UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS
FACULDADE DE DIREITO

O DIREITO À PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL AUTÔNOMO

Uma análise do direito fundamental à proteção de dados sob a ótica de sua separação do direito à privacidade

NICOLE NEPOMUCENO FERREIRA

Rio de Janeiro
2021.1

NICOLE NEPOMUCENO FERREIRA

O DIREITO À PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL AUTÔNOMO

Uma análise do direito fundamental à proteção de dados sob a ótica de sua separação do direito à privacidade

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de Bacharel em Direito, sob a orientação da Professora Me. Júlia Massadas Romeiro Fraga.

Rio de Janeiro

2021.1

NICOLE NEPOMUCENO FERREIRA

O DIREITO À PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL AUTÔNOMO

Uma análise do direito fundamental à proteção de dados sob a ótica de sua separação do direito à privacidade

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de Bacharel em Direito, sob a orientação da Professora Me. Júlia Massadas Romeiro Fraga.

Data da Aprovação:_____/____/_____.

Banca Examinadora:

_____
Orientador

_____
Membro da Banca

_____
Membro da Banca

Rio de Janeiro

2021.1

CIP - Catalogação na Publicação

F383d

Ferreira, Nicole Nepomuceno
O DIREITO À PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL AUTÔNOMO: Uma análise do direito fundamental à proteção de dados sob a ótica de sua separação do direito à privacidade / Nicole Nepomuceno Ferreira. -- Rio de Janeiro, 2021.
86 f.

Orientadora: Júlia Massadas Romeiro Fraga.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade Nacional de Direito, Bacharel em Direito, 2021.

1. Proteção de dados pessoais. 2. Privacidade. 3. Direitos fundamentais. 4. Autonomia. 5. Tutela de dados pessoais no Brasil. I. Fraga, Júlia Massadas Romeiro, orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

AGRADECIMENTOS

Durante minha trajetória acadêmica na prestigiada Faculdade Nacional de Direito, tive a honra e a felicidade de contar com o suporte e o incentivo de muitas pessoas, sem as quais certamente não teria sido tão agradável e proveitosa. Porém, bem antes desse sonho ser possível, fui abençoada por ter sido criada pelos meus maravilhosos pais, que sempre me incentivaram e me proporcionaram o melhor, nunca permitindo que eu duvidasse da minha capacidade de atingir qualquer objetivo que eu estabelecesse para mim mesma: a Rosimara e Sérgio, todo o meu amor e gratidão eternos; sem vocês eu nada seria!

Agradeço à minha família e, principalmente, a minha querida prima Júlia Nepomuceno por sempre me auxiliar, ainda que apenas me ouvindo quando precisei. Obrigada por ser tão generosa, engraçada, confidente e amorosa comigo. Você é uma preciosidade na minha vida, desde que nasceu, e sempre será.

À minha madrinha Tia Denise, que, mesmo não estando mais entre nós para ver meu sucesso (e a tão esperada formatura), sempre torceu por mim e sei que, onde quer que esteja, está muito feliz por eu ter completado esse ciclo.

Aos componentes do Animus Falandi e do Valar Morghulis, agradeço por todas as conversas, geralmente acaloradas, mas sempre mantendo a amizade. Ana Clara Motta, Bernardo Zordan, Daniel Felipe, Eduarda Nascimento, Felipe Almeida, Felipe Santos, Emily Bueri e Pedro Franco: eu não poderia escolher um grupo melhor para me acompanhar nesses cinco anos. Que venham vários anos de disputas acirradas no totó (que permanecerei vencendo)!

A todos os amigos que a UFRJ me deu, por terem sido fonte de apoio dentro e fora da faculdade, em especial às amizades que fortaleci nos últimos anos, as minhas queridas Raquel Nunes e Tayara Causanilhas: vocês foram essenciais na minha jornada dentro e fora dos muros da FND. Vou levar vocês por toda a minha vida. Muito obrigada por tudo.

Obrigada ao meu chefe do coração, Dr. Gustavo Magno, por ter contribuído tanto para o meu crescimento pessoal e profissional. Você é o modelo de chefe que todo gabinete deveria ter! Obrigada, também, pela oportunidade de estagiar no melhor Ofício da PR/RJ, onde conheci pessoas incríveis: Júlio Bandeira e Igor Gaio, vocês são fora de série! Sempre me recordo com muito carinho de todos os momentos que vivi com todos vocês!

Agradeço profundamente ao meu amado Gabriel, por me ensinar tanto e por ter estado comigo todos esses anos, me dando muito amor e suporte em todos os aspectos possíveis. Simplesmente não consigo por em palavras tudo que sinto. Obrigada por topar caminhar todas as jornadas comigo.

Meus sinceros agradecimentos a Deus, a todos que de alguma forma me ajudaram nessa caminhada e à Universidade Federal do Rio de Janeiro, por ter me proporcionado ensino público gratuito e da maior qualidade, podendo, assim, seguir meus sonhos com a certeza de que minha formação me permitirá chegar onde eu quiser.

RESUMO

A crescente utilização de dados pessoais no contexto da Sociedade da Informação criou novos riscos à proteção da pessoa e de seus direitos fundamentais e, nesse sentido, essa pesquisa tem por objetivo analisar o panorama geral da proteção de dados pessoais no ordenamento jurídico brasileiro e seu surgimento enquanto direito fundamental autônomo. Para tanto, inicia-se apresentando sua origem no direito à privacidade e sua evolução até consolidar-se como direito autônomo, utilizando como parâmetro o direito europeu e passando pelo estudo dos seus princípios basilares, bem como impactos no exercício de outros direitos fundamentais. Atingindo o cerne principal, diferencia-se o direito à proteção de dados pessoais do direito à privacidade com base na ideia de liberdade positiva, principalmente considerando o peso da autodeterminação na matéria, pelo que se propõe o abandono do conceito "expansionista" de privacidade em razão da sua insuficiência para tutelar dados pessoais. O reconhecimento do direito fundamental à proteção de dados pessoais como direito fundamental autônomo já pode ser identificado no aspecto institucional, especialmente pelo Supremo Tribunal Federal e por meio de iniciativas legislativas, notadamente a PEC nº 17/2019, que busca incluir o direito fundamental à proteção de dados pessoais expressamente na Constituição Federal.

Palavras-chave: Proteção de dados pessoais; Privacidade; Direitos fundamentais; Autonomia; Impactos; Tutela de dados pessoais no Brasil.

ABSTRACT

The growing use of personal data in the context of the Information Society has created new risks to the protection of the individual and their fundamental rights so, in this sense, this research aims to analyze the general panorama of personal data protection in the Brazilian legal system and its emergence as an autonomous fundamental right. To this end, the present work begins by presenting its origin in the right to privacy and its evolution to consolidation as an autonomous right, using European law as a parameter and going through the study of its basic principles, as well as the impacts on the exercise of other fundamental rights. Reaching the main core, the right to protection of personal data is separated from the right to privacy based on the idea of positive freedom, mainly considering the weight of self-determination on the matter, for which reason it is proposed to abandon the "expansionist" concept of privacy due to its insufficiency to protect personal data. The recognition of the fundamental right to protection of personal data as an autonomous fundamental right can already be identified in the institutional aspect, especially by the Federal Supreme Court and through legislative initiatives, notably PEC no. 17/2019, which seeks to include the fundamental right to protection of personal data explicitily in the Federal Constitution.

Keywords: Data protection; Privacy; Fundamental rights; Autonomy; Impacts; Data protection in Brazil.

SUMÁRIO

INTRODUÇÃO

Há uma grande discussão sobre a ideia de que a privacidade no século XXI está morta, e talvez esteja mesmo, ao menos enquanto considerada como um direito puramente ligado à proteção da intimidade e à vida privada, entretanto esse pensamento provavelmente existe em razão de um problema com a terminologia utilizada: a própria palavra "privacidade". Ela não é mais capaz de traduzir toda a dinâmica criada pelo grande avanço tecnológico e o surgimento da sociedade da informação, expressão que busca traduzir o *status quo* após a profunda transformação gerada na sociedade pela tecnologia e a forma como esses dois elementos se relacionam.

Conforme Castells, algumas características da sociedade da informação são a colocação da informação como elemento central – a tecnologia se desenvolve para incrementar a atividade de agir sobre informação, e não mais o contrário – e o modo como a tecnologia faz parte de toda atividade humana, englobando atividades nos âmbitos individual e coletivo. Estas características são facilmente verificadas no cotidiano, ao passo que diversas atividades são realizadas por meio de dispositivos tecnológicos, como trabalhar pelo computador (o chamado *home office*), relacionar-se com outras pessoas por meio de redes sociais, fazer transações bancárias por aplicativos no celular e comprar por meio de sites[1].

É inegável a profunda transformação operada pela evolução da tecnologia e a forma como ela tornou-se essencial à vida humana, praticamente indissociável até mesmo de atividades triviais. Desse modo, tamanha interconectividade criou novos problemas concernentes à informação que antes não existiam, fazendo com que o direito à privacidade se tornasse insuficiente para atuar nas novas relações que foram estabelecidas e continuam se formando a cada minuto.

A ideia de privacidade, antes constituída sob a concepção de liberdade negativa, isto é, liberdade do indivíduo de impedir intromissões na sua vida privada[2], mostrou-se insuficiente à

---

[1]CASTELLS, Manuel. **A sociedade em rede**. 3. ed. São Paulo: Paz e Terra, 2000, p. 108.

[2]Neste sentido: ANTONIALLI, Dennys. **Privacy and International Compliance: when differences become an issue**. In: Intelligent Information Privacy Management (AAAI Spring Symposium Series), 2010, p. 14. Intelligent Information Privacy Management (AAAI Spring Symposium Series). Disponível em: https://www.aaai.org/ocs/index.php/SSS/SSS10/paper/viewFile/1165/1470. Acesso em 09 mar. 2021. e BIONI, Bruno. **Proteção de dados pessoais: as funções e os limites do consentimento**. In: ___. Estabelecendo um

medida em que não bastava somente fechar a porta de casa para proteger-se de violações. A internet possibilitou um inúmero de relações com o mundo virtual e suas consequências vão além do que o conceito de privacidade pode abarcar.

Um exemplo disso é o rastreamento da atividade virtual dos indivíduos por meio de ferramentas tecnológicas, notadamente os *cookies*, responsáveis pela coleta de dados de navegação. Assim, as interações na internet são traduzíveis em dados reveladores de informações sobre o usuário[3], como seus padrões de comportamento, suas preferências e outras características mais sensíveis, cujo processamento é objeto de interesse por parte dos agentes de tratamento.

A proteção não mais diz respeito somente a espaços ou bens e agora centra-se na própria personalidade da pessoa, atingindo-a tanto em sua esfera pessoal quanto em sua relação com a sociedade. O indivíduo, por sua vez, não possui controle sobre a extração seus dados, tampouco sobre sua posterior utilização por parte dos agentes de tratamento, de modo que é colocado na posição de "mero expectador das suas informações"[4].

Por mais que possa parecer, Simson Garfinkel aponta que a tecnologia não é, em si, neutra, pelo contrário: ela é inerentemente intrusiva. Isso se dá pois ela é estruturada de modo a favorecer os interesses das empresas, justamente pelo fato de que a proteção da privacidade dos usuários não faz parte de seus objetivos[5].

Entretanto, este não é um problema exclusivo do século XXI e a preocupação com a adaptabilidade dos sistemas jurídicos a esse tipo de situação surgiu no século passado, possuindo diversas denominações: privacidade informacional, autodeterminação informativa ou simplesmente proteção de dados pessoais, entre outras. Essa disciplina surge para proteger a autonomia e liberdade dos indivíduos quanto a sua personalidade refletida em seus dados pessoais e, posteriormente, é possível verificar que seus impactos não ficam somente no campo da liberdade, atingindo também a igualdade material, ao passo que a criação de dossiês digitais sobre cada indivíduo determina inclusive as oportunidades sociais que lhe serão permitidas.

---

diálogo entre o direito à privacidade (liberdade negativa) e à proteção dos dados pessoais (liberdade positiva). Rio de Janeiro: Gen, 2019, p. 124-128. *E-book*.

[3] BIONI. *Op. Cit.*, p. 43.

[4] BIONI. *Op. Cit.*, p. 39.

[5] GARFINKEL, Simson. **Database nation**. Sebastopol: O'Reillly, 2000, p. 259-260.

A evolução do conceito de direito à privacidade até o direito à proteção de dados pessoais, juntamente às mudanças sociais que acompanharam o desenvolvimento tecnológico, levaram ao seu reconhecimento por diversos ordenamentos jurídicos como um direito fundamental. A Carta dos Direitos Fundamentais da União Europeia[6], ainda em 2000, positivou em seu artigo 8º o direito à proteção de dados pessoais como um direito fundamental no direito comunitário europeu, uma vez que o cidadão é posto em uma relação assimétrica em que se torna muito mais vulnerável às mais diversas violações de seus direitos informacionais.

No Brasil, as leis expressamente resguardam o sigilo das comunicações, porém, como dito pelo Exmo. Ex-Ministro do STF Sepúlveda Pertence, não é verdadeira a afirmação de que protegem os dados em si. Entretanto, a jurisprudência vem evoluindo no sentido de reconhecer a fundamentalidade e a autonomia do direito à proteção de dados pessoais, notadamente na decisão proferida no bojo da ADI 6387.

Nesse sentido, a Decisão da Corte Constitucional Alemã sobre a Lei do Censo de 1983 cunhou o direito fundamental à autodeterminação informativa a fim de permitir o livre desenvolvimento da personalidade e de dar ao indivíduo poder de determinar o fluxo de informações sobre si mesmo. Nesse sentido, Laura Schertel aponta, com base na decisão, que:

> (...) o moderno processamento de dados pessoais configura uma grave ameaça à personalidade do indivíduo, na medida em que possibilita o armazenamento ilimitado de dados, bem como permite a sua combinação de modo a formar um retrato. O direito fundamental à proteção de dados pessoais completo da pessoa, sem a sua participação ou conhecimento [7].

Portanto, é necessária a tutela diferenciada desse direito inerentemente determinantes para o exercício da própria personalidade do indivíduo e dos demais direitos fundamentais. Conforme afirma Doneda, o reconhecimento da proteção de dados como um direito autônomo

---

[6] A referida legislação foi substituída por nova versão em 2016, após o Tratado de Lisboa de 2009, que conferiu à Carta status vinculativo. Porém, para o argumento proposto, importa o que foi positivado na primeira versão, editada no ano de 2000: UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32000X1218(01)&qid=1617650366391&from=EN. Acesso em 05 mar. 2021.

[7] MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor**. São Paulo: v. 79, jul/set, 2011., p. 4-5.

e fundamental não é um mandamento explícito, mas, sim, em razão da dimensão dos riscos que o tratamento de dados oferece à a princípios constitucionais, como a "igualdade substancial, liberdade e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada"[8].

É neste sentido que se mostra imprescindível o estudo e reflexão sobre o tema, ao passo que tais violações ferem não somente a existência digna de um indivíduo em particular, como também ameaçam o equilíbrio da relação entre a sociedade e a internet num contexto em que é impossível a sua dissociação.

Diante desse cenário, esse trabalho tem como objetivo descobrir se o direito fundamental à proteção de dados existe perante o ordenamento jurídico brasileiro, assim como questiona o aparente descaso da legislação pátria com relação ao tema, haja vista que trata a matéria diversas vezes conforme o direito de vários países que reconhecem o direito fundamental à proteção de dados pessoais, porém não contempla expressamente a autodeterminação afirmativa com status fundamental. Apesar do disposto, é possível identificar uma mudança jurisprudencial e legislativa nesse sentido, como as decisões do STF no ano de 202 e a PEC nº 17/2019.

Isso posto, pretende evidenciar a importância do reconhecimento do status de direito fundamental aos dados pessoais, tomando por base as provisões constitucionais e sua adequação à realidade atual, os fundamentos que deram origem à LGPD, a Declaração de Santa Cruz de La Sierra e a movimentação das Instituições no sentido de reconhecê-lo.

Para tanto, no capítulo 1 tratarei do surgimento do direito à privacidade e sua dissociação fático-temporal do direito à proteção de dados pessoais, passando a expor sobre o desenvolvimento das gerações de leis sobre o tema no continente europeu, com base na teoria de Mayer-Schönberger. Além disso, discorrerei ao final sobre seus princípios basilares a partir das *Privacy Guidelines* da OCDE.

No capítulo 2, será feita uma análise sobre conceitos basilares de dados pessoais, dados sensíveis e dados anônimos ou anonimizados, trazidos pela doutrina, pela LGPD e por

[8]DONEDA, Danilo. **A proteção de dados pessoais como direito fundamental.** v. 12, n. 2. Joaçaba: Espaço Jurídico, 2011, p. 103.

normativas europeias. Logo após, tratarei do assunto sob a ótica dos demais direitos fundamentais: o reconhecimento do direito à proteção de dados pessoais como um novo direito da personalidade e seus impactos na esfera da liberdade e da igualdade.

O capítulo 3, por sua vez, versará sobre o caso europeu, escolhido em razão de sua extensa produção normativa sobre proteção de dados pessoais, discorrendo sobre a célebre decisão do Tribunal Constitucional Alemão sobre da Lei do Censo de 1983, bem como os paradigmas que alteraram a posição de direito fundamental perante o direito comunitário europeu, com a Carta dos Direitos Fundamentais da União Europeia de 2000 e sua regulamentação por meio da *General Data Protection Regulation*.

Por fim, o capítulo 4 concentra-se no contexto brasileiro, expondo os motivos pelos quais o direito à proteção de dados deve ser considerado um direito fundamental e autônomo à privacidade, sob a ótica da característica de interdependência entre o sistema de direitos fundamentais e a de liberdade negativa deste último direito, defendendo o abandono do seu conceito "expansionista" frente à incapacidade de abarcar todas as situações em que a proteção de dados exige tutela específica. A partir disso, analisa-se a sistemática de direitos trazida pela CF/88 e a colocação do Habeas Data como instrumento de efetivação da tutela de dados pessoais, bem como outros instrumentos e disposições esparsas no Código de Defesa do Consumidor e Marco Civil da Internet até a vigência da Lei Geral de Proteção de Dados Pessoais, principal norma infraconstitucional sobre a matéria no Brasil até o momento, e iniciativas legislativas e jurisprudenciais acerca do reconhecimento desse novo direito fundamental.

1 O DIREITO À PROTEÇÃO DE DADOS PESSOAIS COMO UM DIREITO FUNDAMENTAL

Oscar Wilde, em sua obra intitulada "De Profundis"[9] escreveu sobre o isolamento e solidão vividos durante os anos que esteve preso, discorrendo sobre o grande sofrimento causado por estar só: a prisão lhe tornara um homem solitário e negado pela sociedade. Wilde, assim como outros grandes romancistas do século XIX, ocupou-se do tema da exclusão social e solidão, entretanto mal sabia que, no contexto da atual sociedade da informação, conseguir ser deixado sozinho pode ser uma tarefa árdua.

Um grande exemplo desse desafio é serviço de *telemarketing* automatizado, por meio do qual empresas ligam incessantemente para potenciais clientes, causando grande incômodo pela intromissão indesejada. Certamente boa parte da população diria que seu maior desejo é ser esquecido de vez pelas empresas de *telemarketing*, o que inclusive motivou a ANATEL a criar um serviço em que o consumidor poderá ser excluído da lista de telefones de tais empresas[10], às quais, muitas das vezes, sequer sabe como foi inserido.

Entretanto, para chegar no panorama atual de proteção de dados em que é possível o direito de exclusão de informações pessoais dispostas em bancos de dados, como o serviço disponibilizado pela ANATEL, percorreu-se um longo caminho, desde o surgimento do direito à privacidade até sua dissociação ao estudo da proteção de dados pessoais. A fim de compreendê-lo, é preciso entender como se deu o seu desenvolvimento histórico, quais são seus princípios norteadores e como ele se relaciona atualmente com a sociedade da informação, pontos que são o objeto de estudo deste capítulo.

Para tanto, primeiramente será exposta brevemente a gênese o direito à privacidade enquanto direito de estar só e como se deu a sua separação do direito à proteção de dados pessoais, assim como uma análise das leis desta última disciplina e como se deu sua evolução ao longo do tempo de acordo com a experiência europeia. Dados estes passos iniciais, serão

---

[9] WILDE, Oscar. **De Profundis**. Projetos de filosofia. Phoenix-Library, 2001. *E-book*. Disponível em: http://www.dominiopublico.gov.br/pesquisa/DetalheObraForm.do?select_action=&co_obra=3556. Acesso em 20 de ago. 2020.

[10] CADASTRO nacional de "não me perturbe" para serviços de telecom já está disponível. **ANATEL**. Disponível em: https://www.anatel.gov.br/consumidor/noticias/930-cadastro-nacional-de-nao-me-perturbe-para-servicos-de-telecomunicacoes-esta-disponivel-a-partir-de-16-7. Acesso em 18 ago. 2020.

estudados os princípios estabelecidos pela experiência internacional como essenciais à regulação, a fim de melhor situar a matéria a ser estudada.

1.1 ORIGEM: SURGIMENTO DO DIREITO À PRIVACIDADE

Apesar de frequentemente associada aos problemas atuais referentes à sociedade da informação, a proteção de dados pessoais remonta ao século XIX, quando discussões acerca do nascente direito à privacidade começavam a se desenhar. Naquele contexto, bastante marcado pelos ideais liberais e direitos de prestação negativa estatal, o direito à privacidade foi reconhecido como tipicamente burguês, reservado às classes mais elitizadas[11], dados os fatos que originaram tais discussões.

Não há que se falar em direito à privacidade sem mencionar o clássico artigo de Warren e Brandeis, "The Right to Privacy"[12], que trouxe à praça pública a ideia de rompimento entre a antiga ideia de privacidade como direito patrimonial (privacidade enquanto patrimônio individual), associando-o a um direito personalidade[13]. No artigo, cunha-se o que ficou conhecido como o *"right to be let alone"* – o direito de ser deixado só –, em razão do avanço tecnológico no campo da fotografia e da imprensa da época, que permitiu a exposição da vida privada de particulares sem seu consentimento de maneira nunca antes vista[14].

Há de se destacar que o artigo ressalva a aplicação do direito privacidade em relação à publicação de notícias que sejam de interesse público, o que denota mais claramente o interesse principal do trabalho de identificar uma noção de direito protetor dos assuntos que concernem somente à vida doméstica do indivíduo, como diz na passagem:

> *O desenho do direito deve ser no sentido de proteger aquelas pessoas cujos assuntos pessoais a comunidade não possui legítimo interesse de serem arrastadas para uma*

---

[11] MENDES, Laura Schertel. **Transparência e privacidade**: violação e proteção da informação pessoal na sociedade de consumo. Dissertação (Mestrado em Direito). Brasília: Universidade de Brasília, 2008. p. 18.
[12] BRANDEIS, Louis; WARREN, Samuel. **The Right to Privacy**. Harvard Law Review, v. IV, dez. 1890, n. 5. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em 18 ago. 2020.
[13] MENDES. *Op. Cit.*, 2008, p. 17.
[14] "*The right of one who has remained a private individual, to prevent his public portraiture, presents the simplest case for such extension; the right to protect one's self from pen portraiture, from a discussion by the press of one's private affairs, would be a more important and far-reaching one. If casual and unimportant statements in a letter, if handiwork, however inartistic and valueless, if possessions of all sorts are protected not only against reproduction, but also against description and enumeration, how much more should the acts and sayings of a man in his social and domestic relations be guarded from ruthless publicity. If you may not reproduce a woman's face photographically without her consent, how much less should be tolerated the reproduction of her face, her form, and her actions, by graphic descriptions colored to suit a gross and depraved imagination*". BRANDEIS; WARREN. *Op. Cit.*, p. 213-214.

> *indesejável e indesejada publicidade e para proteger todas as pessoas, independentemente de sua posição, podendo ter assuntos que prefiram manter privados tornados públicos contra sua vontade. É a injustificada invasão da privacidade que deve ser repreendida e, dentro do possível, prevenida* [15].

Nessa ótica, "The Rigth to Privacy" foi primeiramente visto como um direito tipicamente burguês e elitista, ao passo que tratava da proteção de personalidades públicas, a exemplo do caso o Príncipe Albert e a Rainha Vitória, no qual um jornalista divulgou sua coleção particular de gravuras[16], ou o romance entre Benito Mussolini de Clara Petacci, entre outros que levaram à construção da ideia de proteção da privacidade[17].

Em seu início, impunha uma atuação negativa do Estado, com fulcro no direito de ser deixado só, todavia a privacidade deixou de ser reservada apenas a celebridades, estendendo-se à população como um todo e essa expansão do direito à privacidade aos demais estratos sociais deu-se por vários motivos, a destacar o surgimento do Estado de Bem-Estar Social ou *Welfare State* durante o século XX. Este período foi marcado pela intensificação do relacionamento entre o Estado e o cidadão, à medida que a atuação estatal na prestação de serviços dependia da individualização dos administrados e burocratização em busca da eficiência dos serviços, o que implicava, necessariamente, da obtenção de dados sobre as pessoas[18].

Ora, a fim de implementar determinada política pública, assim como se dá atualmente, é necessário ter em mãos uma série de informações para a identificação de necessidades, meios de solucionar os problemas e destinatários, e outras atividades inerentes à criação e implementação de prestações estatais.

Desta maneira, a burocratização (necessária ao mapeamento de informações) ocasionou o aumento do fluxo informacional que, conjuntamente ao avanço tecnológico, possibilitaram um maior armazenamento e processamento das informações. Como todos estavam expostos a

---

[15] Tradução livre do trecho original: *"The design of the law must be to protect those persons with whose affairs the community has no legitimate concern, from being dragged into an undesirable and undesired publicity and to protect all persons, whatsoever; their position or station, from having matters which they may properly prefer to keep private, made public against their will. It is the unwarranted invasion of individual privacy which is reprehended, and to be, so far as possible, prevented.". Ibidem*, p. 214-215.

[16] Caso Prince Albert v Strange (1849), no qual a Suprema Corte de Chancery decidiu pela proibição da publicação da coleção pessoal do príncipe. REINO UNIDO. England And Whales High Court. **Prince Albert v Strange**. Disponível em: https://swarb.co.uk/prince-albert-v-strange-chd-8-feb-1849/. Acesso em: 18 ago. 2020.

[17] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**, RENOVAR, 2006, p. 11.

[18] *Ibidem*, p. 12-14.

potenciais violações, o direito à privacidade deixava de ser reservado aos famosos e outras personalidades relevantes, podendo qualquer cidadão ser vítima de suas violações. O aumento da capacidade de fluxo, aliado ao surgimento de técnicas que possibilitavam que fossem tornadas úteis a um custo razoável, aumentou também a importância das informações, já que seu detentor possui um enorme leque de possibilidades de utilização[19].

Como afirma Doneda, os objetivos para a utilização de dados pessoais pelo Estado são, principalmente, o controle e a eficiência. O aparato estatal é eficiente na medida em que conhece a população e identifica seus problemas, utilizando-se, por exemplo de censos e pesquisas e outras maneiras, como "o estabelecimento de regras para tornar compulsória a comunicação de determinadas informações pessoais à administração pública, visando maior eficiência". Além do mais, quanto maior o volume de informação detida, mais o Estado tem poder de controle sobre a população, o que serve também como uma possível explicação para o surgimento de regimes totalitários no século XX[20].

É nesse contexto de rápida evolução tecnológica e expressiva automatização do tratamento de dados que a disciplina da privacidade encontra a da proteção de dados pessoais, alterando permanentemente seu conteúdo. A privacidade não poderia mais ser encarada como um comando de ausência estatal a *la vie privée*[21] do indivíduo, pois passou a abranger a proteção de dados pessoais, que exige ação do Estado, ao passo que representam um importante espectro da personalidade. Em consequência da mudança de conteúdo, surgiram também novas nomenclaturas para denominar essa nova concepção de direito, como privacidade informacional, proteção de dados pessoais, autodeterminação informativa, entre outros. Essa alteração do panorama levou muitos países a protegê-lo constitucionalmente, elevando-o ao patamar de direito fundamental[22].

1.2 DESENVOLVIMENTO DAS LEIS DE PROTEÇÃO DE DADOS PESSOAIS NA EUROPA

[19] *Ibidem*, p. 14.
[20] *Ibidem*, p. 16-17.
[21] Do francês, traduz-se como "a vida privada".
[22] MENDES. *Op. cit.*, 2008, p. 18.

As leis de proteção de dados pessoais surgiram a partir de contextos histórico-culturais diversos aos quais a sociedade foi submetida, sendo a disciplina de proteção de dados pessoais pensada a partir da ótica das iniciativas da Administração Pública no pós-guerra e que, com o desenvolvimento tecnológico e da informática a partir da década de 60, inspiraram modelos de bancos de dados centralizados. As leis que sucederam tiveram como agente catalisador a reação a estes projetos, cuja preocupação inicial que deu origem aos primeiros sistemas de proteção de dados era a posição do Estado enquanto administrador dos dados de seus cidadãos[23].

A seguir, discorrer-se-á como se deu o desenvolvimento das gerações de leis de proteção de dados na Europa a partir da análise de Mayer-Schönberger[24], autor que criou essa divisão e que é referência no tema. Vale ressaltar que fato de ser a obra-base para a grande maioria das obras que tratam desse tema constitui um problema de pesquisa que impende a utilização quase que exclusiva do capítulo do livro *"Technology and privacy: The new landscape"* para elaboração do próximo tópico.

1.2.1 Gerações de leis de proteção de dados pessoais na Europa

O processo de legalização das leis de proteção de dados começou na Europa durante a década de 70, período em que o foco foi a proteção no âmbito nacional, o que significa que cada país incorporou em seu ordenamento jurídico um conceito legal de proteção de dados adequado a sua realidade e especificidades[25].

Com o desenrolar do tempo e das tecnologias disponíveis, o fluxo informacional ultrapassou as barreiras nacionais, o que levou à necessidade de homogeneização das leis de proteção de dados no contexto europeu[26], levando à internacionalização do tema.

A primeira geração de normas teve como catalisador, em linhas gerais, o grande processamento de dados por parte do Estado de Bem-Estar Social e as tentativas de formação de bancos de dados nacionais.

---

[23] DONEDA. *Op. Cit.*, 2006, p. 205-206.
[24] MAYER-SCHÖNBERGER, Viktor. General development of data protection in Europe. *In*: AGRE, Phillip; ROTENBERG, Marc (orgs.). **Technology and privacy:** The new landscape. Cambridge: MIT Press, 1997.
[25] *Ibidem*, p. 220.
[26] *Id*.

A princípio, conforme apontado por Mayer-Schönberger, o surgimento dos computadores na Segunda Guerra Mundial forneceu o ambiente propício para o estabelecimento da burocracia governamental, dado que o W*elfare State* exigia a obtenção de dados para planejamento e implementação de políticas sociais, de forma que esse complexo sistema seria impossível sem o uso dos computadores:

> *Os dados necessitavam ser processados e conectados para criação dos intrumentos necessários ao planejamento a fim de que aquela legislação social complexa pudesse ser aplicada às demandas dos cidadãos. Consequentemente, nos Estados de Bem-Estar Social modernos, o processamento de dados era necessário em duas direções: de baixo para cima (para criação de informações agregadas para o planejamento a partir de milhões de de dados pessoais) e de cima para baixo (para transformar as regulações sociais em prerrogativas sociais concretas)* [27].

O grande interesse governamental levou ao surgimento de propostas de nacionalização de bancos de dados para centralizar a informação e, assim, otimizar seu processamento. A exemplo, na Alemanha foi criado um comitê para reunir os bancos de dados municipais, estaduais e federais em um único sistema[28].

Outro caso interessante na Europa foi o projeto SAFARI (*Système Automatisé pour lês Fichiers Administratifs et lê Répertoire de Individus*), apresentado em 1970 pelo Instituto Nacional de Estatística da França, cujo objetivo era unificar a identificação dos cidadãos por meio de um número perante o Estado. Apesar de hoje ser uma realidade no Brasil, o projeto repercutiu de forma negativa entre a população e os meios de notícias, utilizando-se do argumento da violação da privacidade dos cidadãos, e tal comoção levou o governo francês desistiu de implementá-lo. Por outro lado, o debate estabelecido na sociedade foi catalisador para a edição da lei francesa de proteção de dados pessoais, de 1978[29].

Diante desse cenário, os cidadãos reagiram negativamente por medo do possível controle absoluto que poderia fornecer e voltaram-se contra a tecnologia, acreditando que o problema era a existência de computadores. Em razão disso, a maioria das normas de primeira geração centram-se no controle da tecnologia e não da proteção dos dados em si, focando na contenção

---

[27] Tradução do trecho original: "*Data must be processed and linked together to create the necessary planning instruments, and so that complex social legislation can be applied to the demands of individual citizens. Hence, in modern socialwelfare states data processing is necessary in two directions: from the bottom up (to create aggregated planning information out of millions of personal data items) and from the top down (to transform the perplexing social regulations into concrete individual entitlements)".* MAYER-SCHÖNBERGER. *Op. Cit.*, p. 222.

[28] *Ibidem.*

[29] DONEDA. *Op. Cit.*, 2006, p. 190-191.

das atividades realizadas no computador como forma de domar a tecnologia[30]. As normas de proteção de dados da primeira geração, portanto, tinham como objetivo estabelecer procedimentos complexos de controle e regulação da tecnologia em detrimento da proteção de direitos individuais.

O fracasso dos projetos de criação de bancos de dados centralizados, porém, não se deu somente pela rejeição popular, pois o fator principal foi o fato de que a tecnologia se desenvolveu por outro caminho: ao invés da construção de bancos de dados únicos, o desenvolvimento tecnológico permitiu a descentralização do processamento de dados em diversos bancos menores, o surgimento de minicomputadores, o que alterou de forma significativa a problemática da proteção de dados pessoais[31].

A criação de computadores menores permitiu que pequenas unidades governamentais e privadas descentralizassem o processamento de dados, ocasionando a proliferação do número de bancos de dados existentes e, consequentemente, de possíveis violações, de forma que as leis de proteção de dados em vigor (criadas a partir do panorama de bancos de dados únicos) mostraram-se insuficientes a nova realidade. Ademais, muitos indivíduos já haviam experimentado o potencial de violação de dados pessoais e tais experiências estimularam a consciência popular quanto à necessidade de direitos privacidade e de proteção de dados[32].

A segunda geração, por outro lado, ocupou-se de direitos individuais, visto que as normas anteriores não mais serviam à realidade do tratamento de dados na Europa. A disciplina de proteção de dados estava diretamente ligada ao direito à privacidade: devido ao fato de as ameaças advirem de diversos computadores espalhados pelo território, a solução eleita foi conferir aos cidadãos liberdades negativas para reivindicarem eles próprios eventuais violações à privacidade e, a fim de viabilizar essa busca individual, utilizavam-se de direitos individuais fortes e até mesmo constitucionalmente garantidos. Neste sentido, a chamada privacidade informacional tornou-se constitucional em países como Áustria, Espanha e Portugal[33].

---

[30] MAYER-SCHÖNBERGER. *Op. Cit.*, p. 223.
[31] MENDES. *Op. Cit.*, 2008, p. 30.
[32] MAYER-SCHÖNBERGER. *Op. Cit.*, p. 225.
[33] *Ibidem*, p. 226.

Diferentemente da primeira geração – em que o indivíduo somente poderia requerer correção de dados eventualmente postos erroneamente, sem poder decidir sobre a própria inserção ou não destes –, a solução encontrada foi a inserção do consentimento como maneira de participação ativa do indivíduo no tratamento de seus dados. Apesar do crescimento dos fluxos internacionais de informações, os legisladores permaneceram com a concepção de que o cidadão titular seria o melhor ator capaz de proteger seus dados, sendo o assunto abordado de forma nacional e com base em regras de reciprocidade entre os países.[34].

A delegação de busca pela efetivação de seus direitos ao cidadão reverberou no âmbito institucional, de modo que, com o fortalecimento de tais direitos individuais, tornou-se necessária a criação de instituições encarregadas da proteção de dados, para onde cidadãos pudessem reportar violações[35].

Apesar dos grandes avanços, uma nova problemática nasceu: a exclusão social ocasionada pela negativa de compartilhamento de dados frente ao *welfare state* europeu. Os serviços oferecidos pelo Estado dependiam da burocracia (e detenção de dados dos cidadãos), portanto, fato é que o indivíduo quase nunca tinha efetivo poder de decisão, já que isso poderia significar participar ou não da sociedade[36]. Conforme indaga Mayer-Schönberger:

> *A proteção de dados enquanto liberdade individual pode proteger a liberdade do indivíduo. Ela pode oferecer ao indivíduo a possibilidade de afastar solicitações exageradas de informações. Mas qual é o preço a ser pago por isso? É aceitável que tais liberdades sejam apenas exercidas por eremitas? Teríamos atingido a proteção de dados ideal se garantimos direitos de privacidade que, quando exercidos, irão essencialmente expulsar o indivíduo da sociedade?*[37]

Isso demonstra a fragilidade da concepção de proteção de dados enquanto privacidade, já que seu cerne permite ao indivíduo consentir ou não com o tratamento de seus dados, porém o não consentimento, ou seja, a proteção dos dados enquanto esfera privada, impede a que o cidadão faça parte da sociedade de forma plena.

---

[34] *Ibidem*, p. 227.
[35] *Ibidem*, p. 228.
[36] *Ibidem.*
[37] Tradução do trecho original: "Data protection as individual liberty might protect the freedom of the individual. It might offer the individual the possibility of fending off overboarding societal information requests. But what price does one have to pay for that? Is it acceptable that such data-protection liberties can be exercised only by hermits? Have we reached an optimum of data protection if we guarantee privacy rights that, when exercised, will essentially expel the individual citizen from society?". *Ibidem*, p. 229.

O marco principal da terceira geração foi o estabelecimento de um sistema de proteção que conferia uma maior participação do indivíduo no processo de tratamento de seus dados, conforme decidiu o Tribunal Constitucional Alemão na decisão emblemática de 1983 que popularizou o termo "autodeterminação informacional" ao declarar a inconstitucionalidade da "Lei do Censo", que obrigava os cidadãos a fornecer dados ao governo sem a garantia de devida proteção[38].

Com a nova interpretação, todas as fases de processamento de informações passariam pelo filtro limitador advindo de direitos constitucionais, portanto a participação do indivíduo deve estar presente em todas as fases. Abandona-se a ideia de que o indivíduo deve dar um consentimento, uma decisão "tudo ou nada" sobre ter ou não seus dados processados, característica da segunda geração[39].

O grande avanço tecnológico tornou possível a transmissão mais eficiente e barata de dados por meio das redes eletrônicas, nas quais os bancos de dados passaram a residir; com isso, deixou de ser possível encontrá-los em um endereço físico. A possibilidade de transmissão em segundos aumentou o fluxo, assim como a necessidade de novas medidas de segurança e, consequentemente, de medidas legais mais adequadas, entretanto os legisladores optaram por conferir mais direitos individuais abstratos e de participação em vez de enfrentar o desafio de adaptação da lei à evolução tecnológica[40].

Diversas emendas legislativas da época seguiram essa lógica, como os estatutos de proteção de dados dos estados alemães após a decisão da Corte Constitucional supracitada, a lei austríaca de proteção de dados de 1986 e a extensão de direitos individuais de participação na lei norueguesa de proteção de dados, bem como a adoção de previsão de proteção de dados na Constituição da Holanda, entre outros[41].

A prática, todavia, revelou uma realidade diferente da pintada pelos legisladores da época: ainda que fortalecidos pelas normas, os cidadãos não estavam dispostos a arcar com os altos custos financeiros e sociais para exercer o direito à autodeterminação informativa, já que havia

[38] MENDES. *Op. Cit.*, 2008, p. 37.
[39] MAYER-SCHÖNBERGER. *Op. Cit.*, p. 229.
[40] *Ibidem*, p. 230.
[41] *Ibidem*, p. 231.

contratos que exigiam permissão para tratamento de dados, o que limitou o acesso a certos serviços[42].

Assim, mais uma vez a proteção de dados permaneceu um direito reservados a minorias econômica e socialmente capazes de exercer esses direitos. Quanto ao resto da população, continuou excluída dos novos avanços, diante da impossibilidade de buscar reparações por eventuais violações de seus direitos, uma vez que havia prestado consentimento previamente.

Nas normas de quarta geração, percebe-se uma tentativa de corrigir alguns erros das gerações passadas utilizando-se de duas estratégias: maior fortalecimento da posição do indivíduo[43] e retirada de certas partes do direito de disposição individual, sob a crença de que necessitam de maior proteção[44].

Alinhado com a segunda estratégia, foi proibido, em regra, o processamento de dados sensíveis, como se pode ver pela Diretiva 95/46/CE do Parlamento Europeu de 1995[45], que, em seu artigo 8.1[46], proibiu o processamento de dados relativos à raça, religião, posicionamento político etc., exceto em casos específicos trazidos no 8.2.

Uma particularidade das normas de quarta geração é a sua complementariedade, ou seja, as normais gerais podem ser complementadas por normas setoriais a fim de abranger os diversos setores específicos em que há tratamento de dados pessoais. O que antes era uma realidade apenas em países nórdicos, como a Finlândia e a Noruega, começa a ser incorporado em outros ordenamentos jurídicos, como na Alemanha e Áustria[47].

O apanhado dessa geração normativa é, segundo Mayer-Schönberger, a tentativa de resgatar o direito individual à autodeterminação informativa, agora mais detalhado e reforçado, ao lado da posição suplementar de intervenção direta estatal. Desta forma, o maior retrato da quarta geração é a Diretiva Europeia sobre Proteção de Dados Pessoais de 1995, que trouxe o

---

[42] *Ibidem*, p. 232.
[43] *Ibidem.*
[44] *Ibidem*, p. 233.
[45] UNIÃO EUROPEIA. **Diretiva 95/46 do Parlamento Europeu e do Conselho**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT. Acesso em 24 ago. 2020.
[46] "1. Os Estados-membros proibirão o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual(...)".
[47] MAYER-SCHÖNBERGER. *Op. Cit.*, p. 233.

consentimento como fato permissivo para tratamento de dados, que deve ser dado expressamente no caso de dados sensíveis, bem como os cidadãos podem proibir o processamento de dados pessoais para fins de marketing direto[48].

Levando em consideração que a tecnologia se supera a cada minuto com grande velocidade, é muito fácil compreender que surgirão novas formas de coleta, tratamento e transmissão de dados. Dessa forma, os mecanismos legais precisarão se atualizar para acompanhar o progresso tecnológico que o futuro trará.

1.2.2 Princípios da proteção de dados pessoais

A progressão histórica da disciplina de proteção de dados pessoais, conforme visto na análise de Mayer-Schönberger[49], deu-se ao passo que os países a incorporaram em seus ordenamentos jurídicos internos e, posteriormente, devido à transmissão de dados além das fronteiras dos Estados. Esses acontecimentos, como visto anteriormente, levaram à internacionalização da matéria, bem como sua consequente uniformização, a exemplo da Diretiva Europeia sobre proteção de dados de 1995[50].

O desenvolvimento das gerações de dados pessoais evoluiu desde seu surgimento no direito à privacidade, fixando uma liberdade individual negativa, com o direito de ser deixado só, até o complexo arcabouço legal que foi sendo construído pela necessidade de regulação das atividades[51].

As soluções legislativas, segundo Doneda, buscaram a consolidação de princípios básicos aplicáveis às relações que envolvem tratamento de dados, com ênfase no tocante à proteção da pessoa e aos direitos fundamentais[52]. Tais regras gerais são provenientes das *Privacy Guidelines* emitidas pela OCDE, padrões normativos para edição de leis proteção de dados pessoais pelos Estados-membros, cujo objetivo era garantir o livre fluxo de informações entre estes países, além de evitar a criação de obstáculos injustificados para o seu desenvolvimento. Além de trazer

---

[48] *Ibidem*, p. 233.
[49] Visto no capítulo anterior.
[50] MAYER-SCHÖNBERGER, *Op. Cit.*
[51] *Ibidem.*
[52] DONEDA. *Op. Cit.*, 2011, p. 98.

uma parte geral conceitual, a segunda parte das *guidelines* vinculava os países-membros à incorporação dos princípios lá previstos, afinal visava à criação de um "ambiente regulatório uniforme" para garantir o fluxo informacional[53].

A orientação normativa da OCDE abrange cinco princípios essenciais, quais sejam: a publicidade, a exatidão, a finalidade, o livre acesso e a segurança, que serão explicados a seguir.

O princípio da publicidade, também chamado de princípio da transparência preceitua que deve ser de conhecimento público a existência de bancos de dados, podendo assim ser por meio de prévia autorização ou de notificação a autoridades estatais sobre seu funcionamento, bem como exigência de envio de relatórios periódicos sobre suas atividades[54].

Deve ser obedecido o princípio da exatidão dos dados, portanto de extrema importância a devida coleta e tratamento de dados, pois a formação do banco de dados deve traduzir a realidade e garantir sua atualização para que permaneça fidedigno segundo os seus objetivos[55].

Quanto ao princípio da finalidade, significa que o tratamento dos dados deve ser realizado conforme as finalidades comunicadas aos interessados antes da coleta, para que não haja abuso em seu uso. Serve ao papel também de justificar a limitação de transferência de dos dados a terceiros, bem como para avaliar a razoabilidade do uso de dados alinhado aos fins a que se destina o banco[56].

O princípio do livre acesso, por sua vez, permite ao indivíduo poder acessar suas informações constantes em bancos de dados, obtendo cópias dos registros e podendo, com base no princípio da exatidão, corrigir, atualizar ou acrescentar informações sobre si mesmo[57].

Por fim, o princípio da segurança estabelece que os dados devem ser amparados contra riscos de extravio, destruição, modificação ou transmissão e acesso sem autorização do interessado[58].

---

[53] BIONI. *Op. Cit.*, p. 174.
[54] DONEDA. *Op. Cit.*, 2006, p. 216.
[55] *Ibidem.*
[56] *Ibidem.*
[57] DONEDA. *Op. Cit.*, 2006, p. 217.
[58] *Ibidem.*

Nota-se que a interpretação dos princípios traz a noção do titular dos dados pessoais como o grande protagonista nesse marco regulatório, reiterando que o tratamento é lícito e justo à medida em que é vinculado ao consentimento. Assim o que determina a licitude de qualquer atividade de tratamento de dados pessoais é a participação do indivíduo nas etapas do fluxo informacional. Esta nova diretriz normativa traz em seu cerne o controle do cidadão sobre seus dados pessoais como a autodeterminação informacional, situando as *guidelines* da OCDE entre a terceira e a quarta geração de leis de proteção de dados pessoais. Em 2013, essas diretrizes foram revisadas, entretanto o seu núcleo foi mantido[59].

Analisando os mais de 30 anos de proeminência das *guidelines*, Bruno Bioni destaca sua grande relevância ao influenciar várias legislações sobre o tema, apoiando-se na colocação do titular "como principal ator da dinâmica normativa sobre proteção de dados pessoais", convergindo para o papel de destaque do consentimento em sua evolução histórico-normativa[60].

[59] BIONI. *Op. Cit.*, p. 175.
[60] *Ibidem*, p. 176.

2 MAS, AFINAL, O QUE SÃO DADOS PESSOAIS?

É de suma importância para a compreensão da matéria entender no que consiste o conceito de dados pessoais e como sua utilização pode impactar o exercício de outros direitos fundamentais. Para tanto, esse capítulo se presta a apresentarm o conceito de dados pessoais e suas ramificações relevantes para a análise, quais sajem, dados sensíveis e dados anônimos ou anonimizados.

Além disso, discorre-se sobre a concepção de proteção de dados pessoais enquanto direito da personalidade e seus impactos nas esferas dos direitos fundamentais à liberdade e igualdade.

2.1 INFORMAÇÕES VS. DADOS

Muito embora seus conteúdos frequentemente se sobreponham, dados e informações não são sempre sinônimos, o que pode levar à inadequada utilização de um termo em lugar do outro. De acordo a definição de Doneda, *"ambos os termos servem a representar um fato, um determinado aspecto de uma realidade"*, porém é essencial distingui-los para a estudo do tema, vide possuírem conteúdos diversos. Para o autor, "dado" é classificado como uma informação em potencial, pois encontra-se em um estado bruto associado a uma fase de "pré-informação", anterior ao processo de interpretação. Por outro lado, a informação representa um estado em que pode ser compreendido, o que pressupõe o início do refinamento do conteúdo que o torna compreensível[61].

Complementarmente, segundo Tatiana Malta, o dado nada mais é que a informação em dimensão reduzida, que não necessariamente traz uma mensagem por si só, podendo necessitar do agrupamento com outros dados para que o faça. A informação, por sua vez, é a transmissão desse(s) dado(s) apresentada de forma numérica, gráfica, fotográfica, acústica, entre outros[62].

---

[61] DONEDA. *Op. Cit.*, 2006, p. 152.

[62] VIEIRA, Tatiana Malta. **O Direito à Privacidade na Sociedade da Informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Dissertação (Mestrado em Direito) Brasília: Universidade de Brasília, 2007, p. 224.

Portanto, dado seria a informação no estado "bruto" e que pode exigir o cruzamento com outros dados para que faça sentido e seja compreendido, enquanto a informação é o dado que passou por um tratamento apto a torná-lo utilizável, seja enquanto imagem, som, etc.

Quanto aos dados pessoais, são aqueles que dizem respeito a uma pessoa específica ou que permitem chegar a ela, por exemplo o endereço de IP atribuído ao computador conectado à rede que um indivíduo está utilizando; apesar de isso não conduzir à identificação direta do internauta, ela poderá ser conhecida a partir da interconexão do IP com outros dados armazenados pelo provedor de acesso à internet, *cybercafé*, *cyberoffice* e outros estabelecimentos congêneres aos quais tenha se conectado. Portanto, a identificação é passível de ser feita diretamente pelo detentor dos dados ou indiretamente por recursos de terceiros[63].

Sendo assim, depreende-se que informação é gênero do qual dados são a espécie. Pois bem, não raro, as legislações carecem da utilização dos termos técnicos e sobrepõem os termos indistintamente, como já apontado no início deste tópico. Apesar de "dado" ser o termo de conteúdo mais específico, cometem certo equívoco em suas definições de dados pessoais ao utilizar "dado" como termo genérico; todavia a explanação acima supre eventuais enganos acerca da compreensão dos termos.

Nessa alçada, a Diretiva Europeia 95/46/CE define dado pessoal como "qualquer informação relativa a uma pessoa singular identificada ou identificável", considerando identificável o que é passível de identificação de forma direta ou indireta, por referência a um número de identificação ou outros elementos específicos sobre sua identidade física, fisiológica, psíquica, econômica, cultural ou social.

Já a o novo regulamento europeu sobre proteção de dados pessoais, a *General Data Protection Regulation – GDPR –*[64], define dado pessoal de forma semelhante, adicionando elementos quanto ao que considera "identificável", no sentido de destrinchar e taxar mais

[63] VIEIRA. *Op. Cit.*, p. 224-225.
[64] PARLAMENTO EUROPEU**. REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Acesso em 24 ago. 2020.

detalhadamente hipóteses em que isso é possível, como dados de localização, identificadores por via eletrônica ou elementos específicos da identidade genética e mental da pessoa singular.

No ordenamento jurídico brasileiro, a Lei 13.709/18, conhecida como Lei Geral de Proteção de Dados – LGPD –, traz conceituação mais tímida e menos detalhada, todavia com a mesma essência dos regulamentos europeus, definindo dados pessoais simplesmente como "informação relacionada a pessoa natural identificada ou identificável"[65].

A concepção jurídica tradicional sobre a informação, que se ocupava de fenômenos específicos, como liberdade de imprensa e patentes industriais, hoje assumiu novo papel que exige que o direito a observe com lentes que lhe permitam tratá-la pelo seu aspecto funcional. Isso porque a informação tem como característica ser comunicada ou comunicável, assim, ela se torna um elo entre o emitente e o destinatário. Juridicamente, a relevância do aumento do fluxo informacional deve-se ao fato de que o uso da informação é determinante para o exercício de boa parte das liberdades individuais. Por esse motivo, os novos problemas surgidos com o avanço tecnológico exigem uma abordagem que leve em consideração os interesses conflitantes nas relações jurídicas que envolvem a informação, inclusive direitos constitucionalmente garantidos[66], como, por exemplo, a tensão existente entre a livre circulação de informações e o direito à privacidade.

Uma determinada informação pode revelar algo sobre um indivíduo por possuir um vínculo objetivo com ele, ou seja, pode referir-se as suas características ou ações – como o nome civil – ou a informações sobre seus atos – como dados de consumo ou opiniões manifestadas. De todo modo, é esse vínculo objetivo com a pessoa que afasta as demais categorias de informações que, por mais que sejam referentes a uma pessoa, não traduzem o sentido de informação pessoal propriamente dita. Como bem esclarece Doneda, opiniões alheias sobre um indivíduo ou sua produção intelectual não são, a princípio, informações pessoais, pois o mecanismo determinante para caracterizar uma informação pessoal é "o fato de estar vinculada a uma pessoa, revelando algum aspecto objetivo desta"[67].

---

[65] BRASIL. **Lei nº 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 09 set. 2020.
[66] DONEDA. *Op. Cit.*, 2006, p. 153-155.
[67] *Ibidem*, p. 156-157.

Tendo em vista seu novo papel de destaque e por guardarem aspectos objetivos sobre o indivíduo, resta claro que os dados pessoais são, em última instância, a pessoa em si. O direito à proteção da pessoa também engloba a função de impedir o tratamento de dados pessoais que não leve em conta o seu caráter personalíssimo. Assim, a proteção de dados pessoais é um instrumento legal que visa a tutelar a própria pessoa e, portanto, é imprescindível o reconhecimento de proteção jurídica específica, já que há muito tempo separou-se do conceito de privacidade[68].

2.1.1 Dados sensíveis

Considerando que o dado pessoal é o dado referente à pessoa identificada ou identificável, é razoável compreender que certos dados relativos ao indivíduo possuem conteúdo mais delicado. Carecem, portanto, de maior proteção, tendo em vista a repercussão negativa que sua utilização indiscriminada pode causar. Dados que, por exemplo, sejam relacionados à etnia ou convicção religiosa podem impactar negativamente a projeção social do indivíduo devido ao seu potencial para causar discriminação. Nesta categoria, encontram-se uma espécie de dados pessoais e uma forma de tratamento de dados que pode provocar os mesmos efeitos: os dados sensíveis e o tratamento sensível de dados.

Os dados sensíveis são aqueles que revelam elementos considerados sensíveis ao indivíduo, representando elevado grau de ameaça ou lesão a direitos. A GDPR, em seu artigo 9.1, estabelece a proibição do tratamento de dados pessoais que revelem elementos como a origem étnica ou racial e opiniões políticas, bem como de dados relativos à saúde e à vida sexual de uma pessoa[69], entretanto, assim como fez a antecessora Diretiva Europeia 95/46/CE, trouxe hipóteses de relativização do tratamento desses dados, como o caso do consentimento explícito do titular dos dados[70].

---

[68] BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia**. Elaboração: Danilo Doneda. Brasília: SDE/DPDC, 2010, p. 39.

[69] Segue texto integral do artigo 9.1 da GDPR: "É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa."

[70] Neste sentido, o item 51 do Preâmbulo da GDPR discorre sobre o conceito de dados sensíveis e consentimento: "Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. Deverão incluir-se neste caso os dados pessoais que revelem a origem racial ou étnica, não implicando o uso do termo «origem racial» no presente regulamento que a União aceite teorias que procuram determinar a existência de diferentes raças humanas. O tratamento de

A LGPD, por sua vez, conceitua dados sensíveis em seu artigo 5º, II, e na Seção II dispõe sobre o tratamento de tais dados de forma deveras semelhante ao regramento europeu, inclusive estabelecendo o consentimento, de forma específica e destacada para finalidades também específicas, como principal hipótese autorizativa para tratamento de dados sensíveis.

A criação dessa categoria de dados pessoais sofreu várias críticas, dentre as quais destaca-se a concepção de que não é possível prever os efeitos do tratamento de uma informação, independentemente de sua natureza. Assim, dados não considerados sensíveis podem ser submetidos a tratamentos que revelem aspectos sobre a personalidade de uma pessoa e ensejem práticas discriminatórias em relação a mesma. Em outras palavras, o dado não é inerentemente sensível, mas seu uso pode torná-lo[71]. Essa ideia identificou o chamado tratamento sensível de dados, utilizado com frequência atualmente, e diz respeito à possibilidade de determinar individualidades sensíveis a partir de dados aparentemente triviais[72].

Um ótimo exemplo é a forma como a loja de departamento americana "Target" foi capaz de identificar se uma consumidora estava grávida e até mesmo o seu período gestacional utilizando apenas o histórico de mulheres que haviam depositado lista de presentes para seus chás de bebê e os seus padrões de compras[73]. A partir do cruzamento desses dados, a loja identificou determinados produtos e sua provável relação com a gravidez, o que, junto com o acompanhamento do uso dos cartões de fidelidade, permitiu à empresa identificar a quantidade de consumidoras grávidas e até mesmo estimar a data do parto[74].

---

fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular. Tais dados pessoais não deverão ser objeto de tratamento, salvo se essa operação for autorizada em casos específicos definidos no presente regulamento, tendo em conta que o direito dos Estados-Membros pode estabelecer disposições de proteção de dados específicas, a fim de adaptar a aplicação das regras do presente regulamento para dar cumprimento a uma obrigação legal, para o exercício de funções de interesse público ou para o exercício da autoridade pública de que está investido o responsável pelo tratamento. Para além dos requisitos específicos para este tipo de tratamento, os princípios gerais e outras disposições do presente regulamento deverão ser aplicáveis, em especial no que se refere às condições para o tratamento lícito. Deverão ser previstas de forma explícita derrogações à proibição geral de tratamento de categorias especiais de dados pessoais, por exemplo, se o titular dos dados der o seu consentimento expresso ou para ter em conta necessidades específicas, designadamente quando o tratamento for efetuado no exercício de atividades legítimas de certas associações ou fundações que tenham por finalidade permitir o exercício das liberdades fundamentais."

[71] DONEDA. *Op. Cit.*, 2006, p. 162.

[72] BIONI. *Op. Cit.*, p. 118.

[73] O que a revolução dos dados pode fazer por sua empresa?. **Exame**, [*S.l.*.], 29 de out. de 2013. Disponível em: https://exame.com/pme/a-revolucao-dos-dados/. Acesso em: 09 set. 2020.

74 Sobre o mesmo caso, ver: BIONI. *Op. Cit.*, p. 118.

Pelo exposto, é possível compreender que a disposição de proteção especial somente aos dados sensíveis não é capaz de abarcar a problemática do risco discriminatório, uma vez que o simples tratamento que vise a utilização de dados aparentemente inofensivos para obter informações sensíveis pode gerar o mesmo resultado, tomando dados triviais para transformá-los em conteúdo potencialmente lesivo ao seu titular.

2.1.2 Dados anônimos e anonimizados

Para além da abordagem sobre dados pessoais de uma pessoa determinada – utilizada até o momento –, importante ressaltar que estes também podem referir-se a pessoas indeterminadas, hipótese em que são considerados dados anônimos ou anonimizados[75]. No tocante ao tema, Bioni estabelece relação de oposição entre as espécies, no sentido de que *"a antítese do conceito de dado pessoal seria um dado anônimo, ou seja, aquele que é incapaz de revelar a identidade de uma pessoa"*[76], logo a característica diferenciadora é justamente a capacidade de o dado poder ser revertido até a cognição do seu titular.

Esses dados têm variadas utilidades, a exemplo da coleta para fins estatísticos, sem que seja necessária identificação pessoal, como forma de proteção ao titular[77]. Dados anônimos podem assim ser em razão do processo chamado anonimização, que é a quebra do seu vínculo com a pessoa a qual se referem, recurso utilizado por leis de proteção de dados a fim de reduzir riscos no seu tratamento[78].

A legislação brasileira, por meio do artigo 5º, III, da LGPD, define dados anonimizados como aqueles referentes à pessoa que não possa ser identificada, levando em conta a razoabilidade dos meios técnicos utilizados conforme a ocasião de seu tratamento. Já o processo de anonimização possui definição legal constante do inciso XI do mesmo artigo, no sentido de configurar a "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento,

---

[75] Neste trabalho, trata-se dados anônimos e anonimizados indistintamente, visto que todo dado pessoal advém de uma pessoa identificada e só se torna anônimo por meio da utilização de meios razoáveis de desvinculação com a pessoa. Assim, nenhum dado é anônimo em si, já que todos necessitam passar pelo processo de anonimização para enquadrarem-se na espécie de dados anônimos. O mesmo tratamento é dado pela legislação, como exposto adiante.
[76] BIONI. *Op. Cit.*, p. 104.
[77] MENDES. *Op. Cit.*, p. 71.
[78] DONEDA. *Op. Cit.*, 2006, p. 157-158.

por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo"[79].

Importante ressaltar que, sendo dado pessoal aquele que guarda vínculo objetivo com o seu titular, o dado anônimo, por não possuir elementos identificadores, não estará sujeito à aplicação das disposições de proteção de dados pessoais. Esse entendimento é consolidado nas normativas analisadas, vez que assim dispõe a GDPR[80] e também a LGPD, sendo que esta ressalva as hipóteses em que o processo de anonimização for revertido por meios próprios ou quando puder sê-lo pela utilização de meios razoáveis[81].

Não há uma única maneira de se proceder à anonimização, portanto é necessário analisar no caso concreto como deve ser feita a fim de que não possa ser feita a reidentificação dos dados[82]. Entretanto, acreditar na irreversibilidade do processo de anonimização tem se mostrado problemático, à medida em que a possibilidade agregação entre bases de dados diferentes torna o processo de anonimização total teoricamente impossível[83].

Seguindo este raciocínio, assim como a GDPR[84], a LGPD adotou a estratégia normativa de utilizar a razoabilidade como critério para avaliação do que configura um "risco aceitável-tolerável" quanto à possibilidade de reversão do processo de anonimização de dados, numa tentativa de diferenciá-los do conceito de dados pessoais e mantê-los fora do arcabouço normativo que propõem.

---

[79] "Art. 5º Para os fins desta Lei, considera-se:
(...)
III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
(...)
XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;"

[80] No item 26 das considerações, dispõe "(...) Os princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação."

[81] "Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido."

[82] BIONI. *Op. Cit.*, p. 107.

[83] TEIXEIRA, apud BIONI. *Op. Cit.*, p. 107.

[84] Vide o item 26 do regulamento, principalmente no trecho: "Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular."

2.2 DADOS PESSOAIS: UM NOVO DIREITO DA PERSONALIDADE

Muito se fala sobre a imprescindibilidade da tutela jurídica de dados pessoais como forma de proteção do indivíduo frente à sociedade da informação, entretanto, identificar por que é ela é necessária pode ser um exercício útil à boa compreensão da matéria.[85].

No tocante aos dados pessoais, é de extrema importância compreendê-los como um direito da personalidade no contexto de intensa informatização e utilização de dados pessoais. Isto porque os direitos da personalidade, muito embora a legislação não traga um conceito, podem ser compreendidos a partir de duas perspectivas doutrinárias: como um atributo, prolongamento ou projeção da pessoa humana, ou a partir da esfera relacional – a maneira como o indivíduo se relaciona com a sociedade. Nesse sentido, os direitos da personalidade têm a função precípua de proteger a pessoa humana como princípio fundante do ordenamento jurídico[86], logo o direito é o mecanismo criado para a tutela da pessoa humana e seus desdobramentos, e os direitos da personalidade servem a esse mesmo papel.

Não se pretende nesse trabalho discorrer sobre conceito e definição de direitos da personalidade, mas tão somente identificar a proteção de dados pessoais como uma nova extensão da personalidade da pessoa humana, elemento central do ordenamento jurídico, frente às evoluções tecnológicas e ao real tratamento e utilização conferida aos dados.

Dessa forma, reconhece-se que os dados pessoais e as demais informações extraídas a partir deles representam o próprio indivíduo (seus atributos) e constituem sua própria expressão e representação virtual perante a sociedade (aspecto relacional dos direitos da personalidade). A importância da tutela jurídica neste caso reside no fato de que a identificação e representação de qualquer pessoa na sociedade contemporânea depende da utilização de seus dados, visto que o Estado e os entes privados tomam conhecimento das pessoas a partir de seus dados

[85]Sobre bens jurídicos, Claus Roxin compreende-os como "realidades ou fins que são necessários para uma vida social livre e segura que garanta os direitos humanos e fundamentais do indivíduo, ou para o funcionamento do sistema estatal erigido para a consecução de tal fim". ROXIN, Claus, "Es la proteción de bienes jurídicos una finalidad del Derecho Penal?". In: HEFENDEHL, Roland (ed.). **La teoría del bien jurídico – Fundamento de legitimación del Derecho penal o juego de abalorios dogmático?**. Madrid: Marcial Pons, 2007. p. 448.
[86] BIONI. *Op. Cit.*, p. 98.

computadorizados. Em decorrência disso, os dados pessoais passam a constituir a própria personalidade do indivíduo[87], já que são sua própria representação perante o mundo.

A perspectiva subjetiva do ser humano quanto às características que compõem sua individualidade, como ensina Bioni, guarda larga relação com os seus dados pessoais, já que ela se dá no espectro relacional. Isso significa dizer que os seres humanos afirmam sua própria individualidade em contraposição às demais[88].

O livre desenvolvimento da personalidade é, inclusive, apontado pela LGPD como um objetivo e fundamento da proteção de dados, consoante os artigos 1º e artigo 2º, VII, demonstrando que o legislador brasileiro reconhece essa dimensão e a sua importância para a disciplina.

Essa realidade justifica a inserção da proteção de dados pessoais na disciplina de direitos da personalidade, pois permite, por exemplo, que o indivíduo pleiteie a retificação de seus dados, a fim de que a sua projeção pessoal esteja devidamente representada[89]. A discussão da proteção de dados pessoais perpassa necessariamente o direito da personalidade, fato que se denota claramente nesse exemplo através da correlação entre o princípio da qualidade dos dados pessoais – que garante o direito de retificação – e a expressão da personalidade.

Sendo assim, os dados pessoais são um novo direito da personalidade e uma importante ferramenta para que o indivíduo possa livremente desenvolvê-la, sendo a proteção de tais dados crucial para que não haja discriminação da pessoa por meio de tratamento indevido de dados, e, consequentemente, impedimento do exercício de liberdades fundamentais[90], como se verá nos tópicos a seguir.

2.2.1 Impactos na esfera da liberdade

[87] MENDES. *Op. Cit.*, 2008, p. 69.
[88] Como bem escreve Bruno Bioni: "A noção completa dos direitos da personalidade liga-se necessariamente à tutela jurídica para que a pessoa possa se realizar e se relacionar junto à sociedade, completando justamente a locução, antes mencionada, projeção social". BIONI. *Op. Cit.*, p. 117.
[89] BIONI. *Op. Cit.*, p 99.
[90] *Ibidem*, p. 118.

O exponencial aumento do fluxo informacional nas últimas décadas mudou radicalmente a forma como o indivíduo se relaciona com a sociedade. Em decorrência disso, a crescente representação virtual do indivíduo como maneira preponderante de relacionamento com o Estado e entes privados, assim como a desenfreada utilização de dados pessoais para as mais diversas finalidades, jogou luz sobre os graves embaraços que pode causar ao exercício de direitos fundamentais, notadamente nos direitos à liberdade e à igualdade material[91].

Sendo os dados pessoais os intermediários entre indivíduo e sociedade, a inaptidão destes para representá-lo – seja por falta de exatidão, confiabilidade ou autorização para tanto – retira a pessoa da posição de controle sobre suas próprias informações e, consequentemente, sobre a maneira que é apresentada à sociedade. Isso significa a diminuição da própria liberdade do indivíduo, já que nem mesmo pode decidir sobre a maneira como efetiva sua projeção social[92], ficando sujeito à mercê discricionariedade de organizações públicas e privadas e seus próprios interesses.

A proteção de dados pessoais tem papel indispensável para o livre exercício da liberdade, já que se baseia, entre outros, nos pilares da autodeterminação e autoconformação, ou seja, o poder de decidir e de formar a si mesmo, e a sua personalidade. Isso implica dizer que o indivíduo possui capacidade para delimitar quando a coleta e transmissão de informações pessoais importa ou não na violação da sua personalidade. Nesse aspecto, há de se ressaltar a raiz comum entre a proteção de dados e o direito à privacidade: o caráter central de autocontrole e liberdade do titular dos dados[93].

No cerne da discussão, a liberdade do indivíduo e seu poder decisório, exposto a altos riscos considerando as técnicas de tratamento de dados escolhidas. Neste diapasão, Maria Celina Bodin de Moraes e Chiara Spaccini de Teffé discorrem sobre o exemplo do *profiling*[94], ou seja, criação de perfis digitais sobre indivíduos no âmbito do consumo:

> *Com efeito, um acervo suficientemente amplo de informações permite a elaboração de perfis de consumo, o que se, de um lado, pode ser utilizado para incrementar e personalizar a venda de produtos e serviços, de outro, pode aumentar o controle sobre a pessoa, desconsiderando sua autonomia e dificultando a participação do*

[91] Assunto a ser abordado no ponto 3.3.6.
[92] DONEDA. *Op. Cit.*, 2006, p. 181.
[93] MENDES. *Op. Cit.*, 2008, p. 41.
[94] A referida técnica será explicada no subtítulo 3.3.6.1.

> *indivíduo no processo decisório relativo ao tratamento de seus dados pessoais, de seu patrimônio informativo.*[95]

Defende Mendes que é papel do Estado promover os mecanismos necessários ao exercício do direito de controle do fluxo de informações a seu respeito, tendo em vista que a liberdade, assim como todo direito fundamental, não é absoluta e articula-se em interdependência com o princípio da igualdade, bem como ambos servem à efetivação do preceito da dignidade humana – preceito fundamental do Estado[96].

Visando à obtenção de tal objetivo, foram criados diversos direitos subjetivos, como os direitos de informação, acesso, retificação e cancelamento, visando à materialização do exercício da liberdade do titular quanto a seus dados. Não obstante à ilusão de efetividade desses direitos, na prática, sua implementação é tarefa bastante complexa, principalmente no contexto de sociedade de informação, em que há predominância de interesses dos setores público e privado na obtenção de informações. Por esse motivo, a busca por um modelo que garanta efetivamente a autodeterminação informacional do indivíduo é a característica marcante da evolução das gerações de normas de proteção de dados pessoais, apesar de diversas dificuldades encontradas para sua efetivação[97].

O tema das liberdades individuais é assunto central da discussão sobre dados pessoais e amplamente tratado pela GPDR, que, em seu artigo 1.2, insere nos objetos e objetivos da normativa a defesa aos "direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais", bem como em tantas outras ocasiões, reafirmando o papel da proteção de dados pessoais enquanto liberdade individual.

De igual sorte, a LGPD traz o direito fundamental à liberdade como objetivo e fundamento da disciplina, bem como a estabelece como garantia do titular dos dados no capítulo que trata dos seus direitos. A liberdade é intrínseca à proteção de dados pessoais de modo que se torna impossível a existência de uma sem a outra, principalmente devido aos aspectos estudados na evolução de leis de proteção de dados sobre desenvolvimento da ideia de autodeterminação informativa.

---

[95] MORAES, Maria Celina Bodin de; TEFFÉ, Chiara. Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. **Revista Pensar**, v. 22, n. 1. p. 121. Disponível em: https://periodicos.unifor.br/rpen/article/view/6272. Acesso em 17 set. 2020.
[96] MENDES. *Op. Cit.*, 2008, p. 41.
[97] *Ibidem*, p. 45.

Outro aspecto que demonstra a presença do espectro da liberdade na discussão é a exigência do consentimento enquanto "uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento"[98], conforme a GDPR, e definida pela LGPD como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada"[99]. Mais uma vez, é possível verificar conformidade entre os regulamentos europeu e brasileiro, dessa vez com o consentimento como forma de efetivação da liberdade como característica comum.

O consentimento é, com base em Doneda, o instrumento por excelência da manifestação da autonomia privada e compreende um poder conferido à pessoa de modificar sua esfera jurídica com base na expressão de sua vontade[100]. Ademais, levando-se em consideração que *"o consentimento para o tratamento de dados pessoais toca diretamente elementos da própria personalidade, porém não dispõe destes elementos"*[101], prestar consentimento não significa desinteresse do titular na proteção de seus dados, tampouco importa na renúncia destes: na realidade, configura um verdadeiro ato de exercício do direito de autodeterminação no âmbito das escolhas pessoais.

Cabe ressaltar, por fim, que, devido à característica fundamental de proteção da personalidade, que possui atributo de indisponibilidade, o consentimento pode ser revogado a qualquer tempo pelo titular[102]. A LGPD, em consonância com o exposto, prevê no artigo 8º, § 5º, que o titular poderá revogar o consentimento prestado, a qualquer momento, mediante manifestação expressa e por procedimento facilitado e gratuito. Também a GDPR, em seu artigo 7.3, traz disposição nesse sentido, afirmando, inclusive, que o titular deve ser informado que poderá retirar seu consentimento e que revogá-lo deve ser tão fácil quanto prestá-lo.

2.2.2 Os impactos na esfera da igualdade

[98] Artigo 4.11 da GDPR.
[99] Artigo 5º, XII, da LGPD.
[100] DONEDA. *Op. Cit.*, 2006, p. 371-372.
[101] *Ibidem*, p. 377.
[102] *Ibidem*, p. 380.

Após as discussões sobre como o processamento de dados pelos setores público e privado é capaz de afetar o exercício de direitos fundamentais, com ênfase sobre a liberdade individual – em razão do cerceamento do controle sobre suas próprias informações –, agora volta-se para outro fenômeno que pode ser verificado a partir violação da proteção de dados: a geração de desequilíbrios na esfera do direito à igualdade. Conforme consigna Mendes, a vigilância realizada por organismos privados e estatais pode gerar a discriminação de indivíduos em razão de informações obtidas em bancos de dados, causando expressivo impacto das oportunidades sociais[103].

Quanto ao tema e aos riscos da atividade, advertem Maria Celina Bodin de Moraes e Chiara Spaccini de Teffé:

> *O oferecimento de dados pessoais vem se tornando rotina no ambiente virtual, de forma que, muitas vezes, o indivíduo perde o controle sobre as próprias informações logo após fornecê-las, pouco sabendo sobre sua utilização e se serão repassadas, por meio de trocas comerciais, a terceiros. Uma vez munidas de tais informações, entidades privadas e governamentais tornam-se capazes de "rotular" e relacionar cada pessoa a um determinado padrão de hábitos e de comportamentos, situação que pode favorecer inclusive graves discriminações, principalmente se analisados dados sensíveis.*[104]

A seguir, será feita uma breve análise sobre duas técnicas de tratamento de dados pessoais potencialmente lesivas aos direitos pessoais: o *profiling* e *scoring-system*, a fim de ilustrar como a utilização de dados pode servir a interesses contrários aos direitos fundamentais, bem como será levantada discussão acerca dessas práticas.

2.2.2.1 Profiling

Daniel J. Solove, em seu livro "The Digital Person", chama a atenção para a prática que consiste na coleta de um conjunto de informações sobre um indivíduo que leva em consideração os critérios pré-determinados conforme o interesse de certo ente (público ou privado), o que chamou de "biografias digitais". Em outras palavras, estes entes coletam somente informações que consideram relevantes, o que leva à criação de perfis enviesados que servem à identificação individual. Em decorrência disso, essas biografias não autorizadas são apenas parcialmente verdadeiras à medida em que a informação é organizada de maneira discricionária, produzindo perfis incapazes de traduzir a realidade e, portanto, inexatos[105].

---

[103] MENDES. *Op. Cit.*, 2008, p. 57-58.
[104] MORAES; TEFFÉ. *Op. Cit.*, p. 121.
[105] SOLOVE, Daniel J. **The Digital Person**. New York: NYU PRESS, 2004. p. 46.

Esse é o fenômeno denominado *profiling*, uma técnica de tratamento de dados que consiste na construção de perfis utilizando dados pessoais de um indivíduo para facilitar a tomada de decisões, frente à possibilidade de prever padrões de comportamento do consumidor, como gostos, hábitos e preferências. Ressalta Mendes que os riscos do *profiling* "não residem na sua grande capacidade de junção de dados; na realidade, a ameaça consiste exatamente na sua enorme capacidade de combinar diversos dados de forma inteligente, formando novos elementos informativos"[106].

Essa técnica enseja formas de discriminação, principalmente a grupos sociais já segregados, nesse sentido, a pesquisadora Sandra Wachter da Universidade de Oxford aponta três maneiras em que o monitoramento eletrônico e o *profiling* podem favorecer práticas discriminatórias nos sistemas atuais

> *(a) a coleta de dados que leva à conclusões precipitadas sobre o indivíduo (como suas pesquisas na internet); (b) o profiling em larga escala por meio do cruzamento de bancos de dados oriundos do IoT (as vezes chamado de "sensor fusion"; e (c) o profiling que ocorre quando dados são compartilhados com terceiros, fazendo uma combinação de todos os dados (como empregadores e seguradores).*[107]

A primeira prática, já bastante conhecida, diz respeito à coleta de *cookies* de navegação na internet, o que representa um potencial risco de associação do usuário ao computador por armazenarem dados pessoais do usuário. A solução é a obtenção do consentimento do usuário, exceto nos casos em que a coleta de dados seja imprescindível para o cumprimento do contrato de prestação de serviços (provedores de internet)[108], solução essa já abarcada na legislação como estudado acima.

Quanto à nova realidade denominada IoT, diz respeito ao cenário de grande interconectividade entre aparelhos e serviços, todos adequados conforme os interesses e comportamento do usuário, compartilhando dados entre si sobre um usuário específico, a fim

---

[106] MENDES. *Op. Cit.*, 2008, p. 105.

[107] WACHTER, Sandra. Normative Challenges of Identification in the Internet of Things: privacy, profiling, discrimination, and the gdpr. **Ssrn Electronic Journal**, [*S.l.*], p. 442, 2017. Elsevier BV. http://dx.doi.org/10.2139/ssrn.3083554. Disponível em: https://www.researchgate.net/publication/321959135_Normative_Challenges_of_Identification_in_the_Internet_of_Things_Privacy_Profiling_Discrimination_and_the_GDPR. Acesso em: 16 set. 2020.

[108] MENDES, Laura Schertel. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. **Revista de Direito do Consumidor**. vol. 106. ano 25. p. 13. São Paulo: Ed. RT, jul./ago. 2016. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RDCons_n.106.02.PDF. Acesso em 16 set. 20.

de oferecer uma experiência personalizada[109]. É aqui que se enquadram os dispositivos *"smart"*, como lâmpadas inteligentes, Smart TV's e assistentes virtuais[110], interconectados e compartilhando informações entre si.

Ao agregar essas diversas variáveis sobre dados pessoais, tangencia-se o próprio rumo da vida das pessoas, já que a forma com o que o indivíduo e a sociedade em geral se relacionam perpassa necessariamente a automatização e, consequentemente, os bancos de dados: desde a celebração de contratos e o ato do consumo à – até mesmo – busca pelo acesso à informação[111]. Consoante Doneda, o *profiling* pode ter várias aplicações, como bem expressa:

> *(...) desde, por exemplo, o controle de entrada de pessoas em um determinado país pela alfândega, que selecionaria para um exame acurado as pessoas às quais se atribuísse maior possibilidade de realizar atos contra o interesse nacional; bem como uma finalidade privada, como o envio seletivo de mensagens publicitárias de um produto apenas para seus potenciais compradores, dentre inúmeras outras.*[112]

A grande questão é que, nessa realidade impessoal, a tomada de decisões baseia-se cada vez mais em registros e perfis digitais para avaliar a reputações[113] (se não unicamente neles) e daí advêm os riscos de ataque a direitos fundamentais.

2.2.2.2 Scoring-System

Há outras técnicas potencialmente lesivas de tratamento de dados, como o *Scoring-System* ou *Rating-System*, um sistema de avaliação pessoal que tem como objetivo atribuir uma "pontuação" aos indivíduos. No mercado de consumo, a identificação dos consumidores que mais interessam a empresas para direcionamento de estratégias de fidelização, como recebimento de promoções, garante-lhes vantagens competitivas e manutenção dos níveis de lucratividade. Na análise de Mendes, ressalta que a existência dos "melhores consumidores" pressupõe uma lista de "piores consumidores", a quem serão negadas boas ofertas, podendo ter negado o acesso a determinados bens e serviços pela sua classificação negativa no cadastro de consumidores, como no caso do SERASA Experian, que oferece o serviço de *credit rating*

---

[109] WACHTER, Sandra. *Op. Cit.*, p. 437.
[110] Como o caso da assistente virtual da Amazon, chamada "Alexa", que protagonizou uma polêmica ao revelar que guarda todas os diálogos dos usuários. ÉPOCA NEGÓCIOS ONLINE. Amazon confirma que guarda todas as conversas que clientes têm com a Alexa: segundo a companhia, gravações só são deletadas se houver alguma manifestação dos usuários. **Época Negócios**, [*S.l.*], 04 jul. 2019. Disponível em: https://epocanegocios.globo.com/Empresa/noticia/2019/07/amazon-confirma-que-guarda-todas-conversas-que-clientes-tem-com-alexa.html. Acesso em: 16 set. 2020.
[111] BIONI. *Op. Cit.*, p. 122.
[112] DONEDA. *Op. Cit.*, 2008, p. 173-174.
[113] SOLOVE, p. 49.

(classificação de risco de inadimplência com base no crédito[114]). Na análise da autora, esses serviços são preocupantes no ponto de vista da proteção de dados pessoais, visto que inadequações podem causar graves danos à dignidade e personalidade do consumidor[115].

Apesar de parecer distópico, é interessante analisar o caso do Sistema de Crédito Social Chinês, iniciado em 2014, que tem por objetivo avaliar os 1,4 bilhões de chineses em um ranking baseado na "confiança", incluindo desde maus pagadores a pessoas que comem no metrô, dentre outros desvios da vida comunitária. O sistema se utiliza de dados médicos, atividade em redes sociais, pagamento de impostos e pessoas com as quais o indivíduo se relaciona, bem como também se serve do reconhecimento facial obtido por meio de uma vasta rede de vigilância por vídeo presente por todo o país, e promete ser obrigatório para todo cidadão chinês no ano de 2020.

Para os bem avaliados, muitas vantagens são concedidas, como acesso prioritário a ofertas de emprego, descontos em smartphones, prioridade para reservar um táxi, podendo o Governo Chinês compartilhar dados com empresas parceiras para tanto. Quanto aos indivíduos com baixa "sinceridade social", podem ser proibidos de viajar, de alugar imóveis e até mesmo ser impedidos de matricular seus filhos na escola que desejam. Ademais, opositores que criticam o regime também são incluídos em listas proibitivas[116].

Um fato preocupante é a parceria do governo chinês com empresas em parcerias para obtenção de dados, como o caso da Sesame Credit, que aglutina dados sobre as transações feitas no site Alibaba para abastecer o sistema de crédito social. Apesar de não revelar como os cálculos são feitos, afirma a empresa que utiliza informações sobre os produtos comprados no site, chegando a conclusões precipitadas e discricionárias sobre as pessoas. O diretor de Tecnologia da Sesame afirmou à revista chinesa Caixin, em 2015, que a uma pessoa que joga

---

[114] A empresa fornece serviços de Cadastro de Inadimplência e de Cadastro Positivo, que pode ser cruzado com o sistema Score, permitindo uma análise ainda mais precisa. Além do mais, consegue estimar a SERASA EXPERIAN. **Soluções Cadastro Positivo**. Disponível em: https://www.serasaexperian.com.br/solucoes-cadastro-positivo. Acesso em: 16 set. 2020.

[115] MENDES, Laura Schertel. *Op. Cit.*, p. 106.

[116] Sobre este assunto: MARR, Bernard. Chinese Social Credit Score: Utopian Big Data or Black Mirror on Steroids?. **FORBES**, [*S.l.*], 21 de jan. de 2019. Disponível em: https://www.forbes.com/sites/bernardmarr/2019/01/21/chinese-social-credit-score-utopian-big-data-bliss-or-black-mirror-on-steroids/#4e5df58248b8. Acesso em 16 set. 2019; e CHINA chega à fase final de sistema de avaliação de cidadãos e preocupa Ocidente. **RFI**, [*S.l.*], 02 de jan. de 2020. Disponível em: https://www.rfi.fr/br/mundo/20200102-em-2020-china-termina-de-testar-seu-sistema-de-cr%C3%A9ditos-sociais-e-assusta-ocidente. Acesso em: 16 set. 2020.

videogame por um longo período diário de tempo será atribuída características negativas, enquanto presume-se que as pessoas que compram fraldas são pais e, portanto, possuem senso positivo de responsabilidade[117].

De todo modo, observa-se os riscos e o potencial altamente discriminatório desta técnica de tratamento, já que, muitas das vezes, não necessita nem obter dados sensíveis sobre os usuários para atingir tais fins, bastando simplesmente o tratamento sensível de seus dados de consumo.

2.2.2.3 Breve consideração sobre o direito à não discriminação

O direito à não discriminação é positivado na Constituição Federal da República Federativa do Brasil em várias ocasiões, como pode se extrair do direito fundamental à igualdade (Art. 5º, caput) e o estabelecimento de que a lei punirá discriminação que atente contra direitos e liberdades fundamentais (Art. 5º, XLI), entre outros. É comum, também, às normativas brasileira e europeia de proteção de dados pessoais: enquanto aquela proíbe o tratamento de dados para fins discriminatórios ilícitos ou abusivos[118], essa também se aplica aos tratamentos dessa natureza como disposto no item 75[119] das considerações.

As previsões legais visam a proteger a igualdade material frente a um novo panorama sobre dados, que enquadra pessoas em categorias quanto ao seu valor ou risco. Esta realidade, que desloca a preocupação do escopo exclusivo da privacidade e liberdade, constata a existência

---

[117] O plano chinês para monitorar – e premiar – o comportamento de seus cidadãos. **BBC**, [*S.l.*], 20 de nov. de 2017. Disponível em: https://www.bbc.com/portuguese/internacional-42033007. Acesso em: 16 set. 2020.

[118] Artigo 6º, IX.

[119] "O risco para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, em especial quando o tratamento possa dar origem à **discriminação**, à usurpação ou roubo da identidade, a perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a quaisquer outros prejuízos importantes de natureza económica ou social; quando os titulares dos dados possam ficar privados dos seus direitos e liberdades ou impedidos do exercício do controlo sobre os respetivos dados pessoais; quando forem tratados dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical, bem como dados genéticos ou dados relativos à saúde ou à vida sexual ou a condenações penais e infrações ou medidas de segurança conexas; quando forem avaliados aspetos de natureza pessoal, em particular análises ou previsões de aspetos que digam respeito ao desempenho no trabalho, à situação económica, à saúde, às preferências ou interesses pessoais, à fiabilidade ou comportamento e à localização ou às deslocações das pessoas, a fim de definir ou fazer uso de perfis; quando forem tratados dados relativos a pessoas singulares vulneráveis, em particular crianças; ou quando o tratamento incidir sobre uma grande quantidade de dados pessoais e afetar um grande número de titulares de dados." (grifo nosso)

de consequências diretas nas oportunidades sociais, à medida que a discriminação se torna uma matéria de justiça social[120].

Sob essa ótica, os dados sensíveis possuem grande destaque por seu maior potencial lesivo, porém aqui também se enquadra o tratamento sensível de dados abordado no item 3.3.2, e o princípio da igualdade enquanto proteção contra a discriminação.

Em 2018, o Ministério Público do Estado do Rio de Janeiro ajuizou ação civil pública em face da empresa "Decolar.com" sob a alegação de que os preços e a disponibilidade vagas para hospedagem em hotéis eram manipulados com base na localização e nacionalidade do usuário. De acordo com o Ministério Público, a origem geográfica do consumidor era utilizada como indicador de procedência nacional para bloquear ofertas e atribuir preços mais altos de acordo com a nacionalidade, bem como permitia que o próprio setor hoteleiro discriminasse os clientes, dando a determinadas nacionalidades condições melhores em detrimento das demais, práticas abusivas denominadas *geo-blocking* (bloqueio de ofertas pela localização) e *geo-pricing* (precificação de acordo com a localização)[121].

Ademais, não é necessário ir à China para encontrar outros exemplos de graves violações a direitos fundamentais[122]. Isso nada mais é que um cadastro negativo, com caráter discriminatório evidente, prática que evidencia o potencial de lesividade destas condutas.

Tendo em vista os grandes riscos, mostra-se imprescindível que a tutela dos dados pessoais perpasse não somente a proteção da liberdade, como também da igualdade. A fim de atingir esse objetivo, a matéria deve ocupar-se do combate também à discriminação passível de ocorrer em razão de informações obtidas em bancos de dados, especialmente no tocante aos dados sensíveis e situações potencialmente discriminatórias.

Desse modo, Mendes destaca a existência de uma dupla dimensão da disciplina de proteção de dados pessoais, que abarca tanto os fundamentos de liberdade e igualdade,

---

[120] LYON, David. **Surveillance as social sorting**: privacy, risk, and digital discrimination. New York: Routledge, 2003, p. 1.

[121] BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Agravo de Instrumento nº 00089142420188190000**. Relator: Desembargador João Batista Damasceno. Rio de Janeiro, RJ, 12 de dezembro de 2018. Jusbrasil. Rio de Janeiro. Disponível em: https://tj-rj.jusbrasil.com.br/jurisprudencia/661800302/agravo-de-instrumento-ai-89142420188190000/inteiro-teor-661800312?ref=serp. Acesso em: 16 set. 2020.

[122] MENDES. *Op. Cit.*, p. 67.

"devendo-se refletir sobre o modo como ambos os princípios se conformam e se concretizam na prática da tutela jurídica das informações pessoais"[123], pois a matéria somente pode ser articulada sob a ótica de conciliação desses dois direitos.

A implementação de políticas a fim de proteger a liberdade sem levar em consideração a igualdade é inefetiva perante uma sociedade democrática, pois proteger um ato livre que gere consequências discriminatórias desampara a liberdade de outro cidadão[124], indo diretamente de encontro ao objetivo da proteção de dados pessoais, motivo pelo qual é importante compreender seus impactos na esfera da liberdade e da igualdade e como disciplina pessoais está interligada a esses conceitos. Este também é o propósito da presente monografia.

[123] MENDES. *Op. Cit.*, p. 59-60.
[124] *Ibidem.*

3 O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS: CASO EUROPEU

O continente europeu possui um histórico bastante proeminente no sentido do desenvolvimento de leis de proteção de dados pessoais, tanto no direito comunitário quanto no direito interno dos países-membros, sendo fonte de inspiração para diversas legislações externas ao "velho continente".

A exemplo da histórica decisão do Tribunal Constitucional Alemão sobre a Lei do Censo de 1983, que cunhou efetivamente a expressão autodeterminação informativa e a reconheceu enquanto direito autônomo à privacidade. Tamanha foi a magnitude do julgado que configurou o tom das discussões acerca do tema a partir de então, sendo referência internacional acerca do tema[125].

Outro importante marco é a Carta de Direitos Fundamentais da União Europeia de 2000, cuja importância para o tema justifica-se por ter sintetizado o direito dos países europeus e inserido no direito comunitário formal a proteção de dados pessoais enquanto direito fundamental dos cidadãos europeus. Apesar de apenas ter obtido força vinculativa em 2009, trata-se de importante referência de estudo, pois influenciou a regulação de diversos países dentro e fora da Europa[126].

Mais recentemente, a *General Data Protection Regulation* de 2016, que criou um conjunto de normas aplicáveis a todos os países-membros e inclusive a países de fora do bloco europeu em razão da sua extraterritorialidade, o que motivou até mesmo a edição da LGPD[127].

Dada a relevância dos acontecimentos, o caso europeu foi escolhido como parâmetro do desenvolvimento do direito fundamental à proteção de dados pessoais, tendo em vista sua influência no direito brasileiro, como se poderá verificar no ponto 4.3, quanto à edição da LGPD

---

[125] DONEDA. *Op. Cit.*, 2006, p. 196-197.
[126] AGÊNCIA DE DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA et al. **Manual da legislação europeia sobre proteção de dados**. [*S.l.*], Publications Office, 2014. *DOI.org (CSL JSON)*, https://data.europa.eu/doi/10.2811/73790. p. 21. Disponível em: http://publications.europa.eu/resource/cellar/af9d0b3f-82be-11e5-b8b7-01aa75ed71a1.0017.03/DOC_2. Acesso em 01 de fev. de 2021.
[127] Questão abordada no ponto 4.3.4.

e as decisões proferidas pelo Supremo Tribunal Federal, sem prejuízo da produção doutrinária brasileira que também se utiliza bastante deste parâmetro.

Tendo em vista que não é objetivo deste trabalho proceder a uma análise minuciosa do direito europeu, limitar-se-á a expor em linhas gerais como se deu a consolidação do direito à proteção de dados nesse contexto. Para tanto, serão abordados, sobretudo, a decisão do Tribunal Alemão, a Carta de Direitos Fundamentais da União Europeia e a *General Data Protection*, dentre outros pontos considerados relevantes para a melhor compreensão da matéria.

3.1 DECISÃO DO TRIBUNAL CONSTITUCIONAL ALEMÃO

A decisão judicial mais emblemática sobre autodeterminação informativa no século passado é, provavelmente, a decisão do Tribunal Constitucional Alemão sobre a Lei do Censo de 1983, sendo base de estudo para o tema até hoje. A referida lei possuía o objetivo de realizar o recenseamento populacional alemão e, para tanto, necessitava da coleta de dados pessoais dos cidadãos para a elaboração do estudo demográfico; ocorre que havia uma previsão de comparação e transmissão dos dados a repartições públicas para finalidades não especificadas de execução administrativa, ponto que causou bastante controvérsia e ocasionou o ajuizamento de diversas ações perante o Tribunal[128].

Os cidadãos deveriam responder a 160 perguntas, que seriam submetidas a posterior tratamento informatizado, o que causou inquietação na população alemã pelo receio dos possíveis usos das informações. Eles temiam que certas disposições, como a possibilidade de cruzamento de dados com o registro civil e outras autoridades e a aplicação de multas elevadas àqueles que se recusassem a responder - além do favorecimento daqueles que denunciassem tais indivíduos -, pudessem aumentar o poder de controle do Estado sobre as pessoas, que teria instrumentos coercitivos e diversas informações em mãos[129].

Diante deste cenário, várias reclamações constitucionais foram ajuizadas com o objetivo de obter declaração de inconstitucionalidade da Lei e, apesar de Tribunal ter reconhecido a constitucionalidade da lei em geral, julgou as reclamações parcialmente procedentes – parte

[128] SCHWABE, Jürgen. **Cinqüenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Montevidéu: Fundación Konrad-Adenauer, 2005, p. 233-234.
[129] DONEDA. *Op. Cit.*, 2006, p. 193.

que confere ao julgado tanta relevância nesse caso. Considerou-se nulo o dispositivo sobre compartilhamento dos dados, por reconhecer que a proteção do indivíduo, no que concerne ao armazenamento e outros usos de seus dados pessoais, faz parte do direito fundamental geral de personalidade, portanto o titular dos dados tem o poder de decisão sobre seus usos[130].

A decisão também trouxe pontos importantes, como a discussão acerca da possibilidade de restrição do direito à autodeterminação informativa, somente possível nos casos em que o interesse coletivo se sobreponha ao interesse individual, e também sobre a necessidade de clareza da lei, atenção ao princípio da proporcionalidade, entre outras medidas que têm como finalidade afastar violações ao direito da personalidade. Ressaltou, entretanto, que o compartilhamento de dados para fins científicos, ou seja, para a realização da pesquisa, não feriria a Lei Fundamental Alemã[131].

Para Bruno Bioni, a notoriedade da decisão se dá em razão de dois aspectos sob os quais se apoiou a *ratio decidendi*: a colocação da proteção dos dados pessoais enquanto direito de personalidade autônomo (com a utilização do termo "autodeterminação informativa" além da mera exigência de consentimento, absorvendo a ideia de maior liberdade individual no poder de decisão sobre dados) e o estabelecimento da função e limites para o consentimento[132].

Essa importante e inevitável mudança de perspectiva foi replicada por diversos ordenamentos jurídicos ao redor do mundo e está presente nos sistemas de proteção de dados atuais, dada a sua inteligência para lidar com os atuais desafios da era da informação ao lado da autodeterminação do indivíduo.

3.2 MUDANÇA DO PARADIGMA LEGAL: DA CONVENÇÃO EUROPEIA DE DIREITOS DO HOMEM ATÉ A CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA

Inicialmente, dá riqueza à discussão começar pela menção à Convenção Europeia de Direitos do Homem (CEDH), de 1950, que surge da iniciativa do Conselho da Europa para obrigar os países a atuar conforme suas disposições, com "o objetivo de promover o Estado de

[130] *Ibidem*, p. 234.
[131] *Ibidem*, p. 235.
[132] BIONI. *Op. Cit.*, p. 128.

direito, a democracia, os direitos humanos e o desenvolvimento social"[133]. Em seu artigo 8º, a CEDH garante o direito à privacidade, que posteriormente passou a ser interpretado pelo Tribunal Europeu dos Direitos do Homem de modo a abranger o direito à proteção de dados. O referido Tribunal atualmente possui entendimento no sentido de que a proteção não é somente no sentido de abstenção de violações, como também impõe atos para que seja assegurado ativamente o direito do artigo 8º[134], ou seja, é tanto uma obrigação negativa quanto positiva por parte dos Estados.

Tomando como base o estudo realizado no primeiro capítulo sobre a progressão generacional de leis de proteção de dados na Europa, importante rememorar que as *Privacy Guidelines* da OCDE constituíram a primeira orientação geral europeia sobre o tema – com ênfase no controle do tráfego de dados e não na proteção da pessoa –, entretanto fato é que nunca foram vinculantes aos países-membros da OCDE e logo perderam força. Outro motivo para a decadência da aplicação das *guidelines* é que, após um ano, o Conselho da Europa regulou matéria por meio da Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais, também conhecida como Convenção nº 108/1981 ou Convenção de Strasbourg[135].

A Convenção nº 108, esta sim, possuía força vinculante e permitia que países não membros do Conselho da Europa aderissem a ela, porém sua maior importância, como aponta Danilo Doneda, reside no fato de que elevou a proteção de dados à esfera dos direitos humanos[136]. A normativa busca regular as atividades de coleta e tratamento e dá atenção especial aos dados sensíveis, assim como afirma o direito de ser informado sobre o armazenamento de informações pessoais e de promover as devidas retificações, somente sendo possível aplicar restrições diante de interesses superiores, como de segurança de Estado[137].

Alguns anos depois, após diversos países-membros editarem leis nacionais sobre proteção de dados, foi editada a Diretiva 95/46/CE, com o objetivo de "padronizar efetivamente a proteção de dados pessoais" no direito comunitário europeu, regulando o tratamento e livre

[133]AGÊNCIA DE DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA. *Op. Cit.*, p. 14.
[134] *Ibidem*, p. 15.
[135] DONEDA. *Op. Cit.*, p. 230-231.
[136] *Ibidem*, p. 231-232.
[137] AGÊNCIA DE DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA. *Op. Cit.*, p. 16.

circulação de dados pessoais sob a perspectiva da proteção da pessoa[138]. Todo esse tema é regido por princípios que devem ser observados pelos estados-membros em suas legislações internas, assim como aplica-se tanto ao setor público quanto ao privado[139].

De acordo com o Manual da Legislação Europeia sobre Proteção de Dados, elaborado pela Agência dos Direitos Fundamentais da União Europeia (FRA) e pelo Conselho da Europa, tendo em vista a necessidade de conceder direitos individuais para proteção de direitos humanos no âmbito da União Europeia, o então Tribunal de Justiça das Comunidades Europeias proclamou, em 2000, a Carta dos Direitos Fundamentais da União Europeia[140].

O documento reúne direitos do cidadão europeu, bem como tradições constitucionais dos países-membros e obrigações comuns. Muito embora fosse documento meramente político, adquiriu status vinculante como direito primário em razão do Tratado de Lisboa de 2009. Mais especificamente no que concerne a este trabalho, a Carta reconheceu expressamente, em seu artigo 8º, o direito a proteção de dados como um direito fundamental, entretanto é importante ressaltar que tal fato não constitui inovação jurídica, eis que simplesmente incorporou a legislação preexistente na seara da União Europeia[141].

Essa análise permite observar a evolução legal do direito comunitário europeu sobre a proteção de dados pessoais, primeiramente visto pelo prisma da privacidade (na CEDH) e sua ascensão enquanto direito autônomo e fundamental na Carta de Direitos Fundamentais da União Europeia. Outrossim, a Diretiva 95/46/CE foi, por muito tempo, o principal instrumento legal sobre a matéria, o que mudou com a entrada em vigor da mais recente regulação de proteção de dados no continente: a GDPR.

3.3 NOVA REGULAÇÃO NO CONTEXTO DO SÉCULO XXI: A ADOÇÃO DA *GENERAL DATA PROTECTION REGULATION* EM 2016

Precedida pela Diretiva Europeia 95/46/CE, a GDPR buscou, entre outros, resolver uma questão relevante dentro do sistema legal europeu: diretivas não são diretamente aplicáveis e

[138] DONEDA. *Op. Cit.,* p. 234.
[139] *Ibidem*, p. 238.
[140] AGÊNCIA DE DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA. *Op. Cit.*, p. 20.
[141] *Ibidem*, p. 21.

precisam ser incorporadas ao direito interno para plena eficácia. Esse detalhe abriu certa margem de discricionariedade para que cada país estabelecesse interpretações diferentes para as definições e regras em suas leis nacionais[142].

A *General Data Protection Regulation*, por sua vez, é diretamente aplicável por completo desde 2018, após um período de adaptação de dois anos, quando revogou as disposições da Diretiva. A adoção da GDPR representou grande avanço e modernização na legislação europeia para assegurar o direito fundamental a proteção de dados pessoais no contexto econômico e social da era da informação, como dispõem a FRA e o Conselho de Europa na versão mais atualizada do Manual citado no ponto anterior, sobre a desnecessidade de implementação no direito interno e a proposta de uniformização do tema[143]:

> *A General Data Protection Regulation assim promove por meio de um único conjunto de regras de proteção de dados por toda a União Europeia. Isso cria leis de proteção de dados consistentes pela União Europeia, estabelecendo um ambiente de segurança jurídica do qual operadores econômicos e indivíduos como 'sujeitos de dados' podem se beneficiar*[144]. (tradução livre)

Ademais, tendo em vista as necessidades da era da informação, bem como a indispensabilidade de disponibilizar instrumentos que permitam o avanço tecnológico, em especial a livre circulação de dados, o novo regulamento europeu seguiu a mesma finalidade que a Diretiva 95/46/CE se propôs a cuidar. Assim, o objetivo logo declarado no artigo 1º[145] é proteger os cidadãos europeus, reafirmando o aspecto individual de direitos e liberdades, e, não menos importante, possibilitar a livre circulação de dados no interior da União Europeia.

Por fim, outro aspecto marcante é a questão do consentimento, que mais uma vez assume papel principal no trato de dados pessoais como condição de licitude, assim tratado no artigo 6º[146]. O artigo elenca basicamente duas situações em que é lícito o tratamento: quando for indispensável para a atividade que se presta (discriminadas de 6.1.b a 6.1.f) e quando houver o consentimento do titular para as finalidades específicas.

---

[142] AGÊNCIA DE DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA *et. al*. **Handbook on European Data Protection Law - 2018 edition**. [*S.l.*]: Publications Office Of The European Union, 2018, p. 29-30 Disponível em: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf. Acesso em: 13 fev. 2021.

[143] *Ibidem*, p. 30.

[144] Tradução livre do original: "The General Data Protection Regulation thus provides for a single set of data protection rules across the EU. This creates consistent data protection rules throughout the EU, establishing an environment of legal certainty from which economic operators and individuals as 'data subjects' may benefit." *Ibidem*, p. 30.

[145] Artigo 1º da Diretiva. UNIÃO EUROPEIA. *Op. Cit.*

[146] Artigo 6º. *Ibidem.*

As duas opções são relevantes, já que vão ao encontro das questões discutidas no ponto 2.1.1.4 sobre a quarta geração de direitos de proteção aos dados pessoais. Enquanto sucessora da Diretiva 95/46/CE, grande exemplo dos direitos de quarta geração, a GDPR mantém essa tradição da autodeterminação informativa nas mãos não somente do particular, para que possa decidir sobre a utilização de seus dados pessoas, mas também com a suplementação estatal quanto a temas que julgam dignos da intervenção[147].

O estudo dessas legislações é relevante ao passo que auxiliam como a experiência internacional consolidou a regulamentação do direito à proteção de dados pessoais, levando em conta, inclusive, a carga de liberdade individual e participativa do titular, assim como a participação do Estado para garantir sua efetividade em determinadas matérias. A consequência lógica do reconhecimento dessa concepção tem como pano de fundo a compreensão da sua autonomia e separação do direito à privacidade.

O entendimento pela separação do direito à privacidade advém, principalmente, da compreensão de que, apesar da aparente semelhança, possuem objetos e efeitos diferentes, razão pela qual os riscos de lesão ocasionados pela violação de dados pessoais não fazem parte do arcabouço de proteção da privacidade, gerando lacunas no direito e, assim, expondo o cidadão a flagrantes desrespeito a direitos fundamentais, como será explicado adiante, já trazendo a discussão para o contexto brasileiro.

[147] MAYER-SCHÖNBERGER. *Op. Cit.*, p. 233.

4 RAZÕES PARA QUE A PROTEÇÃO DE DADOS SEJA CONSIDERADA UM DIREITO FUNDAMENTAL AUTÔNOMO E ANÁLISE DO CASO BRASILEIRO

O papel do Direito é regular as relações sociais – isso é indiscutível -, portanto deve acompanhar as mudanças sociais a fim de se adequar à realidade que se propõe a reger, sob pena de tornar-se obsoleto. Com o surgimento da sociedade digital e da era da informação, não seria diferente: é imprescindível que haja adaptação de todo o ordenamento ao novo contexto social, e, assim, certas concepções tornam-se, efetivamente, obsoletas.

A privacidade passou da ideia de ser deixado só a um direito de proteção contra abusos do Estado e outras entidades diante da intromissão na vida privada do indivíduo. Isso denota uma característica de direito "negativo", ou seja, de abstenção geral de intromissões na esfera de privacidade do indivíduo e isso está estampado na Constituição Federal de 1988 quando, em seu art. 5º, X, que *"são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação"*, demonstrando claramente o aspecto de rejeição à interferência no espectro privado da pessoa.

De igual sorte, a proteção aos sigilos das comunicações telegráficas, de dados e telefônicas, prevista no art. 5º, XII, CRFB/88, possui a mesma carga de direito negativo, impedindo interferências exteriores frente à privacidade que a pessoa deve ter em suas comunicações.

Em outras palavras, o direito à privacidade é incapaz de abarcar todos os aspectos advindos da sociedade de informação, onde esta se tornou um ativo econômico, objeto de desejo tanto a nível estatal quanto de entidades privadas. Além disso, os riscos ocasionados pelo tratamento de dados afetam intrinsecamente outros direitos fundamentais, de forma que se tornou vital o reconhecimento de um direito adequado à proteção desses fins específicos:

> *No panorama do ordenamento brasileiro, o reconhecimento da proteção de dados como um direito autônomo e fundamental não deriva de uma dicção explícita e literal, porém da consideração dos riscos que o tratamento automatizado traz à proteção da personalidade à luz das garantias constitucionais de igualdade substancial, liberdade*

> *e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada*[148].

Diante da insuficiência dos institutos clássicos para a proteção dos dados pessoais, tornou-se impossível deixar de reconhecer esse novo direito, imprescindível para a manutenção da efetividade dos direitos fundamentais como um todo, em razão de sua interdependência.

4.1 A INTERDEPENDÊNCIA DOS DIREITOS FUNDAMENTAIS

A base para essa compreensão é da interdependência dos direitos fundamentais, isto é, apesar de autônomos entre si, dependem uns dos outros para sua eficácia. O conteúdo de um direito fundamental vincula-se ao dos demais, na medida em que se complementam ou são desdobramentos uns dos outros. Tendo em vista a dependência mútua entre eles, o desrespeito a um direito fundamental compromete todo o sistema. Por exemplo, a liberdade de informação advém da liberdade de expressão, logo seria impossível a existência de uma imprensa livre (enquanto classe cujo objetivo é fornecer informações à população) sem que seja garantida a liberdade para transmitir a informação, bem como devem respeitar a intimidade e a privacidade, como forma de limitação[149].

Lembrando que esse sistema também tem como base na relatividade, ou seja, os direitos fundamentais não são absolutos, pois encontram limites nos demais direitos igualmente consagrados pela Carta Magna, conforme aduz Alexandre de Moraes:

> *Desta forma, quando houver conflito entre dois ou mais direitos ou garantias fundamentais, o intérprete deve utilizar-se do princípio da concordância prática ou da harmonização, de forma a coordenar e combinar os bens jurídicos em conflito, evitando o sacrifício total de uns em relação aos outros, realizando uma redução proporcional do âmbito de alcance de cada qual (contradição dos princípios), sempre em busca do verdadeiro significado da norma e da harmonia do texto constitucional com sua finalidade precípua.*[150]

Dessa forma, em um conflito entre liberdade de expressão e privacidade, se desatendida totalmente a privacidade, por exemplo, não seria possível dizer que a liberdade de expressão foi atendida, pois o sistema depende da observância de todos os direitos. A exclusão de um prejudica o todo, somente sendo factível a ponderação no caso concreto, buscando atingir o objetivo principal da norma, porém sem extirpar a aplicação de um direito por completo, já que

---

[148] DONEDA. *Op. Cit.*, 2011, p. 103.
[149] ROTHENBURG, Walter Claudius. Direitos Fundamentais e suas características. **Revista dos Tribunais**: Cadernos de Direito Tributário e Finanças Públicas, [*S.l.*], n. 29, out./dez. 1999.
[150] MORAES, Alexandre de. **Direito Constitucional**. 36. ed. p. 45. São Paulo: Atlas, 2020. *E-book*.

são todos desdobramentos do corolário da dignidade da pessoa humana, que fundamenta todos esses direitos e confere unidade[151] ao sistema.

Ademais, durante a Conferência Mundial sobre Direitos Humanos, realizada em 1993, em Viena, foi elaborada a Declaração e Programa de Ação de Viena, a qual dispõe no item I.5 que "todos os Direitos Humanos são universais, indivisíveis, interdependentes e interrelacionados"[152].

O Supremo Tribunal Federal em diversas ocasiões decidiu sobre a colisão de direitos fundamentais, sempre considerando que não se pode excluir um direito fundamental a pretexto de salvaguardar outro. A interdependência é característica inerente e somente pode-se afastar a aplicação de um ou outro no caso concreto conforme a finalidade da norma. Assim decidiu o tribunal em sede da ADI º 4815, em que se buscou a declaração de inconstitucionalidade de dispositivos do Código Civil que, na prática, posicionavam em abstrato o direito à intimidade, à honra e à privacidade em posição superior à liberdade de expressão, condicionando a publicação à autorização prévia do biografado.

> *EMENTA: AÇÃO DIRETA DE INCONSTITUCIONALIDADE. ARTS. 20 E 21 DA LEI N. 10.406/2002 (CÓDIGO CIVIL). PRELIMINAR DE ILEGITIMIDADE ATIVA REJEITADA. REQUISITOS LEGAIS OBSERVADOS. MÉRITO: APARENTE CONFLITO ENTRE PRINCÍPIOS CONSTITUCIONAIS: LIBERDADE DE EXPRESSÃO, DE INFORMAÇÃO, ARTÍSTICA E CULTURAL, INDEPENDENTE DE CENSURA OU AUTORIZAÇÃO PRÉVIA (ART. 5º INCS. IV, IX, XIV; 220, §§ 1º E 2º) E INVIOLABILIDADE DA INTIMIDADE, VIDA PRIVADA, HONRA E IMAGEM DAS PESSOAS (ART. 5º, INC. X). ADOÇÃO DE CRITÉRIO DA PONDERAÇÃO PARA INTERPRETAÇÃO DE PRINCÍPIO CONSTITUCIONAL. PROIBIÇÃO DE CENSURA (ESTATAL OU PARTICULAR). GARANTIA CONSTITUCIONAL DE INDENIZAÇÃO E DE DIREITO DE RESPOSTA. AÇÃO DIRETA JULGADA PROCEDENTE PARA DAR INTERPRETAÇÃO CONFORME À CONSTITUIÇÃO AOS ARTS. 20 E 21 DO CÓDIGO CIVIL, SEM REDUÇÃO DE TEXTO. 1. A Associação Nacional dos Editores de Livros - Anel congrega a classe dos editores, considerados, para fins estatutários, a pessoa natural ou jurídica à qual se atribui o direito de reprodução de obra literária, artística ou científica, podendo publicá-la e divulgá-la. A correlação entre o conteúdo da norma impugnada e os objetivos da Autora preenche o requisito de pertinência temática e a presença de seus associados em nove Estados da Federação comprova sua representação nacional, nos termos da jurisprudência deste Supremo Tribunal. Preliminar de ilegitimidade ativa rejeitada. 2. O objeto da presente ação restringe-se à interpretação dos arts. 20 e 21 do Código Civil relativas à divulgação de escritos, à transmissão da palavra, à produção, publicação, exposição ou utilização da imagem de pessoa biografada. 3. A Constituição do Brasil proíbe qualquer censura. O exercício do direito à liberdade*

---

[151] *Ibidem*, p. 35.

[152] CONFERÊNCIA MUNDIAL SOBRE DIREITOS HUMANOS. **Declaração e Programa de Ação de Viena**. Viena, 1993. Disponível em: https://www.oas.org/dil/port/1993%20Declara%C3%A7%C3%A3o%20e%20Programa%20de%20Ac%C3%A7%C3%A3o%20adoptado%20pela%20Confer%C3%AAncia%20Mundial%20de%20Viena%20sobre%20Direitos%20Humanos%20em%20junho%20de%201993.pdf. Acesso em 24 abr. 2021.

> *de expressão não pode ser cerceada pelo Estado ou por particular. 4. O direito de informação, constitucionalmente garantido, contém a liberdade de informar, de se informar e de ser informado. O primeiro refere-se à formação da opinião pública, considerado cada qual dos cidadãos que pode receber livremente dados sobre assuntos de interesse da coletividade e sobre as pessoas cujas ações, público-estatais ou público-sociais, interferem em sua esfera do acervo do direito de saber, de aprender sobre temas relacionados a suas legítimas cogitações. 5. Biografia é história. A vida não se desenvolve apenas a partir da soleira da porta de casa. 6. Autorização prévia para biografia constitui censura prévia particular. O recolhimento de obras é censura judicial, a substituir a administrativa. O risco é próprio do viver. Erros corrigem-se segundo o direito, não se coartando liberdades conquistadas. A reparação de danos e o direito de resposta devem ser exercidos nos termos da lei.* ***7. A liberdade é constitucionalmente garantida, não se podendo anular por outra norma constitucional (inc. IV do art. 60), menos ainda por norma de hierarquia inferior (lei civil), ainda que sob o argumento de se estar a resguardar e proteger outro direito constitucionalmente assegurado, qual seja, o da inviolabilidade do direito à intimidade, à privacidade, à honra e à imagem. 8. Para a coexistência das normas constitucionais dos incs. IV, IX e X do art. 5º, há de se acolher o balanceamento de direitos, conjugando-se o direito às liberdades com a inviolabilidade da intimidade, da privacidade, da honra e da imagem da pessoa biografada e daqueles que pretendem elaborar as biografias.*** *9. Ação direta julgada procedente para dar interpretação conforme à Constituição aos arts. 20 e 21 do Código Civil, sem redução de texto, para, em consonância com os direitos fundamentais à liberdade de pensamento e de sua expressão, de criação artística, produção científica, declarar inexigível autorização de pessoa biografada relativamente a obras biográficas literárias ou audiovisuais, sendo também desnecessária autorização de pessoas retratadas como coadjuvantes (ou de seus familiares, em caso de pessoas falecidas ou ausentes).*[153]

Identificada a inconstitucionalidade, o STF decidiu pela impossibilidade de censura prévia, ou seja, não se pode estabelecer hierarquia entre direitos fundamentais, considerando que o dispositivo promovia afastamento geral da liberdade de expressão frente a biografias não autorizadas. Assim, é inconstitucional e contrário à sistemática de direitos fundamentais excluir um em detrimento de outro de forma abstrata, somente podendo ser ponderado no caso concreto. A unicidade dos direitos fundamentais está diretamente ligada à sua interdependência, ao passo que somente há efetividade se considerado como um todo.

Sendo assim, a interdependência e a interrelação dos direitos fundamentais é elemento essencial para a compreensão de que o não reconhecimento do direito à proteção de dados pessoais coloca em risco todo o sistema de proteção da dignidade da pessoa humana, pois sem ele diversas situações ocasionadas pela sociedade da informação deixam os indivíduos desamparados e em situação de vulnerabilidade. O não reconhecimento desse direito fundamental causa, portanto, lesão irreparável aos direitos fundamentais, permitindo uma série

---

[153] BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 4815**. Requerente: Associação Nacional dos Editores de Livros - ANEL. Relator: Ministra Carmem Lúcia. Brasília, 01 fev. 2016. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=4271057. Acesso em: 24 abr. 2021.

de violações à liberdade e igualdade e, em última instância, à própria dignidade da pessoa humana e o sistema de direitos fundamentais como um todo.

4.2 A INSUFICIÊNCIA DAS GARANTIAS DE PROTEÇÃO À INFORMAÇÃO NA CONSTITUIÇÃO FEDERAL DO BRASIL DE 1988

A Constituição Brasileira trata da informação, primordialmente, por meio dos direitos de liberdade de expressão, de acesso à informação, de proteção à intimidade e à vida privada e de sigilo das comunicações[154]. Para a análise que se segue, interessam mais as duas últimas garantias, visto que o legislador positivou o direito à privacidade de tal forma que essas garantias representam o escopo de aplicação do referido direito.

Nesse sentido, realizando-se uma análise da técnica legislativa utilizada pelo poder constituinte, que previu a proteção da privacidade (art. 5º, X) – entendida como inviolabilidade da intimidade e da vida privada – e a proteção do sigilo das correspondências e das comunicações telegráficas, de dados e das comunicações telefônicas (art. 5º, XII) em artigos distintos, depreende-se duas importantes conclusões: (i) a privacidade diz respeito àquilo que está no âmbito íntimo e privado do indivíduo, em contraposição a ideia do que é público e (ii) informações e dados pessoais são protegidos somente quanto a sua comunicação[155], não havendo proteção dos dados em si[156].

Resta claro, portanto, que a nomenclatura adotada pelo legislador exclui um inúmero de situações de clara violação à proteção de dados às quais o indivíduo está exposto na sociedade de informação, que não seriam abarcadas pelas garantias trazidas na Constituição. A título de exemplo, informações de origem étnica e racial utilizadas em um banco de dados para fins de *profiling* racial poderiam ser consideradas íntimas ou privadas? Afinal, o fenótipo é algo que pode ser identificado apenas ao olhar para a pessoa, portanto dificilmente teriam esse tipo de proteção, já que, em tese, qualquer um pode saber a cor da pele de alguém e outras características. Também os dados referentes a autores de ações trabalhistas estariam fora dessa

---

[154] MENDES. *Op. Cit.*, 2018, p. 194.
[155] Nesse sentido, o RE 418.416, de relatoria do Ministro Sepúlveda Pertence, que será mencionado no ponto 4.3.1. BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 418.416/SC**. Recorrente: Luciano Hang. Recorrido: Ministério Público Federal. Relator: Ministro Sepúlveda Pertence. Brasília, DF, 10 de maio de 2006. Brasília, 19 dez. 2006. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=395790. Acesso em: 26 abr. 2021.
[156] DONEDA. *Op. Cit.*, 2011, p. 104-105.

proteção, tendo em vista principalmente o caráter público dos processos judiciais, logo a formação de lista negativa desses trabalhadores não encontraria clara garantia nestes dispositivos, ou mesmo dados sobre a suspeita de cometimento de crimes, que também são públicos, dentre tantas outras situações que não se enquadram nessa proteção[157].

A proteção constitucional aos dados somente quanto à sua comunicação, excluindo os casos em que são utilizados fora deste contexto de ligações, envio de e-mails, mensagens etc., deixa de lado toda a gama de situações em que seria necessário protegê-los. Essa separação entre privacidade e a proteção dos dados em si fomenta situações em que se ofende a privacidade de forma indireta, ou seja, pela utilização abusiva de informações pessoais. Em um contexto de interconectividade e tratamento em massa de dados pessoais, as pessoas são identificadas de forma indireta por meio de seus dados, aumentando a relação com o desenvolvimento da personalidade e autodeterminação do indivíduo por meio de dados pessoais[158].

As garantias individuais de sigilo e inviolabilidade acima tratadas possuem grande importância para a efetivação dos direitos fundamentais, entretanto seu escopo concentra-se em situações específicas, tais como a divulgação de informações íntimas ou interceptações telefônicas. A utilização do sigilo como forma de proteger dados pessoais também não é uma solução viável, ao passo que as informações são um importante ativo atualmente e torná-las sigilosas não é o objetivo, mas, sim, permitir que haja tratamento responsável e com respeito aos direitos e garantias individuais, como bem instrui Laura Schertel:

> *não se trata de tornar sigilosas informações que podem causar a discriminação ou a limitação da liberdade pessoal, mas de regular os efeitos das informações da sociedade, por meio da regulação de seu fluxo e da instituição de procedimentos de controle*[159].

Em última análise, apesar da imprescindibilidade dos direitos aludidos, impende concluir que não estão aptos a acompanhar os novos desafios trazidos pelos avanços tecnológicos, deixando os riscos e violações à proteção de dados no limbo jurídico. Em se tratando de matéria tão delicada e afeta a direitos fundamentais, ignorar a temática significa

---

[157] MENDES, Laura Schertel. Habeas Data e Autodeterminação informativa: dois lados da mesma moeda. **Direitos Fundamentais & Justiça**, ano 12, n. 39, p. 185-216, p. 194, jul./dez. 2018. Disponível em: http://dfj.emnuvens.com.br/dfj/article/view/655/905. Acesso em 08 mar. 2021.
[158] DONEDA, *Op. Cit.*, 2011, p. 106.
[159] MENDES. *Op. Cit.*, 2018, p. 194-195.

expor o indivíduo a uma série de violações que lhe afetam, em última instância, a possibilidade de existir de forma digna na sociedade da informação.

4.2.1 Privacidade ou proteção de dados: o necessário abandono da perspectiva "expansionista" de privacidade

Por todo o exposto, compreende-se que privacidade e proteção de dados pessoais não são a mesma coisa conferem a mesma esfera de proteção, tratando-se de direitos distintos, que, apesar da origem comum, ramificaram-se pelas circunstâncias impostas pela sociedade da informação. Por mais que parcela da doutrina defenda que nada mais é que uma nova faceta do direito à privacidade[160], expandindo seu conceito para abarcar as mudanças sociojurídicas, não há dúvidas de que as especificidades da disciplina de proteção de dados a tornem autônoma e, portanto, sujeita a tutela jurisdicional própria.

O risco de se considerar a proteção de dados pessoais como um desdobramento da privacidade é a simplificação de seus fundamentos e a limitação do seu alcance. A proteção de dados sensíveis, por exemplo, tem fundamento na igualdade material e não discriminação, de modo diverso da tutela que a privacidade oferece. Neste sentido, "a proteção de dados pessoais é uma garantia de caráter instrumental, derivada da tutela da privacidade, porém não limitada a ela, e que faz referência a um leque de garantias fundamentais que se encontram no ordenamento brasileiro[161]."

Os dados pessoais se afiguram enquanto espectro dos direitos da personalidade e da autodeterminação do indivíduo, logo o seu uso, observado a partir do avanço das tecnologias de processamento e tratamento de dados, demonstram uma ameaça à existência plena do ser humano em sociedade. Em consequência disso, usufruto dos demais direitos fundamentais

---

[160] Sobre a proteção de dados ser um desdobramento do direito à privacidade: RODOTÁ, Stefano. **A vida na sociedade de vigilância: a privacidade hoje**. A vida na sociedade de vigilância. Rio de Janeiro: Renovar, 2008. Há também um artigo interessante que assim trata o tema: CORRÊA, Rafael. Do direito de estar só à autodeterminação informativa: a evolução da disciplina legal da privacidade sob o enfoque dos direitos da personalidade e sua conformação como fundamento da tutela de dados pessoais. **Revista Eletrônica do Curso de Direito do Centro Universitário UniOpet**. Curitiba-PR. Ano XII, n. 21, jul-dez/2019. ISSN 2175-7119. Disponível em: https://www.academia.edu/42716947/Do_Direito_de_Estar_S%C3%B3_%C3%A0_Autodetermina%C3%A7%C3%A3o_Informativa_A_evolu%C3%A7%C3%A3o_da_disciplina_legal_da_privacidade_sob_o_enfoque_dos_direitos_da_personalidade_e_sua_conforma%C3%A7%C3%A3o_como_fundamento_da_tutela_de_dados_pessoais. Acesso em 08 mar. 2021.

[161] DONEDA. *Op. Cit.*, 2006, p. 326.

também resta prejudicado, ao passo o tratamento inadequado impõe repercussões, de forma mais clara, nos direitos à igualdade e liberdade, bem como, em última instância, na própria dignidade da pessoa humana.

No contexto de interconectividade e compartilhamento de dados entre entes estatais e privados, várias situações expõem a vulnerabilidade o indivíduo, como por exemplo o uso de listas negativas de trabalhadores que já ingressaram com ações trabalhistas, afetando diretamente o direito à empregabilidade.

Já que os dados sobre o indivíduo muitas das vezes constituem a única fonte de informação sobre ele, é inegável que a utilização indevida destes acarreta a perda de oportunidades e a criação de discriminações ilegais, o que causa um desequilíbrio na ideia de igualdade e na liberdade e livre escolha. Tendo em vista a quebra de paradigma ocasionada pelo tratamento de dados pessoais e o atual estado da arte, é necessário abandonar a perspectiva "expansionista" do direito à privacidade e reconhecer que ele é insuficiente para solucionar os problemas que se apresentam.

4.2.2 A diferença crucial entre os direitos à privacidade e à proteção de dados pessoais

Como já dito anteriormente, a proteção de dados pessoais é fruto do processo histórico e social que culminou na sua separação do direito à privacidade, tendo em vista a insuficiência deste frente aos novos desafios apresentados pelo tratamento de dados. Para aprofundar a análise da diferença entre ambos, é crucial entender a carga impositiva que cada um traz: enquanto a privacidade se refere mais a um direito de abstenção, a proteção de dados não impõe sigilos ou inviolabilidades necessariamente, já que seu objetivo não é impedir que dados sejam tratados, mas, sim, permitir que o sejam de forma que não prejudique o exercício de direitos fundamentais do indivíduo.

Tanto a privacidade quanto a proteção de dados são liberdades individuais, porém a primeira tem como objeto a proteção de fatos de ordem pessoal (também comerciais e profissionais) contra o conhecimento público[162], isto é, a criação de uma esfera privada na qual o indivíduo pode impedir a interferência externa. Trata-se de uma imposição de abstenção geral

[162] BRANCO, Paulo Gustavo Gonet; MENDES, Gilmar Ferreira. **Curso de direito constitucional**. 10. ed. São Paulo: Saraiva, 2016, p. 280.

à vida privada do indivíduo, no mesmo sentido do *"right to be let alone"* ou direito de ser deixado só proposto por Warren e Brandeis, para proteger a pessoa da exposição do que considera privado, o que também é pressuposto para o livre desenvolvimento da personalidade:

> *(...) sem privacidade, não há condições propícias para o desenvolvimento livre da personalidade. Estar submetido ao constante crivo da observação alheia dificulta o enfrentamento de novos desafios. A exposição diuturna dos nossos erros, dificuldades e fracassos à crítica e à curiosidade permanente de terceiros, e ao ridículo público mesmo inibiria toda tentativa de autossuperação*[163].

A privacidade, portanto, tem o papel de garantir uma margem de autonomia do indivíduo quanto ao que deseja manter fora do conhecimento das demais pessoas. Assim, o direito à privacidade se propõe a proteger o direito de não ser objeto da observação alheia, seja quanto aos seus assuntos, informações[164] e características a pessoas específicas ou ao público em geral[165].

Da mesma forma, Alan Westin realizou um estudo criterioso sobre a privacidade e identificou as quatro bases da liberdade individual de privacidade: (i) solidão, estado em que o indivíduo está sozinho, separado dos demais, e livre da observação alheia; (ii) intimidade, que é quando a pessoa pode agir como parte separada do grupo e individualmente estabelecer relacionamentos com outras pessoas, como no caso do círculo familiar e de amigos; (iii) anonimato, por meio do qual o indivíduo está exposto ao público, porém está livre da identificação e da vigilância, apesar de não estar livre da observação alheia; e (iv) reserva, por meio da qual a pessoa promove barreiras psicológicas a fim de manter a discrição por meio da limitação da comunicação[166].

O Supremo Tribunal Federal, em diversas oportunidades reafirmou o caráter negativo do direito à privacidade no sentido de oposição à divulgação de informações e dados sobre a pessoa. De forma ilustrativa, declarou a inconstitucionalidade do afastamento do sigilo de dados relativos ao contribuinte com base no direito à privacidade:

> *SIGILO DE DADOS – AFASTAMENTO. Conforme disposto no inciso XII do artigo 5º da Constituição Federal,* ***a regra é a privacidade quanto à correspondência, às comunicações telegráficas, aos dados e às comunicações, ficando a exceção – a***

---

[163] *Ibidem*, p. 280-281.
[164] Lembrando novamente, conforme discutido no ponto anterior, que os instrumentos fornecidos pelo direito à privacidade quanto às informações no direito brasileiro se referem ao sigilo e à inviolabilidade. Para a disciplina de proteção de dados pessoais, entretanto, não se trata de blindar informações: é sobre permitir que sejam usadas para fins idôneos e dar instrumentos ao indivíduo para controlar a utilização de seus dados. Neste sentido: MENDES. *Op. Cit.*, 2018, p. 194-195.
[165] BRANCO; MENDES. *Op. Cit.*, p. 283.
[166] WESTIN, Alan. **Privacy and freedom**. New York: Ig Publishing, 2015. p. 39-40. *E-book*.

> ***quebra do sigilo –*** *submetida ao crivo de órgão equidistante – o Judiciário – e, mesmo assim, para efeito de investigação criminal ou instrução processual penal. SIGILO DE DADOS BANCÁRIOS – RECEITA FEDERAL. Conflita com a Carta da República norma legal atribuindo à Receita Federal – parte na relação jurídico-tributária – o afastamento do sigilo de dados relativos ao contribuinte. (STF - RE 389808 PR, Min. MARCO AURÉLIO, Data de Julgamento: 15/12/2010, Tribunal Pleno, Data de Publicação: DJe-086 DIVULG 09-05-2011 PUBLIC 10-05-2011)* [167] *(grifo nosso)*

Da mesma maneira, traz à baila o entendimento de dados conforme a privacidade, isto é, proteção por meio do sigilo. No Agravo Regimental no Inquérito 3352, o STF decidiu que a investigação de um indivíduo não pode ensejar a quebra de sigilo bancário de seu irmão por suspeita de participação no delito, utilizando sob argumento de que a privacidade traz a regra de sigilo "quanto à correspondência, às comunicações telegráficas, aos dados e às comunicações". Reforça, aqui, o Tribunal a ideia de que a proteção de dados recai somente quanto ao sigilo de suas comunicações, no caso em tela, com a autoridade judiciária, conforme a ementa:

> *COMPETÊNCIA – PRERROGATIVA DE FORO – SIGILO – TERCEIRO – AFASTAMENTO. A competência por prerrogativa de foro é de direito estrito, não se podendo, considerada conexão ou continência, estendê-la a ponto de alcançar a privacidade de dados de cidadão comum não investigado.*[168]

Em decisão mais recente, em 2019 foi fixado o Tema 990 sobre a possibilidade de compartilhamento de dados bancários e fiscais do contribuinte, sem decisão judicial, com o Ministério Público para fins penais, em repercussão geral no bojo do Recurso Extraordinário 1.055.941/SP sob a seguinte ementa:

> *Repercussão geral. Tema 990. Constitucional. Processual Penal. Compartilhamento dos Relatórios de inteligência financeira da UIF e da íntegra do procedimento fiscalizatório da Receita Federal do Brasil com os órgãos de persecução penal para fins criminais. Desnecessidade de prévia autorização judicial. Constitucionalidade reconhecida. Recurso ao qual se dá provimento para restabelecer a sentença condenatória de 1º grau. Revogada a liminar de suspensão nacional (art. 1.035, § 5º, do CPC). Fixação das seguintes teses: 1. É constitucional o compartilhamento dos relatórios de inteligência financeira da UIF e da íntegra do procedimento fiscalizatório da Receita Federal do Brasil - em que se define o lançamento do tributo - com os órgãos de persecução penal para fins criminais sem prévia autorização judicial, devendo ser resguardado o sigilo das informações em procedimentos formalmente instaurados e sujeitos a posterior controle jurisdicional; 2. O compartilhamento pela UIF e pela RFB referido no item anterior deve ser feito unicamente por meio de comunicações formais, com garantia de sigilo, certificação*

---

[167] BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário 389.808/PR**. Recorrente: G.V.A. INDÚSTRIA E COMÉRCIO S/A. Recorrido: União. Relator: Ministro Marco Aurélio, 15 de dezembro de 2010. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=622715. Acesso em 02 mar. 2021.

168 BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Agravo Regimental no Inquérito 3352/DF**. Agravante: Ministério Público Federal.: Agravado: Geraldo Resende Pereira. Relator: Ministro Marco Aurélio, 18 de março de 2017. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=4163787. Acesso em 02 mar. 2021.

> *do destinatário e estabelecimento de instrumentos efetivos de apuração e correção de eventuais desvios.*[169]

Mais uma vez, o cerne da questão é o compartilhamento de dados, protegidos por meio do sigilo quanto às suas comunicações. Todos esses entendimentos vão ao encontro o STF possuía entendimento no sentido de que a inviolabilidade dos dados se restringia apenas a sua comunicação, isto é, somente seria inviolável caso seja efetivamente violada a comunicação, não abarcando a proteção dos dados em si, como decidiu o Exmo. Min. Sepúlveda Pertence[170] no julgamento do RE 418.416 de 10/05/2006.

Pela análise dos julgados, destaca-se que o fim demonstrado no que concerne ao direito à privacidade é abarcar aquilo que é efetivamente privado em face da exposição. O objetivo, portanto, desse direito é estabelecer-se em antítese à publicidade.

Pode-se perceber que a questão apontada no direito à privacidade é a separação entre público e privado, sendo este último objeto de proteção contra o primeiro. Entretanto, retornando à proteção de dados pessoais, características como cor da pele e ajuizamento de processos trabalhistas certamente gozam de publicidade, pois são passíveis de identificação por meio da observação da pessoa em si e pelo acesso ao site de algum tribunal para encontrar processos, por exemplo. Assim, depreende-se que são de conhecimento público, logo não se pode reclamar o direito à privacidade para garantia desses dados e informações.

É essa oposição que dá o conteúdo do direito à privacidade, pois este se coloca enquanto liberdade negativa para prevenir a interferência alheia na sua esfera privada, cuja violação ocorre quando há acesso arbitrário ou não autorizado. Quando colocado no contexto digital, esse conceito se torna problemático pela dificuldade em estabelecer qual dado é público e qual é privado[171], a exemplo de perfis de redes sociais e a indagação sobre a natureza pública ou privada das informações ali postas.

---

[169] BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário 1055914/SP**. Recorrente: Ministério Público Federal. Recorridos H.C.H; T.J.H. Relator: Dias Toffoli, 04 de dezembro de 2019. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5213056. Acesso em 02 mar. 2021.

[170] RE 418.416, Tribunal Pleno, julg. em 10/05/2006, public. em 19/12/2006 no DJU.

[171] ANTONIALLI, Dennys. **Privacy and International Compliance: when differences become an issue**. In: Intelligent Information Privacy Management (AAAI Spring Symposium Series), 2010. Intelligent Information Privacy Management (AAAI Spring Symposium Series). Disponível em: https://www.aaai.org/ocs/index.php/SSS/SSS10/paper/viewFile/1165/1470. Acesso em 09 mar. 2021.

Outrossim, Dennys Antonialli identifica que, enquanto o direito à privacidade é uma liberdade negativa, o direito à proteção de dados pessoais confere à pessoa uma liberdade positiva, por meio da qual o indivíduo tem poder de controlar seus dados, sejam eles privados ou não. Isso pois o mero direito de resistir a intromissões alheias não oferece a proteção devida no contexto digital de tratamento de dados sem que haja a violação da esfera privada: "se um pedaço de informação for coletado, será necessária a notificação e autorização do usuário em razão de um real poder de controle em vez de um mero poder de resistir."[172]

Assim, o direito a proteção de dados pessoais se estabelece enquanto direito autônomo, pois sequer opera perante o pressuposto de esfera privada, bastando que o dado seja referente a uma pessoa identificada ou identificável para que seja aplicado. Por exemplo, os direitos de acesso e retificação de informações em bancos de dados atuam na esfera pública; esses dados estão expostos a cognição alheia e basta que os dados representem de forma fidedigna o seu titular. Ademais, o direito à proteção de dados pessoais está diretamente ligado a liberdades individuais que a privacidade não abarca, como a proteção da igualdade material e não discriminação, afastando-se ainda mais estes direitos.[173]

Por fim, depreende-se que o fluxo informacional e a sociedade da informação impendem o reconhecimento de que é necessário o reconhecimento dos dados pessoais como prolongamento da pessoa[174] e que afeta o exercício de outros direitos fundamentais, estabelecendo como liberdade positiva, ou seja, que dá poder ao indivíduo sobre o controle de seus dados (privados ou não) e, consequentemente, sobre a forma como se apresenta perante a sociedade no contexto de tratamento em massa de informações, ao invés de um mero direito de repelir o acesso à esfera privada. O direito à proteção de dados pessoais emerge, portanto, enquanto direito fundamental e autônomo à privacidade pela incompatibilidade de seus pressupostos (como a informação privada), mecanismos de proteção, consequências práticas (sigilo e inviolabilidade), entre outros.

4.3 CONSIDERAÇÕES ACERCA DO REGIME BRASILEIRO DE PROTEÇÃO DE DADOS

[172] "(…) if a piece of data is collected, notification and authorization of the user are required due to an actual *power of control* rather than the mere *power to resist*". *Ibidem,* p. 14.
[173] BIONI. *Op. Cit.*, p. 127.
[174] *Ibidem*, p. 128.

O quadro brasileiro de leis de proteção de dados deriva da provisão constitucional trazida pela Constituição de 1988 e de leis específicas, editadas nos últimos 20 anos, diante dos desafios postos pelo processamento de dados, que culminou na edição da Lei Geral de Proteção de Dados, a primeira lei brasileira que se propôs a regular a temática de forma geral.

O Brasil, apesar de tratar a matéria diversas vezes conforme o direito de vários países que reconhecem o direito fundamental à proteção de dados pessoais, não faz parte do rol de países que cujo ordenamento contempla a autodeterminação afirmativa com status fundamental. Na contramão dessa realidade, está em trâmite a PEC nº 17/2019, que busca inserir explicitamente o direito à proteção de dados pessoais no rol de direitos fundamentais da constituição, assim como concepção ventilada também pelo STF no ano de 2020.

Há várias leis que podem ser citadas como parte do regime de proteção de dados no ordenamento jurídico brasileiro, porém não é parte do objetivo deste trabalho proceder a uma análise detalhada do panorama brasileiro, mas tão somente levantar aspectos legais relevantes para a compreensão da matéria. Para tanto, far-se-á uma breve análise de alguns aspectos concernentes à Constituição Federal, ao Código de Defesa do Consumidor, ao Marco Civil da Internet e à LGPD. Por fim, serão tecidos comentários acerca da jurisprudência do STF e sobre a referida PEC.

4.3.1 Constituição Federal de 1988 e Habeas Data

A Constituição de 1988, como bem analisa Danilo Doneda, aborda o tema da informação através do confronto de garantias individuais, como liberdade de expressão e direito à informação, com a proteção à personalidade, como através do direito à privacidade – ou seja, trata-se do aspecto relacional de sopesamento entre valores positivos (permissão) e negativos (proibição) a serem analisados no caso concreto. A bem dizer, o estudo sobre um sistema de proteção de dados pessoais no ordenamento brasileiro é fruto da interpretação de normas esparsas que possuem como matriz a cláusula geral de proteção à personalidade[175], como observado no pela ausência de norma constitucional expressa no sentido da proteção de dados

[175] DONEDA. *Op. Cit.*, 2006, p. 323.

pessoais. Cumpre ressaltar que somente houve uma regulação mais enxuta e centralizada após a edição da LGPD.

No que tange à privacidade, a Carta Maga positiva desdobramentos deste direito fundamental, a saber, a inviolabilidade da vida privada e da intimidade[176], assim como o sigilo das comunicações telegráficas, telefônicas e de dados[177], entre outros[178]. Pois bem, neste último caso, é importante ressaltar que o STF exarou entendimento no sentido de que a inviolabilidade dos dados se restringiria ao seu compartilhamento, isto é, somente gozaria de proteção caso seja efetivamente violada a comunicação, não abarcando a proteção dos dados em si. Assim, por muito tempo entendeu-se que o artigo 5º, XII da Constituição somente conferia proteção ao sigilo das comunicações, ou seja, na via de um direito negativo, de abstenção estatal. A despeito disso, a jurisprudência adotou posicionamento diverso quando, em 2020, o STF reconheceu o direito fundamental à proteção de dados, assunto que será melhor discutido no ponto 4.3.6.

Feitas essas observações, passa-se a tratar do instrumento legal trazido pela CRFB/88 chamado Habeas Data, previsto no art. 5º, LXXII, com o objetivo de permitir que o cidadão tenha conhecimento de informações suas armazenadas em bancos de dados de caráter público e promover respectiva retificação. Entretanto, por mais que possa parecer que sua criação seja originária dos direitos de proteção de dados que já vinham se consolidando na Europa, é imprescindível entender sua criação a partir do momento histórico e político em que foi criada a ação: após o fim da Ditadura Militar e o trauma pelo uso autoritário de informações pessoais. É, portanto, forma de efetivar o cumprimento de direitos fundamentais e fomentar a cultura democrática no país[179].

Além de não ter sido criado como uma ferramenta moderna de proteção de dados no contexto brasileiro, da mesma forma não se desenvolveu posteriormente para assim ser, impondo uma série de limitações à efetivação do direito à proteção de dados que tornam o Habeas Data relativamente custoso e devagar, como os requisitos da prévia tentativa frustrada de resolver diretamente com o detentor dos dados e da necessidade de um advogado para impetrar a ação. Em razão disso, foram criados outros instrumentos que se propõem a resolver

[176] Art. 5º, X, CRFB/88.
[177] Art. 5º, XII, CRFB/88.
[178] DONEDA. *Op. Cit.*, 2006 p. 323-324.
[179] DONEDA. *Op. Cit.*, 2006, p. 326-328.

de forma mais dinâmica a problemática da proteção de dados no Brasil[180], como o direito de exigir a correção de informações sobre si dispostas em bancos de dados, prazo máximo pelo qual podem permanecer armazenadas e outros direitos inicialmente regulados de forma geral pelo direito consumerista, que o fez por meio do Código de Defesa do Consumidor.

4.3.2 Código de Defesa do Consumidor

No Brasil, o direito do consumidor possui raízes constitucionais bastante claras e provém de várias disposições que têm como objetivo o estabelecimento da matéria consumerista como essencial para o sistema jurídico, visto que o artigo 170, V, da CRFB/88 dispõe que a proteção do consumidor é um princípio da ordem econômica, assim como um direito fundamental do cidadão conforme o artigo 5º, XXXII, o que é relevante também na matéria de proteção de dados, como exposto a seguir.

No âmbito das relações de consumo, o tratamento de dados pessoais toma roupagem mais delicada, tendo em vista a vulnerabilidade do consumidor, a abrangência do mercado de consumo e o seu potencial lesivo, como estudado nos pontos 3.3.5 e 3.3.6 sobre as possíveis lesões à isonomia e à liberdade. Nesse sentido, diz Laura Schertel Mendes, há que se considerar a vulnerabilidade do consumidor no que concerne ao tratamento de seus dados pessoais, pois:

> *(...) assim como as demais informações extraídas a partir deles, constituem-se em uma representação virtual da pessoa perante a sociedade, ampliando ou reduzindo as suas oportunidades no mercado, conforme a sua utilização. O risco ao consumidor que tem os seus dados coletados e processados ocorre, principalmente, quando o tratamento dos dados é realizado de forma equivocada ou discriminatória, acarretando a sua classificação e discriminação no mercado de consumo. Isso acaba por afetar expressivamente o seu acesso a bens e serviços e as suas oportunidades sociais*[181].

Assim, recaiu sobre os ombros do Código de Defesa do Consumidor regular parcialmente a matéria e assim o fez no seu artigo 43[182] sobre bancos de dados, explicitando

---

[180] DONEDA, Danilo; MENDES, Laura Schertel. **Data Protection in Brazil: New Developments and Current Challenges.** In: GUTWIRTH, Serge; LEENS, Ronald; DE HERT, Paul. Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges. Springer, 2014, p. 6. *E-book*.

[181] MENDES. *Op. Cit.*, 2007, p. 129.

[182] Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
§ 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
§ 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.

princípios clássicos, como os do acesso, da exatidão e da finalidade. No mesmo artigo, estabeleceu o marco temporal de 5 (cinco) anos para armazenamento de informações de caráter negativo para o consumidor, assim como o direito de exigir a correção e retirada dessas informações inexatas ou que já tenham ultrapassado tal prazo[183].

A inserção desses elementos no sistema legal confere ao consumidor ferramentas para sua proteção, possibilitando que, enquanto titular dos dados pessoais, possa exercer controle sobre suas informações. Dessa forma, o Código de Defesa do Consumidor figura como importante instrumento de efetivação do direito à proteção de dados pessoais e, importante ressaltar, ajuda a construir a ideia de autodeterminação informativa no ordenamento jurídico brasileiro[184].

4.3.3 O Marco Civil da Internet

O Marco Civil da Internet – MCI – surgiu com o objetivo de regular especificamente as relações estabelecidas na internet e, por isso, percorreu um longo processo até sua promulgação em 2014. O grande período de discussão se deve ao fato de que a matéria interfere diretamente nos interesses empresariais e a lei se propôs a enfrentar temas que, até então, estavam em aberto, como a própria proteção aos registros e aos dados pessoais, a neutralidade da rede, a responsabilidade civil dos provedores de conexão e de aplicações de internet, entre outros[185], que careciam de regulação específica.

Ademais, o MCI, como destaca Bioni, foi uma reação da sociedade às propostas legislativas de regulamentação penal da internet, em detrimento de uma legislação que estabelecesse direitos e garantias aos usuários da rede. Para afastar uma possível legislação

§ 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.
§ 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.
§ 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.
§ 6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor.

[183] BIONI. *Op. Cit.*, p. 181.
[184] *Ibidem*.
[185] MORAES; TEFFÉ. *Op. Cit.*, p. 111.

penal, que, consequentemente, teria efeitos restritivos e atuaria contra o avanço tecnológico, a problemática foi resolvida por meio do estabelecimento de diversos princípios fim de estabelecer parâmetros legais para tais situações[186].

De fato, a liberdade de expressão foi especialmente destacada na normativa, enquanto fundamento e um princípio da utilização da internet no Brasil, bem como uma condição para o pleno exercício do direito de acesso, em convergência com outros princípios a fim de permitir o livre desenvolvimento da personalidade do usuário da internet[187].

O destaque para a evolução normativa no sentido de consolidação do direito à autodeterminação informativa se dá na inserção do consentimento para o tratamento de dados, que deve ser dado de forma livre, expressa e informada, a partir de informações claras e completas, das cláusulas contratuais destacadas e das suas políticas de uso. São estes elementos que justificam a coleta dos dados pessoais, ao passo que permitem ao titular a esfera de decisão acerca de seus dados, podendo, ainda, requerer a exclusão definitiva de seus dados pessoais quando encerrada a relação[188]. Neste sentido, Bruno Bioni aponta que:

> *Pela combinatória de tais dispositivos, verifica-se ser a autodeterminação informacional o parâmetro normativo eleito pelo MCI para a proteção de dados pessoais. Todas as normas desembocam na figura do cidadão-usuário para que ele, uma vez cientificado a respeito do fluxo de seus dados pessoais, possa controlá-lo por meio do consentimento. Essa perspectiva de controle perpassa desde a fase de coleta e compartilhamento dos dados com terceiros até o direito de deletá-los junto ao prestador de serviços e produtos de Internet ao término da relação*[189].

Assim, é possível verificar que o Marco Civil da Internet representou mais um passo na construção legislativa de um sistema legal que coloca o titular dos dados pessoas como protagonista, preservando o sentido das leis de quarta geração.

4.3.4 LGPD

O quadro legal anterior à vigência Lei nº 13.709/2018, mais conhecida como Lei Geral de Proteção de Dados ou LGPD, consistia em um conjunto de leis setoriais esparsas e sem uniformidade, comparado por Bruno Bioni a uma "colcha de retalhos", cuja inconsistência regulatória deixava desamparados diversos temas e setores importantes da economia no tocante

---

[186] BIONI. *Op. Cit.*, p. 183
[187] MORAES; TEFFÉ. *Op. Cit.*, p. 111.
[188] BIONI. *Op. Cit.*, p. 183-184.
[189] *Ibidem.*

à proteção de dados. Seja no âmbito público – como no caso da formulação de políticas públicas[190] ou para a formação parcerias público-privadas que dependem da transferência de dados – ou no privado – já que nem mesmo o próprio cidadão podia contar com uma lei que lhe fornecesse proteção ampla frente a tantas atividades cotidianas que demandam o fornecimento de dados –, fato é que a incapacidade das leis até então existentes de promover a devida regulação gerava insegurança jurídica para diversos processos que envolvem o tratamento de dados[191].

Nessa linha de raciocínio, a LGPD centrou-se na formulação de normas que permitissem o tratamento de dados nos setores público e privado, assim como o avanço tecnológico, mas, ao mesmo tempo, buscou manter a redoma de proteção ao titular dos dados pessoais e seus direitos fundamentais. Essa vontade do legislador pode ser verificada a partir da análise dos artigos iniciais da lei, principalmente o artigo 2º, onde expressamente se propõe a compatibilizar fundamentos econômico-tecnológicos com a proteção da pessoa, sua liberdade e privacidade, entre outros[192].

O reconhecimento de que o tratamento de dados oferece riscos e causa impactos à vida do indivíduo é o que permite o desenvolvimento tecnológico e inovação cada vez mais prudentes, respeitando a cláusula geral da dignidade da pessoa humana sem impedir que a economia avance. Sendo assim, ainda que aparentemente contraditórios à primeira vista, a compatibilização de tais fundamentos se mostra essencial na era da informação, visto que a consideração conjunta destes diferentes pontos fornece ferramentas que possibilitam a construção gradual de um ambiente digital cada vez mais seguro.

Um dos pontos de maior destaque para esse trabalho é que a lei traz expressamente a autodeterminação informativa como fundamento em seu artigo 2º, II, na mesma linha da quarta

---

[190] Essa questão específica foi tratada no artigo 7º, III, que permite que a administração pública realize tratamento de dados necessários à execução de políticas públicas.
[191] BIONI. *Op. Cit., p.* 133
[192] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I - o respeito à privacidade;
II - a autodeterminação informativa;
III - a liberdade de expressão, de informação, de comunicação e de opinião;
IV - a inviolabilidade da intimidade, da honra e da imagem;
V - o desenvolvimento econômico e tecnológico e a inovação;
VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

geração de leis de proteção de dados europeia, demonstrando também um empenho de promover ou possibilitar a participação ativa do indivíduo durante todas as etapas de processamento de dados. Essa intenção pode ser verificada em diversos artigos da LGPD, dentre os quais destaca-se o art. 18, que traz a possibilidade de o titular acessar seus dados, requerer a correção de dados incompletos, inexatos ou desatualizados, eliminar dados pessoais tratados com o seu consentimento, revogar o consentimento, entre outros.

Na mesma esteira da análise histórico-evolutiva estudada ao longo dos capítulos, não é surpresa encontrar a valorização do consentimento como elemento legitimador do tratamento de dados, identificado no artigo 7º, I, que traz também outras hipóteses de finalidades legítimas nos demais incisos.

O artigo 8º se aprofunda na questão do consentimento, que, apesar de não ser a única hipótese permissiva de tratamento de dados pessoais, possui destaque por representar a carga participativa do indivíduo que fundamenta a disciplina. Isso se dá não somente por ter sido alocado em posição topograficamente superior (o consentimento está no inciso I), mas também por poder ser identificado em diversos outros artigos[193] e estar intrinsecamente presente nos princípios trazidos pela lei, indicando sua posição de superioridade em relação às demais hipóteses. Seguindo a linha evolutiva do direito comunitário europeu e da quarta geração de leis de proteção de dados pessoais, a LGPD, assim como a GDPR, defende que o consentimento deve ser livre, informado, inequívoco e possuir finalidade determinada[194]. Nesse sentido:

> *O principal vetor para alcançar tal objetivo é franquear ao cidadão controle sobre seus dados pessoais. Essa estratégia vai além do consentimento do titular dos dados, pelo qual ele autorizaria o seu uso. Tão importante quanto esse elemento volitivo é assegurar que o fluxo informacional atenda às suas legítimas expectativas e, sobretudo, não seja corrosivo ao livre desenvolvimento da sua personalidade*[195].

Apesar de a LGPD ter entrado em vigor após a GDPR e das semelhanças entre alguns dispositivos, a lei brasileira não utilizou a normativa europeia como base para sua confecção, isso pois seu anteprojeto e discussão são cronologicamente anteriores. Porém, pode-se dizer que a vigência da *General Data Protection Regulatio*ne exerceu influência em determinados

[193] O próprio artigo 8º da LGPD dedica-se inteiramente à questão do consentimento, assim como pode ser encontrada menção nos artigos 9º, parágrafo 2º; 11, I; 14 etc.
[194] BIONI. *Op. Cit*, p. 185.
[195] *Ibidem*, p. 134.

pontos pontos, de forma que a redação é bastante similar à GDPR, sendo um argumento que pode explicar as semelhanças entre as leis, apontadas ao longo deste trabalho[196].

4.3.5 Outros elementos que indicam a existência do direito fundamental a proteção de dados pessoais no ordenamento brasileiro

Logo de início impende ressaltar que na XIII Cúpula Ibero-americana de Chefes de Estado e Governo, realizada em 14 e 15 de novembro de 2003, o Brasil firmou a Declaração de Santa Cruz de La Sierra, documento que reconhece formalmente o direito fundamental à proteção de dados pessoais e a importância da regulação da matéria, nos seguintes termos:

> *Estamos também conscientes de que a protecção de dados pessoais é um direito fundamental das pessoas e destacamos a importância das iniciativas reguladoras iberoamericanas para proteger a privacidade dos cidadãos, contidas na Declaração de Antigua, pela qual se cria a Rede Ibero-Americana de Protecção de Dados, aberta a todos os países da nossa Comunidade*[197].

Apesar de o documento não possuir força impositiva, trata-se de um compromisso firmado perante a Ibero-américa e um argumento a favor do reconhecimento de tal direito fundamental.

Seguindo essa tendência, dezesseis anos depois foi proposta a PEC nº 17/2019 de autoria do Senador Eduardo Gomes, pela inclusão expressa da proteção de dados pessoais no rol de direitos fundamentais do artigo 5º, CRFB/88, e pelo estabelecimento da competência privativa da União para legislar sobre a matéria. Na justificação inicial, os autores da proposta sustentam a importância de tal direito enquanto evolução histórica e adoção por diversos países, que vale a leitura do trecho colacionado abaixo:

> *Isso porque o assunto, cada vez mais, na Era informacional, representa riscos às liberdades e garantias individuais do cidadão. O avanço da tecnologia, por um lado, oportuniza racionalização de negócios e da própria atividade econômica: pode gerar empregabilidade, prosperidade e maior qualidade de vida. Por outro lado, se mal utilizada ou se utilizada sem um filtro prévio moral e ético, pode causar prejuízos incomensuráveis aos cidadãos e à própria sociedade, dando margem, inclusive, à concentração de mercados. Por isso, países de todo o planeta já visualizaram a*

---

[196] MONTEIRO, Renato Leite. **Lei Geral de Proteção de Dados do Brasil: análise contextual detalhada**: A LGPD terá um impacto na sociedade como poucas leis antes tiveram. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada-14072018. Acesso em: 26 fev. 2021.

[197] XIII CÚPULA IBERO-AMERICANADE CHEFES DE ESTADO E GOVERNO. **Declaraçao de Santa Cruz de La Sierra**. Santa Cruz de La Sierra, Disponível em: https://www.segib.org/wp-content/uploads/DECLARASAO-STA-CRUZ-SIERRA.pdf. Acesso em: 27 fev. 2021.

> *importância e imprescindibilidade de se regular juridicamente o tratamento de dados dos cidadãos*[198].

O trecho demonstra a necessidade de reconhecimento expresso da autonomia do direito fundamental à proteção de dados pessoais e se utiliza dos impactos ao direito à igualdade e da não discriminação, ligados principalmente à seara das oportunidades sociais na vida de um indivíduo, como no caso da empregabilidade. O tratamento irresponsável (e ilegal) de dados fomenta a criação de dossiês digitais relativos às pessoas e a consequência disso foi levantada no ponto 3.3.6.1 do presente trabalho, desde casos perfis de compradores por grandes redes de lojas até a utilização de dados sensíveis, a exemplo dos dados de convicção política, para promover um recorte social negativo.

O STF também seguiu essa linha e proferiu decisões importantes no ano de 2020 reconhecendo a existência do direito fundamental autônomo à proteção de dados pessoais no ordenamento jurídico brasileiro. No julgamento da ADI 6387[199] em face da Medida Provisória 954/2020, que dispõe sobre o compartilhamento de dados das empresas de telecomunicação com o IBGE para fins estatísticos, o STF suspendeu liminarmente a eficácia da medida tendo em vista a violação à autodeterminação informativa enquanto direito fundamental autônomo que se extrai da leitura da Constituição Federal de 1988[200].

Tal qual o caso alemão sobre a Lei do Censo que culminou na decisão histórica de 1983 reconhecedora do direito à autodeterminação informativa, mais uma vez debate-se a coleta de dados pelo Estado para fins estatísticos. Levanta, ainda, a tônica do livro 1984 de George Orwell, demonstrando a preocupação com uma possível vigilância estatal com desvio de finalidade, uma vez que, por mais que o contexto da pandemia de COVID-19 pareça justificar

---

[198] Documento completo da tramitação em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node01cc5haoypzfqe1qzawtptsjpri5125197.node0?codteor=1856527&filename=Avulso+-PEC+17/2019. Acesso em 02 mar. 2021

[199] BRASIL. **Proposta de Emenda à Constituição nº 17/2019**. Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Brasília: Senado Federal [2019]. Disponível em https://www25.senado.leg.br/web/atividade/materias/-/materia/135594 Acesso em 02 mar. 2021.

[200] BRASIL. Supremo Tribunal Federal (Plenário). **Ação Direta de Inconstitucionalidade nº 6387/DF.** Medida Cautelar em Ação Direta de Inconstitucionalidade. Referendo. Medida Provisória Nº 954/2020. Emergência de Saúde Pública de Importância Internacional Decorrente do Novo Coronavírus (Covid-19). Compartilhamento de Dados dos Usuários do Serviço Telefônico Fixo Comutado e do Serviço Móvel Pessoal, Pelas Empresas Prestadoras, Com O Instituto Brasileiro de Geografia e Estatística. Fumus Boni Juris. Periculum In Mora . Deferimento. Legitimado: Conselho Federal da Ordem dos Advogados do Brasil - CFOAB. Relator: Ministra Rosa Weber, 06 de maio de 2020. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165. Acesso em: 27 abr. 2021

a adoção de tais medidas, é possível que medidas como essas continuem sendo tomadas e que esses dados coletados sofram tratamento inadequado, sendo utilizados para finalidades diversas daquela inicialmente informada. Demonstra, portanto, a também íntima relação entre dados pessoais e democracia, regime tão caro e recente no país.

Isso representa uma evolução, visto que a jurisprudência da Corte era no sentido de não haver proteção constitucional aos dados em si, somente à comunicação deles, como no famoso RE 418.416-8/SC de relatoria do Min. Sepúlveda Pertence citado no ponto 4.3.1.

Por fim, cumpre destacar que o Ministro Gilmar Mendes, na página 109 do Acórdão, escreve um tópico para falar especificamente sobre a autonomia do direito fundamental à proteção de dados pessoais, destacando que essa compreensão advém de uma interpretação integrada do texto constitucional com base na dignidade da pessoa humana, na proteção à intimidade e suas reinterpretações diante dos novos riscos criados pelo avanço tecnológico e no reconhecimento do Habeas Data como instrumento de tutela material do direito fundamental à autodeterminação informativa.

CONCLUSÃO

Buscou-se, por meio dessa pesquisa e dentro dos limites que uma monografia impõe, estudar a existência do direito fundamental à proteção de dados pessoais no ordenamento jurídico brasileiro e, para tanto, iniciou-se pelo direito que deu origem a essa moderna concepção: o direito à privacidade. A formação e consolidação desse direito forneceu as bases para a compreensão do que hoje entende-se por proteção de dados pessoais e, ressalte-se, não se confundem entre si. Por mais que o surgimento deste tenha se dado no bojo da privacidade, os caminhos foram separados por diversas incompatibilidades geradas pela sociedade da informação, tendo como cerne sua característica de liberdade positiva, em contraposição à carga de liberdade negativa que a privacidade traz.

O mandamento de abstenção estatal do âmbito privado do indivíduo – entendido constitucionalmente no Brasil, em linhas gerais, como intimidade e vida privada (art. 5º, X, CF/88) e sigilo das comunicações (art. 5º, XII, CF/88) – que fundamenta a privacidade tem início com o *"right to be let alone"*, direito primeiramente compreendido como pertencente às elites em oposição à possibilidade de exposição não consentida de suas esferas privadas na mídia do século XIX. Aos poucos o perfil dos destinatários foi sendo mudado, já que a ascensão da burocracia e prestação de serviços públicos tornou-se uma política implementada pelo *Welfare State* durante o século XX, o que exigia a obtenção de uma grande quantidade de dados sobre a população para viabilizar medidas sociais.

Esse fator, aliado ao crescente desenvolvimento tecnológico que possibilitou a criação de bancos de dados automatizados, em contraposição aos bancos de dados físicos onde a informação ficava geograficamente localizada naquele endereço, fomentou o aumento do fluxo informacional e, com isso, o estopim para o surgimento da disciplina de proteção de dados. É nesse momento que ela se separa da privacidade, pois não se trata mais de protegê-los por meio de inviolabilidades e abstenções estatais e privadas, já que negar o acesso às suas informações significava ser excluído das políticas públicas e, consequentemente, da sociedade.

Atualmente permanece essa realidade, pois o objetivo da proteção de dados, diferentemente da privacidade, não é afastar proibir a utilização de dados, isolando-se na redoma da chamada esfera individual, mas, sim, permitir a circulação e tratamento de dados preservando-se o exercício de direitos fundamentais e, ao mesmo tempo, permitindo o

desenvolvimento econômico, tecnológico e a inovação. Aqui pontua-se a diferença crucial entre os referidos direitos: um remonta a uma liberdade negativa, de exigir abstenção externa diante de sua intimidade e vida privada, enquanto o outro afigura-se como liberdade positiva, conferindo ao seu titular a capacidade de autodeterminação, controle sobre os dados que se referem a ele, independentemente de serem privados, sendo suficiente que o dado seja sobre uma pessoa determinada ou determinável para que faça jus à proteção.

Nesse sentido, não configura pressuposto o dado ser privado, é uma classificação indiferente para que faça parte do escopo da proteção de dados pessoais, o que, por si só, já demonstra uma distinção determinante em relação à privacidade, pois nem é necessário considerar o pressuposto da esfera privada.

O coração desse trabalho se encontra na autonomia do direito à proteção de dados pessoais, cujo fundamento principal é a carga de liberdade positiva que possui. É em razão dessa característica que dados pessoais, por exemplo, sobre origem étnica ou sobre cor da pele, demandariam um grande malabarismo teórico para tentarem ser alocados numa possível esfera privada, até pelo fato de que podem traduzir características identificáveis a olho nu, porém carecem de proteção. O tratamento de dados é capaz de criar distorções de realidade que afetam diretamente a vida do indivíduo na sociedade, a exemplo dos dossiês digitais enquanto única forma de representação da pessoa, podendo carregar dados potencialmente lesivos e até mesmo determinando quais oportunidades sociais cada pessoa obterá.

A proteção de dados pessoais está, assim, diretamente ligada a liberdade, livre desenvolvimento da personalidade, igualdade material e a não discriminação, direitos que possibilitam a autodeterminação do indivíduo. Sua existência busca resguardar pessoas de situações como formação de listas negativas com base na nacionalidade em aeroportos, evitando que o simples fato de ser nacional de determinado país determine os locais onde pode estar; a circulação de listas sobre supostos autores de crimes, sem a devida comprovação da autoria em juízo, limitando suas escolhas de vida por terem seus nomes dispostos de forma lesiva e defesa em lei[201], muitas vezes por circulação de boatos; confecção das já citadas listas

[201] Sobre os perigos da perseguição por supostos criminosos, ver: CARPANEZ, Juliana. Veja o passo a passo da notícia falsa que acabou em tragédia em Guarujá. **Folha de São Paulo**. São Paulo, 27 set. 2018. Disponível em: https://www1.folha.uol.com.br/cotidiano/2018/09/veja-o-passo-a-passo-da-noticia-falsa-que-acabou-em-tragedia-em-guaruja.shtml. Acesso em: 26 abr. 2021. e MARTÍN, Maria. "Brasil tem um linchamento por dia, não é nada excepcional": Homem morto por vizinhos no Maranhão escancara a rotina da violência no Brasil. **El País**.

negativas de trabalhadores que já buscaram no Poder Judiciário a efetivação de seus direitos, cujos integrantes têm cerceados seu direito ao trabalho, já que a circulação dessas listas entre empregadores impede que sejam contratados. A saber, nenhum desses dados parece ter escopo no direito a privacidade, ou seja, nacionalidade, boatos sobre cometimento de crimes e ajuizamento de ações judiciais (em que os dados são, inclusive, públicos) dificilmente poderiam ser enquadradas na esfera individual e livre de intromissões.

Também por esses motivos é preciso abandonar um conceito "expansionista" de privacidade, que busca alargar seu significado para coletar os novos riscos surgidos pelo uso de dados pessoais. Além de operar perante pressupostos distintos (dicotomia público e privado), seus instrumentos (sigilos e inviolabilidades) não são suficientes para conter as novas ameaças a direitos fundamentais. Forçoso reconhecer, portanto, a insuficiência da privacidade diante de tais situações e, consequentemente, a autonomia do direito à proteção de dados.

De certo que as disposições constitucionais se atualizam conforme a realidade social, além dos direitos fundamentais já citados, é apontada uma releitura do Habeas Data enquanto principal instrumento constitucional em busca da efetivação do direito fundamental à proteção de dados pessoais, pois parece buscar concretizar os direitos de acesso e retificação de dados pessoais dispostos em bancos de dados de caráter público. Assim também entendeu Gilmar Mendes, afirmando que o reconhecimento do direito fundamental à autodeterminação informativa decorre de uma interpretação da Constituição que leva em consideração da cláusula geral da dignidade da pessoa humana, da atualização dos mandamentos de proteção à intimidade e a colocação do Habeas Data como principal instrumento desse direito.

Por fim, apesar de suscitar grande discussão doutrinária, a jurisprudência brasileira caminha nesse sentido, tendo sido reconhecida a fundamentalidade e autonomia do direito à proteção de dados pessoais pelo Supremo Tribunal Federal no bojo da ADI nº 6387/DF. As soluções legislativas seguem o mesmo passo, a exemplo da PEC Nº 17/2019, que busca inserir expressamente esse novo direito no rol do artigo 5º da Constituição Federal.

São Paulo, 08 jul. 2015. Disponível em: https://brasil.elpais.com/brasil/2015/07/09/politica/1436398636_252670.html. Acesso em: 26 abr. 2021.

Diante do exposto, a relevância impende que os indivíduos sejam melhor informados sobre dados pessoais, sendo uma intervenção necessária, que pode ser feita por meio de intervenções governamentais e campanhas publicitárias educacionais a fim de instruir os cidadãos acerca do valor e possíveis usos de dados, bem como urge esforço dos juristas brasileiros no que concerne à abrangência do direito no ambiente digital, principalmente quanto ao fato de que as categorias jurídicas até então utilizadas parecem insuficientes para tutelar as lesões provocadas pela circulação em massa de dados pessoais.

Conclui-se, com essa monografia, que o estudo da proteção de dados pessoais galga degraus da mais alta importância, não só no contexto atual como nos futuros, tendo em vista os diversos riscos que podem advir do tratamento dos dados. A legislação infraconstitucional, notadamente a Lei Geral de Proteção de Dados, demonstra a inevitável necessidade de regulação da matéria e representa um passo importante na seara da proteção de dados, assim como para a inserção do Brasil na lista de países que busca conferir um nível de proteção adequado. De certo que ainda enseja debate, a proteção de dados pessoais deve ser pauta frequente dos juristas brasileiros, eis que tutelar os direitos fundamentais, notadamente a dignidade da pessoa humana, a liberdade e a igualdade não é mera escolha legislativa, mas, sim efetivo mandamento constitucional e dever do Estado.

REFERÊNCIAS BIBLIOGRÁFICAS

AGÊNCIA DE DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA et al. **Manual da legislação europeia sobre proteção de dados**. [*S.l.*] Publications Office, 2014. *DOI.org (CSL JSON)*, https://data.europa.eu/doi/10.2811/73790. Disponível em: http://publications.europa.eu/resource/cellar/af9d0b3f-82be-11e5-b8b7-01aa75ed71a1.0017.03/DOC_2. Acesso em 01 de fev. de 2021.

AGÊNCIA DE DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA *et. al*. **Handbook on European Data Protection Law - 2018 edition**. [*S.l.*]: Publications Office Of The European Union, 2018. Disponível em: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf. Acesso em: 13 fev. 2021.

ANTONIALLI, Dennys. **Privacy and International Compliance: when differences become an issue**. In: Intelligent Information Privacy Management (AAAI Spring Symposium Series), 2010. Intelligent Information Privacy Management (AAAI Spring Symposium Series). Disponível em: https://www.aaai.org/ocs/index.php/SSS/SSS10/paper/viewFile/1165/1470. Acesso em 09 mar. 2021.

BIONI, Bruno. **Proteção de dados pessoais: as funções e os limites do consentimento**. Rio de Janeiro: Gen, 2019.

BRANCO, Paulo Gustavo Gonet; MENDES, Gilmar Ferreira. **Curso de direito constitucional**. 10. ed. São Paulo: Saraiva, 2016.

BRANDEIS, Louis; WARREN, Samuel. **The Right to Privacy**. Harvard Law Review, v. IV, dez. 1890, n. 5. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em 18 ago. 2020.

BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia**. Elaboração: Danilo Doneda. Brasília: SDE/DPDC, 2010.

BRASIL. **Lei nº 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 09 set. 2020.

BRASIL. Supremo Tribunal Federal (Plenário). **Ação Direta de Inconstitucionalidade nº 6387/DF.** Legitimado: Conselho Federal da Ordem dos Advogados do Brasil - CFOAB. Relator: Ministra Rosa Weber, 06 maio 2020. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165. Acesso em: 27 abr. 2021

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Agravo Regimental no Inquérito 3352/DF**. Agravante: Ministério Público Federal.: Agravado: Geraldo Resende Pereira. Relator: Ministro Marco Aurélio, 18 mar. 2017. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=4163787. Acesso em 02 mar. 2021.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário 1055914/SP**. Recorrente: Ministério Público Federal. Recorridos H.C.H; T.J.H. Relator: Dias Toffoli, 04 dez. 2019. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5213056. Acesso em 02 mar. 2021.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário 389.808/PR**. Recorrente: G.V.A. INDÚSTRIA E COMÉRCIO S/A. Recorrido: União. Relator: Ministro Marco Aurélio, 15 dez. 2010. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=622715. Acesso em 02 mar. 2021.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 4815**. Legitimado: Associação Nacional dos Editores de Livros - ANEL. Relator: Ministra Carmem Lúcia. Brasília, 01 fev. 2016. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=4271057. Acesso em: 24 abr. 2021.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 418.416/SC**. Recorrente: Luciano Hang. Recorrido: Ministério Público Federal. Relator: Ministro Sepúlveda Pertence. Brasília, DF, 10 maio 2006. Brasília, 19 dez. 2006. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=395790. Acesso em: 26 abr. 2021.

BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. **Agravo de Instrumento nº 00089142420188190000**. Relator: Desembargador João Batista Damasceno. Rio de Janeiro, RJ, 12 dez. 2018. Jusbrasil. Rio de Janeiro. Disponível em: https://tj-rj.jusbrasil.com.br/jurisprudencia/661800302/agravo-de-instrumento-ai-89142420188190000/inteiro-teor-661800312?ref=serp. Acesso em: 16 set. 2020.

CADASTRO nacional de "não me perturbe" para serviços de telecom já está disponível. **ANATEL.** Disponível em: https://www.anatel.gov.br/consumidor/noticias/930-cadastro-nacional-de-nao-me-perturbe-para-servicos-de-telecomunicacoes-esta-disponivel-a-partir-de-16-7. Acesso em 18 ago. 2020.

CARPANEZ, Juliana. Veja o passo a passo da notícia falsa que acabou em tragédia em Guarujá. **Folha de São Paulo**. São Paulo, 27 set. 2018. Disponível em: https://www1.folha.uol.com.br/cotidiano/2018/09/veja-o-passo-a-passo-da-noticia-falsa-que-acabou-em-tragedia-em-guaruja.shtml. Acesso em: 26 abr. 2021.

CASTELLS, Manuel. **A sociedade em rede**. 3. ed. São Paulo: Paz e Terra, 2000.

CHINA chega à fase final de sistema de avaliação de cidadãos e preocupa Ocidente. **RFI**, [*S.l.*], 02 jan. 2020. Disponível em: https://www.rfi.fr/br/mundo/20200102-em-2020-china-termina-de-testar-seu-sistema-de-cr%C3%A9ditos-sociais-e-assusta-ocidente. Acesso em: 16 set. 2020.

COMO o caso da assistente virtual da Amazon, chamada "Alexa", que protagonizou uma polêmica ao revelar que guarda todas os diálogos dos usuários. **Época Negócios**, [*S.l.*], 04 jul. 2019. Disponível em: https://epocanegocios.globo.com/Empresa/noticia/2019/07/amazon-confirma-que-guarda-todas-conversas-que-clientes-tem-com-alexa.html. Acesso em 16 set. 2020.

CONFERÊNCIA MUNDIAL SOBRE DIREITOS HUMANOS. **Declaração e Programa de Ação de Viena**. Viena, 1993. Disponível em: https://www.oas.org/dil/port/1993%20Declara%C3%A7%C3%A3o%20e%20Programa%20de%20Ac%C3%A7%C3%A3o%20adoptado%20pela%20Confer%C3%AAncia%20Mundial%20de%20Viena%20sobre%20Direitos%20Humanos%20em%20junho%20de%201993.pdf. Acesso em 24 abr. 2021.

CORRÊA, Rafael. Do direito de estar só à autodeterminação informativa: a evolução da disciplina legal da privacidade sob o enfoque dos direitos da personalidade e sua conformação como fundamento da tutela de dados pessoais. **Revista Eletrônica do Curso de Direito do Centro Universitário UniOpet**. Curitiba-PR. Ano XII, n. 21, jul-dez/2019. ISSN 2175-7119. Disponível em: https://www.academia.edu/42716947/Do_Direito_de_Estar_S%C3%B3_%C3%A0_Autodetermina%C3%A7%C3%A3o_Informativa_A_evolu%C3%A7%C3%A3o_da_disciplina_legal_da_privacidade_sob_o_enfoque_dos_direitos_da_personalidade_e_sua_conforma%C3%A7%C3%A3o_como_fundamento_da_tutela_de_dados_pessoais. Acesso em 08 mar. 2021.

DONEDA, Danilo; MENDES, Laura Schertel. **Data Protection in Brazil: New Developments and Current Challenges.** In: GUTWIRTH, Serge; LEENS, Ronald; DE HERT, Paul. Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges. Springer, 2014. *E-book*.

DONEDA, Danilo. **A proteção de dados pessoais como direito fundamental.** v. 12, n. 2. Joaçaba: Espaço Jurídico, 2011.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**, RENOVAR, 2006.

GARFINKEL, Simson. **Database nation**. Sebastopol: O'Reillly, 2000.

LYON, David. **Surveillance as social sorting**: privacy, risk, and digital discrimination. New York: Routledge, 2003.

MARR, Bernard. Chinese Social Credit Score: Utopian Big Data or Black Mirror on Steroids?. **FORBES**, [*S.l.*], 21 jan. 2019. Disponível em: https://www.forbes.com/sites/bernardmarr/2019/01/21/chinese-social-credit-score-utopian-big-data-bliss-or-black-mirror-on-steroids/#4e5df58248b8. Acesso em 16 set. 2019.

MARTÍN, Maria. "Brasil tem um linchamento por dia, não é nada excepcional": Homem morto por vizinhos no Maranhão escancara a rotina da violência no Brasil. **El País**. São Paulo, 08 jul. 2015. Disponível em: https://brasil.elpais.com/brasil/2015/07/09/politica/1436398636_252670.html. Acesso em: 26 abr. 2021.

MAYER-SCHÖNBERGER, Viktor. General development of data protection in Europe. *In*: AGRE, Phillip; ROTENBERG, Marc (orgs.). **Technology and privacy:** The new landscape. Cambridge: MIT Press, 1997.

MENDES, Laura Schertel. Habeas Data e Autodeterminação informativa: dois lados da mesma moeda. **Direitos Fundamentais & Justiça**, ano 12, n. 39, p. 185-216, jul./dez. 2018.

Disponível em: http://dfj.emnuvens.com.br/dfj/article/view/655/905. Acesso em 08 mar. 2021.

MENDES, Laura Schertel. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. **Revista de Direito do Consumidor**. vol. 106. ano 25. São Paulo: Ed. RT, jul./ago. 2016. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RDCons_n.106.02.PDF. Acesso em 16 set. 20.

MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor**. São Paulo: v. 79, jul/set, 2011.

MENDES, Laura Schertel. **Transparência e privacidade**: violação e proteção da informação pessoal na sociedade de consumo. Dissertação (Mestrado em Direito). Brasília: Universidade de Brasília, 2008.

MONTEIRO, Renato Leite. **Lei Geral de Proteção de Dados do Brasil: análise contextual detalhada**: A LGPD terá um impacto na sociedade como poucas leis antes tiveram. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada-14072018. Acesso em: 26 fev. 2021.

MORAES, Alexandre de. **Direito Constitucional**. 36. ed. p. 45. São Paulo: Atlas, 2020. *E-book*.

MORAES, Maria Celina Bodin de; TEFFÉ, Chiara. Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. **Revista Pensar**, v. 22, n. 1. Disponível em: https://periodicos.unifor.br/rpen/article/view/6272. Acesso em 17 set. 2020.

O plano chinês para monitorar – e premiar – o comportamento de seus cidadãos. **BBC**, [*S.l.*], 20 nov. 2017. Disponível em: https://www.bbc.com/portuguese/internacional-42033007. Acesso em: 16 set. 2020.

O que a revolução dos dados pode fazer por sua empresa?. **Exame**, [*S.l.*.], 29 out. 2013. Disponível em: https://exame.com/pme/a-revolucao-dos-dados/. Acesso em: 09 set. 2020.

PARLAMENTO EUROPEU. **Diretiva 95/46/CE**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex:31995L0046. Acesso em 24 ago. 2020.

REINO UNIDO. England And Whales High Court. **Prince Albert V Strange**. Disponível em: https://swarb.co.uk/prince-albert-v-strange-chd-8-feb-1849/. Acesso em: 18 ago. 2020.

RODOTÁ, Stefano. **A vida na sociedade de vigilância: a privacidade hoje**. A vida na sociedade de vigilância. Rio de Janeiro: Renovar, 2008.

ROTHENBURG, Walter Claudius. Direitos Fundamentais e suas características. **Revista dos Tribunais**: Cadernos de Direito Tributário e Finanças Públicas, [*S.l.*], n. 29, out./dez. 1999.

ROXIN, Claus, “Es la proteción de bienes jurídicos una finalidad del Derecho Penal?”. In: HEFENDEHL, Roland (ed.). **La teoría del bien jurídico – Fundamento de legitimación del Derecho penal o juego de abalorios dogmático?**. Madrid: Marcial Pons, 2007.

SCHWABE, Jürgen. **Cinqüenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Montevidéu: Fundación Konrad-Adenauer, 2005.

SERASA EXPERIAN. Soluções Cadastro Positivo. Disponível em: https://www.serasaexperian.com.br/solucoes-cadastro-positivo. Acesso em: 16 set. 2020.

SOLOVE, Daniel J. **The Digital Person**. New York: NYU PRESS, 2004.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32000X1218(01)&qid=1617650366391&from=EN. Acesso em 05 mar. 2021.

UNIÃO EUROPEIA. **Diretiva 95/46 do Parlamento Europeu e do Conselho**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT. Acesso em 14 fev. 2021.
VIEIRA, Tatiana Malta. **O Direito à Privacidade na Sociedade da Informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Dissertação (Mestrado em Direito) Brasília: Universidade de Brasília, 2007.

PARLAMENTO EUROPEU**. REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Acesso em 24 ago. 2020.

WACHTER, Sandra. Normative Challenges of Identification in the Internet of Things: privacy, profiling, discrimination, and the gdpr. **Ssrn Electronic Journal**, [*S.l.*], 2017. Elsevier BV. http://dx.doi.org/10.2139/ssrn.3083554. Disponível em: https://www.researchgate.net/publication/321959135_Normative_Challenges_of_Identification_in_the_Internet_of_Things_Privacy_Profiling_Discrimination_and_the_GDPR. Acesso em: 16 set. 2020.

WESTIN, Alan. **Privacy and freedom**. New York: Ig Publishing, 2015. *E-book.*

WILDE, Oscar. **De Profundis**. Projetos de filosofia. Phoenix-Library, 2001. *E-book.* Disponível em: http://www.dominiopublico.gov.br/pesquisa/DetalheObraForm.do?select_action=&co_obra=3556. Acesso em 20 de ago. 2020.

XIII CÚPULA IBERO-AMERICANADE CHEFES DE ESTADO E GOVERNO. **Declaraçao de Santa Cruz de La Sierra**. Santa Cruz de La Sierra, Disponível em: https://www.segib.org/wp-content/uploads/DECLARASAO-STA-CRUZ-SIERRA.pdf. Acesso em: 27 fev. 2021.