamento das comunicações e o volume no fluxo de dados entre as fronteiras dos países europeus fez com que a OCDE publicasse um conjunto de orientações sobre a proteção da privacidade e o fluxo transfronteiriço de dados, como referido no tópico anterior. Importa chamar a atenção, porém, para a expressa preocupação com as questões relativas aos grandes volumes de dados pessoais processados, à necessidade de harmonização da disparidade nas legislações de proteção de dados, aos constantes avanços tecnológicos e à prevenção de violações de direitos humanos fundamentais decorrentes do tratamento ilegítimo de dados, como consta no prefácio das *guidelines*. Referido documento lançaria as bases para a Diretiva 95/46/CE, e para o *General Data Protection Regulation* (GDPR) europeu, no qual a Lei Geral de Proteção de Dados Pessoais (LGPD) viria a se inspirar depois, inclusive em relação às terminologias e conceitos utilizados.

No ano seguinte, o Conselho da Europa produziu um documento de força vinculante chamado *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Convenção para a Proteção de Indivíduos a respeito do Tratamento Automatizado de Dados Pessoais), também chamado de Tratado de Estrasburgo ou também Convenção 108+, com vistas a estabelecer parâmetros de proteção contra abusos decorrentes do tratamento ilegítimo de dados pessoais e harmonizar esta necessidade com a regulamentação do tratamento internacional de dados.

Em relação a esta convenção, Danilo Doneda (2021, pp. 200-201) ressalta três pontos importantes em relação às normas e orientações que a precederam: o primeiro, no sentido de que ela foi pioneira para a construção de um sistema integrado europeu de proteção de dados pessoais; o segundo, de que sua perspectiva universalista admitia a adesão de países que não faziam parte do Conselho da Europa; por fim, e de modo fundamental, a convenção consistia em uma declaração expressa de que o Conselho da Europa compreendia a proteção de dados como um tema de direitos humanos.

Em 07 de dezembro de 2000, o Parlamento Europeu, o Conselho da União Europeia e a Comissão Europeia promulgaram conjuntamente a Carta de Direitos Fundamentais da União Europeia, incluindo a principiologia estabelecida na Corte Europeia de Direitos Humanos para alçar tanto o direito à privacidade como o direito à proteção de dados ao patamar de direitos fundamentais, consoante disposto nos arts. 07º e 08º:

Artigo 7.o

Respeito pela vida privada e familiar

Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.

Artigo 8.o

Proteção de dados pessoais

1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito.
2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação.
3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente (PARLAMENTO..., 2000).

A Diretiva 95/46/CE, de novembro de 1995, editada pelo Conselho da Europa reitera o compromisso com estes direitos fundamentais já nos seus Considerandos, fixando uma terminologia básica e vinculando a coleta e tratamento de dados pessoais a um conjunto de princípios, que deverão ser incluídos na legislação dos Estados-Membros, juntamente com uma série de limites e exceções ao tratamento de dados pessoais, sendo aplicáveis tanto ao setor público como ao privado (DONEDA, 2021, p. 205). A Diretiva 95/46/CE permaneceu em vigor até 25 de maio de 2018, cessando de produzir efeitos nesta data em virtude dos problemas de harmonização das normas fragmentárias e díspares produzidas pelos Estados-Membros mencionados no tópico anterior.

Assumiu o seu lugar o Regulamento Geral de Proteção de Dados (GDPR), aperfeiçoando a diretiva, estabelecendo o *European Data Protection Board* em substituição ao *Article 29 Working Party* como órgão consultivo e modificando o escopo espacial da tutela da privacidade e da proteção de dados para abranger diretamente todos os países da comunidade europeia, a despeito da incorporação do regulamento às normas de direito interno de cada país integrante.

Ao cabo de toda esta apreciação do tema sob o prisma dos direitos humanos, verifica-se que, com o reconhecimento tanto da privacidade como da proteção de dados simultaneamente como direitos humanos e fundamentais, no que concerne ao tema deste trabalho, perde a relevância a distinção terminológica clássica entre direitos humanos e direitos fundamentais.

Tal distinção é postulada pela doutrina jurídica germânica, segundo a qual os direitos humanos seriam valores positivados na esfera do direito internacional enquanto direitos

fundamentais seriam os direitos humanos reconhecidos no plano do direito interno e positivados nas Constituições.

Dentre adeptos da corrente pela distinção das duas expressões, podemos citar na doutrina luminares como Fábio Konder Comparato (2008, p. 58) e George Marmelstein (2011, p. 27); ao passo que também há aqueles que defendem que tal distinção hoje resta superada, como André de Carvalho Ramos (2021, pp. 122-123), posição esta última, para os fins deste trabalho, à qual nos filiamos. Como veremos no tópico a seguir, este é o posicionamento que também creditamos estar filiada a Constituição da República Federativa do Brasil de 1988.

4 EVOLUÇÃO DO DIREITO À PROTEÇÃO DE DADOS NO ORDENAMENTO JURÍDICO BRASILEIRO

4.1 Elementos afeitos à privacidade na Constituição Federal de 1988 e a proteção de dados como direito fundamental

Em matéria de privacidade, a Constituição Federal de 1988 representa um esforço na harmonização ética complementar à evolução tecnológica propugnada por Fábio Konder Comparato e com base nos direitos humanos como fator de fortalecimento da “comunhão universal humana” (COMPARATO, 2008, p. 39).

A princípio, o texto constitucional homenageou o direito à privacidade através das garantias individuais de inviolabilidade da intimidade e da vida privada (art. 5º, inciso X), do domicílio (art. 5º, XI), do sigilo de correspondência (art. 5º, XII), bem como outros direitos em relação dialética com o fenômeno da informação, como a livre manifestação do pensamento (art. 5º, IV), o direito de resposta (art. 5º, V), o sigilo da fonte (art. 5º, XIV), o acesso à informação (art. 5º, XIV, XXXIII e LXXII) e o segredo de justiça (art. 5º, LX). Desta feita, o Constituinte - ainda que não conseguisse se antecipar às transformações promovidas pela tecnologia nos anos recentes - demonstrou atenção “aos efeitos da circulação e da não circulação da informação sobre os indivíduos e a sociedade”, regulando-os pela via da tutela dos direitos fundamentais (MENDES, 2014, p. 314).

Em relação ao disposto no art. 5º, inciso X, temos a privacidade na sua acepção mais básica, fruto da compreensão liberal deste direito como um dever de abstenção a proteger o indivíduo da devassa indevida de seus dados pessoais sem o seu consentimento (MARMELSTEIN, 2011, p. 143). Aqui, o constituinte utilizou as expressões “intimidade” e “vida privada” sem estabelecer o seu conteúdo, de modo que à primeira vista, a escolha dos termos parece remeter à teoria dos círculos concêntricos de Hubmann e Henkel. No entanto, tal compreensão seria anacrônica, tendo em vista que, como evidenciado no tópico anterior, tanto o direito à privacidade como o direito à proteção de dados pessoais expandiram seu conteúdo ao longo do tempo, além do que a interpretação da Constituição Federal não pode se dar de modo estanque - pelo contrário, o espírito constitucional vive através da dinâmica social, atualizando-se conforme se operam mudanças em seu seio. Em verdade, o alcance da privacidade compreende tanto a esfera íntima, como a das relações familiares e afetivas, mas, acima de tudo, as informações que uma pessoa opta ou não por revelar a seu próprio respeito a terceiros, valendo-se de sua autodeterminação informativa (COLOMBO, 2015, p. 04).

A essa expansão do conceito de privacidade soma-se a gradativa acomodação jurisprudencial em torno do tema, como a que se verifica no âmbito do Supremo Tribunal Federal, a quem compete o zelo pela Constituição, quando da apreciação do Recurso em *Habeas Data* n.º. 22/DF, onde, em que pese o remédio constitucional à época não ter prosperado em virtude da ausência do interesse de agir pela mera falta de requisito formal (ausência de requerimento na via administrativa), o Ministro Celso de Mello consignou em seu voto de divergência a compreensão de “um dos aspectos mais expressivos da tutela jurídica dos direitos da personalidade”:

Discute-se nesta sede recursal, em face do novo ordenamento constitucional, a questão referente à “*disclosure of the information*”, e à consequente acessibilidade dos registros, informáticos ou não, existentes no extinto Serviço Nacional de Informações (SNI).

Esse tema tem suscitado grande discussão, especialmente porque envolve um dos aspectos mais expressivos da tutela jurídica dos direitos da personalidade.

A garantia de acesso a informações de caráter pessoal, registradas em órgãos do Estado, constitui um natural consectário do dever estatal de respeitar a esfera de autonomia individual, que torna imperativa a proteção da intimidade. (BRASIL, 1991, pp. 18-19)

Ainda, o voto do Ministro Celso de Mello faz menção ao *right of privacy* do direito norte-americano (BRASIL, 1991, p. 20) e à privacidade pessoal (BRASIL, 1991, p. 21), portanto notadamente há uma correlação entre a vida privada e a intimidade e os novos contornos que as expressões adquirem sob o guarda-chuva da privacidade.

Na mesma linha, para Laura Schertel Mendes (2014, p. 250), ao aplicar o disposto no art. 43 do Código de Defesa do Consumidor em demanda referente aos bancos de dados de proteção ao crédito por meio do acórdão no Recurso Especial n.º. 22.337-9/RS, julgado em 13 de fevereiro de 1995, o relator Ministro Ruy Rosado de Aguiar evidenciou o conceito de privacidade em seus contornos contemporâneos.

Nesse mesmo sentido, vide o acórdão proferido no Recurso Especial n.º. 1.168.547/RJ¹², onde resta expressamente a existência de um novo conceito de privacidade, com fundamento no princípio da autodeterminação informativa.

Saindo da discussão terminológica acerca das expressões contidas no art. 5º, inciso X, da Constituição Federal de 1988 (CF 1988), prosseguindo na análise dos direitos fundamentais afeitos à privacidade e à proteção dos dados assegurados pela Carta Magna, temos em seguida os direitos à inviolabilidade do domicílio (art. 5º, inciso XI) e o sigilo de

12 REsp n. 1.168.547/RJ, relator Ministro Luis Felipe Salomão, Quarta Turma, DJe de 7/2/2011.

correspondência, das comunicações telegráficas, de dados e das comunicações telefônicas (art. 5º, inciso XII).

Em relação ao disposto no art. 5º, inciso XII, cumpre mencionar controvérsia que se firmou acerca da proteção dos dados pessoais, na qual se questionava se, uma vez que os dados pessoais servissem para identificar uma pessoa, esses dados pessoais se constituíam ou não como objeto imediato de proteção constitucional com base no direito à privacidade e no sigilo de dados contido no inciso XII.

Acolhendo a tese de Tércio Sampaio Ferraz Júnior, em decisão relatada pelo Ministro Sepúlveda Pertence no Recurso Extraordinário n.º 418.416-8/SC, o Supremo Tribunal Federal se posicionou no sentido de que a garantia fundamental inscrita no art. 5º, inciso XII, da Constituição de 1988, diria respeito tão somente à comunicação de dados, e não aos dados (para o que nos interessa, dados pessoais) em si mesmos.

No entanto, dois problemas vieram à constatação. O primeiro escancarou a dificuldade em tratar acerca dos dados pessoais e sua proteção de uma forma que não fosse “binária - sigilo/abertura, público/privado - dificultando a devida consideração da complexidade da matéria da informação” (DONEDA, 2021, p. 271), que se trata de um problema multifacetado. Tal dificuldade se fundava em um anacronismo que redundava em uma insuficiência da proteção constitucional no que diz respeito aos dados pessoais em si considerados (FERREIRA, 2021, p. 34)..

O segundo evidenciou uma lacuna: sendo a privacidade um direito fundamental, se os dados pessoais não desfrutam da proteção do art. 5º, inciso XII, da Carta Magna, que tutela específica receberiam à luz do ordenamento constitucional? (MENDES, 2014, p. 324).

Saltava aos olhos, portanto, a necessidade de um direito fundamental à proteção de dados, que sanasse essa lacuna entre a tutela da privacidade constitucionalmente assegurada e a das informações pessoais, que, por gozar de uma proteção mitigada no entendimento da corrente que prevaleceu, poderia ensejar o desrespeito a outros direitos fundamentais de forma oblíqua através da utilização abusiva das informações pessoais armazenadas em bancos de dados (DONEDA, 2021, p. 271).

À medida que o país ingressava cada vez mais no modelo da economia de dados da sociedade da informação, a imposição da vontade da técnica de forma cada vez mais marcante em face do avanço tecnológico em detrimento da pessoa humana individualmente considerada (DONEDA, 2021, pp.52-53).

Escândalos como o caso Snowden, a espionagem de autoridades brasileiras pelos EUA em 2015, o caso da *Cambridge Analytica* de influência indevida em processos eleitorais e o

aumento no número de casos de vazamentos de dados pessoais trouxeram mais uma vez à atenção para a necessidade de uma tutela efetiva da proteção de dados pessoais.

Em 2020, durante o cenário de pandemia pelo coronavírus (COVID-19), a Medida Provisória (MP) n.º 954/2020 dispôs sobre o compartilhamento de dados (nomes, números de telefone e endereços) da base de consumidores das empresas de telecomunicações com o Instituto Brasileiro de Geografia e Estatística - IBGE para “produção de estatística oficial”, o que ensejou um aprofundamento no debate sobre a natureza constitucional do direito à proteção de dados pessoais.

A MP foi alvo de críticas referentes à regulação genérica e precária do procedimento de compartilhamento, à ausência de salvaguardas específicas para os dados pessoais a serem transferidos e à desproporção entre o grande volume dos dados, que ultrapassava 141 milhões de assinantes (DONEDA, 2021, p. 274), eventualmente sendo ajuizadas as Ações Diretas de Inconstitucionalidade 6387, 6388, 6389, 6390 e 6393.

No julgamento das ADIs, o STF modificou concretamente seu posicionamento anterior quanto ao sigilo no julgamento do RE 418.416-8/SC, reconhecendo a existência de um direito fundamental à proteção de dados pessoais e, por vias indiretas, resignificando a importância do *habeas data*, consoante se denota do voto do Ministro Gilmar Mendes.

Finalmente, em 10 de fevereiro de 2022, o Congresso Nacional promulgou a Emenda Constitucional n.º 115/2022, que alterou a Constituição para incluir expressamente, no art. 5.º, inciso LXXIX, o direito fundamental à proteção de dados pessoais, inclusive nos meios digitais.

Em que pese a grande importância da positivação deste direito no sentido de trazer mais segurança aos cidadãos brasileiros no âmbito da sociedade da informação, através da revitalização do *habeas data* como instrumento compatível com a autodeterminação informativa, o novo destaque adquirido pelo remédio constitucional demanda por uma simplificação dos seus mecanismos de impetração, bem como a mudança das condições processuais características desse tipo de ação, a saber, o interesse de agir, a necessidade de representação por advogado e o esgotamento das vias administrativas (MENDES, 2014, p. 335), para que seja viabilizado o exercício deste direito fundamental.

2.2 Previsões correlatas no ordenamento infraconstitucional

Por sua especial relevância e pertinência para o presente trabalho, debruçamo-nos de modo breve e sem pretensões de exaustividade na análise de outras normas

infraconstitucionais importantes que contribuíram para o avanço da disciplina da privacidade e da proteção de dados no país. Para fins de delimitação de escopo, nos ateremos apenas àquelas que consideramos ser as mais importantes para o tema aqui proposto.

Deste modo, em que pese haver previsões envolvendo o tema em diplomas legais como o Código Comercial (primeira parte, arts. 17 a 19, acerca da exibição de livros mercantis), a Lei n.º. 4565/64 (Sistema Financeiro Nacional, art. 38, sigilo bancário), o Código Tributário Nacional (art. 198, sigilo fiscal), o Código Penal (arts. 150 a 154, violação de domicílio, correspondência e segredos, com uma ressalva para a invasão de dispositivos informáticos introduzida no art. 154-A pela Lei n.º. 12.737/2012 - Lei Carolina Dieckmann) e outras normas setoriais como a Lei n.º. 5.988/73 (antiga lei de direitos autorais, art. 123, reprodução e divulgação indevida), estes ficarão de fora da apreciação perfunctória aqui realizada pelas razões supracitadas.

Usualmente, a doutrina consagra o Código de Defesa do Consumidor como um dos primeiros diplomas legais, a resguardar as informações dos cidadãos; no entanto, embora seja mesmo um dos primeiros, poucos mencionam uma norma importante que a antecedeu, qual seja, a Lei n.º. 7.232, de 29 de outubro de 1984, que instituiu a Política Nacional de Informática com vistas a promover o “a capacitação nacional nas atividades de informática, em proveito do desenvolvimento social, cultural, político, tecnológico e econômico da sociedade brasileira” (art. 2.º. caput).

Em 1984, a Política Nacional de Informática já trazia em seu bojo a preocupação com a privacidade das pessoas naturais no contexto da entrada das tecnologias de informação e comunicação no Brasil, determinando a proteção dos dados e instituindo o direito de acesso e retificação deles em bases de dados públicas ou privadas (art. 2.º, incisos VIII e IX).

A despeito disto, a Política Nacional de Informática foi alvo de críticas sobre o fechamento do mercado brasileiro e a conseqüente defasagem científica e tecnológica até hoje sentida no país em virtude da institucionalização de uma reserva de mercado, que por sua vez impediu a entrada de tecnologia de ponta, a entrada de capital estrangeiro que poderia abrir novos mercados e linhas de pesquisa, além de gerar ameaças de retaliações comerciais por parte dos EUA (PAESANI, 2012, p. 31).

Dois anos após a promulgação da Constituição Federal, a privacidade e a proteção dos dados pessoais tiveram seu alcance ampliado com a entrada em vigor do Estatuto da Criança e do Adolescente (ECA) e do Código de Defesa do Consumidor (CDC).

O primeiro, no seu artigo 17, versava sobre o direito ao respeito à inviolabilidade da criança e do adolescente na sua integridade física, psíquica e moral, incluindo sua imagem,

identidade e autonomia, o que se coaduna com a garantia fundamental consolidada no art. 5º, inciso X, da Carta Magna. Ademais, o ECA foi posteriormente alterado pela Lei nº. 12.010, de 2009, para incluir o artigo 100, inciso V, que trata sobre as medidas específicas de proteção, onde o dispositivo menciona expressamente o princípio da privacidade.

O CDC, por sua vez, considerando a posição hipossuficiente do consumidor, trata em vários de seus dispositivos acerca de direitos que guardam afinidade com a acepção moderna de privacidade no contexto da relação consumerista, por exemplo, quanto ao direito de acesso do consumidor aos seus dados pessoais (art. 43, caput), de transparência (art. 4º, caput), referência ao princípio da qualidade das informações (art. 43, §1º), bem como de correção dos dados (art. 43, §3º). Em relação à amplitude do direito disciplinado no art. 43 do CDC, Bruno Bioni (2019, pp. 126-127) chama a atenção para o fato de que o enunciado legal diz respeito a todo e qualquer dado pessoal do consumidor, não se restringindo àqueles que dizem respeito à sua situação creditícia, assim sendo porque a *mens legis* do texto seria abarcar todas as bases de dados que digam respeito ao livre desenvolvimento da personalidade do consumidor, na medida em que hábitos de consumo se reportam a seus gostos e preferências particulares e o cruzamento de dados pode ensejar situações violadoras da privacidade dos cidadãos (MONTEIRO; BIONI, 2015). Para Laura Schertel Mendes (2014, p. 274), a consequência direta do art. 43 do CDC é a possibilidade de se impetrar ações de habeas data contra bancos de dados de consumidores, na medida em que são considerados de caráter público, como estabelece expressamente a letra do art. 43, §4º do diploma consumerista.

Em 1997, após nove anos sem regulamentação, o *habeas data* veio a receber tratamento legal infraconstitucional por meio da Lei nº. 9.507, de 12 de novembro de 1997, até então sendo regido pelo rito do mandado de segurança através de aplicação analógica. Apesar de seus defeitos, a Lei do *Habeas Data* continha previsões acerca do direito de acesso (art. 7º, I), de retificação (art. 7º, II) e à qualidade dos dados (art. 7º, III). Por outro lado, a necessidade de se intentar uma ação judicial para fazer valer o direito, de contratar advogado e o condicionamento à recusa administrativa - que não trazia nenhuma sanção - acabaram esvaziando o instituto até que seu valor fosse resgatado recentemente pelo reconhecimento da proteção de dados como um direito fundamental.

Todavia, com a recente alçada da proteção de dados como direito fundamental pelo Congresso Nacional, fazem-se necessárias uma atualização e uma reformatação do instituto do *habeas data*, seja pluralizando-o para atender os múltiplos desdobramentos do direito à privacidade e à proteção de dados pessoais, seja tornando-o meramente um instrumento dentre outros a serem criados para a estruturação de um sistema de proteção de dados pessoais

(DONEDA, 2021, p. 301), eliminando seus entraves e democratizando seu acesso à população.

Em seguida, no ano de 2002, o Código Civil foi promulgado para tutelar as relações na sociedade civil, sendo utilizado de forma subsidiária em outras legislações, como por exemplo em relação ao CDC. No tocante ao tema da privacidade, por sua natureza eminentemente privatista, o diploma civil timidamente consignou, no seu art. 21, a inviolabilidade da vida privada da pessoa natural, não tratando mais do assunto. Todavia, é pertinente mencionar os enunciados n.º. 404 e 405 da V Jornada de Direito Civil do Conselho da Justiça Federal sobre o dispositivo em comento, os quais estabelecem uma dimensão contextual do local, da finalidade e do tempo de tratamento de dados pessoais, sobretudo aqueles dados classificados como sensíveis, que podem ensejar situações de discriminação e violação a outros direitos fundamentais como a dignidade da pessoa humana.

Em junho de 2007, o governo brasileiro implementou o Cadastro Único para Programas Sociais, através do Decreto n.º. 6.135, de 26 de junho de 2007, cujo art. 8º estabelecia o sigilo dos dados de identificação das famílias, bem como únicas finalidades para seu processamento a formulação e a gestão de políticas públicas e a realização de estudos e pesquisa, eliminando outras finalidades por via de exclusão. Referido decreto veio a ser recentemente revogado pelo Decreto n.º. 11.016, de 29 de março de 2022, o qual expressamente estabelece como diretriz a proteção dos dados pessoais (art. 3º, inciso V), reitera o sigilo (art. 13, caput) e o princípio da finalidade (art. 13, I e II) do decreto anterior, além de incluir o princípio da minimização (art. 13, §2º), com referência à Lei Geral de Proteção de Dados Pessoais.

No ano de 2008, o Decreto n.º. 6.523, de 31 de julho de 2008, que estabelece e regulamenta normas gerais para o Serviço de Atendimento ao Consumidor (SAC), ao tratar da qualidade do atendimento, de igual modo dispunha sobre o sigilo dos dados pessoais do consumidor e a finalidade de sua utilização (art. 11). Recentemente, referido decreto foi revogado pelo Decreto n.º. 11.034, de 05 de abril de 2022, o qual remete expressamente à Lei Geral de Proteção de Dados ao versar sobre os dados pessoais do consumidor, na letra do art. 9º do decreto supra.

Por sua vez, ao tratar sobre o censo anual da educação, o Decreto n.º. 6.425, de 04 de abril de 2008, incumbia o poder público e os representantes legais dos estabelecimentos privados de educação de preservar a exatidão e fidedignidade das informações prestadas (art. 2º, §§1º e 2º, princípio da qualidade dos dados), além de assegurar o sigilo, a proteção dos dados pessoais e sua utilização para finalidades fidedignas (art. 6º).

Já a Lei do Cadastro Positivo (Lei 12.414, de 9 de junho de 2011) surgiu para trazer mais segurança jurídica nas relações creditícias por meio da formação de um histórico de crédito dos consumidores, contendo informações sobre a natureza da relação, data da concessão do crédito, montante concedido, pagamentos realizados e pendentes, entre outras informações, a fim de estabelecer perfis de bons pagadores e com isso diminuir o risco das operações de concessão de crédito.

Ela trazia no texto alguns princípios atinentes à qualidade dos dados (art. 3º, §§ 1º e 2º, com seus incisos); ao direito de acesso, retificação e exclusão (art. 5º, incisos II e III); à finalidade do processamento (art. 2º, inciso I; art. 5º, inciso VII; e art. 7º, incisos I e II); e à proibição do armazenamento de informações excessivas - princípio da minimização - ou sensíveis (art. 3º, §3º e incisos). Traziam, porém, novidades referentes ao consentimento (arts. 4º e 9º) e a revisão de decisões realizadas exclusivamente por meios automatizados (art. 5º, inciso VI).

Acerca do consentimento, cumpre observar que a inclusão do consumidor em base de dados para fins de score de crédito demandava autorização expressa e informada deste, devendo constar em instrumento específico. No entanto, a Lei do Cadastro Positivo foi alterada pela Lei Complementar nº. 116, de 8 de abril de 2019, para retirar a obrigatoriedade do consentimento do consumidor, efetivamente autorizando a inclusão automática de milhões de pessoas físicas e jurídicas na base de dados creditícia, introduzindo um risco potencial à privacidade e à proteção dos dados em caso de vazamento, sem realizar um juízo de proporcionalidade entre a vantagem da praticidade e as salvaguardas necessárias aos direitos dos cidadãos. Além disto, a Lei do Cadastro Positivo elasteceu para quinze anos (art. 14) o prazo de cinco anos previsto no CDC para a manutenção das informações no cadastro.

Quanto à revisão de decisões realizadas por tratamento exclusivamente automatizado de informações, este direito ganha destaque considerando a inclusão nesse sistema de avaliação de crédito, possibilitando ao consumidor questionar a pontuação recebida e os critérios para seu estabelecimento, podendo solicitar a correção de dados equivocados, desatualizados ou de inclusão vedada (MENDES, 2014, p.282).

Também do ano de 2011 é a Lei nº. 12.527, de 18 de novembro de 2011, alcunhada de Lei de Acesso à Informação (LAI), que busca regular a fronteira nebulosa entre o direito à privacidade e o direito à informação previsto no art. 5º, inciso XXXIII da Constituição Federal (MENDES, 2014, p. 292), delimitando conceitos, diretrizes, classificação de informações e hipóteses de dispensa de consentimento, relacionados à publicização de informações por parte da Administração Pública e entidades privadas que auferem recursos

públicos para realização de ações de interesse público. Ela estabelece os conceitos de informação pessoal (art. 4º, IV) e de tratamento da informação (art. 4º, V), refere-se aos princípios da transparência (art. 6º, I) e da qualidade (art. 4º, VI, VII e VIII), trata do direito ao acesso (art. 10), da proteção de informações pessoais (art. 31) e do consentimento (art. 31, §1º, II), bem como suas hipóteses de dispensa (art. 31, §3º e incisos).

Por razão de afinidade temática, a LAI guarda uma relação de complementaridade com o *habeas data*, na medida em que ambos versam sobre o acesso do cidadão às suas informações pessoais (MENDES, 2014, p. 287). Em verdade, o direito à informação abarcado pela LAI é de ordem material e o *habeas data*, embora sua concepção tenha tido o desígnio de direito material, se trata de um instrumento processual para concretizá-lo em caso de recusa administrativa.

Em 2014, foi promulgado o Marco Civil da Internet - MCI (Lei nº. 12.965, de 23 de abril de 2014), que visava tutelar os direitos e garantias dos cidadãos no uso da Internet. O MCI trouxe um acréscimo na segurança jurídica para os provedores de aplicações da Internet, numa época de turbulentas decisões que revelavam desconhecimento das particularidades técnicas que envolviam os casos judiciais sobre remoção de conteúdo na Internet.

O MCI estabeleceu um modelo de responsabilidade de provedores de aplicações que fosse compatível com suas capacidades técnicas, com a funcionalidade dos serviços de Internet, com os direitos dos usuários da rede e com os potenciais danos gerados (LEONARDI, 2019, p. 85).

De acordo com Marcel Leonardi (2019), o Marco Civil da Internet estabeleceu uma relação de sintonia com o Código de Defesa do Consumidor, afirmando como fundamentos expressos os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais (art. 2º, II), bem como a livre iniciativa, a concorrência e a defesa do consumidor (art. 2º, V), guiando-se por princípios como a responsabilização (art. 3º, VI), a guarda da natureza participativa da rede (art. 3º, VII), a privacidade (art. 3º, II) e a proteção de dados pessoais (art. 3º, III).

Esta sintonia se revela ao estabelecer o dever de informação sobre coleta e tratamento de dados pessoais (art. 7º, VIII), a exigência do consentimento para referido tratamento e compartilhamento (art. 7º, VII e IX), a vigência dos princípios da finalidade (art. 7, VIII, c) e da minimização (art. 7, VIII, a), bem como o respeito à liberdade de expressão e à privacidade como garantias para o pleno exercício do direito de acesso à internet (art. 8º).

Um ponto controverso no Marco Civil da Internet, porém, é a questão da retenção dos dados de navegação pelos provedores de conexão e aplicação, guarda esta obrigatória por

imposição legal (arts. 10, 13 e 15), durante o prazo de seis meses para os provedores de aplicações (art. 15) e um ano para os provedores de conexão (art. 13). A quizila diz respeito à escolha entre dois modelos de guarda de dados, em uma dicotomia de *preservação x retenção*, tendo sido adotado o modelo mais radical, que beira a inconstitucionalidade, além de violar a presunção de inocência, no parecer de Bruno Bioni (2019, p. 227).

Como se vê, o Marco Civil da Internet impôs um modelo de guarda obrigatória de dados para os provedores de conexão e aplicações, e não facultativa, como originalmente previsto. Adotou, assim, um modelo único de retenção de dados de forma indiscriminada, em oposição a um modelo de preservação dos dados efetivamente ligados a um ato ilícito praticado, o que implica tratar todos os usuários de Internet como suspeitos da prática de atos ilícitos, com sérias implicações para sua privacidade.

Posteriormente, foi editado o Decreto n.º. 8.771, de 11 de maio de 2016, o qual definiu os conceitos de dado pessoal (art. 14, I) e tratamento de dados pessoais (art. 14, II), invocou os princípios da finalidade (art. 13, §2º, I) e da minimização do tratamento de dados pessoais (art. 13, §2º, II) e nomeou o Comitê Gestor da Internet – CGI.br para estabelecer as diretrizes para os requisitos técnicos, bem como a Agência Nacional de Telecomunicações (ANATEL), a Secretaria Nacional do Consumidor (SENACON) e o Sistema Brasileiro de Defesa da Concorrência para realizar a fiscalização, cada um em sua área de competência (arts. 17, 18 e 19).

Os conceitos utilizados pelo MCI para a definição de dados pessoais e tratamento de dados pessoais vieram, posteriormente, explícita ou implicitamente a influenciar a definição utilizada pela Lei Geral de Proteção de Dados Pessoais - LGPD (Lei n.º. 13.709, de 14 de agosto de 2018). Com efeito, a LGPD destinava-se, em princípio, a ser uma alteração do MCI, porém adquiriu nomeação e regulamentação próprias em virtude de demandas de mercado, uma vez que as normas setoriais infraconstitucionais careciam de um sistema coeso de proteção de dados pessoais.

Fortemente inspirada no *General Data Protection Regulation* (GDPR) europeu, a LGPD foi a culminação de todo o avanço regulatório, doutrinário, jurisprudencial, ora retomando, ora explanando, ora desenvolvendo, ora aperfeiçoando conceitos e disposições dadas “em pinceladas rápidas” nas normas até aqui examinadas, no tocante à temática da privacidade e da proteção de dados pessoais, com foco na tutela da pessoa humana em face de situações potenciais de violação de direitos fundamentais acarretadas pelos caminhos imprevisíveis que a evolução tecnológica pode enveredar.

A LGPD estabelece, no seu art. 2º, um rol de fundamentos para a proteção dos dados pessoais, dos quais destacamos o respeito à privacidade (art. 2º, I); a autodeterminação informativa (art. 2º, II); a inviolabilidade da intimidade, da honra e da imagem (art. 2º, IV); e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (art. 2º, VII).

Não obstante, ao mesmo tempo que consagra a tutela da pessoa humana e sua dignidade como valor central, a lei busca harmonizá-los com os interesses do mercado e o desenvolvimento econômico e tecnológico, como se denota dos fundamentos contidos no art. 2º, incisos V e VI.

Desde já, de plano, importa referir que a LGPD trata, nos arts. 1º e 3º, acerca do escopo material e espacial da proteção que por ela é conferida, depreendendo-se destes dispositivos um conjunto de assertivas que delimitam o conteúdo da tutela e sua abrangência.

Assim, em relação ao seu conteúdo, a lei compreende apenas dados pessoais, isto é, aqueles que digam respeito à pessoa natural identificada ou identificável, isto é, que possa ser imediatamente identificada sem a utilização de dados adicionais (por exemplo, uma foto, impressões digitais ou o código genético) ou de modo mediato através do cruzamento com outros dados (ex.: número do CPF, endereço físico, endereço IP etc.). Por se tratar apenas de pessoa natural, por exclusão, as disposições da LGPD não alcançam os dados da pessoa jurídica. Além disso, estão protegidos por força do art. 3º os dados pessoais independentemente do meio (físico ou eletrônico) em que sejam tratados, seja por pessoa natural, por pessoa jurídica de direito público ou de direito privado.

Um questionamento que se faz acerca do escopo material da LGPD é se o mesmo compreende os dados pessoais de pessoas falecidas, o que não ocorre no GDPR por disposição do regulamento europeu nos Considerandos nº. 27, 158 e 160, que excluem a aplicação do regulamento aos dados pessoais de pessoas mortas, delegando a matéria ao critério da competência regulatória de cada um dos Estados-Membros da União Europeia.

No Brasil, o legislador silenciou a esse respeito na LGPD e até o momento ainda não houve posicionamento da Autoridade Nacional de Proteção de Dados (ANPD) nem da jurisprudência, sendo defensável o argumento fundado no art. 6º do Código Civil, que trata da cessação da personalidade diante do evento morte, de modo que, por via de consequência, não expressamente reconhecida, a LGPD não se aplicaria aos dados pessoais de pessoas falecidas (MOTA; MOTA, 2021).

Este questionamento possui particular relevância quando se trata do assunto que a doutrina vem chamando de herança digital, tendo em vista a projeção que a personalidade

assume quando inserida no ciberespaço, transcendendo as limitações de um espaço-tempo definidos e produzindo “imortalidades no *cyberspace*”, tendo em vista, por exemplo, que o uso das redes sociais faz com que os dados nela inseridos continuam sendo tratados mesmo após a morte do titular (M. ESPERANÇA, 2020, *apud* BATISTA, 2021, pp. 49-50).

A lei também estabelece, no artigo 4º e seus incisos, categorias de dados que, embora possam ser considerados dados pessoais, seu tratamento envolve finalidades específicas excepcionadas, quais sejam, o tratamento de dados pessoais realizado por pessoa natural para fins particulares e não econômicos - por exemplo, catálogo pessoal de telefones ou lista particular de nomes e aniversários (art. 4º, I); o tratamento realizado para fins exclusivamente jornalísticos, artísticos ou acadêmicos (art. 4º, II, alíneas ‘a’ e ‘b’); e o tratamento de dados pessoais atinentes a questões de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (art. 4º, III, alíneas ‘a’, ‘b’, ‘c’ e ‘d’).

Sobre o tratamento realizado para fins exclusivamente acadêmicos, é mister pontuar que este se encontra condicionado ao fornecimento do consentimento por parte do titular ou deverá se enquadrar nas demais bases legais previstas no art. 7º ou, em se tratando de dados pessoais sensíveis, constantes do art. 11. A Medida Provisória n.º. 869/2018 tentou remover tais restrições - exigência de consentimento ou enquadramento nas outras bases legais -, no entanto, a este respeito, o enunciado legal previamente estipulado prevaleceu, restaurando as exigências supracitadas.

Já em relação às hipóteses de tratamento constantes do inciso III do art. 4º, este será regulamentado por lei específica, consoante previsão no art. 4º, §1º, da LGPD. Estão em curso, porém, os debates acerca do Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal, apelidado de “LGPD Penal”, elaborado pela Comissão de Juristas instituída por Ato do Presidente da Câmara dos Deputados, de 26 de novembro de 2019. Referido anteprojeto foi apresentado em 05 de novembro de 2020 e se refere a duas problemáticas centrais, consoante exposição de motivos:

[...] O primeiro problema diz respeito à própria eficiência investigativa dos órgãos brasileiros, visto que a falta de adequação aos padrões internacionais de segurança quanto ao fluxo e ao tratamento de dados obsta a integração do Brasil com órgãos de inteligência e de investigação de caráter internacional (v.g., INTERPOL), obstando o próprio acesso a bancos de dados e a informações relevantes, e coloca o uso de aplicações tecnológicas em segurança pública e a adoção de técnicas modernas de investigação sob questionamento de sua validade jurídica.

Em segundo lugar, há um enorme déficit de proteção dos cidadãos, visto que não há regulação geral sobre a licitude, a transparência ou a segurança do tratamento de

dados em matéria penal, tampouco direitos estabelecidos ou requisitos para utilização de novas tecnologias que possibilitam um grau de vigilância e monitoramento impensável há alguns anos. Apesar do crescimento vertiginoso de novas técnicas de vigilância e de investigação, a ausência de regulamentação sobre o tema gera uma assimetria de poder muito grande entre os atores envolvidos (Estado e cidadão). Nesse contexto, o titular dos dados é deixado sem garantias normativas mínimas e mecanismos institucionais aplicáveis para resguardar seus direitos de personalidade, suas liberdades individuais e até a observância do devido processo legal. (CÂMARA..., 2020, pp. 1-2)

A despeito da iniciativa, porém, há um impasse nas discussões, tendo o Ministério Público tomado posicionamento contrário ao anteprojeto sob o fundamento de possível comprometimento da capacidade de investigação do Ministério Público. Após reunião em 30 de junho de 2021, como resultado da Ação 04/2021, a Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro (ENCCLA), uma rede de articulação entre órgãos dos Poderes Executivo, Legislativo, Judiciário, incluindo Ministério Público, nos âmbitos federal, estadual e municipal (quando cabível), produziu Nota Técnica contendo a avaliação do anteprojeto, chegando à conclusão de que está:

“em absoluto descompasso com a imprescindível integração entre os órgãos envolvidos, direta ou indiretamente, na investigação criminal, repressão penal e/ou segurança pública. Em verdade, o anteprojeto poderá causar graves entraves ao exercício das funções institucionais dos órgãos e instituições competentes para as atividades de persecução penal e de segurança pública, impedindo sua atuação a fim de garantir a ordem pública.” (ENCCLA, 2021, pp. 02-03).

Sendo assim, até o presente momento, permanece o vácuo legislativo sobre a matéria constante no art. 4º, inciso III, da LGPD.

Por fim, a última exceção contida no art. 4º, inciso IV, visa trazer segurança jurídica para empresas estrangeiras que queiram armazenar dados no país, através de filial em território nacional ou mediante a contratação de uma empresa brasileira (VAINZOF, *apud* MALDONADO; BLUM; 2019, p. 83). Os requisitos estipulados no dispositivo também buscam “aumentar a competitividade internacional brasileira, estimulando a contratação de empresas nacionais de serviços de Tecnologia da Informação, como *hosting* tradicional ou em nuvem, *IT Outsourcing*, *analytics*, entre outros” (VAINZOF, *apud* MALDONADO; BLUM, 2019, p. 84).

Quanto ao escopo espacial da LGPD, este se encontra previsto no art. 3º e incisos, dotado de caráter extraterritorial para compreender: a) o tratamento de dados pessoais que tenham sido coletados no Brasil (podendo as demais fases do tratamento realizarem-se no exterior), independentemente da nacionalidade do titular, com exceção aos dados cujo

tratamento se enquadre na situação do art. 4º, inciso IV, comentada mais acima; b) as operações de tratamento de dados pessoais realizadas no território nacional, constando uma definição bastante ampla do que significa tratamento de dados pessoais no art. 5º, inciso X, da LGPD; c) com destaque para a finalidade do tratamento, as operações de tratamento que visem oferecer bens ou serviços a indivíduos localizados no Brasil.

O art. 5º da Lei Geral de Proteção de Dados Pessoais, por sua vez, traz um conjunto de definições que orientarão a interpretação dos dispositivos, sendo de particular relevância os conceitos de dados pessoais sensíveis (art. 5º, II), dados anonimizados (art. 5º, III), controlador (art. 5º, VI), operador (art. 5º, VII) e encarregado (art. 5º, inciso VIII).

Os dados pessoais sensíveis são aqueles que dizem respeito a particularidades da pessoa natural que poderão ensejar tratamento discriminatório e violações de direitos fundamentais, como origem racial ou étnica, credo religioso, opinião ou filiação política, saúde ou vida sexual, dados biométricos ou genéticos.

Já os dados anonimizados são aqueles que passam por técnicas para descaracterizá-los de forma que não possam ser associadas a um indivíduo em particular, buscando inviabilizar sua identificação. Não se trata, porém, de um método 100% confiável, podendo ser revertido em alguns casos, razão pela qual, via de regra, os dados anônimos não são considerados pessoais, exceto quando o processo de anonimização puder ser revertido por meios próprios ou esforços razoáveis (art. 12).

Bruno Bioni (2019, p. 78), porém, aponta para o fato de que mesmo o tratamento de dados anonimizados, com a sofisticação dos algoritmos de mineração de dados, *Big Data* e inteligência artificial, pode ocultar práticas discriminatórias em prejuízo da coletividade e de pessoas singulares, razão que ressalta cada vez mais a importância da agenda de regulação de algoritmos e Inteligência Artificial, cujos debates prosseguem por meio do Projeto de Lei nº. 2338/2023, que visa a regulamentação da inteligência artificial no Brasil e ora se encontra sob análise pelo Senado Federal¹³.

Há também que se distinguir as técnicas de anonimização daquelas de pseudonimização (art. 13, §4º), onde, embora a LGPD recomende a anonimização ou pelo menos a pseudonimização dos dados, como na hipótese do art. 13 (realização de estudos de saúde pública), apenas os dados anonimizados não são considerados dados pessoais (e mesmo assim, com as limitações do art. 12), o que não se estende aos dados pseudonimizados que, portanto, deverão se conformar aos parâmetros da lei.

13 SENADO FEDERAL. **Senado analisa projeto que regulamenta a inteligência artificial.** Fonte: Agência Senado. Disponível em: <<https://www12.senado.leg.br/noticias/materias/2023/05/12/senado-analisa-projeto-que-regulamenta-a-inteligencia-artificial>>. Acesso em: 01 jul. 2023.

Em relação aos conceitos de controlador e operador de tratamento de dados pessoais, a lei define o controlador como o agente de tratamento responsável por tomar as decisões acerca da finalidade, dos meios, do período e outras especificações do tratamento de dados pessoais, sendo por essa razão o responsável principal nos casos de tratamento de dados ilegítimo, isto é, em realizado em desacordo com a lei. Por sua vez, o operador é aquele que realiza o tratamento em nome do controlador, seguindo estritamente as diretrizes deste e responsabilizando-se solidariamente caso realize tratamento ilegítimo ou descumpra as orientações do controlador.

A despeito da clareza da definição legal, por um certo período, os conceitos geraram um misto de confusão com, em alguns casos, transferência de responsabilidades e terrorismo psicológico das empresas sobre os empregados, havendo quem dissesse que, por realizarem tratamento de dados sob as ordens do comando da empresa, empregados e colaboradores se enquadrariam no conceito de operador (QUEDEVEZ; SIMONI, 2021), o que é uma falácia.

Para dirimir as controvérsias nesse sentido, a Autoridade Nacional de Proteção de Dados elaborou, em maio de 2021, um Guia Orientativo para Definições dos Agentes de Tratamento e do Encarregado, o qual atualmente se encontra em sua segunda versão e explicita que empregados, administradores, sócios, servidores e outras pessoas naturais que integram a pessoa jurídica não são considerados operadores. Segundo o entendimento da ANPD, “o operador será sempre uma pessoa distinta do controlador, isto é, que não atua como profissional subordinado a este ou como membro de seus órgãos.” (AUTORIDADE..., 2021, pp. 17-18).

Em relação ao encarregado pelo tratamento de dados pessoais, este atuará como um canal de comunicação entre o controlador, os titulares de dados e a ANPD, servindo como porta-voz e mediador no atendimento das requisições de exercício de direitos por parte dos titulares, no recebimento e adoção de providências quanto às comunicações com a ANPD, na orientação e treinamento dos colaboradores quanto ao *compliance* em proteção de dados pessoais e na execução “das demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares” (art. 41, §2º, IV).

O encarregado encontra seu análogo na figura do *Data Protection Officer* (DPO) do GDPR europeu, porém, diferentemente do que ocorre com o encarregado, o DPO se reportará, por incumbência legal do artigo 38 do GDPR, ao nível administrativo mais alto do controlador ou do operador, além de que deverá ter sua autonomia assegurada de modo a não incorrer em conflito de interesses. As atribuições e poderes do DPO são mais amplas que a do encarregado, nos termos do artigo 39 do GDPR, assemelhando-se à figura de um auditor, o

que não ocorre com o encarregado de tratamento de dados.

Uma análise comparativa do art. 39 do GDPR com o art. 41, §2º, inciso IV, da LGPD revela que, em que pese as atribuições do encarregado parecerem mais simples que as do DPO, o controlador na normativa brasileira possui um poder de ingerência muito maior sobre o trabalho do encarregado, o que, a depender do caso concreto, poderá dar ensejo ao clientelismo e o conflito de interesses.

Em relação à nomeação do encarregado, temos que o art. 41, *caput*, estabelece que todo controlador, seja pessoa física, jurídica de direito privado ou jurídica de direito público, deverá indicar um encarregado pelo tratamento de dados pessoais, com exceção para as hipóteses de dispensa desta indicação a critério da ANPD, conforme o porte e a natureza da organização (art. 41, §3º).

Nessa toada, a Autoridade Nacional de Proteção de Dados publicou a Resolução CD/ANPD nº 2, de 27 janeiro de 2022, regulamentando estas hipóteses de dispensa para os agentes de tratamento de pequeno porte que se enquadrarem nas previsões do art. 2º, inciso I, da Resolução, exceto nos casos em que o tratamento envolva alto risco para os titulares (art. 3º, I), auferirem receita bruta superior ao limite legal para o regime específico de cada empresa (art. 3º, II) ou configurem grupo econômico de fato ou de direito cuja receita global ultrapasse o limite legal do inciso anterior (art. 3º, III) (AUTORIDADE..., 2022).

Também cumpre observar que, embora a nomenclatura utilizada pela lei pareça sugerir, o encarregado não é responsável pelo tratamento de dados pessoais, cuja responsabilidade compete ao controlador e ao operador, na medida de suas atribuições. O encarregado, portanto, via de regra, não é responsável por eventual desconformidade da organização com os requisitos de proteção de dados exigidos por lei, exceto quando houver dolo (SILVA BRUNO, *apud* MALDONADO; BLUM, 2019, p. 321). A orientação da ANPD acerca da responsabilidade do encarregado, embora a autoridade tenha se manifestado no sentido de regulamentar a figura do encarregado em mais detalhes em normas posteriores, coaduna-se com este parecer.

Além dos fundamentos e definições, a LGPD estabelece, no seu art. 6º e incisos, um conjunto de princípios que, além da boa-fé, deverão ser observados no tratamento de dados pessoais, a saber, os princípios da finalidade, da adequação, da necessidade, do livre acesso, da qualidade, da transparência, da segurança, da prevenção, da não-discriminação e da responsabilização. Alguns destes já constavam em diplomas normativos anteriores, outros foram retomados e aprimorados, como o do livre acesso, o da qualidade, o da transparência e o da finalidade e outros foram introduzidos na lei de proteção de dados.

A Lei Geral de Proteção de Dados Pessoais também estabelece, no seu art. 7º e incisos, um conjunto de bases legais que legitimam o tratamento de dados pessoais, sendo estas o consentimento (inciso I), o cumprimento de obrigação legal ou regulatória pelo controlador (inciso II), o tratamento e uso compartilhado de dados pela Administração Pública para fins de execução de políticas públicas (inciso III), a realização de estudos por órgãos de pesquisa (inciso IV), execução de contratos ou tratativas pré-contratuais nas quais o próprio titular seja parte interessada (inciso V), o exercício regular de direitos (inciso VI), a proteção da vida e da integridade física (inciso VII), a tutela da saúde (inciso VIII), os interesses legítimos do controlador ou de terceiro (inciso IX) e a proteção do crédito (inciso X). Destas, pela pertinência especial com o tema deste trabalho, destacamos as bases legais dos incisos I, III, IV e VIII do art. 7º, em que pese a relevância e a abertura dos demais para o debate, notadamente a base legal do “legítimo interesse”.

A LGPD também consagra, nos arts. 17 a 22, um rol de direitos aos titulares de dados, direitos estes que materializam os princípios anteriormente vistos e possuem aplicabilidade imediata, independentemente de requisição (art. 18, por meio da expressão “a qualquer momento”), tais como: informação acerca do tratamento de dados pessoais, direito de acesso aos próprios dados pessoais pelo titular, à portabilidade de dados pessoais, à qualidade dos dados, à sua anonimização, bem como eliminação dos dados armazenados, entre outros.

Quanto à fiscalização do cumprimento da lei, a LGPD estabelece no art. 55-K a prevalência da ANPD no exercício do poder de polícia envolvendo a aplicação de sanções no que diz respeito à proteção de dados pessoais, em que pese a atuação concorrente da ANPD com outras entidades ou órgãos da administração pública que são dotados de competência normativa ou sancionatória.

Assim, nos arts. 52 a 54, a LGPD estabelece o regime de sanções aplicáveis às infrações cometidas, dispondo sobre o escalonamento punitivo, os parâmetros de apuração e a destinação da arrecadação, bem como condições prévias para a aplicação de parcela das sanções administrativas, constantes do rol elencado nos incisos I a XII.

O capítulo referente às sanções já se mostrava controverso desde os debates legislativos nos principais projetos de lei concorrentes que antecederam a versão atual da LGPD, evidenciando uma notória preocupação em modular o poder fiscalizatório estatal, o rigor das sanções e seu impacto potencial na continuidade das atividades de tratamento de dados pessoais (e, por via de consequência, na manutenção dos próprios negócios e serviços em si, públicos ou privados), variando entre a ausência de sanções (como o Projeto de Lei nº. 131, de 2014) e algo mais próximo do que temos hoje (vide PL nº. 5276, de 2016).

No caso da sanção com multa pecuniária, entretanto, a LGPD simplificou sua aplicação ao mesmo tempo em que trouxe à tona uma contradição apontada por Fabrício da Mota Alves (*apud* MALDONADO; BLUM, 2019, p. 370), na medida em que a lei penaliza de modo severo o controlador de pequeno e médio porte ao mesmo tempo em que atenua a eficácia punitiva contra grandes grupos ou conglomerados que tratam dados pessoais de forma massiva, justamente aqueles que estão sujeitos a maior risco regulatório em razão do volume de dados em sua guarda.

Outra problemática que a lei introduziu foi a aplicação da multa “por infração”, sem definir expressamente o escopo desta expressão, uma vez que é possível termos múltiplos titulares atingidos, múltiplos incidentes e múltiplas normas desrespeitadas em decorrência de uma mesma violação à LGPD.

Com efeito, o art. 83 do GDPR estabelece, dentre os critérios para apuração das multas, o número de titulares de dados atingidos e a gravidade dos danos provocados. Embora a gravidade dos direitos pessoais afetados e o grau do dano provocado sejam referidos no art. 52, §1º, incisos I e VI, a LGPD não faz menção ao número de titulares de dados atingidos pela violação como parâmetro para fixação da multa pecuniária. Registre-se, também, a existência do Projeto de Lei n.º 3420/2019, atualmente em tramitação, que se propõe a suprimir o termo “por infração” constante no art. 52, inciso II, da LGPD, que, segundo o autor do projeto, demonstraria “uma excessiva vontade de punir de forma comensal a atividade empresarial” (CÂMARA..., 2019, p. 02).

Ainda, no tocante à destinação dos recursos arrecadados, a LGPD estabelece, no art. 52, §5º, que o produto da arrecadação das multas será destinado ao Fundo de Defesa dos Direitos Difusos, criado pela Lei n.º 7.347, de 24 de julho de 1985 e regulamentado pela Lei n.º 9.008, de 21 de março de 1995.

Pelas considerações até aqui expendidas, contemplando a evolução do conceito de privacidade, o surgimento do direito à proteção de dados e a importância que a LGPD estabelece para as iniciativas de promoção da conformidade, temos que todos estes fatores tiveram grande preponderância para a formação de uma cultura de *compliance* em matéria de privacidade e proteção de dados, essencial para resguardar a proteção da pessoa humana em face do desenvolvimento exponencial da tecnologia.

5 CONSIDERAÇÕES FINAIS

Embora a LGPD esteja próxima de completar cinco anos de sua promulgação, verifica-se, portanto, que o debate acerca dos temas que ela trata ainda não se fez suficientemente presente a ponto de assegurar o amplo conhecimento de suas determinações, bem como dos direitos e salvaguardas a que os titulares de dados fazem jus. É com esse conhecimento que o acadêmico e o profissional do direito deverão se munir para buscar a tutela dos direitos dos titulares de dados pessoais, seja a nível individual, seja a nível coletivo, com o intuito de garantir a cidadania e materializar o espírito da Constituição Federal. E apenas conhecendo o nascedouro destes direitos e salvaguardas, o manancial principiológico que lhe dá corpo e o sentido para o qual flui é que será possível alcançarmos uma tutela justa e efetiva destes direitos na vida em sociedade.

Tendo este mote como bússola e horizonte, a presente pesquisa se destinou a examinar este fluxo com o intento de, através deste resgate histórico, subsidiar estudos posteriores acerca de questões controversas e ainda não solucionadas no que tange o direito à privacidade e o direito à proteção de dados, tais como, a título de exemplo: autonomia do encarregado pelo tratamento de dados pessoais; tratamento de dados pessoais de pessoas mortas x herança digital; responsabilidade do Estado em incidentes de vazamento de dados pessoais; o dilema da Administração Pública entre o controle e a publicidade dos dados, entre outras questões.

A problemática acerca da autonomia do encarregado envolve considerações sobre até que ponto a sua atuação pode ser considerada isenta de conflito de interesses quando o encarregado está diretamente subordinado ao controlador dentro do organograma institucional, diferentemente do que ocorre no *General Data Protection Regulation* europeu, onde, embora haja permissivo para a contratação de um *data protection officer* (figura à qual o encarregado da LGPD se assemelha), o regulamento europeu considera a questão como um assunto chave (*key issue*), tratando disso explicitamente no Considerando n° 97 e no art. 38, inciso 3. Ademais, à maneira do que ocorre com a LGPD no art. 41 e incisos, o *data protection officer* também pode acumular tarefas e deveres, a diferença estando no fato de que o GDPR também estabelece categoricamente a obrigação do controlador ou do operador de tratamento de dados em garantir que tais encargos não resultem em conflito de interesses, ressalva esta que não consta do texto do art. 41 da LGPD. Ainda, a expressão “executar as demais atribuições” contida no art. 41, §2º, inciso IV, da LGPD poderá servir como uma cláusula em branco, esvaziando as salvaguardas e pondo em risco os direitos dos titulares de dados pessoais.

Acerca do tratamento de dados pessoais de pessoas mortas, a discussão se dá em razão de que a LGPD considera, no art. 5º, incisos I e II, a necessária vinculação à pessoa natural para fins de classificação dos dados como dados pessoais e dados pessoais sensíveis; entretanto, o Código Civil de 2002 estabelece, no art. 6º, o fim da existência da pessoa natural, em tese não havendo que se falar em tratamento de dados pessoais relativos a pessoa falecida. Porém, mesmo após o evento morte, certos direitos da personalidade continuam produzindo efeitos - inclusive econômicos -, sendo objeto de tutela jurídica na forma do art. 12, parágrafo único do Código Civil, como é o caso da honra e dos direitos autorais. Não poderia ser diferente, portanto, em relação aos direitos à privacidade e à proteção dos dados pessoais, visto que estes compõem a universalidade de direitos, pois na vida cotidiana da sociedade da informação nossa *persona* no mundo digital compõe parte de nossa identidade e nosso patrimônio, como no caso dos *digital influencers*, *youtubers* e *streamers*. Fica, portanto, aparente um possível conflito de normas, o qual o diploma civil não foi capaz de antecipar diante do avanço das tecnologias. Todavia, o entendimento de que os dados referentes à pessoa morta merece a tutela jurídica não pode ser considerado unânime, tratando-se de discussão que deve ser suficientemente maturada.

Já a questão sobre a responsabilidade do Estado na hipótese de vazamento de dados pessoais dos cidadãos parece resolvida na superfície, uma vez que a LGPD dispõe expressamente sobre a base legal para o tratamento de dados pessoais pelo Poder Público (art. 7º, inciso III), as condições em que poderá ocorrer (arts. 23 a 32) e as sanções aplicáveis em caso de tratamento ilegítimo de dados pessoais (arts. 52 a 54). O problema é que as exceções que a lei estabelece para as sanções ao Poder Público no âmbito da fiscalização administrativa, na prática tornam as sanções inócuas, o que, na hipótese de vazamento de dados pessoais (*data breach*), viola o princípio da responsabilização da Administração Pública perante os administrados e contraria o espírito da Constituição Federal. Logo, em que pese disposições expressas na lei versando sobre tais exceções, pode-se discutir sobre sua eventual inconstitucionalidade.

Sobre a situação da Administração Pública no impasse de, por um lado, necessitar tratar dados pessoais dos cidadãos a fim de controlar o funcionamento da máquina administrativa e do serviço público para cumprir seu propósito de buscar o bem comum, contraposto, por outro lado, pelo imperativo de dar publicidade com o desiderato de assegurar a transparência e a isonomia na relação com os administrados, cumpre sempre lembrar a discussão que ainda segue curso acerca do projeto alcinhado de LGPD Penal, o qual versa sobre o tratamento de dados pessoais no contexto da segurança pública, especialmente

considerando a polêmica acerca da adoção de câmeras corporais por parte dos policiais do Rio de Janeiro. Na mesma toada, podemos citar o debate envolvendo o uso do reconhecimento facial nos transportes públicos, como no caso do metrô de São Paulo. O enquadramento entre o controle e os controlados evidencia a necessidade do constante equilíbrio por parte do Poder Público, onde a ausência de mecanismos de controle poderá prejudicar a execução de serviços públicos essenciais e o excesso do controle colocará poder demais nas mãos do Estado, o que é perigoso em se tratando de um país com ciclos autoritários e atos antidemocráticos ao longo da história, como a invasão à sede dos três poderes ocorrida em Brasília no dia 08 de janeiro de 2023. Todas estas questões envolvendo privacidade, proteção de dados, publicidade e controle estão intrinsecamente relacionadas, porém o exame detido delas foge ao escopo específico do presente trabalho.

Diante do exposto até aqui, denota-se imprescindível o conhecimento do processo formativo tanto do direito à privacidade como do direito à proteção de dados de modo a ter acesso e respeitar o manancial principiológico e normativo de onde surgiram, bem como saber como estes direitos deverão se acomodar na conjuntura social contemporânea, a fim solucionar as questões, problemas e tensões envolvendo os direitos dos titulares de dados pessoais na economia da sociedade da informação.

REFERÊNCIAS

- AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**. Disponível em:
https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf. Acesso em: 01 jul, 2023.
- AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Resolução CD/ANPD nº 2, de 27 janeiro de 2022**. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Diário Oficial da União, edição 20, seção 1, página 6, publicação: 28 jan., 2022. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019>. Acesso em: 01 jul, 2023.
- BATISTA, Ellen Thaís Akemi N. **A (im)possibilidade de proteção *post mortem* dos dados sensíveis com fundamento no princípio da dignidade humana**, 2021, 97 páginas. Área de concentração: Ciências Jurídicas e Sociais. Universidade Federal do Rio Grande do Sul, Porto Alegre, ano de defesa: 2021. Disponível em:
<https://www.lume.ufrgs.br/handle/10183/236484>. Acesso em: 01 jul, 2023.
- BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.
- BONAVIDES, Paulo. **Curso de Direito Constitucional**, 28ª ed. atual., São Paulo: Malheiros, 2013.
- BRASIL, [AI-5 (1968)] **Ato Institucional n.º 5, de 13 de dezembro de 1968**. São mantidas a Constituição de 24 de janeiro de 1967 e as Constituições Estaduais; O Presidente da República poderá decretar a intervenção nos estados e municípios, sem as limitações previstas na Constituição, suspender os direitos políticos de quaisquer cidadãos pelo prazo de 10 anos e cassar mandatos eletivos federais, estaduais e municipais, e dá outras providências. Brasília, DF: Casa Civil, 1968. Disponível em: http://www.planalto.gov.br//CCIVIL_03/AIT/ait-05-68.htm. Acesso em: 01 jul, 2023.
- BRASIL, [Constituição (1824)]. **Constituição Política do Império do Brasil**: outorgada em 25 de março de 1824. Disponível em:
http://www.planalto.gov.br/ccivil_03/constituicao/constituicao24.htm. Acesso em: 01 jul, 2023.
- BRASIL, [Constituição (1891)]. **Constituição da República dos Estados Unidos do Brasil**: promulgada em 24 de fevereiro de 1891. Disponível em:
http://www.planalto.gov.br/ccivil_03/constituicao/constituicao91.htm. Acesso em: 01 jul, 2023.
- BRASIL, [Constituição (1934)]. **Constituição da República dos Estados Unidos do Brasil**:

promulgada em 16 de julho de 1934. Disponível em:

http://www.planalto.gov.br/ccivil_03/constituicao/constituicao34.htm. Acesso em: 01 jul, 2023.

BRASIL, [Constituição (1937)]. **Constituição dos Estados Unidos do Brasil**: outorgada em 10 de novembro de 1937. Disponível em:

http://www.planalto.gov.br/ccivil_03/constituicao/constituicao37.htm. Acesso em: 01 jul, 2023.

BRASIL, [Constituição (1946)]. **Constituição dos Estados Unidos do Brasil**: promulgada em 18 de setembro de 1946. Disponível em:

http://www.planalto.gov.br/ccivil_03/constituicao/constituicao46.htm. Acesso em: 01 jul, 2023.

BRASIL, [Constituição (1967)]. **Constituição da República Federativa do Brasil**:

promulgada em 24 de janeiro de 1967. Disponível em:

http://www.planalto.gov.br/ccivil_03/constituicao/constituicao67.htm. Acesso em: 01 jul, 2023.

BRASIL, [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**: promulgada em 05 de outubro de 1988. Disponível em:

http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 01 jul, 2023.

BRASIL. **Decreto nº. 592, de 6 de julho de 1992**. Promulga o Pacto Internacional sobre Direitos Civis e Políticos. Brasília, DF: Casa Civil, 1992. Disponível em:

http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm. Acesso em: 01 jul, 2023.

BRASIL. **Decreto nº. 678, de 6 de novembro de 1992**. Promulga a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 22 de novembro de 1969.

Brasília, DF: Casa Civil, 1992. Disponível em:

http://www.planalto.gov.br/ccivil_03/decreto/d0678.htm. Acesso em: 01 jul, 2023.

BRASIL. **Decreto nº. 6.135, de 26 de junho de 2007**. Dispõe sobre o Cadastro Único para Programas Sociais do Governo Federal e dá outras providências. Brasília, DF: Casa Civil, 2007. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2007/decreto/d6135.htm. Acesso em: 01 jul, 2023.

BRASIL. **Decreto nº. 6.425, de 04 de abril de 2008**. Dispõe sobre o censo anual da educação. Brasília, DF: Casa Civil, 2008. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/decreto/d6425.htm. Acesso em: 01 jul, 2023.

BRASIL. **Decreto nº. 6.523, de 31 de julho de 2008**. Regulamenta a Lei no 8.078, de 11 de setembro de 1990, para fixar normas gerais sobre o Serviço de Atendimento ao Consumidor - SAC. Brasília, DF: Casa Civil, 2008. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/decreto/d6523.htm. Acesso em: 01

jul, 2023.

BRASIL. **Decreto nº. 8.771, de 11 de maio de 2016.** Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Brasília, DF: Casa Civil, 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm. Acesso em: 01 jul, 2023.

BRASIL. **Decreto nº. 11.016, de 29 de março de 2022.** Regulamenta o Cadastro Único para Programas Sociais do Governo Federal, instituído pelo art. 6º-F da Lei nº 8.742, de 7 de dezembro de 1993. Brasília, DF: Casa Civil, 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/D11016.htm. Acesso em: 01 jul, 2023.

BRASIL. **Decreto nº. 11.034, de 05 de abril de 2022.** Regulamenta a Lei nº 8.078, de 11 de setembro de 1990 - Código de Defesa do Consumidor, para estabelecer diretrizes e normas sobre o Serviço de Atendimento ao Consumidor. Brasília, DF: Casa Civil, 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Decreto/D11034.htm. Acesso em: 01 jul, 2023.

BRASIL. **Lei nº. 3.071, de 1º de janeiro de 1916 (Código Civil de 1916).** Código Civil dos Estados Unidos do Brasil. Brasília, DF: Casa Civil, 1916. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l3071.htm. Acesso em: 01 jul, 2023.

BRASIL. **Lei nº. 7.232, de 29 de outubro de 1984.** Dispõe sobre a Política Nacional de Informática, e dá outras providências. Brasília, DF: Casa Civil, 1984. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7232.htm. Acesso em: 01 jul, 2023.

BRASIL. **Lei nº. 8.069, de 13 de julho de 1990.** Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF: Casa Civil, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 01 jul, 2023.

BRASIL. **Lei nº. 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Casa Civil, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 01 jul, 2023.

BRASIL. **Lei nº. 10.406, de 10 de janeiro de 2002.** Institui o Código Civil. Brasília, DF: Casa Civil, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 06 jul, 2023.

BRASIL. **Lei nº. 12.414, de 9 de junho de 2011.** Disciplina a formação e consulta a bancos de dados com informações de adimplimento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, DF: Casa Civil, 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 01 jul,

2023.

BRASIL. **Lei nº. 12.965, de 23 de abril de 2014 (Marco Civil da Internet)**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Casa Civil, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 01 jul, 2023.

BRASIL. **Lei nº. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Casa Civil, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 01 jul, 2023.

BRASIL. **Lei nº. 13.787, de 27 de dezembro de 2018**. Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. Brasília, DF: Casa Civil, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13787.htm. Acesso em: 01 jul, 2023.

BRASIL. **Medida Provisória nº. 954, de 17 de abril de 2020**. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Brasília, DF: Casa Civil, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. Acesso em: 01 jul, 2023.

BRASIL. Superior Tribunal de Justiça. Quarta Turma. **Acórdão no Recurso Especial nº. 22.337-8/RS**, Relator: Ministro Ruy Rosado de Aguiar, Brasília, DF, julgamento: 13 fev, 1995, publicação: 20 mar. 1995, **Revista do Superior Tribunal de Justiça**, nº. 77, ano 1996, Quarta Turma. Disponível em: https://www.stj.jus.br/docs_internet/revista/electronica/stj-revista-electronica-1996_77_capQuartaTurma.pdf. Acesso em: 01 jul, 2023.

BRASIL. Superior Tribunal de Justiça. Quarta Turma. **Acórdão no Recurso Especial nº. 1.168.547/RJ**, Relator: Ministro Luís Felipe Salomão, Brasília, DF, julgamento: 11 maio, 2010, publicação: 07 fev. 2011, online. Disponível em: https://processo.stj.jus.br/processo/pesquisa/?src=1.1.3&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&num_registro=200702529083. Acesso em: 01 jul, 2023.

BRASIL. Superior Tribunal de Justiça. Quarta Turma. **Acórdão no Recurso Especial nº. 1348532/SP**, Relator: Ministro Luís Felipe Salomão, Brasília, DF, julgamento: 10 out., 2017, publicação: 30 nov. 2017, online. Disponível em: <https://processo.stj.jus.br/processo/pesquisa/?aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&termo=REsp%201348532>.

Acesso em: 01 jul, 2023.

BRASIL. Supremo Tribunal Federal. Tribunal Pleno. **Acórdão no Recurso de Habeas Data nº. 22-8/DF**, ementário nº. 1798-01, Relator: Ministro Marco Aurélio, Brasília, DF, julgamento: 19 set, 1991, publicação: 01 set. 1995, online. Disponível em: <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=362613>. Acesso em: 01 jul, 2023.

BRASIL. Supremo Tribunal Federal. Tribunal Pleno. **Acórdão no Recurso Extraordinário nº. 418-416-8/SC**, ementário nº. 2261-06, Relator: Ministro Sepúlveda Pertence, Brasília, DF, julgamento: 10 maio, 2006, publicação: 19 dez. 2006, online. Disponível em: <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=395790>. Acesso em: 01 jul, 2023.

BRASIL. Supremo Tribunal Federal. Tribunal Pleno. **Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.389 Distrito Federal**. Relator: Ministra Rosa Weber, Brasília, DF, julgamento: 07 maio, 2020, publicação: 12 nov., 2020, online. Disponível em: https://jurisprudencia.stf.jus.br/pages/search?classeNumeroIncidente=%22ADI%206389%22&base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&sort=_score&sortBy=desc&isAdvanced=true. Acesso em: 01 jul, 2023.

CÂMARA DOS DEPUTADOS. **Exposição de motivos do Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal**, online. Disponível em: <https://escola.mpu.mp.br/a-escola/comunicacao/noticias/especialistas-discutem-anteprojeto-da-lgpd-penal/anteprojeto-lgpd-penal.pdf>. Acesso em: 01 jul, 2023.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº. 3420/2019**. Altera o a (sic) Lei nº 13.709, de 14 de agosto de 2018, a fim de alterar o critério da multa aplicada às entidades de direito privado em caso de vazamento de dados pessoais, online. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2207337>. Acesso em: 01 jul, 2023.

CARDOSO, Carlos. **Armazenagem de dados em DNA atinge densidade teórica de 215 petabytes por grama**. Disponível em: <<https://meiobit.com/387476/armazenagem-de-dados-em-dna-atinge-densidade-teorica-de-215-petabytes-por-grama/>>. Acesso em: 01 jul, 2023.

COLOMBO, Cristiano. (2017). Antecedentes Históricos Sobre o Direito de Privacidade no Direito Brasileiro. **Revista Eletrônica Direito & TI**, 1(7), 5. Disponível em: <https://www.direitoeti.com.br/direitoeti/article/view/74>. Acesso em: 01 jul, 2023.

COLOMBO, Cristiano (2015). Da Privacidade como Direito de Personalidade no Mundo Virtual e sua Positivização no Ordenamento Jurídico Brasileiro. **Revista Eletrônica Direito & TI**, 1(2), 6. Disponível em: <https://www.direitoeti.com.br/direitoeti/article/view/16>. Acesso em: 01 jul, 2023.

COMITÊ GESTOR DA INTERNET NO BRASIL. **92 milhões de brasileiros acessam a**

Internet apenas pelo telefone celular, aponta TIC Domicílios 2022. Disponível em: <<https://www.cgi.br/noticia/releases/92-milhoes-de-brasileiros-acessam-a-internet-apenas-pelo-telefone-celular-aponta-tic-domicilios-2022/>>. Acesso em: 01 jul, 2023.

COMPARATO, Fábio Konder. **A afirmação histórica dos direitos humanos.** 6ª ed. rev. e atual. São Paulo: Saraiva, 2008.

CONSELHO DA JUSTIÇA FEDERAL. **V Jornada de Direito Civil**, Organização: Ministro Ruy Rosado de Aguiar Jr. Brasília, DF: CJF, 2012. Disponível em: <https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/vjornadadireitocivil2012.pdf>. Acesso em: 01 jul, 2023.

COUNCIL OF EUROPE. 1981. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data** (ETS No. 108). Disponível em: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108>. Acesso em: 01 jul, 2023.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: Fundamentos da Lei Geral de Proteção de Dados**, 3ª edição. São Paulo: Thomson Reuters, 2021.

ESTRATÉGIA NACIONAL DE COMBATE À CORRUPÇÃO E À LAVAGEM DE DINHEIRO. **Nota Técnica contendo a avaliação, propostas de alterações, contrastando o texto do anteprojeto com Convenções, recomendações e melhores práticas internacionais, em relação ao Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal – LGPD-Penal**, online. Disponível em: <http://enccla.camara.leg.br/acoes/arquivos/resultados-enccla-2021/e2021a4-enccla-2021-nota-tecnica-lgpd-penal>. Acesso em: 01 jul, 2023.

EUROPEAN COMMISSION. **Article 29 Working Party. Opinion 03/2013 on purpose limitation.** Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. Acesso em: 01 jul, 2023.

EUROPEAN COUNCIL, 1995. **Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.** Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=cele>. Acesso em: 01 jul, 2023.

EUROPEAN COURT OF HUMAN RIGHTS. **Convention for the Protection of Human Rights and Fundamental Freedoms (Convenção Europeia de Direitos Humanos).** Disponível em: <https://www.echr.coe.int/Pages/home.aspx?p=basictexts/convention>. Acesso em: 01 jul, 2023.

FACHINETTI, Aline Fuke; CAMARGO, Guilherme. **Convenção 108+: o tratado de proteção de dados e a relevância do tema para o Brasil.** Disponível em: <https://www.conjur.com.br/2021-jul-04/opinioao-convencao-108-relevancia-protacao-dados>. Acesso em: 01 jul, 2023.

FEDERAÇÃO BRASILEIRA DE BANCOS. **LGPD está fora da realidade de 80% das empresas no Brasil, diz estudo.** Disponível em:

<<https://febrabantech.febraban.org.br/blog/lgpd-esta-fora-da-realidade-de-80-das-empresas-no-brasil-diz-estudo>>. Acesso em: 01 jul, 2023.

FERREIRA, Natália Augusta de Paula Almeida da Silva. **Proteção de dados pessoais: conformidade à luz da lei 13.709/2018**, 2021. 101 páginas. Área de concentração: Ciências Humanas e Sociais. Universidade Federal Fluminense, Volta Redonda, ano de defesa: 2021. Disponível em: <https://app.uff.br/riuff/bitstream/handle/1/24333/NATHALIA%20AUGUSTA%20DE%20PAULA%20ALMEIDA%20DA%20SILVA%20FERREIRA.pdf?sequence=1>. Acesso em: 01 jul, 2023.

GIBSON, William. Johnny Mnemonic (1981). **Revista Omni Magazine**, issue May 1981.

Disponível em:

https://ia800108.us.archive.org/1/items/OMNI197908/OMNI_1981_05.pdf. Acesso em 01 jul. 2023.

GOVERNMENT OF CANADA. Revised Statutes of Canada: **Privacy Act**, 1985. Disponível em: <https://laws-lois.justice.gc.ca/eng/acts/P-21/page-1.html>. Acesso em: 01 jul, 2023.

GOVERNMENT OF CANADA. Statutes of Canada: **Personal Information Protection and Electronic Documents Act**, 2000. Disponível em: <https://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-1.html#h-416885>. Acesso em: 01 jul, 2023.

GOVERNMENT OF JAPAN, 2003. Act n° 57 of 2003: **Act on the Protection of Personal Information (APPI)**. Versão inglesa através das revisões do Act n° 119 de 2003 em conformidade com o Dicionário Bilingue Padrão (edição de março de 2006) do original japonês. Disponível em: <https://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf>. Acesso em: 01 jul, 2023.

GUERRA, Sidney. **Curso de direitos humanos**. 6. ed. São Paulo: Saraiva, 2020. E-book.

HARARI, Yuval Noah. **Sapiens - uma breve história da humanidade**, 33ª edição. Porto Alegre, RS: L&PM, 2018, pp. 31-32.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. **Internet já é acessível em 90,0% dos domicílios do país em 2021**. Disponível em:

<<https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/34954-internet-ja-e-acessivel-em-90-0-dos-domicilios-do-pais-em-2021>>. Acesso em: 01 jul, 2023.

KALVEN JUNIOR, Harry. Privacy in Tort Law - Were Warren and Brandeis Wrong? **Law and Contemporary Problems**, vol. 31, n° 2. Duke Law Scholarship Repository, 1966.

Disponível em: <https://scholarship.law.duke.edu/lcp/vol31/iss2/7/>. Acesso em: 01 jul, 2023.

KERSHNER, Michael. **Data isn't the new oil - Time is**. Disponível em:

<<https://www.forbes.com/sites/theyec/2021/07/15/data-isnt-the-new-oil--time-is/>>

[sh=230cd84d35bb](#) >. Acesso em: 01 jul, 2023.

LARGHI, Natália. **Veja o ranking das empresas mais valiosas do mundo (e saiba quem é a única latino-americana)**. Disponível em: <<https://valorinveste.globo.com/mercados/renda-variavel/empresas/noticia/2022/06/15/veja-o-ranking-das-empresas-mais-valiosas-do-mundo-e-saiba-quem-e-a-unica-latino-americana.ghtml>>. Acesso em: 01 jul, 2023.

LUZ SEGUNDO, Elpídio Paiva. Direitos da personalidade: quo vadis?. **Revista de Direito da Faculdade Guanambi**, Guanambi, v. 7, n. 01, e280, jan./jun. 2020. doi: <https://doi.org/10.29293/rdfg.v7i01.280>. Disponível em: <http://revistas.faculdadeguanambi.edu.br/index.php/Revistadedireito/article/view/280>. Acesso em: 01 jul, 2023.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de Dados comentada** / coordenadores: Viviane Nóbrega Maldonado e Renato Opice Blum. - 2ª ed. rev., atual. e ampl.; - São Paulo: Thomson Reuters Brasil, 2019.

MARMELSTEIN, George. **Curso de Direitos Fundamentais**. 3. ed. São Paulo: Atlas, 2011 (1ª edição, 2008).

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

MONTEIRO, Renato Leite; BIONI, Bruno. **Que tal uma pizza de tofu com rabanetes? Você vai adorar!**. Disponível em: <https://renatoleitemonteiro.jusbrasil.com.br/artigos/198336962/que-tal-uma-pizza-de-tofu-com-rabanetes-voce-vai-adorar>. Acesso em: 01 jul, 2023.

MOTA, Júlia Cláudia R. da C.; MOTA, Juliana da C. **Breves considerações sobre a Lei Geral de Proteção de Dados e sobre o Registro Civil das Pessoas Naturais**. Instituto Brasileiro de Direito de Família (IBDFAM), online. Disponível em: <https://ibdfam.org.br/artigos/1669/Breves+considera%C3%A7%C3%B5es+sobre+a+Lei+Geral+de+Prote%C3%A7%C3%A3o+de+Dados+e+sobre+o+Registro+Civil+das+Pessoas+Naturais>. Acesso em: 01 jul, 2023.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. Disponível em: <https://www.ohchr.org/en/human-rights/universal-declaration/translations/portuguese?LangID=por>. Acesso em: 01 jul, 2023.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, 1980. **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**. Disponível em: <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsopersonaldata.htm>. Acesso em: 01 jul, 2023.

PAESANI, Liliana Minardi. **Direito de informática: comercialização e desenvolvimento**

internacional do software. - 8ª ed.. São Paulo: Atlas, 2012.

PARLAMENTO EUROPEU; CONSELHO; COMISSÃO, 2000. **Carta dos Direitos Fundamentais da União Europeia**. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:12012P/TXT>. Acesso em: 01 jul, 2023.

PASCOAL, Flávia. **A tutela da privacidade na internet**. Disponível em: <https://flaviapascoal.jusbrasil.com.br/artigos/487527109/a-tutela-da-privacidade-na-internet>. Acesso em: 01 jul, 2023.

QUEDEVEZ, Gustavo Fiuza; SIMONI, André. **O empregado como operador de dados pessoais: como as relações de trabalho se encaixam na LGPD?** Disponível em: <https://administradores.com.br/noticias/o-empregado-como-operador-de-dados-pessoais-como-as-relacoes-de-trabalho-se-encaixam-na-lgpd>. Acesso em: 01 jul, 2023.

RAMOS, André de Carvalho. **Curso de direitos humanos**. 8. ed. São Paulo: Saraiva, 2021. E-book.

REPUBLIC OF SOUTH AFRICA, 2013. **Act nº. 04 of 2013: Protection of Personal Information Act (POPIA)**. Versão inglesa do original no idioma sul-africano constante na Government Gazette, vol. 581, nº. 912, Cape Town, 2013. Disponível em: https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf. Acesso em: 01 jul, 2023.

SENADO FEDERAL. **Constituições brasileiras**. Disponível em: <https://www12.senado.leg.br/noticias/glossario-legislativo/constituicoes-brasileiras>. Acesso em: 01 jul, 2023.

SENADO FEDERAL. **Promulgada emenda que trata da proteção de dados pessoais**. Disponível em: <https://www12.senado.leg.br/tv/programas/noticias-1/2022/02/promulgada-emenda-constitucional-que-trata-da-protacao-de-dados-pessoais>. Acesso em: 23 maio, 2022.

SENADO FEDERAL. **Senado analisa projeto que regulamenta a inteligência artificial**. Disponível em: <<https://www12.senado.leg.br/noticias/materias/2023/05/12/senado-analisa-projeto-que-regulamenta-a-inteligencia-artificial>>. Acesso em: 01 jul. 2023.

SORRENTINO, Eduardo. **Poucos brasileiros sabem o que é LGPD, aponta pesquisa**. Disponível em: <<https://olhardigital.com.br/2021/08/10/videos/poucos-brasileiros-sabem-o-que-e-lgpd-aponta-pesquisa/>>. Acesso em: 01 jul, 2023.

SUPERIOR TRIBUNAL DE JUSTIÇA. Primeira Turma. **Súmula nº. 2**. Não cabe o habeas data (CF, art. 5.0., LXXII, letra a) se não houve recusa de informações por parte da autoridade administrativa. DJ 10.05.1990, p. 4359. Disponível em: https://www.stj.jus.br/docs_internet/revista/eletronica/stj-revista-sumulas-2005_1_capSumula2.pdf. Acesso em: 01 jul, 2023.

SUPREME COURT OF GEORGIA. **Pavesich v. New England Life Ins. Co.** Publicado em: 03 mar. 1905. Disponível em: <https://casetext.com/case/pavesich-v-new-england-life-ins-co>. Acesso em: 01 jul, 2023.

SUPREME COURT OF THE UNITED STATES OF AMERICA. **Griswold v. Connecticut**, 381, US 479 (1965). Disponível em: <https://supreme.justia.com/cases/federal/us/381/479/>. Acesso em 16 fev. 2022.

SUPREME COURT OF THE UNITED STATES OF AMERICA. **Olmstead v. United States**, 277 U.S. 438 (1928). Decidido em: 04 jun. 1928. Disponível em: <https://supreme.justia.com/cases/federal/us/277/438/>. Acesso em: 01 jul, 2023.

SUPREMO TRIBUNAL FEDERAL. **Supremo começa a julgar compartilhamento de dados de usuários de telefonia com o IBGE.** Disponível em: <https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442823&ori=1>. Acesso em: 01 jul, 2023.

UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR).** Disponível em: <https://gdpr-info.eu/>. Acesso em: 01 jul, 2023.

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT. **Data Protection and Privacy Legislation Worldwide.** Disponível em: <<https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>>. Acesso em: 06 jul, 2023.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, vol. 4, n° 5, pp. 193-220. Disponível em: https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html#:~:text=Harvard%20Law%20Review.&text=hat%20the%20individual%20shall%20have,and%20extent%20of%20such%20protection. Acesso em: 01 jul, 2023.

ZANINI, Leonardo Estevam de Assis. O surgimento e o desenvolvimento do right of privacy nos Estados Unidos. **Revista de Doutrina da 4ª Região**, Porto Alegre, n.64, fev. 2015. Disponível em: https://revistadoutrina.trf4.jus.br/artigos/edicao064/Leonardo_Zanini.html. Acesso em: 01 jul, 2023.