MILTON HENRIQUE FREITAS MOREIRA

LEI Nº 13.709/2018 E A PROTEÇÃO DE DADOS PESSOAIS NO ÂMBITO DO E-COMMERCE

UNIVERSIDADE FEDERAL DE UBERLÂNDIA

FACULDADE DE DIREITO

UBERLÂNDIA - MG

2022

LEI Nº 13.709/2018 E A PROTEÇÃO DE DADOS PESSOAIS NO ÂMBITO DO *E-COMMERCE*

Projeto de Trabalho de Conclusão de Curso apresentado à Faculdade de Direito da Universidade Federal de Uberlândia.

Orientador: Prof. Dr. Almir Garcia Fernandes

UBERLÂNDIA - MG

2022

LEI Nº 13.709/2018 E A PROTEÇÃO DE DADOS PESSOAIS NO ÂMBITO DO E-COMMERCE

Trabalho de conclusão de curso orientado pelo Prof. Dr. Almir Garcia Fernandes, apresentado à Faculdade de Direito da Universidade Federal de Uberlândia, como requisito para obtenção do grau de bacharel em Direito, aprovado pela banca examinadora formada por:

Uberlândia, 21 de março de 2022.

_____

Prof. Dr. Almir Garcia Fernandes

Orientador - UFU

_____

Prof.ª Dra. Keila Pacheco Ferreira

Examinadora Interna – UFU

AGRADECIMENTO

Agradeço à minha mãe, Maria Patrícia, pelo apoio incondicional, e por sempre ter me oferecido suporte material e emocional para que eu buscasse meus objetivos.

Agradeço também a todos os professores da minha graduação em Direito, por transmitirem conhecimento com maestria.

Registro aqui um agradecimento especial ao Prof. Dr. Almir Garcia Fernandes, orientador deste Trabalho de Conclusão de Curso. Sua paciência, sabedoria e receptividade foram essenciais para o desenvolvimento desta produção acadêmica.

RESUMO

As repercussões criadas pela lei nº 13.709/2018 (LGPD) no comércio eletrônico, principalmente no que se refere ao tratamento de dados pessoais, exigem um profundo estudo acerca do tema pelos estudantes e operadores do Direito. A Lei Geral de Proteção de Dados pode ser compreendida como diploma normativo que procura regulamentar a proteção de dados pessoais no Brasil, e possui o objetivo de conciliar o progresso econômico-científico com as garantias fundamentais de liberdade e privacidade da pessoa natural. Por sua vez, o *e-commerce* pode ser definido como ramo da atividade comercial em que as transações acontecem por meio de equipamentos eletrônicos e que se utiliza dos dados pessoais de consumidores para criar sua estratégia de crescimento. Nesse sentido, o presente trabalho de conclusão de curso teve como objetivo demonstrar que a Lei nº 13.709/2018 representou uma mudança de paradigma no que diz respeito à proteção de dados no âmbito do comércio eletrônico, bem como ressaltar a importância de um tratamento de dados que respeite a privacidade e a liberdade do titular durante as transações comerciais que ocorrem em meio virtual. Para tanto, foi utilizado como método de pesquisa o indutivo e dedutivo, por meio de estudo dogmático-jurídico e histórico. Nessa orientação, buscou, de início, discorrer sobre as origens históricas do direito à privacidade e seu local na contemporaneidade. Em seguida, tratou acerca da proteção de dados pessoais como aspecto do direito à privacidade e o papel do consentimento do titular. Por fim, procurou abordar sobre o comércio eletrônico como marca da sociedade informacional diante da Lei nº 13.709/2018, a fim de que sejam encontrados caminhos que harmonizem o desenvolvimento econômico proporcionado pelo *e-commerce* e o justo tratamento dos dados pessoais dos titulares, conforme os ditames legais e constitucionais.

Palavras-chave: Privacidade; LGPD; dados pessoais; consentimento; comércio eletrônico.

ABSTRACT

The impact of the General Data Protection Law (LGPD) on electronic commerce, especially regarding the personal data processing, require a deep study on the subject by law students and professionals. The General Data Protection Law is a piece of legislation that seeks to regulate personal data protection in Brazil and its objective is to reconcile economic and scientific progress and the fundamental rights of freedom and privacy. In turn, e-commerce can be defined as a branch of commercial activity in which transactions take place through electronic equipment and which uses the personal data of consumers to create its growth strategy. In this sense, the present undergraduate thesis aimed to demonstrate that General Data Protection Law represented a paradigm shift in e-commerce's data protection, as well to highlight the significance of privacy and freedom towards the data subject in the context of commercial transactions that take place in a virtual environment. Therefore, this thesis used the inductive and deductive research method, through legal and historical study. In this sense, it sought, at first, to discuss the historical origins of the right to privacy and its place in contemporaneity. Then, it dealt with the personal data protection as an aspect of the right to privacy and the role of the data subject's consent. Finally, it sought to address electronic commerce as a symbol of the informational society in the face of the General Data Protection Law, in order to find ways to harmonize the economic development provided by e-commerce and the fair treatment of the subject's personal data, in accordance with legal and constitutional standards.

Key words: Privacy; LGPD; personal data; consent; e-commerce.

SUMÁRIO

INTRODUÇÃO

Vislumbrado primeiramente como garantia essencialmente individual, o direito à privacidade, em meados do século XIX, estava relacionado ao liberalismo clássico, e era concebido como direito a ser deixado só. No entanto, essa perspectiva atrelada ao isolamento e à tranquilidade tomou novos rumos com o advento de uma sociedade informacional, em que o fluxo de dados, auxiliado pelo desenvolvimento tecnológico, foi intensificado de maneira exponencial. Diante disso, surge uma preocupação não apenas com o que se denomina *zero relationship*, mas com o desenvolvimento da pessoa humana, em que se discute a criação de um ambiente de coexistência entre as novas tecnologias e o respeito aos direitos fundamentais (DONEDA, 2019).

Em face dessa perspectiva, mister se faz a edição de normas que dispõem sobre dados pessoais e seus respectivos tratamentos de forma condizente com o próprio projeto social previsto na Constituição Federal de 1988. Nesse sentido, foi sancionada, no dia 14 de agosto de 2018 a lei nº 13.709, mais conhecida como Lei Geral de Proteção de Dados (LGPD), que busca, essencialmente, manter um equilíbrio entre o desenvolvimento de negócios da economia digital e a proteção da privacidade como direito fundamental do indivíduo (PINHEIRO, 2020, p. 233). A referida norma dispõe sobre as etapas do tratamento de dados, agentes de tratamento, regras de governança de dados, sanções administrativas em caso de descumprimento dos dispositivos da lei, entre outros assuntos. Ainda traz, conceitos que ajudam na interpretação das normas que compõem a própria LGPD, como por exemplo, definições de banco de dados, anonimização, consentimento, finalidade e adequação.

A Lei nº 13.709/2018, que entrou em vigor no dia 18 de setembro de 2020, representa uma profunda transformação no tocante à proteção de dados pessoais no Brasil. A partir do referido diploma, o procedimento de tratamento de informações deverá respeitar a liberdade e privacidade do titular, bem como estar adstrito à finalidade proposta. Nesse sentido, ensina Patrícia Peck Pinheiro:

> [...] a legislação visa fortalecer a proteção da privacidade do titular dos dados, a liberdade de expressão, de informação, de opinião e de comunicação, a inviolabilidade da intimidade, da honra e da imagem e o desenvolvimento econômico e tecnológico. (PINHEIRO, 2020, p. 33)

Por seu turno, o *e-commerce* pode ser definido como ramo da atividade comercial em que as transações acontecem por meio de equipamentos eletrônicos como computadores,

smartphones, *notebooks*, *tablets*, entre outros. Esa matriz empresarial, mais comumente representada pelas inúmeras lojas *online* espalhadas pela internet, se aliou ao desenvolvimento da internet para criar um modelo de negócios inovador e promissor. Em que pese se encontrar em constante evolução, diante do progresso avassalador das ferramentas tecnológicas, o comércio eletrônico, em qualquer de suas variações, se estrutura em torno dos dados pessoais de seus consumidores para criar sua estratégia de crescimento.

Assim, em face do intenso fluxo de informações proveniente decorrente de transações comerciais feitas pela Internet, os dados pessoais, coletados por instrumentos eletrônicos, se mostram como um dos principais ativos financeiros dessas empresas, e merecem atenção especial no que se refere à garantia de um tratamento justo e conforme os ditames constitucionais referentes à privacidade e liberdade do titular dos dados.

Conforme estudo da *WorldPay from FIS*, de 2021, o volume de transações no comércio eletrônico brasileiro cresceu mais de 22% em 2020. De acordo com o mesmo relatório, há uma estimativa de que a receita do comércio eletrônico cresça em até 50% (cinquenta por cento) até 2024, alcançando a marca de U$ 56 bilhões, em comparação com a arrecadação de U$ 36 bilhões em 2020 (WORLDPAY FOR FIS, 2021).

Dessa forma, considerando o vultoso crescimento do comércio eletrônico (*e-commerce)* no Brasil, principalmente durante o período de distanciamento social causado pela pandemia de COVID-19, é indiscutível que os dados dos consumidores durante as transações virtuais estarão sob o escrutínio das empresas de comércio digital e, por conseguinte, inseridas no âmbito protetivo regulado pela LGPD.

Portanto, buscou-se reunir informações com o intuito de responder às seguintes indagações: Quais as origens históricas do direito à privacidade? Como a percepção de privacidade evoluiu para o que se denomina proteção de dados pessoais? Qual o papel do consentimento informado na garantia de um tratamento de dados justo e que respeitas as garantias fundamentais do titular no contexto da sociedade informacional? Como a privacidade é tutelada no ordenamento jurídico brasileiro? Quais as mudanças significativas que a lei nº 13.709/2018 trouxe em relação ao comércio eletrônico?

O objetivo do presente trabalho de conclusão de curso é, portanto, demonstrar que a lei nº 13.709/2018, conhecida com LGPD, representou, no contexto brasileiro, uma mudança de paradigma no que diz respeito à proteção de dados no âmbito do comércio eletrônico, bem como ressaltar a importância de um tratamento de dados que respeite a privacidade e a liberdade do titular durante as transações comerciais que ocorrem em meio virtual. Nesse sentido, também é

imprescindível apontar disposições específicas da lei nº 13.709/2018 que repercutem na seara do comércio eletrônico; destacar a importância da lei nº 13.709/2018 como diploma que passou a dar proteção efetiva à algumas garantias fundamentais previstas na Constituição Federal de 1988; apresentar o desenvolvimento histórico da concepção de privacidade; e sugerir meios de adequação do e-commerce à lei nº 13.709/2018.

A realização do presente estudo se justifica tendo em vista a pertinência do tema de proteção de dados no cenário atual. O desenvolvimento cada vez mais robusto da economia digital, propiciado pelo intenso fluxo de dados, principalmente pessoais, suscitou o surgimento de diversas legislações que abordassem acerca da salvaguarda da privacidade, no sentido de estabelecer limites e regramentos no que se refere ao *free data flow*.

Diante disso, é indiscutível a importância do estudo referente à proteção à privacidade, considerado como direito humano e garantia fundamental constitucionalmente prevista. Na atualidade, em face do intenso fluxo de dados, propiciado pelo advento da tecnologia e característico de uma sociedade informacional, a preocupação com a intimidade torna-se cada vez mais flagrante.

É nessa esteira que, no sentido de dar efetividade ao projeto social constitucionalmente previsto na Carta de 1988 e nos documentos internacionais alusivos à temática, sancionou-se a lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados. Assim, percebe-se que o referido diploma traz uma série de disposições referentes à conceitos técnicos como banco de dados e anonimização, bem como concernentes à criação de uma autoridade reguladora de proteção de dados e à uma serie de sanções administrativas em caso de descumprimento das normas e regulações atinentes ao assunto.

Posto isso, vale ressaltar como a proteção de dados está inserida na contemporaneidade. Em que pese se tratar sobre a proteção de dados pessoais em todas as esferas, é no âmbito digital que a lei 13.709/2018 terá sua aplicação mais evidenciada. Isso porque o uso da internet, bem como de instrumentos tecnológicos como smartphones e aplicativos, revolucionaram o fluxo de informações e, principalmente, de dados pessoais. Estes, movimentados de forma muito mais intensa em relação a um modelo anterior não informatizado, requerem uma proteção rígida e em respeito à liberdade e privacidade do titular.

Por esse motivo é que se discute a aplicação da lei 13.709/2018 no *e-commerce*. O surgimento de inúmeros estabelecimentos virtuais, de forma ainda mais intensa em um período de distanciamento social ocasionado pela pandemia do novo coronavírus (COVID-19), os dados

dos consumidores estão cada vez mais expostos nos bancos de dados de fornecedores e vulneráveis à diversos interesses, tantos legítimos quanto desarrazoados.

Para o desenvolvimento do presente trabalho, será utilizado como método de pesquisa o indutivo, a saber, aquele destinado a verificar constatações particulares e, possibilitar, que se produzam generalizações sobre o tema, além do método dedutivo, na tentativa de se fazer das regras gerais, a solução para casos específicos. Os processos metodológicos a serem utilizados serão o estudo dogmático jurídico, visto a impossibilidade de um estudo profundo sem que se recorra à lei, à doutrina ou à jurisprudência neste sentido; e o histórico, que "consiste na investigação dos acontecimentos, processos e instituições do passado, para verificar a sua influência na sociedade de hoje" (ANDRADE, 1995, p.23).

O presente trabalho de conclusão de curso estrutura-se em 5 (cinco) capítulos. No primeiro capítulo, abordará as origens históricas do direito à privacidade e seu local na contemporaneidade. No segundo capítulo, discorrerá sobre o conceito de privacidade a partir da identificação de seus problemas. No terceiro capítulo, tratará sobre o direito à privacidade sob a ótica da proteção de dados pessoais e os limites do consentimento. No quatro capítulo discutirá especificamente sobre a Lei nº 13.709/2018 e suas disposições concernentes à proteção de dados. Por fim, o quinto capítulo abordará o *e-commerce* enquanto marca da sociedade informacional e os impactos da LGPD, bem como apresentará algumas adaptações necessárias no âmbito comércio eletrônico em face da entrada em vigor da lei 13.709/2018.

I. ORIGENS HISTÓRICAS DO DIREITO À PRIVACIDADE E SEU LOCAL NA CONTEMPORANEIDADE

Compreender as origens históricas do direito à privacidade é essencial para entender seu papel na sociedade atual. É possível afirmar que a privacidade nasce concomitantemente com o surgimento e desenvolvimento da esfera privada do ser humano, e tem raízes culturais influenciadas por fatores políticos, econômicos e sociais. Nesse sentido, afirma Danilo Doneda:

> (...) nos atemos portanto à ideia de que a privacidade é uma noção cultural induzida no curso do tempo por condicionantes sociais, políticos e econômicos, pelo que justifica proceder no plano histórico para sua contextualização jurídica. Para levar bom termo essa tarefa cabe traçar um esboço da formação da *esfera privada* do ser humano – de bases sociais, culturais e políticas; dessa forma, enfileiramo-nos com uma tradição que reconhece que "sem a suas bases não positivas, não se pode compreender o direito positivo. (DONEDA, 2019, loc. 1567)

Muitos fenômenos vinculados à esfera privada do ser humano, apesar de não serem tratados sob a ótica da privacidade, já eram abordados por estruturas políticas e sociais, e não necessariamente por um sistema jurídico. Dessa forma, é possível verificar referências à privacidade em várias sociedades antigas, ainda que de forma diferente da dinâmica atual reservada ao tema. Nesse sentido, Danilo Doneda discorre:

> Na filosofia antiga, podemos encontrar várias menções a situações relacionadas à privacidade: a solidão, o retiro, a interiorização, e outras – Sêneca, por exemplo, considerava a amizade e a fidelidade entre os mais altos sentimentos humanos, e a intimidade e o retiro eram os instrumentos necessários apara alcançá-las. (DONEDA, 2019, loc. 1645)

Nesse contexto, a compreensão do valor conferido à privacidade é essencial para a identificação de sua posição dentro de uma determinada sociedade. A filosofia grega e romana antigas, por exemplo, contemplavam "a personalidade jurídica do homem dentro dos limites e termos que provinham de sua própria organização política (DONEDA, 2019). Prudente, portanto, traçar distinções entre a noção de privacidade nessas sociedades, que se dava pela liberdade empreendida na esfera pública, com a percepção atual caracterizada pela existência de direitos individuais. Assim, feitas as devidas considerações referentes às peculiaridades de cada organização social, é necessário ressaltar a importância de analisar a posição da privacidade em diferentes comunidades:

> Levar em conta a natureza e o valor conferido à esfera privada em determinadas sociedades, de todo modo, é indispensável para realizara a valoração de sua configuração atual. A ela corresponderam funções diversas em gênero e amplitude, funções que hoje devem ser conhecidas para adequá-las ou não ao nosso momento. (DONEDA, 2019, loc. 1649)

Durante a Idade Média, ainda restava ausente uma concepção de privacidade semelhante à difundida atualmente. Alguns senhores feudais, no entanto, começaram a desenvolver uma esfera privada baseada no sentimento de intimidade, relacionada à habitação privada. Essa dimensão, no entanto, não consegue se enquadrar nos moldes atuais conferidos à privacidade, pois diz respeito apenas às estruturas hierárquicas presentes na Idade Média e não atribuem qualquer valor à privacidade. (DONEDA, 2019)

Com efeito, a privacidade, em sua acepção atual, é fruto da disseminação do individualismo nas relações sociais e da consolidação da burguesia diante da criação dos estados nacionais em contraposição ao absolutismo. Nesse sentido:

> A bem da verdade, qualquer noção de privacidade deve fundar-se em uma percepção da relação do indivíduo com a sociedade, e a gênese de sua atual concepção evoca duas causas principais: a emergência do estado-nação, da sociedade civil e das teorias de sua soberania nos séculos XVI e XVII, que formaram a noção moderna do ente público; e também o estabelecimento de uma esfera privada livre de ingerências desse ente público, como reação ao absolutismo, tendências aceleradas pelo fim da sociedade feudal e, posteriormente, pela Revolução Industrial.
> A privacidade passa a ser prerrogativa de uma emergente classe burguesa que, com seu forte componente individualista, dela se utiliza para marcar sua identidade na sociedade e também para que o solitário burguês se isole dentro de sua própria classe. (DONEDA, 2019, loc. 1726).

Dessa forma, considerando a influência dos ideais liberais na formação e fortalecimento da classe burguesa, a moderna concepção de privacidade é intimamente relacionada à proteção da propriedade privada. Segundo Doneda (2019), a propriedade era admitida como condição para o desenvolvimento da pessoa humana e, por conseguinte, o direito à propriedade era pressuposto para o estabelecimento da privacidade.

Além da difusão da concepção individualista, que marcou a transição feudo-capitalista, a disponibilidade de meios materiais também foram cruciais para o surgimento da noção moderna de privacidade. O desenvolvimento da tecnologia permitiu uma clara "delimitação de espaços entre os ocupantes de uma mesma casa" (DONEDA, 2019, loc. 1672), por meio do aperfeiçoamento da infraestrutura doméstica. Ao mesmo tempo, visualizava-se a massificação

dos meios de comunicação, que alteraram a expectativa de privacidade e exigiam a criação de ferramentas que atenuassem a intrusão na vida privada do indivíduo.

Nesse contexto, diante dos impactos causados pela Revolução Industrial no século XIX, a ideia de privacidade é aperfeiçoada, e passa a ser compreendida como forma de "resistência do homem frente à tendência de massificação da sociedade industrial" (BALDASSARE, 1974, apud DONEDA, 2019, loc. 1741). Samuel D. Warren, um advogado de Boston, Massachussetts, irritado com a frequente invasão da imprensa em sua vida privada, decide redigir, em conjunto com seu colega Louis D. Brandeis, o ilustre artigo *The Right to Privacy*, um dos textos mais importantes na literatura da privacidade, e que, segundo Doneda (2019), moldou a moderna doutrina em relação ao tema. Os dois juristas discutiam, portanto, o "desenvolvimento de novas tecnologias que representavam uma ameaça potencial à privacidade". (SOLOVE, 2009, loc. 191, tradução nossa)[1]. Ademais, argumentavam que:

> Invenções recentes e métodos de negócios chamam a atenção para o próximo passo que deve ser dado para a proteção da pessoa e para garantir ao indivíduo o que o juiz Cooley chama de "o direito de ser deixado em paz". Fotografias instantâneas e empreendimentos jornalísticos invadiram os recintos sagrados da vida privada e doméstica; e numerosos dispositivos mecânicos ameaçam cumprir a previsão de que "o que é sussurrado no armário será proclamado dos telhados.[2] (BRANDEIS; WARREN, 1890, página 6, tradução nossa).

Uma das principais inovações veiculadas pelo artigo *The Right to Privacy* foi a fundamentação da proteção privacidade desassociada da proteção da propriedade. Segundo Doneda (2019), o princípio a ser observado quando se pretende proteger a privacidade é a *inviolate personality*, ou seja, um direito de natureza eminentemente pessoal. Em que pese a necessidade de tecer ponderações acerca das diferenças entre a noção de privacidade nos sistemas de *common law* e do *civil law*, é possível, afirmar que o artigo de Warren e Brandeis marcou o "início do moderno debate sobre a privacidade. (DONEDA, 2019)

Atualmente, segundo Doneda (2019), a discussão em torno da privacidade está intimamente ligada ao processamento de dados em massa. Um exemplo disso é o *Fair Credit Reporting Act*, de 1970, legislação americana que buscou regular os bancos de dados de

[1] No original: "Warren and Brandeis began by describing new technological developments that were posing a potential threat to privacy".

[2] No original: "Recent inventions and business methods call attention to next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls "the right to be let alone". Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanic devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops".

consumidores no tocante à proteção de crédito. Dessa forma, a proteção da esfera privada se desprende da ideia vinculada à comodidade individual, em que o cidadão poderia simplesmente renunciá-la, para se tornar um verdadeiro pressuposto para o desenvolvimento da personalidade humana, livre do controle social que poderia, em tese, suprimir sua individualidade. Nesse sentido:

> A privacidade assume, portanto, posição de destaque na proteção da pessoa humana, não somente tomada como escudo contra o exterior – na lógica da exclusão – mas como elemento indutor da autonomia, da cidadania, da própria atividade política em sentido amplo e dos direitos de liberdade de uma forma geral. Nesse papel, ela é pressuposto de uma sociedade democrática moderna, da qual o dissenso e o anticonformismo são componentes orgânicos. (DONEDA, 2019, loc. 1858)

Essa mudança de paradigma, que buscou não limitar a proteção da privacidade à formulação *the right to be let alone*, presente no artigo de Warren e Brandeis e que prevê a privacidade como "espécie de imunidade ou isolamento"[3] (SOLOVE, 2008), é característica de um período histórico marcado, segundo Doneda (2019), pelos movimentos sociais e pelo intenso fluxo de informações, propiciado pelo desenvolvimento da tecnologia. Por conseguinte, facilitou-se a coleta e processamento de dados dos indivíduos em geral, e não apenas de personalidades de grande relevo social, a que a privacidade se prestava a proteger anteriormente, sob uma perspectiva abalizadamente individualista.

Segundo Doneda (2019), a vantagem técnica que propiciou a utilização de informações pessoais em larga escala foi exercida primeiramente pelo Estado. Um exemplo disso foi a realização de diversos censos e pesquisas que tinham como objetivo a coleta de informação dos indivíduos para a concretização do princípio da eficiência da administração pública.

Por outro lado, na esfera privada, a utilização de dados era escassa. Segundo Doneda (2019), isso se deu em razão dos altos custos no tratamento de dados. No entanto, o progresso da informática permitiu a redução de despesas com a coleta e processamento de dados, bem como tornou a utilização de informações pessoais ainda mais profícua.

O aumento de operações associadas ao tratamento de dados pessoais foi, obviamente, acompanhado por uma série de problemas relacionados à privacidade. De início, segundo Doneda (2019), foram veiculadas diversas previsões exageradas e sensacionalistas, que anunciavam "o fim da privacidade". Em reação a esse fenômeno, muitos estudiosos procuraram

[3] No original: "The right to be let alone views privacy as a type of immunity or seclusion".

desenvolver a teoria da *privacy excepcionality*, que consistia em um "excesso de atenção à tutela da *privacy* em detrimento de outros bens comuns igualmente dignos de proteção" (DONEDA, 2019).

A tutela de privacidade, no entanto, deve ser abordada de forma pragmática. Doneda (2019) afirma que, em face da impossibilidade de dissociar a tecnologia da estrutura social atual, é necessário formular um ambiente de coexistência entre essas novas tecnologias e os direitos fundamentais. Solove (2008) também enfatiza a ideia de equilíbrio no tocante à matéria da privacidade, e afirma que a sua proteção não é soberana em relação ao demais interesses que a disputam, e tampouco é uniforme, pois cada sociedade atribui um valor diferente à privacidade e aos seus os interesses contrapostos.

Feitas essas considerações, é possível compreender a posição da privacidade na sociedade atual, que, segundo Doneda (2019), é marcada pelo intenso fluxo de informações pessoais e pelo desenvolvimento tecnologia, e não pode mais ser compreendida simplesmente como prerrogativa de isolamento e reclusão.

II. O CONCEITO DE PRIVACIDADE

1. A importância da privacidade

Louis Brandeis, juiz da Suprema Corte dos Estados Unidos, afirmou que a privacidade é "o mais abrangente dos direitos e o direito mais valorizado pelo homem civilizado". (BRANDEIS, 1928, apud SOLOVE, 2008, loc. 36)[4]. Conforme ensina Solove (2008), a privacidade é um assunto vital para a democracia e a liberdade**.** Nesse sentido**,** Assim dispõe o art. 12 da Declaração Universal de Direitos Humanos:

> **Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação.** Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques. (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1948, grifo nosso)

Nesse sentido, também estabelece o art. 17 do Pacto Internacional dos Direitos Civis e Políticos:

> 1. **Ninguém poderá ser objetivo de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais às suas honra e reputação**.
> 2. Toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas. (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1966, grifo nosso)

Por fim, cumpre ressaltar os ditames presentes no art. 5º, X, XI, XII e LXXII da Constituição Federal de 1988:

> Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> X - são invioláveis a **intimidade, a vida privada, a honra e a imagem das pessoas**, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> XI - **a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador**, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;
> XII - **é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas**, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;
> LXXII - conceder-se-á habeas data:

[4] No original: "the most comprehensive of rights and right most valued by civilized man".

> a) para **assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados** de entidades governamentais ou de caráter público;
> b) **para a retificação de dados,** quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo. (BRASIL, 1988, grifo nosso)

Diante disso, é indiscutível a importância do estudo referente à proteção à privacidade, considerado como direito humano e garantia fundamental constitucionalmente prevista. Na atualidade, em face do intenso fluxo de dados, propiciado pelo advento da tecnologia e característico de uma sociedade informacional, a preocupação com a intimidade torna-se cada vez mais flagrante.

No entanto, juristas encontram uma enorme dificuldade em definir o que seria privacidade. Segundo Miller (1972 apud SOLOVE, 2008), se trata de um conceito demasiadamente vago e instável. A dificuldade de conceituar o direito à privacidade e delimitar a sua importância pode, inclusive, tornar a legislação sobre a matéria inoperante. A definição sobre os contornos da privacidade é, portanto, fundamental.

Conquanto o debate sobre a privacidade pode ser observado em diversas sociedades ao longo da história, é inegável que o desenvolvimento da tecnologia fez com que a privacidade se tornasse um assunto de grande visibilidade. Nesse contexto, Bettellheim (1968 apud SOLOVE, 2008), afirmou que "em todos os lugares que se olha hoje em dia parece que o direito à privacidade está constantemente sob ataque".[5]

2. Teorias da Privacidade

Solove (2008) preleciona que o conceito de privacidade, atualmente, engloba a liberdade de pensamento, controle sobre o próprio e corpo e sobre dados pessoais, isolamento, proteção contra vigilância, proteção da reputação, entre outros. No entanto, com objetivo de elaborar um conceito sobre privacidade, muitos estudiosos buscam eleger aspectos essenciais a cada uma das áreas anteriormente mencionadas, e acabam desenvolvendo teoria muitas vagas ou limitadas. Segundo Solove (2008): "O problema mais prevalente com as concepções é que elas são muito limitadas porque não incluem os aspectos da vida que normalmente vemos como particulares ou muito amplas porque não excluem assuntos que não consideramos privados".[6]

[5] No original: "everywhere one turns these days it seems that the right to privacy is constantly under assault"
[6] No original: "The most prevalent problem with the conceptions is that they are either too narrow because they fail to include the aspects of life we typically view as private or too broad because they fail to exclude matters we do not deem private".

Solove (2008), então, aborda 6 (seis) teorias que considera as mais importantes no tocante ao conceito de privacidade: a formulação do "direito de ser deixado em paz"; a proteção contra acessos indesejados; a ocultação de certas informações; o controle sobre os dados pessoais; a proteção da personalidade, individualidade e dignidade do sujeito; e a proteção da intimidade.

2.1. O direito de ser deixado em paz

Warren e Brandeis (1890), em seu influente artigo *The Right to Privacy*, sustentaram que o direito à privacidade deveria ser definido como o "direito de ser deixado em paz"[7]. Segundo Solove (2008), o artigo, considerado uma das mais importantes contribuições para a legislação sobre privacidade nos Estados Unidos, estava inserido em um contexto marcado pelo desenvolvimento de novas tecnologias. A criação de aparelhos que permitiam tirar fotos instantâneas e o comportamento sensacionalista da imprensa ameaçavam o direito à privacidade. Nesse sentido:

> "A intensidade e a complexidade da vida, decorrentes do avanço da civilização, tornaram necessário algum afastamento do mundo, e o homem, sob a influência refinadora da cultura, tornou-se mais sensível à publicidade, de modo que a solidão e a privacidade se tornaram mais essenciais ao indivíduo; mas as invenções e empreendimentos modernos, por meio de invasões de privacidade, o submeteram a dores e sofrimentos mentais muito maiores do que poderiam ser infligidos por mera lesão corporal".[8] (BRANDEIS; WARREN, 1890, p. 6, tradução nossa)

Warren e Brandeis (1890) desenvolvem, em seu artigo, um conceito de privacidade dissociado da ideia de proteção da propriedade. Segundo os autores, o princípio que fundamenta o direito à privacidade não é o da propriedade privada, mas sim o da "personalidade inviolável"[9], que não se relaciona com o direito de aferir lucro oriundo da publicação de produções pessoais, mas impedem a publicação dessas criações. Dessa forma, conforme preleciona Solove (2008), o direito à privacidade, nessa perspectiva, é concebido como uma espécie de imunidade ou reclusão.

[7] No original: "The right to be let alone".
[8] No original: "The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions of privacy subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury".
[9] No original: "Inviolate personality".

No entanto, muitos teóricos sustentam que a definição da privacidade como o "direito de ser deixado em paz" é muito ampla, e abrange aspectos que não são considerados particulares. Sob essa perspectiva, qualquer conduta ofensiva dirigida a alguém seria concebida como violação da privacidade, o que torna essa conceituação demasiadamente vaga. (ALLEN, 1988 apud SOLOVE, 2008)

2.2. Teoria do Acesso Limitado ao Indivíduo

Outra teoria a ser abordada é a do acesso limitado ao indivíduo. De acordo com essa conceituação, a privacidade pode ser definida como a preferência exercida pelo indivíduo sobre quais informações pessoais devem ser compartilhadas. Dessa forma: privacidade constituiria o "direito de decidir quanto conhecimento dos pensamentos e sentimentos pessoais [de uma pessoa] (…) feitos e assuntos privados (...) o público em geral deve ter.[10] (GODKIN, 1890 apud SOLOVE, 2008, loc. 243, tradução nossa).

No entanto, essa teoria não aponta quais são as informações consideradas privadas. Por conseguinte, não indica quais são as razões pelas quais o acesso a determinadas informações se relaciona com a privacidade. Assim sendo, essa concepção se torna demasiadamente vaga.

2.3. A Privacidade como Segredo

Outra concepção que merece atenção é aquela que define a privacidade como estado de segredo de uma determinada informação. Segundo Solove (2008), sob esta perspectiva, a privacidade é violada quando informações consideradas secretas ou sigilosas são reveladas ao público.

Contudo, a mencionada tentativa de conceitualização falha ao não reconhecer que, em certas situações, indivíduos optam por manter secretas informações para apenas algumas pessoas, e não todas. Isto é, "às vezes as pessoas não querem sigilo absoluto, mas sim a confidencialidade, que consiste em compartilhar informações com um seleto grupo de pessoas de confiança". (SOLOVE, 2008, loc. 298, tradução nossa).[11]

[10] No original: "privacy constituted the "right to decide how much knowledge of [a person's] personal thought and feelings (…) private doings and affairs (…) the public at large shall have

[11] No original: "sometimes people do not want complete secrecy, rather, they desire confidentiality, which consists of sharing information with a select group of trusted people".

2.4. Teoria do Controle sobre as Informações Pessoais

Adicionalmente, Solove (2008) aborda sobre a privacidade definida como controle sobre informações pessoais, uma das teorias mais predominantes da atualidade. Assim sendo, privacidade seria "a reivindicação de indivíduos, grupos ou instituições para determinar por si mesmos quando, como e em que medida as informações sobre eles são comunicadas a outras pessoas". (WESTIN, ano, apud SOLOV, 2008, loc. 298, tradução nossa).

Essa teoria, todavia, também apresenta alguns problemas. Solove (2008), discute que a concepção de privacidade como controle sobre informações pessoais é, ao mesmo tempo, limitada, por não tratar a privacidade apenas no campo informacional, e excluir questões envolvendo a liberdade sobre tomar decisões sobre o próprio corpo, reprodução, ou sobre paternidade; e demasiadamente vaga, pois não indica quais os tipos de informação que o indivíduo deve ter controle.

Ainda, os teóricos adeptos à essa concepção não explicam satisfatoriamente quais são as implicações do controle sobre as informações pessoais. Segundo Solove (2008), muitos compreendem que o controle deve ser tratado como propriedade sobre a informação. No entanto, há problemas com essa percepção. Segundo Solove (2008), primeiramente, a informação pessoal é facilmente transmitida e, uma vez compartilhada, dificilmente é possível retirá-la do ideário das pessoas que a receberam. Além disso, muitas informações pessoais não são construídas inteiramente pelas pessoas a qual se referem, mas sim a partir do relacionamento com outras pessoas e pela utilização de diversas ferramentas. Um exemplo disso é o valor das informações para fins de marketing e publicidade, que é formado após o tratamento de dados, a partir de ferramentas como a compilação e categorização, e não apenas pela divulgação do titular das informações.

Ademais, a presente teoria falha ao restringir a privacidade ao controle de informações estritamente pessoais. Dessa forma, é possível verificar invasões de privacidade quando o indivíduo é "forçado a consumir propaganda, sendo manipulado por anúncios subliminares ou sendo interrompido de uma maneira que frustra a capacidade de pensar ou ler"[12]. (SOLOVE, 2008, loc. 354, tradução nossa). Nessas situações, não há nenhuma interferência no controle sobre informações pessoais, mas, ainda assim, denota-se a existência de problemas envolvendo a privacidade do indivíduo.

[12] No original: "(…) forced to read propaganda, being manipulated by subliminal advertisements, or being disrupted in a manner that thwarts one's ability to think or read".

Por fim, o conceito de privacidade concebido como controle sobre informações pessoais também é limitado por se concentrar na escolha individual dos titulares de dados, e não considerar a privacidade como um aspecto social. Segundo Solove (2008), a privacidade, além de se relacionar o controle individual sobre informações, também se insere em uma estrutura regulatória concernente a essas informações.

2.5. Privacidade e a Proteção da Personalidade

Também é importante ressaltar que muitos teóricos concebem a privacidade como a proteção da personalidade dos indivíduos. Não se trata de uma teoria em apartado, mas sim como um complemento às outras percepções, oferecendo valor à privacidade e delimitação à privacidade. Sob essa perspectiva, a privacidade deve proteger o indivíduo de ataques que possam ofender sua dignidade e individualidade.

No caso *Planned Parenthood v. Casey*[13], a Suprema Corte americana assim dispôs sobre o direito constitucional à privacidade:

> Essas questões, envolvendo as escolhas mais íntimas e pessoais que uma pessoa pode fazer na vida, escolhas centrais para a dignidade e autonomia pessoais, são centrais para a liberdade protegida pela Décima Quarta Emenda. No coração da liberdade está o direito de definir o próprio conceito de existência, de significado, do universo e do mistério da vida humana. Crenças sobre essas questões não poderiam definir os atributos da personalidade se fossem formadas sob compulsão do Estado. (US SUPREME COURT, 1992, apud SOLOVE, 2008, loc. 389, tradução nossa).[14]

Dessa forma, segundo Solove (2008) e sob a ótica da proteção à personalidade, a privacidade pode ser compreendida como a não interferência do Estado em questões essenciais à formação da personalidade do indivíduo. Essa afirmação, no entanto, sofre de algumas imperfeições.

A primeira delas diz respeito ao grau de interferência do Estado. Ao vislumbrar um comportamento impetuoso e arbitrário do Estado em relação ao indivíduo, a teoria da privacidade como proteção à personalidade falha em não considerar que, por vezes, a

[13] Caso em que se discutia a validade de restrições ao direito de aborto nos Estados Unidos. (JUSTIA, 2022.

[14] No original: “These matters, involving the most intimate and personal choices a person may make in a lifetime, choices central to personal dignity and autonomy, are central to the liberty protected by the Fourteenth Amendment. At the heart of liberty is the right to define one's own concept of existence, of meaning, of the universe, and of the mystery of human life. Beliefs about these matters could not define the attributes of personhood were they formed under compulsion of the State”.

privacidade do indivíduo é violada por meio de pequenas perturbações na sua esfera privada. Essas agitações, separadamente, não se caracterizam como nítidas violações ao desenvolvimento da personalidade. No entanto, quando realizadas rotineiramente e analisadas conjuntamente, é possível verificar um problema relacionado à privacidade. Solove (2008) exemplifica essa situação ao afirmar que uma única informação sobre um indivíduo não é verdadeiramente reveladora, mas um conjunto dessas informações conseguem retratar nossas identidades.

O segundo problema dessa concepção se dá por afirmar que todas as interferências estatais são perniciosas. Segundo Solove (2008), a privacidade deve ser compreendida como um direito negativo e positivo. Assim sendo, existem situações em que a ação do Estado é deve atuar para proteger a privacidade dos indivíduos por meio dos dispositivos legais concernentes à matéria. As proteções legais contra o estupro e a invasão de propriedade, por exemplo, são responsáveis por criar um ambiente seguro que proporciona o desenvolvimento da personalidade dos indivíduos.

2.6. A Privacidade como Intimidade

Por fim, é necessário abordar sobre a teoria da privacidade como forma de intimidade. Segundo Solove (2008), essa concepção não engloba apenas a promoção da individualidade, mas o desenvolvimento das relações humanas. Dessa forma, a privacidade deve ser alcançada para a manutenção dos relacionamentos interpessoais.

Essa teoria, no entanto, sofre alguns problemas, principalmente no tocante à definição do que seria considerado íntimo. Intimidade pode ser conceituada como "a consciência da mente em seu acesso a seus próprios e a outros corpos e mentes, na medida em que, pelo menos, estes são geral ou especificamente isolados do acesso de pessoas não convidadas”[15] (GERETY, 1977 apud SOLOVE, 2008, loc. 461), e relacionada às expressões de individualidade e autonomia. No entanto, expressões como individualidade e autonomia são demasiadamente amplas e podem caracterizar qualquer ação de um indivíduo, sem que seja considerada íntima. Por outro lado, a teoria da privacidade como forma de intimidade também é considerada limitada.

Conforme Solove (2008), essa teoria destaca o papel da afinidade oriunda das relações pessoais para delimitar a intimidade das pessoas. No entanto, sentimentos como amor e carinho

[15] No original: “the consciousness of the mind in its access to its own and other bodies and minds, insofar, at least, as these are generally or specifically secluded from the access of the uninvited”.

não estão sempre presentes em relacionamentos e, mesmo assim, são considerados íntimos. Por outro lado, muitas atitudes que expressão afinidade não são consideradas íntimas. Outra imperfeição dessa teoria pode ser observada quando não há consideração sobre a vida privada experienciada apenas pelo indivíduo, sem que este esteja em um relacionamento com outra pessoa.

3. Taxonomia da Privacidade

Apesar de todas as teorias abordadas por Solove (2008) apresentarem reflexões importante sobre o tema da privacidade, essas concepções acabam sendo muito genéricas ou, em contrapartida, insuficientes para os fins que se destinam. Esses problemas são oriundos do método tradicional de conceituação, em que os teóricos buscam elementos comuns que diferenciam a privacidade de outras concepções, como autonomia e liberdade. A utilização do método tradicional de conceituação, portanto, não se mostra muito adequado para a formulação do conceito de privacidade.

Solove (2008), portanto, sustenta que é necessário conceber uma teoria pluralista de privacidade, que foca em um conjunto de proteções relacionados aos diversos tipos de problemas envolvendo privacidade. Para tanto, o método, proposto por Daniel J. Solove para conceituar a privacidade é extraído da ideia do filósofo australiano Ludwig Wittgenstein chamada de "semelhanças de família". Sob essa concepção, "a privacidade não é definida pela busca de um denominador comum em todas as coisas que vemos sob a rubrica de privacidade. Em vez disso, devemos entender a privacidade de maneira pluralista. Privacidade não é uma coisa, mas um conjunto de muitas coisas distintas, porém relacionadas".[16]

Solove (2008) argumenta que uma teoria da privacidade deve focar nos problemas que interferem nas atividades dos indivíduos de maneiras relacionadas, e não na natureza da privacidade em abstrato. Ainda, sustenta uma concepção que oferece um grau de generalização, a fim de ajudar a elaborar leis e políticas relacionadas à matéria, e que seja variável, com o objetivo de se encaixar no contexto histórico e cultural de cada sociedade. Sob uma ótica pluralista, a privacidade não possui valor absoluto, mas tem definida a sua importância quando ponderada em face de outros interesses.

[16] No original: "Privacy is not defined by looking for a common denominator in all things we view under the rubric of privacy. Instead, we should understand privacy in a pluralistic manner. Privacy is not one thing, but a cluster of many distinct yet related things.

A fim de conceber uma teoria pluralista, Solove (2008) propõe uma taxonomia da privacidade. Considerando que "uma violação de privacidade ocorre quando determinada atividade causa problemas que afetam um assunto ou atividade privada"[17] (SOLOVE, 2008, loc. 1270, tradução nossa), é necessário analisar cada uma dessas atividades que, embora sejam diferentes, compartilham de certas semelhanças. Não se busca uma essência que conecta cada uma dessas atividades, mas o problema oriundo de cada uma delas em determinados contextos.

Nessa estrutura taxonômica, existem 4 (quatro) grupos de atividades que são capazes de causar problemas relacionados à privacidade: coleta, processamento e disseminação de informações; e invasão.

3.1. Coleta de Informações

Solove (2008) argumenta que, mesmo que nada seja revelado publicamente, a coleta de informações pode resultar em ofensas à privacidade. Nesse contexto, é possível identificar 2 (duas) formas de coleta de informações: a vigilância e o interrogatório.

A ciência do indivíduo de que é constantemente vigiado pode ocasionar mudanças em seu comportamento. Isso não é inteiramente prejudicial, visto que o controle social proporcionado pela vigilância dos indivíduos ajuda a combater uma série de problemas sociais, como, por exemplo, o crime.

No entanto, a vigilância realizada em certos contextos, ou em excesso, pode ocasionar problemas. Isso em razão do chamado "chilling effect"[18], proporcionado por esse monitoramento, que pode ocasionar impactos negativos na liberdade e na criatividade dos indivíduos. Verifica-se, dessa forma, que "a vigilância inibe a liberdade de escolha e colide com a autodeterminação"[19]. (SCHWARTZ, 2000, apud SOLOVE, 2008, loc. 1.345, tradução nossa).

Ao argumentar que a vigilância é prejudicial não apenas na esfera privada, mas também em ambientes público, Solove (2008) exemplifica um problema relacionado com a vigilância: "Defender crenças radicais e fazer coisas não convencionais exige uma coragem tremenda; o olhar atento, especialmente o do governo, pode fazer com que esses atos pareçam ainda mais

[17] No original: "A privacy violation occurs when certain activity causes problems that affect a private matter or activity".
[18] Tradução livre: "Efeito amedrontador".
[19] No original: "surveillance inhibits freedom of choice and impinges upon self-determination".

ousados e seus riscos potenciais ainda mais inibitórios". (SOLOVE, 2008, loc. 1403, tradução nossa).[20]

Outra forma de coleta de informações é o interrogatório, prática em que o indivíduo é pressionado a divulgar informações. Segundo Solove (2008), são variadas as causas dos problemas relacionados ao interrogatório.

O interrogatório faz com que as pessoas se sintam preocupadas sobre como a recusa será interpretada, na medida em essa resposta negativa pode inferir que o indivíduo esteja escondendo algo. Além disso, há a possibilidade de distorção de informações resultantes do interrogatório. Isso porque o interrogador, ordinariamente, se encontra em posição de controle sobre a maneira que as informações são extraídas do interrogado. Essas informações, portanto, podem ser deturpadas, sendo interpretadas de maneira diversa daquela preterida pelo seu titular, visto que as perguntas podem ser elaboradas de forma a desconsiderar o contexto em que estão inseridas, gerando respostas por vezes enganosas.

3.2. Processamento de Informações

Segundo Solove (2008), o processamento de dados pode ser definido como o uso, armazenamento e manipulação de informações. Verifica-se, nesse sentido, 5 (cinco) formas de processamento de informações: agregação, identificação, insegurança, uso secundário e exclusão.

A agregação diz respeito à reunião de dados sobre um indivíduo. Segundo Solove (2008), uma informação isolada sobre um indivíduo diz pouco a seu respeito, mas um conjunto de informações, combinadas e analisadas, pode revelar fatos que o indivíduo, titular das informações, não previa quando esses dados foram coletados.

Um dos problemas causados pela agregação de informações, inclusive, se dá porque os indivíduos têm expectativas sobre o que deve ser compartilhado sobre eles próprios. A reunião de dados, no entanto, não se amolda a essas expectativas, visto que a combinação de informações não foi necessariamente prevista pelo titular dos dados, e pode revelar novos fatos e novas características sobre o indivíduo.

Além disso, segundo Solove (2008), a agregação pode afetar o poder que os indivíduos têm uns sobre os outros. Isso porque a reunião de dados cria, principalmente no ambiente

[20] No original: "Espousing radical beliefs and doing unconventional things take tremendous courage; the attentive gaze, especially the government's, can make these acts seem all the more daring and their potential risks all the more inhibitory".

virtual. uma espécie de dossiê do indivíduo, que é usado para realizar diversas análises, como a concessão de crédito. Nesse sentido:

> O governo e as empresas estão combinando repositórios de informações pessoais no que chamo de "dossiês digitais" - extensos registros relativos a pessoas. Cada vez mais, cada indivíduo está vivendo ao lado de uma contraparte que existe no mundo dos bancos de dados de computador, uma pessoa digital construída não de carne e osso, mas de bits e bytes de dados. (SOLOVE, 2008, loc. 1479, tradução nossa)[21]

Logo, pode-se afirmar que a agregação causa problemas relacionados à privacidade quando a reunião de informações aumenta consideravelmente o que é conhecido sobre um indivíduo.

No que tange à identificação, é possível concebê-la como o ato de conectar informações a pessoas. Essa conexão, no entanto, tem o poder de afetar negativamente a identidade do indivíduo. Isso porque, em algumas situações, o indivíduo é caracterizado por informações que gostaria que fossem esquecidas. Além disso, "a identificação e o medo de represálias podem impedir discussões perfeitamente pacíficas sobre assuntos públicos de importância"[22] (US SUPREME COURT, 1960, apud SOLOVE, 2008, loc. 1563, tradução nossa), intimidado a liberdade de expressão.

Por sua vez, a maneira como as informações manipuladas e protegidas também pode ocasionar problemas relacionados à privacidade. É o que Solove (2008), chama de insegurança. Alguns exemplos são: roubo de identidade, vazamento de dados e uso ilícito de informações pessoais. Esses lapsos de segurança acabam por expor os titulares de dados à riscos futuros, que podem ser concretizados pela divulgação das informações obtidas ou até mesmo pela sua distorção.

Um outro aspecto relacionado ao processamento de informações é o uso secundário. Segundo Solove (2008), o uso secundário pode ser definido com a utilização de informações para objetivos diversos daqueles expostos quando da coleta dos dados, sem que o titular das informações expresse seu consentimento. Essa atividade, assim como as outras anteriormente mencionadas, podem causar diversos problemas.

---

[21] No original: "The government and businesses are combining repositories of personal information into what I call "digital dossiers" - extensive records pertaining to people. Increasingly, each individual is living alongside a counterpart who exists in the world of computer databases, a digital person constructed not of flesh and blood but of bits and bytes of data".

[22] No original: "identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance".

O uso secundário de informações pode resultar na vulnerabilidade do titular dos dados, visto que este não tem controle sobre como suas informações serão usadas no futuro. Além disso, quando as informações não estão mais inseridas no contexto inicial, quando da sua coleta, esses dados podem interpretados de forma diversa daquela pretendida originalmente.

Por fim, no que tange ao processamento de informações, é necessário abordar a exclusão, que se caracteriza quando o titular dos dados não está ciente sobre o uso de suas informações pessoais. Dessa forma, o indivíduo se mostra impotente no que concerne à utilização e manipulação de seus dados, visto que é negada a sua participação no processamento dessas informações, o que se traduz em um problema vinculado à privacidade. Nesse sentido:

> Quando as pessoas não podem participar da manutenção e uso de suas informações, elas podem ficar impotentes. Alguns podem argumentar que há muitos aspectos da vida nos quais somos impotentes e que não há nada de especial na impotência em relação às informações pessoais. Mas em um mundo onde as informações das pessoas são cada vez mais usadas para tomar decisões importantes sobre elas, a impotência nessa área pode ser significativamente problemática. A exclusão despoja as pessoas do controle de suas vidas de forma substantiva. (SOLOVE, 2008, loc. 1677, tradução nossa)[23]

3.3. Disseminação de Informações

Um outro grupo importante que aborda atividades que podem causas prejuízos à privacidade é o da disseminação de informações. Solove (2008) identifica 7 (sete) tipos de atividades relacionadas ao assunto: violação de confidencialidade (*breach of confidentiality*), divulgação (*disclosure*), exposição (*exposure*), acessibilidade aumentada (*increased accessibility*), extorsão (*blackmail*), apropriação (*appropriation*) e distorção (*distortion*).

A violação de confidencialidade se dá pela quebra de confiança em uma relação específica. Segundo Solove (2008), o prejuízo causado por essa atividade é configurado não apenas pela divulgação da informação considerada sigilosa ou privada, mas sim caracterização de uma verdadeira traição em relação ao titular dos dados, que depositava sua confiança na outra parte. Um exemplo é a atuação do terapeuta, que tem o dever de não divulgar informações sobre seu paciente, sob pena de violar a confidencialidade própria da profissão.

[23] No original: “When people are unable to participate in the maintenance and use of their information, they can be rendered powerless. Some might argue that there are many aspects of life in which we are powerless, and that there is nothing special about powerlessness with respect to personal information. But in a world where people's information is increasingly used to make important decisions about them, powerlessness in this arena can be significantly troublesome. Exclusion divests people of control of their lives in a substantive way”.

Por sua vez, a divulgação de informações também pode causar prejuízos ao titular dos dados. Segundo Solove (2008), a divulgação ocorre quando informações verdadeiras sobre um indivíduo são reveladas aos outros, e o problema causado por essa atividade se relaciona com o dano à reputação do titular, que desejava que a informação tornada pública fosse mantida em segredo, ou circulasse apenas com um seleto grupo de pessoas.

A divulgação de informações também pode prejudicar a segurança do titular dos dados. Um exemplo notório é a publicação do endereço do indivíduo que, a depender de certas circunstâncias, o torna vulnerável e mais suscetível a ser vítima de crimes. Por fim, o risco de divulgação de informações sobre um indivíduo pode limitar seu próprio desenvolvimento, impedindo que participe de determinadas atividades por receio de represálias.

Já a exposição, conforme ensina Solove (2008), se relaciona com a exibição de características físicas e emocionais do indivíduo. Quando expostas ao público, esses atributos, como nudez, rotinas sexuais, necessidades fisiológicas, traumas, assuntos relacionados à saúde, ocasionam profundo constrangimento ao indivíduo. Isso porque "desenvolvemos práticas sociais para ocultar aspectos da vida que achamos animalescos ou repugnantes" (SOLOVE, 2008, loc. 1844, tradução nossa). Dessa forma, quando essas informações são reveladas, o indivíduo sofre humilhação e perda de autoestima, impactando negativamente na participação do titular em sociedade.

Uma outra atividade relacionada com a disseminação de dados, conforme Solove (2008), é a da acessibilidade aumentada, que ocorre quando uma informação, que já é publica, se torna ainda mais acessível. Registros acessíveis de candidatos a vagas de emprego, por exemplo, podem facilitar o processo de contratação de uma empresa.

No entanto, essa atividade também pode ocasionar prejuízos à privacidade, pois pode contribuir para que as informações, tornadas públicas por um propósito, sejam utilizadas para outros objetivos que não foram concebidos originalmente. Um exemplo disso se encontra presente no caso *United States Department of Justice v. Reporters Committee for Freedom of the Press*. Nesse contexto, a Suprema Corte dos EUA concluiu que a divulgação de fichas criminais de indivíduos pelo *Federal Bureau of Investigation* (FBI) constituía uma invasão de privacidade nos termos do Freedom of Information Act (FOIA), legislação americana sobre liberdade da informação. (JUSTIA, 2022) Ora, as informações relacionadas aos crimes cometidos por indivíduos são dados públicos, mas quando tornados facilmente acessíveis por um órgão de investigação federal, a divulgação de fichas criminais configura invasão de privacidade. (SOLOVE, 2008)

A extorsão, ou chantagem, também é considerado um problema ligado à privacidade, e ocorre quando há uma ameaça de divulgação de informações a fim de obter uma espécie de vantagem do titular, configurando uma verdadeira dominação de um indivíduo sobre o titular dos dados. Segundo Solove (2008), esse controle, caracterizado por ações coercitivas sobre o titular de dados, é a razão pela qual a chantagem é criminalizada pelas mais variadas legislações penais.

Outra atividade a ser considerada quando da disseminação de informações é a apropriação. Segundo Solove (2008), a apropriação se dá quando alguém usa a identidade e personalidade de outrem, a fim de alcançar objetivos próprios. Muitos tribunais reconhecem a apropriação como relacionada ao direito à propriedade, em uma concepção próxima à proteção da propriedade intelectual. No entanto, Solove (2008), argumenta que os problemas oriundos da apropriação possuem outra dimensão, ligada à interferência da liberdade e do autodesenvolvimento do titular das informações.

Um exemplo disso é o caso *Pavesich v. New England Life Insurance Co*., decidido pela Suprema Corte do Estado da Geórgia. A companhia de seguro de vida, *New England*, utilizou a imagem de Paolo Pavesich em um anúncio ao lado de uma pessoa doente. A propaganda exaltava a saúde de Pavesich em contraste com o enfermo. Mesmo assim Pavesich processou a companhia, e a Corte concluiu que a imagem de Pavesich não poderia ser usada sem o seu consentimento, pois isso caracterizaria uma afronta a liberdade do indivíduo. (GEORGIA SUPREME COURT, 1905 apud SOLOVE, 2008), Dessa forma, a apropriação causa problemas porque se trata de "uma violação da liberdade da vítima na autoria de sua auto narrativa, não apenas em sua perda de lucros".[24] (SOLOVE, 2008, loc. 1.936, tradução nossa).

Por fim, no que tange à disseminação de dados, é necessário tratar sobre o problema da distorção de informações, uma forma de deturpar a imagem do indivíduo, a partir da propagação de informações falsas. Essa atividade "não afeta apenas o indivíduo lesado, mas também a sociedade que o julga. Ela interfere em nossos relacionamentos com esse indivíduo e inibe nossa capacidade de avaliar o caráter daqueles com quem lidamos"[25](SOLOVE, 2008, loc. 2000, tradução nossa).

3.4. Invasão

[24] No original: "(…) an impingement on the victim's freedom in the authorship of her self-narrative, not merely her loss of profits."
[25] No original: "Distortion not only affects the aggrieved individual but also the society that judges that individual. It interferes with our relationships to that individual, and it inhibits our ability to assess the character of those we deal with".

O último grupo de atividades que ameaçam a privacidade é o da invasão. Segundo Solove (2008), é importante destacar 2 (duas) formas de invasão: intrusão (*intrusion*) e interferência decisória (*decisional interference*).

A proteção contra a intrusão está relacionada como "direito de ser deixado em paz", veiculado por Warren e Brandeis em seu artigo *The Right to Privacy*. Isso porque a intrusão envolve incursões na vida do indivíduo, atrapalhando sua vida cotidiana. Um exemplo de proteção à intrusão se dá pela inviolabilidade de domicílio, que protege o cidadão contra buscas desarrazoadas por parte do Estado. A Constituição Federal do Brasil, por exemplo, promove essa proteção, conforme art. 5º, XI, da Carta Política:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial; (BRASIL, 1988)

Para que possa exercer uma vida pública de qualidade, o indivíduo necessita de refúgio, ainda que temporário, da esfera comunitária. Segundo Solove (2008), o fato de o indivíduo estar sozinho permite que ele desenvolva ideias políticas, artísticas e religiosas, que serão posteriormente valorizadas quando introduzidas na esfera pública. A intrusão, portanto, pode se mostrar problemática porque interfere na capacidade indivíduo de se isolar de sua comunidade.

Por fim, é necessário tratar também sobre a interferência decisória. Trata-se da "interferência governamental nas decisões das pessoas em relação a certos assuntos em suas vidas".[26](SOLOVE, 2008, loc. 2.080, tradução nossa). A interferência decisória, por sua vez, gera problemas relacionados à privacidade ao permitir a intervenção do Estado na decisão dos indivíduos a respeito de suas próprias vidas.

Um exemplo disso é o caso *Union Pacific Railway v. Botsford*, de 1891, em que uma mulher processou uma companhia de viagem ferroviária ao ser atingida por uma cama durante o trajeto, o que supostamente causou-lhe sérias lesões nervosas. A companhia, por sua vez, sustentou que a requerente deveria, sem seu consentimento, ser submetida a exames para que

[26] No original: "(…) governmental interference with people's decisions regarding certain matters in their lives".

fosse demonstrada a extensão do dano oriundo do acidente. Nesse contexto, a Suprema Corte dos EUA decidiu que a mulher não poderia ser compelida a realizar tais procedimentos, visto que "obrigar alguém, especialmente uma mulher, a desnudar o corpo ou submetê-lo ao toque de um estranho, sem autoridade legal, é indignidade, agressão e transgressão". (US, 1891, apud SOLOVE 2008, loc. 2095, tradução nossa)[27]

4. A privacidade sob uma nova perspectiva

Solove (2008) propõe uma taxonomia focada em atividades que podem ofender a privacidade dos indivíduos. Essas atividades são divididas em 4 (quatro) grupos: coleta, processamento, e disseminação de informações; e invasão. Essa concepção não busca identificar elementos comuns da privacidade, como dita o método tradicional de conceituação, mas aborda problema relacionados à privacidade que são costumeiramente enfrentados pela esfera legal. A privacidade, nesse contexto:

> (...) envolve um conjunto de proteções contra um grupo de problemas diferentes, mas relacionados. Esses problemas impedem atividades valiosas que a sociedade deseja proteger e, portanto, a sociedade cria maneiras de lidar com esses problemas. (SOLOVE, 2008, loc. 2167, tradução nossa)[28]

Essas atividades, que podem oferecer risco à privacidade, não são completamente intoleradas pela sociedade. A vigilância, por exemplo, pode ser uma atividade que ajuda a combater práticas criminosas. No entanto, a partir de uma perspectiva que foca nos problemas oriundos dessas atividades, é possível realizar um exercício de ponderação, tornando possível examinar os aspectos positivos e negativos dessas atividades, e formular respostas práticas para enfrentar possíveis problemas relacionados à privacidade. (SOLOVE, 2008)

Atualmente, os problemas relacionados à privacidade não são mais restritos a incursões físicas na esfera privada do indivíduo ou à distorção de informações. Na contemporaneidade, discute-se problemas oriundo de práticas como a agregação: é possível conhecer informações

[27] No original: "to compel anyone, and especially a woman, to lay bare the body, or to submit it to the touch of a stranger, without lawful authority, is and indignity, an assault, and a trespass".
[28] No original: "(...) involves a cluster of protections against a group of different but related problems. These problems impede valuable activities that society wants to protect, and therefore society devises ways to address these problems".

sobe um indivíduo sem requisitá-las ao seu titular, muito menos invadi-lo em seu espaço privado. Essa atividade consiste simplesmente em reunir informações sobre espalhadas em diversas fontes, estabelecendo um verdadeiro "retrato" do indivíduo. (SOLOVE, 2008)

Na sociedade informacional, a tecnologia ocupa uma posição central no debate acerca dos problemas relacionados à privacidade. Nesse contexto:

> (...) a tecnologia está envolvida em vários problemas de privacidade porque facilita a coleta, processamento e disseminação de informações. Os problemas de privacidade, no entanto, não são causados apenas pela tecnologia, mas principalmente por *atividades* de pessoas, empresas e governos. Essas atividades interrompem outras atividades que valorizamos e, portanto, criam um problema. A maneira de resolver os problemas de privacidade é reconciliar os conflitos entre as atividades. (SOLOVE, 2008, loc. 2361, tradução nossa)[29]

Ainda que não se trate de uma concepção fechada e definitiva, a teoria pluralista proposta por Solove (2008) busca justamente oferecer uma estrutura que permite essa reconciliação. Ao focar nos problemas relacionadas à privacidade, a taxonomia apresentada no capítulo anterior oferece um substrato às Cortes e aos legisladores a fim de que possam realizar um exercício de ponderação entre a privacidade e seus interesses conflitantes.

[29] No original: "(…) technology is involved in various privacy problems because it facilitates the gathering, processing, and dissemination of information. Privacy problems, however, are caused not by technology alone, but primarily through activities of people, businesses, and governments. These activities disrupt other activities that we value and thus create a problem. The way to address privacy problems is to reconcile conflicts between activities.

III. DO DIREITO À PRIVACIDADE COMO PROTEÇÃO DE DADOS PESSOAIS E OS LIMITES DO CONSENTIMENTO: DESAFIOS INERENTES AO ADVENTO DA TECNOLOGIA

No momento atual, a sociedade encontra-se organizada em torno dos dados pessoais, que se tornaram um componente essencial para o desenvolvimento econômico. Isso se dá pelo progresso tecnológico, que permitiu a criação de sistemas que possuem a capacidade de processar e disseminar informações em enorme escala e velocidade. (BIONI, 2021)

Os dados pessoais, portanto, são considerados como uma espécie de ativo econômico, vital para a atividade empresarial da sociedade contemporânea. A organização dos negócios rompe com as concepções tradicionais fordistas e permite que o consumidor possa interferir diretamente na produção de um determinado bem, por meio de suas avaliações e reações. É o que se entende por *prosumer*: o consumidor não apenas consome o bem (*consumption*), mas também o produz (*production)*. (BIONI, 2021)

A função dos dados pessoais também contribuiu significativamente para transformar as estratégias publicitárias dos negócios. Anteriormente padronizadas, as propagandas se tornaram mais direcionadas, tendo em vista que a tecnologia permite, principalmente nos ambientes virtuais, que o consumidor seja monitorado constantemente. Dessa forma, é possível traçar um verdadeiro perfil do titular dos dados, por meio de seu comportamento, que indica seus gostos e preferências, o que acaba por incorporar a estratégia de publicidade de uma determinada empresa. (BIONI, 2021)

O papel de um diploma legal que tenha como objetivo a proteção de dados pessoais deve considerar essa vigilância ininterrupta do indivíduo, e deve buscar um equilíbrio entre o controle de dados pelo seu titular, a atividade de monitoramento que dita o modelo de negócios na sociedade da informação. (BIONI, 2021)

A disciplina dos dados pessoais, portanto, deve ser encaixada na categoria de direitos da personalidade. Não se restringe apenas à intimidade do seu titular, mas sim à uma correspondência fidedigna entre os dados pessoais e a sua projeção diante da sociedade. Esse enquadramento, além de proteger a esfera privada do indivíduo, permite resguardar a exatidão dos dados pessoais, por meio de sua retificação. (BIONI, 2021)

Nessa seara, os dados pessoais são vistos como a extensão do indivíduo, e moldam a sua imagem perante a sociedade. Dessa forma, a regulação concernente à proteção de dados

pessoais deve garantir os direitos fundamentais dos indivíduos, como a liberdade e a privacidade, mas também deve possibilitar o progresso econômico. (BIONI, 2021)

Assim dispõe o art. 170, caput e inciso V, da Constituição Federal:

> A ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, tem por fim assegurar a todos existência digna, conforme os ditames da justiça social, observados os seguintes princípios:
> (...)
> V - defesa do consumidor; (BRASIL, 1988).

A fim de harmonizar tanto os princípios constitucionais da livre iniciativa e da proteção do consumidor, houve a provação da Lei Geral de Proteção de Dados. Esse exercício de ponderação é feito logo no art. 2º, da Lei nº 13.709/2018, que assim preleciona:

> 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. (BRASIL, 1988)

O principal mecanismo oferecido ao titular de dados, a fim de que o equilíbrio dos interesses acima dispostos seja respeitado, é o do controle de dados pessoais pelo indivíduo. Além disso, é necessário "assegurar que o fluxo informacional atenda às suas legítimas expectativas e, sobretudo, não seja corrosivo ao livre desenvolvimento da sua personalidade" (BIONI, 2021, p. 152).

A primeira geração de leis de proteção de dados estava relacionada com a esfera governamental. O desenvolvimento da tecnologia, aliado à formação do Estado moderno, permitiu que os dados pessoais fossem agrupados em um banco unificado. Nesse contexto, temia-se uma vigilância exacerbada e orwelliana. Assim, foram criadas leis que dispunham rigidamente acerca do uso da tecnologia no que tange ao processamento de dados. (BIONI, 2021)

No entanto, o tratamento de dados passou a não ser mais restrito ao âmbito estatal. É nesse momento que surgem as leis de proteção de dados de segunda geração, que tratam sobre bases de dados também na esfera privada, cuja proteção não seria feita pelo Estado, mas sim de maneira autônoma pelo indivíduo Nesse contexto, "se antes o fluxo das informações pessoais

deveria ser autorizado pelo Estado, agora cabe ao próprio cidadão tal ingerência que, por meio do consentimento, estabelece as suas escolhas no tocante à coleta, uso e compartilhamento dos seus dados pessoais" (BIONI, 2021, p. 203).

O ápice dessa autodeterminação informacional se dá com a formulação de leis de proteção de dados de terceira geração. Nessa fase, garante-se ao titular de dados participação em todo o procedimento de tratamento, que vai desde a coleta até o compartilhamento. Assim, o indivíduo possui um amplo controle sobre seus próprios dados. (BIONI, 2021)

No entanto, a transferência de responsabilidade ao indivíduo pela proteção de seus dados não foi imune a críticas. Para participar de diversas atividades sociais, inclusive o acesso aos bens de consumo, o indivíduo precisa necessariamente fornecer seus dados pessoais. Dessa forma, não fornecer os próprios dados pode significar a própria exclusão do titular da esfera social.

Nesse sentido, surgem as leis de proteção de dados de quarta geração, que buscam suprir as deficiências dos marcos regulatórios anteriores. O consentimento não deixa de desempenhar um papel decisivo, mas é qualificado e reavaliado, cedendo espaço para a atuação de autoridades independentes na proteção de certas categorias de dados pessoais, como os sensíveis. (BIONI, 2021)

Em 1980 e 1985, diante da centralidade do processamento de dados pessoais para o progresso econômico e social, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) emitiu, respectivamente, as chamadas *privacy guidelines* e *declaration on transborder data flows*. Esses documentos buscavam uniformizar o tratamento de dados nos países membros da organização, a fim de permitir o fluxo de informações. Além disso, essas normativas influenciaram diplomas legais no mundo todo relacionados à proteção de dado. Essas diretrizes, que se encaixam nas leis de proteção de dados de terceira geração, estabeleceram o protagonismo do titular de dados pessoais, que deve fornecer, em todo o fluxo de informações, seu consentimento para que o tratamento de dados seja considerado lícito. Essas orientações emitidas pela OCDE podem ser incluídas entre a terceira e a quarta geração de leis de proteção de dados. (BIONI, 2021)

Por sua vez, a Diretiva de Proteção de Dados Pessoais da União Europeia, busca qualificar o consentimento, com o intuito de enfrentar o controle de informações pouco eficaz pelo titular dos dados. A diretiva é amplamente influenciada pelas orientações emitidas pela OCDE, mas aperfeiçoa a abordagem da organização ao estabelecer seu foco tanto no titular de dados quanto no controlador de dados. (BIONI, 2021)

Essa diretiva, portanto, se encaixa como um exemplo de lei de proteção de dados de quarta geração, "marcada pela promulgação de normas que procuram emponderar o titular de dados pessoais e, por isso, expandem seu espectro para todos os sujeitos inseridos ao longo da cadeia do fluxo informacional" (BIONI, 2021, p. 209).

No ordenamento jurídico brasileiro, é importante ressaltar as disposições do Código de Defesa do Consumidor (CDC), de 1990. Assim dispõe o art. 43, do diploma consumerista:

> O consumidor, sem prejuízo do disposto no art. 86, terá **acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo** arquivados sobre ele, bem como sobre as suas respectivas fontes.
> §1° Os cadastros e dados de consumidores devem ser **objetivos, claros, verdadeiros e em linguagem de fácil compreensão**, **não podendo conter informações negativas referentes a período superior a cinco anos.**
> §2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
> §3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, **poderá exigir sua imediata correção**, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.
> §4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.
> §5° Consumada a **prescrição relativa** à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.
> §6º **Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis**, inclusive para a pessoa com deficiência, mediante solicitação do consumidor. (BRASIL, 1990, grifo nosso)

Nesse contexto, o CDC adota o mesmo padrão regulatório das diretrizes da OCDE, e tem como objetivo garantir a autodeterminação informacional do consumidor, por meio do acesso das próprias informações (art. 43, caput) e da possibilidade de retificação de dados (art. 43, §3º), e até mesmo pela restrição ao armazenamento de dados negativos por mais de 5 (cinco) anos (art. 43, §1º). (BIONI, 2021)

Outra legislação importante no contexto da proteção de dados pessoais no Brasil é a Lei nº 12.414/2011, chamada de Lei do Cadastro Positivo. A fim de resguardar a autodeterminação informacional do titular, ela determina que os bancos de dados criados para fins de operações de crédito não sejam apenas formados por informações negativas, como dívidas em aberto, mas também de elementos positivos do postulante de crédito, como o histórico de adimplemento. (BIONI, 2021) Além disso, a referida lei, em seu art. 3º, §3º, proíbe a anotação de informações

excessivas, não ligadas a análise de crédito, e de informações sensíveis, vinculadas à saúde ou às convicções políticas e religiosas do titular, por exemplo. (BRASIL, 2011)

A Lei nº 12.965/2014, também chamada de Marco Civil da Internet, procurou estabelecer os direitos, garantias e deveres dos indivíduos no ambiente eletrônico. A legislação em comento tem o seu foco na proteção da privacidade dos titulares de dados, em reação ao vazamento, realizado por Edward Snowden em 2013, de informações confidenciais dos Estados Unidos, que divulgou uma série de programas governamentais que tinham como base a vigilância em massa dos indivíduos. O Marco Civil da Internet, além de oferecer protagonismo do usuário na proteção de seus dados, também buscou qualificar o consentimento oferecido pelo usuário. (BIONI, 2021) Nesse sentido, assim dispõe o art. 7º, VII, da Lei nº 12.965/2014:

> O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> (...)
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, **salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei**. (BRASIL, 2014, grifo nosso)

A referida lei ainda assegurou o direito de exclusão dos dados pessoais, conforme art. 7º, X:

> O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> (...)
> X - **exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais**. (BRASIL, 2014, grifo nosso)

Todos esses dispositivos acabam por garantir a autodeterminação informacional dos titulares de dados. Nesse sentido:

> (...) 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. (BIONI, 2021, pp. 214-215).

Por fim, é necessário discorrer, no âmbito da proteção de dados, sobre a Lei nº 13.709/2018, amplamente conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD). Assim dispõe o art. 7º do referido diploma normativo:

> O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. (BRASIL, 2019)

A partida leitura do referido dispositivo, é possível afirmar que o consentimento não foi disposto como a única base legal para o tratamento de dados, e nem mesmo hierarquicamente superior às outras hipóteses que permitem o tratamento de dados pessoais. No entanto, o consentimento não perdeu sua posição central no contexto da LGPD, visto que a anuência do titular de dados foi extensivamente adjetivada, devendo ser livre, informada, inequívoca e utilizada para uma finalidade determinada, conforme art. 5º, XII, da referida Lei. Nessa seara, a LGPD constrói sua estrutura em torno do controle do titular sobre seus próprios dados por meio do consentimento. (BIONI, 2021)

Do estudo das diversas normativas acerca da proteção de dados pessoais, desde a emissão de diretrizes pela OCDE em 1980 até a promulgação da LGPD no Brasil em 2019, é possível perceber a centralidade do controle de dados pelo próprio titular por meio de seu consentimento. Em que pese ser constantemente desafiado, esse paradigma parte da premissa

de que o indivíduo é “um ser capaz, racional e hábil para controlar as suas informações pessoais” (BIONI, 2021, p. 218).

No entanto, o cidadão é vulnerável diante do mercado informacional. Assim como ocorrer nas relações de trabalho, em que há uma assimetria entre o empregado e o empregador, justificando a existência de uma legislação protetiva, o titular de dados deve ser considerado vulnerável em face dos agentes econômicos do mercado informacional. (BIONI, 2021)

São vários os motivos que tornam assimétrica a relação entre o titular de dados e os atores do mercado de dados. Um desses fatores é a concentração de sujeitos em um dos polos dessa relação. Nesse contexto, é possível citar as práticas de publicidade direcionada. De um lado, há o titular, que fornece seus dados pessoais. De outro, há uma imensa gama de atores que realizam atividades diversas: veiculadores (*publishers*), que exibem publicidade; anunciantes (*advertisers*), que querem anunciar um produto; redes de publicidade (*ad networks*), que conectam anunciantes e veiculadores e colaboram entre si; e *data brokers*, que comercializam dados pessoais dos consumidores. (BIONI, 2021)

Outro elemento que torna assimétrica a relação em comento advém do próprio modelo de negócio típico da economia informacional. Dados pessoais servem como pagamento pelo bem de consumo. Não há efetiva contraprestação pecuniária, mas sim o oferecimento de dados pessoais como moeda de troca. Esses dados, após coletados, são processados e agregados, e permitem identificar os hábitos de seu titular, e são utilizados em campanhas publicitárias (BIONI, 2021). Nessa dinâmica, o consumidor não tem ciência da extensão do uso de seus dados:

> O consumidor “compra agora para pagar depois”. Esse quadro de incertezas é a *eloquência* de uma *nova vulnerabilidade*, na medida em que o titular de dados pode ser “machucado” pela má utilização de seus dados pessoais, cuja potência da “ferida” não pode nem mesmo ser antevista. (BIONI, 2021, p. 254)

Além dessas indefinições, é importante ressaltar que o titular de dados possui limitações cognitivas que atrapalham a sua tomada de decisão. O indivíduo, ao concentrar-se nos benefícios imediatos decorrentes do acesso ao produto ou serviço ofertado, deixa de considerar prejuízos à privacidade que podem se tornar reais apenas futuro, de forma mediata. Ao mesmo tempo, o titular é guiado pela percepção de que as perdas decorrentes das operações envolvendo dados são maiores que os ganhos dela advindos. Nesse contexto, o indivíduo acaba por praticar dissonâncias cognitivas, a fim de esconder as contrariedades das suas próprias ações. Ou seja,

em que pese se preocuparem com a proteção de seus próprios dados, os titulares acabam por tomar decisões que colocam em risco essa proteção. Trata-se, portanto, de uma constatação que desafia a premissa de que o indivíduo é um ser racional e capaz de proteger os próprios dados. (BIONI, 2021)

Para exemplificar essa simetria, Bioni (2021) discorre sobre uma pesquisa empírica da Faculdade de Comunicação Annenberg, da Universidade da Pensilvânia, nos Estados Unidos. Essa pesquisa consistiu em uma entrevista realizada com 1.506 (um mil quinhentas e seis) pessoas adultas, com objetivo de compreender a visão dos consumidores sobre o oferecimento de seus dados pessoais em troca de produtos e serviços que não exigem contraprestação pecuniária, ou seja, "gratuitos".

Em um primeiro momento, questionou-se, por exemplo, se os entrevistados concordariam com a criação de perfis oriundo de seus dados pessoais para aperfeiçoar os serviços a eles oferecidos. Em resposta a essa pergunta, 45% (quarenta e cinco por cento) dos entrevistados responderam de forma positiva. No entanto, foram feitas perguntas complementares, a fim de refinar o resultado da pesquisa. Quando questionados, por exemplo, se concordariam em compartilhar seus dados pessoas para que fossem deduzidas suas capacidades financeiras ou suas origens étnico-raciais, o percentual caiu de forma considerável: apenas 21% (vinte um por cento) e 19% (dezenove) concordaram com o câmbio troca (*trade-off*) oriundo desse compartilhamento de dados pessoais. (BIONI, 2021)

Nesse contexto, o estudo concluiu que os consumidores se encontram resignados à economia de dados pessoais. Não há uma variedade de opções ao consumidor, que certamente escolheriam uma alternativa que propiciasse uma melhor proteção de seus dados. Há, na verdade, uma submissão do titular de dados à dinâmica imposta pela economia de dados:

> Com efeito, a programada autonomia dos consumidores para controlar seus dados pessoais é sufocada por todo um mercado sedento por tal ativo econômico. A lógica da economia dos dados pessoais prevalece e impõe as suas forças sobre a parte mais vulnerável dessa relação. Os consumidores mostram-se impotentes para fazer valer o seu desejo de controlar seus dados pessoais, sendo tal *assimetria de poder* a mola propulsora de tal resignação. (BIONI, 2021, p. 250)

A assimetria presente nas relações que ocorrem na economia informacional justifica a edição de leis e regulamentos concernentes à proteção de dados. Exige, inclusive, o diálogo entre as mais variadas fontes do direito, tendo em vista a sobreposição de vulnerabilidades que

afetam o consumidor. No entanto, essas disposições legais não devem limitar-se à transferência de responsabilidade ao titular pela proteção de dados por meio do consentimento. Nesse sentido:

> Deve-se, contudo e concomitantemente, pensar em disposições normativas que interfiram no próprio fluxo informacional, não deixando, apenas, sobre os ombros dos titulares de dados pessoais, o *fardo normativo* da proteção de dados pessoais. A tutela jurídica deve ir muito além do *raciocínio bifásico* centrado na escolha do indivíduo em consentir ou não com o tratamento de dados pessoais. (BIONI, 2021, p. 258).

Em que pese a qualificação do consentimento por diversas legislações que regulam a proteção de dados, inclusive a LGPD, percebe-se que não há uma operacionalização dessa adjetivação. Em outras palavras, a legislação é omissa sobre como o titular de dados pode consentir de forma livre, informada e inequívoca. As políticas de privacidade, elaboradas por cada modelo de negócios que integram a economia de dados, não permite a instrumentalização do assentimento, pois se são documentos extensos, complexos e elaborados de forma unilateral pelo fornecedor de produtos e serviços. Ao consumidor, resta aceitar os termos presentes na política de privacidade ou ser tolhido de usufruir de determinado bem ou serviço. (BIONI, 2021)

A tecnologia, elemento essencial da economia de dados, pode ser um aliado no processo de operacionalização da adjetivação do consentimento. São as chamadas *Privacy Enhancing Technologies*/PETS. Essas tecnologias são construídas com o objetivo de proteger a privacidade, por meio da metodologia *Privacy by Design*. Em outras palavras, toda a plataforma que oferece m produto ou serviço é construída visando a proteção dos dados pessoais. (BIONI, 2021)

Um exemplo de PET é o *Do Not Track* (DNT). Essa tecnologia é idealizada em meio ao debate, principalmente na União Europeia, a respeito do uso de *cookies* (ferramenta de rastreamento de navegação do usuário). Discutia-se se o titular de dados a serem rastreados deveria consentir anteriormente à coleta, de forma individual (*opt-in*) ou após a sua coleta, por meio do ajuste nas configurações do navegador (*opt-out*). Ambas as estratégias se mostraram problemáticas: o método *opt-in* submetia o usuário da internet a uma infinidade de caixas de texto, tornando a experiência desagradável e desgastante. Por outro lado, o método *opt-out* também se mostrou deficitário, tendo em vista ausência de consenso sobre a disponibilização e padronização das configuradores do navegador (*browser*). (BIONI, 2021)

Nesse contexto, propôs-se a criação do DNT, que consiste em um dispositivo vinculado ao navegador que funciona como uma espécie de interruptor: quando ativada, bloqueia o

rastreamos do usuário; quando desativada, permite o uso de *cookies* pelos *websites* visitados. A ferramenta simplificaria o controle de dados pelos titulares, e ajudaria a enfrentar a assimetria das relações da economia informacional. No entanto, a tecnologia encontrou diversos problemas e resistências: ausência de definição sobre quem implementaria a ferramenta; ausência de consenso sobre a própria concepção do DNT, visto que cada companhia a definia de forma diferente; e críticas do setor empresarial, que entendia que a ferramenta significaria o fim da publicidade comportamental na internet. (BIONI, 2021)

A dificuldade de implementar o DNT, bem como outras PETs com funcionalidades importantes, expôs o fracasso da autorregulação do mercado. Mostrou-se necessário, portanto, atribuir obrigatoriedade ou, pelo menos, incentivar a adoção dessas PETs pelos atores da economia informacional. (BIONI, 2021)

Essa relação entre direito e tecnologia, que podem atribuir dimensão normativa às PETs, se justifica pelo cumprimento do dever de informação, lastreado na boa-fé entre as partes de um negócio jurídico. Ao mesmo tempo, as PETs "devem ser de uso fácil e amigáveis (*usable-friendly*), a fim de despertar no usuário uma real capacidade no gerenciamento de suas informações" (BIONI, 2021, p. 286), sob pena de minar o objetivo da legislação concernente à proteção de dados, que é justamente equalizar a assimetria nas relações presentes na economia de dados e enfrentar o problema da vulnerabilidade do consumidor.

No entanto, a proteção de dados pessoais não pode ser compreendida apenas sob o prisma do consentimento. A negociabilidade consubstanciada pelo controle do indivíduo sobre os próprios dados não é ilimitada. (BIONI, 2021)

Conforme já se demonstrou, a proteção de dados pessoais se encaixa na seara dos direitos da personalidade, que são intransmissíveis e irrenunciáveis, conforme disciplina do art. 11 do Código Civil (BRASIL, 2002). Dessa forma, a autonomia da vontade do titular de dados não pode ser considerada irrestrita.

Uma análise que complementa a autodeterminação informacional para além da disciplina do consentimento é a proposta por Helen Nissebaum, cunhada de "privacidade contextual". Sob essa perspectiva, o fluxo de informações é adequado ou não dependendo do contexto das relações em que são originadas essas informações. Cada situação, portanto, criará uma expectativa de privacidade diferente no titular de dados em relação ao seu receptor. Em uma relação médico-paciente, por exemplo, é adequado o fluxo de informações relacionados à saúde do paciente. Não é adequado, por sua vez, o compartilhamento de informações

concernentes às convicções político-partidárias do indivíduo, por se desvincular do contexto em que está inserida a relação comento. (BIONI, 2021)

Posto isso, é possível afirmar que "a autonomia da vontade deve ser, portanto, limitada, assegurando-se que o fluxo informacional seja apropriado para o livre desenvolvimento da personalidade". (BIONI, 2021, p. 397).

Um exemplo dessa limitação se dá no art. 14 da Lei nº 12.965/2014, que assim dispõe: "Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet" (BRASIL, 2014). Proíbe-se, portanto, o armazenamento de dados que dizem respeito ao conteúdo acessado pelos usuários da internet pelos provedores de conexão. Não se atenta, nessa seara, ao consentimento do titular de dados, pois a referida prática seria considerada inadequada sob o prisma da privacidade contextual, visto que não respeitaria o contexto das relações firmadas pelo usuário da internet, e representaria um atentado à sua privacidade, pois possibilitaria que provedores de conexão registrassem, por completo, a vida digital dos titulares de dados. (BIONI, 2021)

Dessa forma, em face da assimetria constatada nas relações presentes na economia de dados, percebe-se duas dimensões da autodeterminação informacional: uma focada no controle de dados pelo próprio titular, por meio do consentimento, que é operacionalizado pela PETs; e outra em que a autodeterminação do indivíduo é desconsiderada, por meio de uma interferência na economia da informação, a fim de que seja resguardado o valor social da proteção de dados, por meio de normas informacionais, que limitam o fluxo de informações.

IV. A LEI Nº 13.709/2018 COMO MARCO REGULATÓRIO NO TOCANTE À PROTEÇÃO DE DADOS

O que motivou o surgimento de legislações concernentes à proteção de dados pessoais ao redor do mundo, principalmente a partir de 1990, foi o desenvolvimento da economia digital, propiciada pelo progresso tecnológico. (PINHEIRO, 2020)

As normas que tratam sobre proteção de dados pessoais têm como princípio essencial a transparência. Dessa forma, esses dispositivos têm uma composição principiológica e técnica, que preveem uma série de itens de controle para o tratamento adequado de dados pessoais, bem como analisam se o mandamento normativo está sendo cumprido por meio de auditorias.

A discussão sobre a criação de um diploma normativo que regulasse o chamado *free data flow* (expressão utilizada para caracterizar a livre circulação de dados pessoais) começou na União Europeia, por inciativa do partido *The Greens*. Promulgou-se, então, o GDPR (Regulamento Geral de Proteção de Dados Pessoais Europeu[30] nº 679), que foi aprovado no dia 27 de abril de 2016 e começou a aplicar as penalidades previstas 2 (dois) anos depois.

Considerando que o GDPR exigia um mesmo nível regulatório dos países que mantinham relações econômicas com a União Europeia, o referido diploma acabou por influenciar o desenvolvimento de uma legislação semelhante na América Latina e, por conseguinte, no Brasil.

Nesse contexto, em 14 de agosto de 2018, foi promulgada a Lei nº 13.709, também conhecida como Lei Geral de Proteção de Dados Pessoais. Segundo Patrícia Peck Pinheiro, o aludido diploma:

> (...) é um novo marco legal brasileiro de grande impacto, tato para instituições privadas quanto públicas, por tratar da proteção dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais, por qualquer meio, seja apor pessoa natural, seja por pessoa jurídica. É uma regulamentação que traz princípios, direitos e obrigações relacionados ao uso de um doa ativos mais valiosos da sociedade digital, que são as bases de dados relacionados às pessoas. (PINHEIRO, 2020, p. 12)

A proteção de dados pessoais é considerada um direito fundamental. No Brasil, as leis nº 12.414/2011 e 12.965/2014, conhecidas respectivamente como Lei do Cadastro Positivo e Marco Civil da Internet, já previam a proteção de dados pessoais como um direito. No entanto,

[30] No original: "General Data Protection Regulation"

as mencionadas normas não dispõem sobre padrões mínimos de segurança ou sobre os parâmetros adequados para o tratamento de dados. A LGPD busca exatamente suprir essa lacuna apresentada por outras normas setoriais, ao tratar sobre a proteção de dados de forma objetiva e precisa, bem como impor penalidades em caso de desrespeito às suas disposições. (PINHEIRO, 2020)

1. Organização da LGPD

A Lei nº 13.709/2018 é dividida em 10 (dez) capítulos e possui 65 (sessenta e cinco artigos). O **primeiro capítulo** (arts. 1º-6º), trata sobre disposições preliminares, como os fundamentos, princípios e conceitos presentes na LGPD. Já o **segundo capítulo** (art. 7º-16) aborda sobre os critérios exigidos para o tratamento de dados. Por sua vez, o **terceiro capítulo** (arts. 17-22) versa sobre os direitos do titular, como o acesso e a correção de seus dados. Em seguida, o **quarto capítulo** (arts. 23-32) desenvolve sobre o tratamento de dados pessoais especificamente pelo Poder Público. Após, o **quinto capítulo** (arts. 33-36) ocupa-se sobre o tratamento internacional de dados.

Por seu turno, o **sexto capítulo** (arts. 37-45) dispõe sobre os agentes de tratamento de dados, como o controlador e operador, bem como a responsabilidade desses atores. Já o **sétimo capítulo** (arts. 46-51) traz disposições concernentes à segurança e boas práticas no tocante ao tratamento de dados. Em seguida, o **oitavo capítulo** (arts. 52-54) aborda sobre como se dá a fiscalização referente à proteção de dados por meio de sanções administrativas.

Posteriormente, o **nono capítulo** (arts. 55-59) dispõe sobre a Autoridade Nacional de Proteção de Dados (ANPD) e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. No tocante a este capítulo, é necessário realizar uma breve digressão. Houve, inicialmente, veto presidencial em relação à criação da ANPD e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. Nesse contexto, temia-se que a regulamentação concernente à proteção de dados se tornasse deficitária ante a ausência de uma autoridade nacional responsável pela fiscalização do cumprimento dos dispositivos da LGPD. Além disso, existia uma preocupação de que a ausência de uma Autoridade Nacional de Proteção de Dados significasse que o Brasil não possuía uma legislação do mesmo nível do GDPR que, por seu turno, dispõe sobre uma autoridade central de proteção de dados. Assim existia uma possibilidade de problemas comerciais envolvendo o Brasil e a União Europeia. (PINHEIRO, 2020)

Felizmente, a criação da ANPD e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade foi prevista pela lei nº 13.853/2019, que alterou a Lei Geral de Proteção de Dados Pessoais (LGPD). Destaque-se, portanto, "a importância do papel orientativo da Autoridade (ANPD) e a relevância de sua atuação proativa junto à sociedade e às instituições, para encontrar medidas viáveis de implementação da nova regulamentação, que gerem menor impacto possível nos setores produtivos e que sejam adaptados e aderentes aos usos e costumes". (PINHEIRO, 2020, p. 19).

Por fim, **o décimo capítulo** (arts. 60-65) versa sobre as disposições finais e transitórias da LGPD, como a sua entrada em vigor.

2. Alterações da LGPD

A Lei Geral de Proteção de Dados Pessoais (LGPD) sofreu algumas alterações pela Medida Provisória nº 869/18, convertida na lei nº 13.853/2019.

No tocante ao **primeiro capítulo** (art. 1º-6º), a lei nº 13.853/2019 obrigou a observância da LGPD por todos os entes federativos (art. 1º, §1º); proibiu o tratamento integral de informações classificadas dentro dos requisitos do art. 4º, III, por pessoas de direito privado, exceto para empresas privadas constituídas integralmente por capital advindo do Poder Público (art. 4º, §4º); estabeleceu que o encarregado de dados pode ser pessoa física ou jurídica (art. 5º, VIII e Art. 5º, XVIII e XIX); foi omissa no aspecto de permitir que softwares realizem o fornecimento de encarregado de dados (art. 5º, VIII e Art. 5º, XVIII e XIX); dispôs que tanto o Operador quanto o Controlador devem indicar um Encarregado (art. 5º, VIII e Art. 5º, XVIII e XIX); e afirmou que a ANPD será um órgão da administração pública, e terá competência em todo o território nacional (não será mais da administração pública indireta) (art. 5º, VIII e Art. 5º, XVIII e XIX). (PINHEIRO, 2020)

Em relação ao **segundo e ao terceiro capítulos** (arts. 7º-22), a lei nº 13.853/2019 estabeleceu a exclusividade no tratamento de dados pessoais de saúde aos profissionais da área, serviços de saúde e autoridade sanitária (art. 7º, VIII); permitiu que o ente que trate os dados pessoais de saúde não seja obrigado a informar ao titular quando seus dados forem tratados quando esse tratamento se der pelo cumprimento de obrigação legal ou regulatória pelo controlador, dados essenciais à execução de políticas públicas (art. 7º, §1º e 2º); autorizou a adição de novas finalidade de tratamento dos dados de saúde, considerando a necessidade do tratamento (art. 7º, §7º); aprovou o compartilhamento de dados sensíveis de saúde entre

controladores, a fim de prestar serviços de saúde, assistência à saúde e farmacêutica, até mesmo quando os controladores buscarem vantagem econômica, desde que essa seja em benefício dos interesses dos titulares dos dados (art. 11, f, §4º e 5º); proibiu o tratamento de dados sensíveis de saúde para análise de contratação e exclusão de beneficiários (art. 11, f, §4º e 5º); dispôs que a ANPD será responsável por regulamentar a portabilidade de dados pessoais, e que o controlador não tem a obrigação de comunicar os outros agentes de tratamento quando a comunicação for comprovadamente impossível ou exija esforço desproporcional (art. 18, V e §6º); e dispôs que o titular dos dados tem direito de pedir a revisão das decisões tomadas por tratamento automatizado de seus dados, quando aquelas impactarem seus interesses, como definição de perfil pessoal, profissional, de consumo e de crédito (art. 20, caput, §1º e §2º). (PINHEIRO, 2020)

No que se refere ao **quarto capítulo** (arts. 23-32), a lei nº 13.853/2019 disciplinou que deve ser indicado um Encarregado de Dados quando houver tratamento daqueles mencionados pelo art. 39, mas não vedou o compartilhamento de dados de dados pessoais dos requerentes da Lei de Acesso à Informação entre pessoas jurídicas de direito público e privado (art. 23, III e IV); permitiu a transferência de dados das pessoas jurídicas de direito pública para as pessoas jurídicas de direito privado, quando existir contratos, convênios, no intuito de prevenir fraudes ou para garantir a integridade de dados do titular, mesmo sem o consentimento deste (art. Art. 26, IV e V); estabeleceu que a ANPD deverá ser comunicada antes do efetivo compartilhamento de dados pessoais entre pessoas jurídicas de direito público e pessoas jurídicas de direito privado (art. 27, parágrafo único); e que a agência poderá solicitar informações aos órgãos e entidades do governo (art. 29). (PINHEIRO, 2020)

No tocante ao quinto capítulo (arts. 33-36), que aborda o tratamento internacional de dados, não foram observadas quaisquer alterações. Já em relação ao **sexto capítulo, sétimo e oitavo capítulos** (arts. 37-54), a lei nº 13.853/2019 trouxe as seguintes atualizações: estabeleceu que o Encarregado não precisa mais possuir conhecimentos jurídicos e regulatórios para prestar seu serviço, todavia, a ANPD poderá regulamentar posteriormente sobre normas complementares referentes à definição e atribuições do encarregado; (art. 41, §4º); previu as penalidades de suspensão parcial do funcionamento do banco de dados, suspensão do exercício da atividade de tratamento de dados e proibição total ou parcial do exercício de atividades relacionadas ao tratamento desses dados (art. 52, X, XI, XII, §3º e §6º); dispôs que, se o controlador estiver submetido a órgão que possui competências sancionatórias, a ANPD poderá agir em conjunto deste, no entanto, possui competência exclusiva quando se trata de conflitos

de proteção de dados Difusos (art. 52, X, XI, XII, §3º e §6º); e autorizou a conciliação entre controlador e titular de dados no caso de vazamento, conforme art. 46 (art. 52, §7º). (PINHEIRO, 2020)

A Lei nº 13.853/2019 também alterou significativamente o **nono capítulo** da LGPD (arts. 55-59), que trata sobre a ANPD e o Conselho Nacional de Proteção de Dados Pessoais. Conforme exposto no subcapítulo anterior, a lei em comento procurou trazer disposições sobre a criação da autoridade e conselho nacionais, visto que tais disposições foram vetadas quando da aprovação do texto original em 2018.

Nesse sentido, exclusivamente no tocante à Autoridade Nacional de Proteção de Dados, a Lei nº 13.853/2019 dispôs que a ANPD será ente vinculado à Presidência da República, mas poderá ser transformado em autarquia após 2 (dois) anos, em caso de proposta feita pela Presidência (art. 55-A); será composta por conselho diretor, conselho nacional de proteção de dados, corregedoria, ouvidoria, órgão de assessoramento jurídico próprio, unidades administrativas e unidades especializadas (art. 55-C); deverá zelar pela proteção de dados pessoais, elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, bem como fiscalizar e aplicar sanções em caso de tratamento de dados, realizado em descumprimento à legislação, por meio de processo administrativo; (art. 55-J).

Além disso, a ANPD deverá analisar requerimento do titular de dados contra o controlador, comprovada a apresentação de reclamação em face deste que não foi solucionada dentro do prazo regulamentar, promover na população o conhecimento das normas de proteção de dados e de políticas públicas, solicitar às entidades de poder público informes sobre a natureza e âmbito dos dados tratados, realizar auditorias sobre o tratamento de dados pelos agentes de tratamento, editar normas e orientações para que ME, EPP e *startups*, possam se adequar à LGPD, garantir que o tratamento de dados seja feito de forma clara e acessível, conforme a LGPD e o Estatuto do Idoso (art. 55-J). Por fim, a lei nº 13.853/2019 ainda afirmou que é competência exclusiva da ANPD aplicar as sanções previstas na LGPD, bem como prevalecerá em caso de conflito com outros órgãos que tem o intuito de proteger dados pessoais (art. 55-K). (PINHEIRO, 2020)

A única alteração oriunda da lei nº 13.853/2019 em relação **ao décimo capítulo** (arts. 60-65), que trata sobre disposições finais e transitórias foi a alteração da data de entrada em vigor de alguns dispositivos da LGPD. Segundo o art. 65, I-A, da LGPD, os arts. 53, 53 e 54 da LGPD (que tratam sobre as sanções administrativas) entraram em vigor no dia 1º de agosto de 2021, segundo a lei nº 14.010/20. No entanto, conforme alteração da lei nº 13.853/19, os

arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B (que tratam sobre a criação da ANPD e o Conselho Nacional de Proteção de Dados Pessoais) entraram em vigor no dia 28 de dezembro de 2018. Por fim, as demais disposições da LGPD entraram em vigor 24 (vinte e quatro) meses após da data de publicação da LGPD. (BRASIL, 2018)

3. Conceitos, princípios e requisitos do tratamento de dados pessoais

Feitas as considerações sobre a organização e as alterações da LGPD, é importante abordar os conceitos, princípios e requisitos veiculados pela Lei nº 13.709/2018 no tocante ao tratamento de dados.

A LGPD traz um extenso rol de conceitos que orientam sua interpretação e aplicação. Estão presentes no art. 5º da Lei nº 13.709/2018, incisos I ao XIX. No entanto, alguns deles são essenciais para a devida compreensão e adequação à LGPD. São eles: titular, tratamento de dados, dados pessoais, dados pessoais sensíveis, dados anonimizados, anonimização, consentimento, agentes de tratamento, encarregado, e transferência internacional de dados. (PINHEIRO, 2020)

O conceito de titular está presente no art. 5º, V, da LGPD e, no âmbito de sua aplicação, significa qualquer pessoa natural atrelada aos dados pessoais que se submetem ao tratamento. Por sua vez, a definição de tratamento está disposta no art. 5º, X do mesmo diploma, e compreende todas as operações realizadas com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

A Lei nº 13.709/2018, por meio de seu art. 5º, I, ainda dispõe sobre o conceito de dados pessoais: são informações vinculadas a uma pessoa natural identificada ou identificável. Verifica-se que o legislador brasileiro, ao também reconhecer como dado pessoal aquele atrelado à indivíduo identificável, optou por uma concepção expansionista de dados pessoais, a fim de tornar mais ampla a qualificação de um dado como pessoa e, por conseguinte, aumentar o escopo da proteção legislativa. (BIONI, 2021)

Por seu turno, o conceito de dado pessoa sensível está presente no art. 5º, II, da LGPD, e é assimilado como um dado pessoal que revelam informações relacionadas à origem racial ou étnica, religião, vertente política, filiação a sindicato ou a organização de caráter religioso,

filosófico ou político, bem como dados referentes à saúde, vida sexual, dado genético ou biométrico que se encontram vinculados a uma pessoa natural. (BRASIL, 2018)

Ademais, importante destacar o conceito de dado anonimizado. A definição, exposta no art. 5º, III, da Lei nº 13.709/2018, abrange os dados relativos a um indivíduo que não pode ser identificado, considerando meios técnicos razoáveis e disponíveis quando de seu tratamento. (BRASIL, 2018)

Relevante também apontar a noção de anonimização, conforme o art. 5º, XI, da LGPD. Consiste em um procedimento, realizado com a partir de técnicas razoáveis e disponível no momento do tratamento, em que o dado perde a sua possibilidade de vinculação, direta ou indireta, ao seu titular. (BRASIL, 2018)

Além disso, frise-se o conceito de consentimento, figura central na Lei nº 13.709/2018. É conceituado por meio do art. 5º, XII, do aludido diploma, e compreende a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. (BRASIL, 2018)

Também é imprescindível absorver os conceitos relacionados aos agentes de tratamento. Conforme o art. 5º, IX, da LGPD, agentes de tratamento são o controlador e o operador. Estes são especificamente tratados nos incisos VI e VII do mesmo dispositivo. Controlador pode ser entendido como a pessoa natural ou jurídica, de direito público ou privado, que tomam as decisões concernentes ao tratamento de dados. Por seu turno, o operador é pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados por ordem do controlador. (BRASIL, 2018)

Nesse contexto, também é pertinente abordar sobre a figura do encarregado. Segundo o art. 5º, VIII, da Lei nº 13.709/2018, encarregado é uma pessoa indicada pelo operador e controlador, e têm a função de atuar como canal de comunicação entre o controlador, o titular de dados e a ANPD. (BRASIL, 2018)

Por fim, é importante tratar sobre o conceito de transferência internacional de dados, que consiste na transferência de dados pessoais para país estrangeiro ou organismo internacional, conforme disciplina o art. 5º, XV, da LGPD. (BRASIL, 2018)

No tocante aos princípios que devem ser atendidos durante o tratamento, estes estão dispostos no art. 6º da LGPD. São eles: finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas. (BRASIL, 2018)

O tratamento de dados, portanto, deve ser realizado em conformidade com propósitos legítimos e específicos, que devem ser informados ao titular, a fim de que a atividade de tratamento atenda ao princípio da finalidade. Além disso, para ser adequado, o tratamento de dados deve estar circunscrito à sua finalidade, com objetivo de obedecer ao princípio da necessidade. (BRASIL, 2018)

Os titulares de dados ainda têm direito de consultar seus próprios dados de maneira facilitada e integral. Além disso, deve ser garantido aos titulares que as informações armazenadas sobre eles sejam claras, verdadeiras e atualizadas. Tudo isso garante que a atividade de tratamento seja guiada pelos princípios do livre acesso e da qualidade de dados. (BRASIL, 2018)

Ademais, os procedimentos de tratamento, bem como os atores envolvidos nessa atividade, devem ser acessíveis aos titulares dos dados. Ao mesmo tempo, é necessário empregar protocolos de segurança que impedem a divulgação não autorizada de dados pessoais, bem como a sua eliminação ou adulteração. Dessa forma, o tratamento de dados pode ser considerado transparente e seguro. (BRASIL, 2018)

O princípio da prevenção ainda dispõe que é preciso adotar estratégias para prevenir a ocorrência de danos decorrentes do tratamento de dados. Esse tratamento também não pode ser discriminatório ou abusivo, a fim de respeitar o princípio da não discriminação. (BRASIL, 2018)

Por fim, conforme dita o princípio da responsabilização e prestação de contas, o agente de tratamento de dados deve demonstrar que atende aos requisitos impostos pela legislação de proteção de dados. (BRASIL, 2018)

Além da observância dos princípios acima elencados, é necessário se atentar para os requisitos do tratamento de dados.

O principal deles, conforme já abordado no capítulo 3 desse trabalho, é o consentimento do titular, que ocupa posição central na LGPD e em diversas outras legislações. O consentimento do titular como pressuposto ao tratamento de dados está presente no art. 7º, I, da Lei nº 13.709/2018. No entanto, o assentimento do titular pode ser excepcionado. Essas ressalvas estão presentes nos incisos II ao X do mesmo dispositivo. Alguns exemplos de tratamento de dados que não exigem o consentimento do titular são: para o cumprimento de obrigação legal pelo controlador de dados (art. 7º, II), para a realização de políticas públicas pelo Estado (art. 7º, III); para o exercício regular de direito em processo judicial, administrativo

ou arbitral (art. 7º, VI); e para a proteção da vida e integridade do titular de dados ou terceiro (art. 7º, VIII). (BRASIL, 2018)

4. Direitos dos titulares de dados pessoais

Outra questão central da Lei Geral de Proteção de Dados Pessoais são os direitos dos titulares dos dados. Essas garantias estão dispostas no art. 18 da Lei nº 13.709/2018. São eles: confirmação da existência de tratamento; acesso aos dados coletados; correção de dados incompletos, inexatos ou desatualizados; anonimização, bloqueio ou eliminação de dados excessivos, desnecessários ou tratados em desarmonia com a LGPD; portabilidade dos dados a outro fornecedor de produto ou serviço; eliminação dos dados pessoais tratados, ressalvadas as exceções legais; informação das entidades públicas e privadas com as quais o controlador compartilhou os dados do titular; informação sobre a possibilidade de não consentimento com o tratamento, bem como as consequências desse desacordo; e a revogação do consentimento, nos termos da LGPD. (BRASIL, 2018)

Diante da entrada em vigor da LGPD, é necessário que entidades públicas e privadas respeitem os direitos acima aludidos. Nesse sentido:

> "Um dos grandes impactos da LGPD está relacionado à necessidade de se garantir os direitos dos titulares, alguns deles novos para o ordenamento jurídico e para as empresas públicas e privadas, tais como o direito à portabilidade dos dados pessoais. Sendo assim, em resumo, passaram a ser direitos dos titulares e que a instituições devem estar preparadas para atender dentro de um prazo razoável, pela lei brasileira." (PINHEIRO, 2021, p. 35)

Vislumbra-se, portanto, a importância da atenção aos direitos dos titulares como forma de garantir o justo tratamento de dados pessoais.

5. Aplicação e Penalidades da LGPD

Realizadas as ponderações acerca dos conceitos, princípios e requisitos do tratamento de dados de acordo com a LGPD, bem como a respeito dos direitos dos titulares de dados, mostra-se essencial discorrer como se dá a aplicação da referida norma, bem como quais são as sanções previstas em caso de descumprimento dos ditames da Lei nº 13.709/2018.

A aplicação territorial da LGPD é disposta em seu art. 3º. De acordo com o referido dispositivo, a Lei nº 13.709/2018 é aplicada quando o tratamento de dados ocorrer em território

nacional, quando a atividade de tratamento tenha como finalidade a oferta ou fornecimento de bens ou serviços ou tratamento de dados de indivíduos localizados no território nacional; e quando os dados pessoais tratados tenham sido coletados no Brasil. (BRASIL, 2018)

Nesse sentido, segundo Pinheiro (2020), é possível afirmar que a LGPD tem aplicação extraterritorial, pois pode incidir em operações de tratamento que ocorrem fora do Brasil, mas que a coleta tenha sido efetuada no Brasil, ou em razão da comercialização de produto ou serviço estrangeiro ofertado aos indivíduos que estejam no Brasil.

Por outro lado, também é importante estabelecer quando a LGPD é inaplicável. Essa matéria é tratada no art. 4º da Lei nº 13.709/2018. Nesse contexto, a LGPD não incide sobre operações de tratamento: realizadas por pessoas particulares para fins exclusivamente particulares ou não econômicos; realizadas para fins exclusivamente jornalísticos, artísticos, acadêmicos, segurança pública, defesa nacional, segurança d Estado ou investigação e repressão de infrações penais. Além disso, A LGPD não se aplica quando os dados pessoais tratados são provenientes do exterior e não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que esse país, em que se originam os dados, proporcione grau de proteção adequado ao previsto pela Lei nº 13.709/2018. (BRASIL, 2018)

Além disso, é fundamental abordar sobre as penalidades prevista pela LGPD.

De início, importante ressaltar que as sanções originalmente previstas na legislação em comento, fortemente inspirada pelo GDPR, sofreram veto presidencial e foram suavizadas, com o intuito de adaptá-las à realidade brasileira. Além disso, frise-se que as sanções administrativas, no âmbito da LGPD, devem ser aplicadas em obediência ao princípio da proporcionalidade, e após procedimento administrativo que permita a ampla defesa. (PINJEIRO, 2020)

Essas penalidades estão previstas no art. 52, I ao XII, da Lei nº 13.709/2018. São elas:

> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III - multa diária, observado o limite total a que se refere o inciso II;
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - eliminação dos dados pessoais a que se refere a infração;
> VII - (VETADO);

> VIII - (VETADO);
> IX - (VETADO).
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (BRASIL, 2019)

Importante salientar que, conforme dita o art. 52, §6º, da LGPD, as penas mais graves, previstas nos incisos X ao XX do referido dispositivo (suspensão parcial do funcionamento do banco de dados, suspensão do exercício da atividade de tratamento dos dados pessoais e proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados, respectivamente) só poderão ser aplicadas após ter sido imposta pelo menos 1 (uma) das penas compreendidas como mais brandas, previstas nos incisos II, III, IV, V e VI do artigo supracitado (multa simples, multa diária, publicização da infração; e bloqueio e eliminação de dados pessoais, respectivamente), referentes ao mesmo caso. (BRASIL, 2018)

Nos termos do art. 55-K, da LGPD, essas penalidades são aplicadas pela ANPD. A autoridade, ao sancionar uma agente de tratamento que esteja em desconformidade com a Lei nº 13.709/2018, deve observar os parâmetros e critérios do era. 52, §1º, quais sejam: gravidade e natureza da infração; boa-fé do infrator; vantagem auferida ou pretendida pelo infrator; condição econômica do infrator; verificação de reincidência; o grau do dano cometido; a cooperação do infrator; a adoção de protocolos internos capazes de minimizar o dano e que garantam o tratamento seguro e adequado de dados; a adoção de política de boas práticas e governança; a imediata adoção de medidas corretivas e a proporcionalidade entre a conduta irregular e a intensidade da penalidade. (BRASIL, 2018)

6. O papel da Autoridade Nacional de Proteção de Dados

Além de abordar sobre a aplicação da LGPD e suas penalidades, é fundamental discorrer sobre a Autoridade Nacional de Proteção de Dados (ANPD).

Trata-se, em suma, de uma autoridade incumbida de orientar a correta aplicação da LGPD. Sua estrutura e funcionamento está disposta nos arts. 55-A ao 55-K. É um órgão ligado à Presidência da República, mas poderá, em até 2 (dois) anos após a entrada em vigor da LGPD, se transformar em autarquia, que poderá conferir mais independência à ANPD. Sua estrutura é

formada pelo Conselho Diretor, Conselho Nacional de Proteção de Dados, Corregedoria, Ouvidoria, Órgão de Assessoramento Jurídico Próprio e Unidades Administrativas e Unidades Especializadas. (BRASIL, 2018)

No art. 55-J, da LGPD, são previstas 24 (vinte e quatro) competências da ANPD. As principais atribuições dessa autoridade são: zelar pela proteção de dados pessoais (art. 55-J, I), elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade (art. 55-J, III); fiscalizar e aplicar sanções em caso de tratamento de dados realizados em desconformidade com a legislação (art. 55-J, IV); apreciar petições de titular contra controlador após comprovada a apresentação de reclamação não resolvida pelo controlador no prazo estabelecido em regulamentação (art. 55-J, V); promover o conhecimento das normas e das políticas públicas sobre a proteção de dados pessoais e privacidade (art. 55-J, VI); solicitar, a qualquer momento, que entidade públicas informem sobre o os detalhes das operações de tratamento que estão envolvidas, bem como elaborar parecer técnico a fim de garantir o cumprimento da Lei nº 13.709/2018 (art. 55-J, XI); realizar auditorias, ou determinar sua realização, no seu âmbito de atuação fiscalizatória, a respeito do tratamento de dados pessoais efetuado por agentes públicos e privados (art. 55-J, XVI); editar normas, orientações e procedimentos simplificados e diferenciados, a fim de as microempresas, empresas de pequeno porte e *startups* possam se adequar à LGPD (art. 55-J, XVIII); e garantir que o tratamento de dados de idosos seja efetuado de maneira simples, calar, acessível e adequada ao seu entendimento (art. 55-J, XIX). (BRASIL, 2018)

Diante dessas considerações, verifica-se que a atuação da ANPD é essencial para uma correta aplicação da LGPD, bem como para que os entes públicos e privados se adequem à legislação. Nesse sentido:

> (...) pode-se afirmar que a constituição da ANPD é essencial para que o *enforcement* da Lei de Proteção de Dados seja possível, ou seja, é esse regulamento que torna a aplicação da lei possível. Isso ocorre porque um regulamento com previsão de sanções sem órgão fiscalizador não tem efetividade nem garantia de funcionamento. (PINHEIRO, 2020, pp. 45-46)

Feitas as devidas considerações em relação à Autoridade Nacional de Proteção de Dados, o presente capítulo finaliza seu objetivo ao abordar a Lei nº 13.709/2018 como marco regulatório concernente à proteção de dados pessoais. Não se buscou esgotar todos os dispositivos da referida legislação, mas apontar quais foram as suas maiores contribuições no tocante à matéria no Brasil.

V. *E-COMMERCE* ENQUANTO MARCA DA SOCIEDADE INFORMACIONAL E OS IMPACTOS DA LGPD

Atualmente, o Brasil é o país com o 5º maior número de usuários de internet no mundo, com aproximadamente 149 milhões de internautas. (MINIWATTS MARKETING GROUP, 2020). Ainda, conforme estudo da *WorldPay from FIS*, de 2021, o volume de transações no comércio eletrônico brasileiro cresceu mais de 22% (vinte e dois porcento) em 2020, e obteve uma arrecadação de aproximadamente U$ 36 (trinta e seis) bilhões. Esse valor deve crescer em 50 % (cinquenta por cento) até 2024, alcançando uma arrecadação de cerca de U$ 56 (cinquenta e seis) bilhões. (WORLDPAY FROM FIS, 2021)

Esse acesso massivo à internet favoreceu o desenvolvimento do comércio eletrônico no Brasil (TEIXEIRA, 2021). Inegável, portanto, a importância do comércio eletrônico na sociedade atual. No mesmo sentido, é extremamente relevante entender a relação do *e-commerce* com a disciplina de proteção de dados, principalmente no tocante à Lei nº 13.709/2018.

Dessa forma, propõe-se uma breve descrição sobre os contornos do comércio eletrônico e, após, os impactos da LGPD sobre essa atividade.

1. Breve descrição sobre os contornos do comércio eletrônico

O comércio eletrônico, ou em inglês, *e-commerce*, pode ser definido como

> uma extensão do comércio convencional, (...), tratando-se de um ambiente digital em que as operações de troca, compra e venda e prestação de serviço ocorrem com o suporte de equipamentos e programas de informática, por meio dos quais se possibilita realizar a negociação, a conclusão e até a execução do contrato, quando for o caso de bens intangível. (TEIXEIRA, 2021, p. 28)

Nos tempos primitivos, a troca de bens era extremamente restrita. Com a introdução de um ator intermediário (comerciante), que satisfazia o interesse de seus clientes, houve um crescimento do comércio, em que as pessoas procuravam importar os bens desejados e exportar os bens e excesso. Com o passar do tempo, esses comerciantes passaram a se fixar em estabelecimentos físicos, principalmente nas grandes cidades, em contraposição à figura do comerciante "nômade". (TEIXEIRA, 2021)

O advento da Revolução Industrial possibilitou o desenvolvimento dos meios de transporte, e a produção de bens e consumo massificados, e, por causa disso, o comércio se tornou ainda mais amplo. Soma-se a esse contexto o desenvolvimento do computador, e o fato de, em 1969, o exército americano, a fim de estabelecer uma comunicação mais eficaz entre suas bases militares, criou a "Arpanet", considerada a precursora da atual internet. (TEIXEIRA, 2021).

Com o passar do tempo, a utilização da internet não ficou mais restrita à esfera militar, mas liberada também o uso comercial. Esse fenômeno, aliado à difusão da informática, possibilitou uma nova forma de contratação, realizada em ambiente eletrônico. Esse desenvolvimento da tecnologia da informação causou uma série de consequências no comércio. (TEIXEIRA, 2021).

Um desses efeitos é a redução de custos, visto que o estabelecimento, que antes era físico, passa a ser virtual. O funcionamento deste é bem menos custoso que aquele, visto que não há gastos em relação à manutenção de estoque, que pode ficar sob responsabilidade de terceiros; encolhimento da mão de obra, redução de despesas locatícias, entre outros. (TEIXEIRA, 2021).

Ademais, vislumbra-se que, no ambiente eletrônico, não há limites geográficos para a venda de produtos e serviços, ampliando o alcance da divulgação de bens e serviços. Além disso, na vigência do comércio eletrônico, as empresas podem comercializar seus produtos e serviços de forma ininterrupta, sem se preocupar com limites de horário de funcionamento. (TEIXEIRA, 2021).

Outra repercussão da ascensão do comércio eletrônico é a redução da cadeia de distribuição de bens. Nas negociações realizadas em ambiente virtual, os fornecedores podem vender seus produtos e serviços de forma direta ao consumidor, sem a necessidade de intermediários. Em outros contextos, em que o conhecimento de técnicas de venda é valorizado, o comércio eletrônico acaba por afirmar a atividade do comerciante, que faz a intermediação de negociações na internet. Um exemplo é o MercadoLivre, que conecta vendedores e compradores. (TEIXEIRA, 2021).

Apesar das diversas facilidades oriundas do comércio eletrônico acima expostas, também é necessário destacar que o *e-commerce* também lida com situações desafiadoras:

> É preciso compreender e lidar com o novo perfil do consumidor, com a exposição da empresa/marca nas redes que pode ser postiva, negativa, e, além de golpes, fraudes nas compras, estorno de pagamentos (*chargeback*), há a preocupação com segurança, com ferramentas, sistemas, logística dos

> bastidores, que envolve controle de estoque, envio, acompanhamento da entrega, reposição e troca, bem como a gestão indispensável, ainda que se utilizem sistemas de automação de processos. (LIMA, 2021, p. 140).

Um outro desafio do comércio eletrônico está na figura do "e-consumidor", que é mais exigente e aspira pela prestação de serviços de forma cada vez mais veloz, transparente e acessível. Nessa seara, o *marketing* ocupa uma posição fundamental no comércio eletrônico, pois visa atender as necessidades desse consumidor inserido no ambiente virtual. No entanto, essa prática deve estar adstrita às normas de proteção ao consumidor, como, por exemplo, ao Código de Defesa do Consumidor, à Lei do *E-commerce* (Decreto nº 7.962/2013), ao Marco Civil da Internet e à Lei Geral de Proteção de Dados Pessoais (LIMA, 2021), sendo esta última o enfoque deste trabalho.

O fato é que a popularização do acesso à internet promoveu a criação de diversas empresas no ambiente digital, as chamadas "lojas virtuais". Esse fenômeno se tornou ainda mais acentuado com a eclosão da pandemia de COVID-19. A emergência sanitária colocou diversos entraves para o funcionamento físico dos estabelecimentos, fazendo com que diversas empresas verificassem a necessidade de migração para o ambiente virtual, a fim de resguardarem a continuidade de suas atividades. No entanto, é possível que muitos desses empreendimentos, que se movimentaram para o âmbito virtual, não ofereçam proteção satisfatória aos seus consumidores (LIMA, 2021).

Nesse contexto, a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais, dispôs sobre uma série de proteções aos consumidores, impactando diversas empresas e organizações que realizam alguma espécie de tratamento de dados pessoais (LIMA, 2021).

2. Impactos da LGPD e adaptações necessárias no âmbito do comércio eletrônico

A Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais, tem como objetivo proteger direitos fundamentais do titular de dados, como sua privacidade e intimidade. Esse diploma surge em meio ao contexto de desenvolvimento da tecnologia, que tornou a informação um ativo econômico de grande importância para o setor público e privado. (PINHEIRO, 2020)

O aumento na quantidade de operações dentro da esfera digital, principalmente no âmbito do *e-commerce*, que envolvem o compartilhamento de dados pessoais, tornou evidente a necessidade de elaboração de uma legislação que oferecesse proteção aos dados pessoais dos titulares. Em que pese a LGPD proteger os dados pessoais tanto na esfera física como na virtual,

conforme dispõe seu art. 1º, caput, (BRASIL, 2018), é nesse último contexto em que a demanda por proteção é mais perceptível, justamente porque, no âmbito digital, o tratamento de dados se dá em um volume massivo, devido ao suporte oferecido pela informática, conforme já abordado no capítulo 1 deste trabalho.

A obrigatoriedade de adequação à LGPD provocará uma grande repercussão nas instituições do país, principalmente nas startups, pequenas empresas e entidades públicas. É possível afirmar que, a fim de se adaptarem às disposições legais, essas empresas tenham um aumento no custo de funcionamento. (PINHEIRO, 2020). Além disso, a adequação à LGPD também impactará na cultura das empresas, que necessitarão do apoio de seus dirigentes com o objetivo de implementar essa legislação. (LIMA, 2021)

Insta, portanto, identificar os principais impactos da LGPD sobre as empresas que negociam no âmbito digital. Não se pretende esgotar o tema, mas sim trazer algumas percepções sobre as mudanças que inevitavelmente deverão ocorrer a fim de uma bem-sucedida adaptação dos empreendimentos à legislação de proteção de dados do Brasil.

Muitas empresas que atuam no *e-commerce* também possuem uma esfera física que dá suporte à atividade *online*. O respeito à LGPD, por sua vez, deve ocorrer em todas as fases da negociação, a fim de proteger os dados consumidores titulares desses dados. De uma forma geral, a adequação dessas empresas depende do treinamento de seus colaboradores, que deve ser incessante. (LIMA, 2021)

A depender do porte da empresa, a criação de um comitê de privacidade é de suma importância a fim de que o negócio se adeque à LGPD. Esse comitê ficaria responsável por implementar a adaptação do empreendimento, envolvendo os mais diversos setores da empresa, como diretoria, departamento jurídico, recursos humanos, *marketing*, e segurança e tecnologia da informação. Além disso, nessa fase inicial é de suma importância a designação do encarregado (LIMA, 2021). Conforme já exposto no capítulo 4 deste trabalho, o encarregado atua como elo entre a ANPD, o controlador e os titulares de dados. No processo de tratamento de dados, o controlador deve indicar um encarregado para se incumbir dessas responsabilidades, conforme art. 41, caput, da Lei nº 13.709/2018 (BRASIL, 2018).

Também é essencial que a empresa guarde registro de todas as operações envolvendo o tratamento de dados pessoais (LIMA, 2021). Isso porque, de acordo com o art. 37 da LGPD, tanto o controlador como o operador devem manter esse registro de operações, especialmente quando o tratamento de dados for baseado no legítimo interesse. (BRASIL, 2018).

Ao cumprir esse requisito da LGPD, possibilita-se à empresa ter uma perspectiva geral sobre os dados pessoais que se encontram sob sua responsabilidade. Esse mapeamento permite apontar a localização desses dados, a necessidade de sua guarda, e a finalidade do tratamento, bem como proporciona entender o ciclo de vida dos dados, desde a sua coleta até a sua exclusão (LIMA, 2021). Importante ressaltar que, após o fim do tratamento, os dados pessoais devem ser eliminados, e só podem ser conservados para o cumprimento de obrigação legal ou regulatória; para estudo por órgão de pesquisa, garantida anonimização; transferência à terceiros, cumpridos os requisitos da Lei nº 13.709/2018; e para uso exclusivo do controlador, desde que os dados sejam anonimizados e vedado o acesso destes por terceiros, conforme dita o art. 16 da LGPD (BRASIL, 2018). Por fim, frise-se que esse procedimento de mapeamento de dados deve ser atualizado periodicamente, visto que novos dados continuarão a ser tratados pela empresa (LIMA, 2021).

A LGPD também ressalta a importância da elaboração de um Relatório de Impacto à Proteção de Dados Pessoais (LIMA, 2021). Trata-se de um documento que pode ser requisitado pela ANPD, e deve conter, pelo menos, a descrição de todos os dados coletados, a metodologia da coleta e da segurança da informação, além de análise do controlador sobre quais as medidas adotadas em relação à mitigação de riscos, nos termos do art. 38, parágrafo único, da LGPD. (BRASIL, 2018).

As empresas podem buscar inspiração para elaboração desses documentos nas legislações e regulações estrangeiras que o Brasil se inspirou na elaboração da LGPD. Alguns exemplos são: art. 30 do Regulamento Geral de Proteção de Dados Pessoais (GDPR), da União Europeia, que dispõe sobre o registro de atividades de tratamento de dados; e diretrizes da autoridade de proteção de dados do Reino Unido, *Information Comissioner's Office* (ICO), que oferecem orientações para elaboração do *legitimate interest assessment* (LIA), documento que avalia qual o legítimo interesse das empresas no tratamento dedados dos consumidores. (LIMA, 2021)

Ademais, empreendimentos que terceirizam algumas de suas atividades devem verificar se seus operadores estão em harmonia com a legislação de proteção de dados, por meio de auditorias Isso porque, em caso de qualquer incidente com os dados pessoais, a responsabilidade incidirá sobre a empresa com quem o titular de dados se relacionou. (LIMA, 2021). Importante destacar que, conforme já abordado no capítulo anterior, operador é aquele que realiza o tratamento de dados em nome do controlador, nos termos do art. 5º, VII, da LGPD. (BRASIL, 2018).

A Lei nº 13.709/2018 ainda impôs a produção, exame e retificação de alguns documentos e contratos, a fim de que estejam em harmonia com os ditames da legislação. Nesse sentido, têm-se as políticas de privacidade, que devem informar sobre a postura esperada dos colaboradores da empresa. Empreendimentos que envolvam a área de recursos humanos, por exemplo, possuem uma vasta quantidade de dados pessoais (e até sensíveis), logo seus funcionários devem estar cientes da importância da proteção desses dados. (LIMA, 2021)

A LGPD também impactou de forma profunda o campo da segurança da informação. Empresas, em especial aquelas voltadas ao comércio eletrônico, devem estar atentas à possíveis ataques que coloquem risco a proteção de dados pessoais tanto no ambiente físico quanto no digital (LIMA, 2021). Nessa seara, conforme art. 46, caput, da Lei nº 13.709/2018:

> Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. (BRASIL, 2018)

A fim de comprovar o emprego dessas técnicas, as empresas podem elaborar alguns documentos, tais como políticas de segurança da informação, registro de atividades de tratamento, e de estratégias de resposta incidentes. (LIMA, 2021) No tocante à segurança da informação, insta ressaltar o disposto no art. 44, parágrafo único, da LGPD, que afirma que, em casos de violação da segurança dos dados, e constatada a ausência de medidas de segurança previstas na legislação, o controlador e o operador respondem pelos danos decorrentes do incidente. (BRASIL, 2018).

Por outro lado, uma reflexão importante é que as medidas de segurança de dados, por mais eficazes que sejam, não são capazes de impedir a integralidade dos incidentes. Nesse sentido, medidas de mitigação de danos também são importantes, como a anonimização de dados, aliada à conscientização dos colaboradores e adoção de boas práticas de tratamento. As empresas, portanto, devem realizar diagnósticos sobre a atual condição da segurança da informação no âmbito dos seus negócios, a fim de que sejam identificados os riscos e vulnerabilidades de suas atividades. Um exemplo de como isso pode ser feito é a realização de auditorias externas. (LIMA, 2021).

Outra forma de garantir a segurança da informação nas empresas é pela criação de um comitê de crise. Nessas organizações, são simulados os mais variados incidentes que podem colocar em risco a proteção de dados, como invasões perpetradas por *hackers* e existência de

vírus nos sistemas da empresa. Por meio desse comitê, a empresa poderá adotar protocolos e estratégias sobre como reagir à essas adversidades. Recomenda-se utilização de documentos emitidos pela *International Organization for Standardization* (ISO)[31]. As normas ISO 27000 e 31000 tratam, especificamente, sobre segurança da informação e gestão de riscos, e são de grande valia apara elaboração das estratégicas aludidas. (LIMA, 2021).

Ante todo o exposto, no âmbito de adequação à LGPD, inegável a importância de adoção de práticas que visem a segurança da informação. Nesse sentido:

> (...) ferramentas capazes de garantir maiores níveis de segurança aos sistemas são bem-vindas, tais como de gerenciamento de *logs*[32], de consentimento, antivírus, sistemas de controle de acesso, *firewall*[33], *softwares*[34] de monitoramento de redes e infraestruturas, não se esquecendo do seguro cibernético, que possibilita que a empresa se sinta segura, ainda que haja um incidente. (LIMA et al, 2021, p. 149).

O processo de harmonização dos empreendimentos de *e-commerce* à LGPD acarretará mudanças no site das empresas. Esses ambientes devem apresentar informações claras, precisas e acessíveis aos consumidores em geral. Da mesma forma, as políticas de privacidade da empresa devem apresentar os direitos dos titulares, a natureza dos dados coletados, etapas e finalidade do tratamento, compartilhamento de dados com terreiros, o canal de comunicação com o cliente, entre outros. (LIMA, 2021).

Muitos sites de comércio eletrônico empregam os chamados *cookies*[35]. Nota-se que essa prática também deve estar adstrita à Lei nº 13.709/2018. A forma de utilização de *cookies* também deve ser informada de maneira simples e compreensível ao titular dos dados, e este deve possui a faculdade de fazer ajustes a esse mecanismo. Nesse sentido, insta salientar que o arranjo de caixas pré-selecionadas para obter o consentimento do titular não está de acordo com os ditames da LGPD (LIMA, 2021).

O site ainda deve apresentar seus termos de uso. Trata-se de documentos que detalham os contornos da relação comercial entre a empresa e o consumidor, tais como meio de pagamento, frete, prazo de entrega e políticas de reembolso. Além disso, no caso de o empreendimento possuir clientes de outro país além do Brasil, o site ainda deve obedecer às

[31] Entidade que desenvolve padrões internacionais. (ISO, 2021)
[32] *Logs* são arquivos que registram os eventos em um determinado Sistema. (LA ROSA, 2018)
[33] *Firewall* pode ser entendido como um dispositivo de segurança que fiscaliza o fluxo de informações em uma rede. (CISCO, 2022)
[34] *Software* é o conjunto de instruções que orientam o funcionamento do computador (JOHNSON, 2021)
[35] *Cookies* são "(...) arquivos de internet que armazenam temporariamente o que o internauta está visitando na rede". (UOL SEGURANÇA DIGITAL, 2013)

disposições sobre proteção de dados dessas localidades. Todas essas informações presentes no site de *e-commerce* torna o tratamento de dados mais transparente ao titular. (LIMA, 2021). Vale lembrar que a transparência é um importante princípio no âmbito da Lei nº 13.709/2018, conforme dispõe seu art. 6º, VI. (BRASIL, 2018).

Por fim, resta consignar que não existe um plano de adaptação uniforme a todas as empresas que praticam o comércio eletrônico. Nesse sentido:

> Não há receita ou fórmula mágica para um projeto de adequação eficiente, não há ferramenta que deixe a empresa *compliant* com a LGPD. A Adequação está muito relacionada com pessoas, treinamento e mudança de cultura. Importante compreender que sem apoio de quem está à frente da empresa não haverá mudança. (LIMA et al, 2021, p. 154)

Ainda, a dimensão, a área de atuação do empreendimento capacidade financeira do empreendimento são fatores que influenciarão a elaboração de uma estratégia que visa a proteção de dados. (LIMA, 2021)

CONCLUSÃO

No primeiro capítulo deste trabalho, buscou-se analisar, de forma suscinta, as origens históricas do direito à privacidade, bem como seu lugar na sociedade atual. Verificou-se que, nas mais variadas épocas históricas, até mesmo as mais antigas, o homem se preocupava com a sua privacidade. No entanto, a acepção atual de privacidade nasceu com a Revolução Industrial, em que as tecnologias, principalmente aquelas relacionadas aos meios de comunicação, se desenvolveram de forma extremamente veloz. O artigo jurídico de Warren e Bradeis, *The Right to Privacy*, de 1890 considerado como o surgimento da moderna doutrina da privacidade, é emblemático: sustenta o direito do homem ser deixado em paz, em reação ao escrutínio massificado da imprensa.

No entanto, Warren e Brandeis não foram os únicos a conceituarem a privacidade. Com o passar do tempo, diversos outros estudiosos formularam a sua própria teoria sobre o tema, buscando a identificação de quais seriam os elementos essenciais da privacidade. Essa abordagem tradicional, no entanto, não se mostrou adequada, visto que ora era demasiadamente abrangente, ora era bastante limitada. Em vista disso, Solove (2008) traz uma abordagem interessante: a proposição de uma taxonomia da privacidade, que foca nas atividades que costumeiramente trazem problemas ligados à privacidade. Essa estratégica, bastante pragmática, pode ajudar legisladores e julgadores a enfrentarem de forma mais adequada as questões envolvendo a privacidade, pois se desvencilha das insuficiências recorrentemente apresentadas pelas teorias anteriores.

Contemporaneamente, é possível classificar a sociedade como informacional, e os dados pessoas ocupam o seu núcleo essencial. Dessa forma, a discussão sobre a proteção da privacidade, atualmente, está vinculada à proteção de dados pessoais. Vislumbrado como um direito fundamental, o direito à proteção de dados justificou a criação de diversas legislações ao redor do mundo. Conforme ensina Bioni (2021), essas legislações, mesmo que em intensidade diferentes, são estruturadas em torno do consentimento do titular como forma de controle de dados. Em que pese o papel do titular ser importante, apenas ele não é suficiente para garantir uma proteção de dados adequada. Por vezes, é necessário o desenvolvimento de tecnologias para auxiliar o titular na tomada de decisões (PETs). Em outras situações, o consentimento do titular simplesmente não deve ser considerado, em face de normas informacionais que, em razão do contexto da operação de dados, afastam a atuação do titular para garantir sua liberdade e privacidade.

Feitas essas considerações sobre o papel do consentimento, o presente trabalho passou a analisar a Lei nº 13.709/2018 de forma detalhada. Tratou sobre sua estrutura, conceitos, princípios. Abordou também os requisitos do tratamento de dados no Brasil e as penalidades em caso de descumprimento da lei. A partir da leitura do texto legal, bem como dos comentários de estudiosos renomados como Patrícia Peck Pinheiro (2020), conclui-se que a LGPD pode ser considerada um marco na legislação brasileira, isso porque normatizou e padronizou os contornos do lícito tratamento de dados no Brasil, e passou a dar proteção efetiva à algumas garantias fundamentais previstas na Constituição Federal de 1988, como direito à proteção da intimidade e da vida privada, presente no art. 5º, X, da Carta Magna (BRASIL, 1988).

Nesse contexto político, econômico, social e jurídico, estão incluídas as empresas que atuam no comércio eletrônico. Essas atividades, possibilitadas pelo desenvolvimento da internet e pela sofisticação da informática, lidam com uma imensa quantidade de dados de consumidores no âmbito de suas atividades. Assim, inegável que esse ramo econômico foi fortemente impactado com a entrada em vigor da LGPD.

Tem-se, então, a última análise proposta por esse trabalho: verificar a repercussão específica da Lei nº 13.709/2018 na esfera do *e-commerce*. Nessa seara, concluiu-se que os empreendimentos que praticam o comércio virtual não poderão negligenciar os dados de seus clientes. Cada empresa desse setor se adaptará de uma maneira diferente, a depender das circunstâncias fáticas em que estão inseridas, mas todas deverão implementar medidas que garantam o tratamento de dados em conformidade com a LGPD. Uma política eficiente de segurança da informação, bem como alterações que aumentem a acessibilidade e transparência dos sites eletrônicos, são medias que, conquanto não esgotem o tema, oferecem um panorama geral de adequação à LGPD para os empreendimentos virtuais.

REFERÊNCIAS BIBLIOGRÁFICAS

ANDRADE, Maria Margarida de. **Como prepara trabalhos para Cursos de Pós-graduação** – noções práticas. São Paulo: Atlas, 1995.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** A função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. 499 p. ISBN 978-85-309-9409-9. *E-book.*

BRANDEIS, Louis D.; WARREN, Samuel D. **The Right to Privacy.** [S. l.]: Quid Pro Books, 2010. 35 p. ISBN 9780982750490. *E-book.*

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988.** [S. l.: s. n.], 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 31 maio 2021.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. [S. l.], 12 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 31 maio 2021.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. [S. l.], 11 jan. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 31 maio 2021.

BRASIL. **Lei nº 12.414, de 9 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. [S. l.], 10 jun. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 3 mar. 2022.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. [S. l.], 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 3 mar. 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). [S. l.], 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 31 maio 2021.

CISCO. **What is a Firewall?** [*S. l.*], 2022. Disponível em: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html. Acesso em: 3 mar. 2022.

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters, Revista dos Tribunais, 2019. 432 p. ISBN 978-65-5065-030-8. *E-book*.

GUTIERREZ, Andriei; VILELA, Camila Maria de Moura; REOLON, Carlos; FALCÃO, Cintia Maria Ramos; RICCO, Cintia; LÓSSIO, Claudio Joel Brito; LUCENA, Claudio; SANTOS, Coriolano Aurélio Almeida Camargos; SLEIMAN, Cristina Moraes; KELLER, Elaine Zordan; SILVA, Fabiani Oliveira Borges da; PALHARES, Felipe; GUERRA, Gustavo Rabay; NÓBREGA, Juliana Targino; CRESPO, Liana I.A. Cunha; SATO, Luiza; BARBOSA, Maria Beatriz Saboya; DERDERIAN, Philip Mario; FERREIRA, Raissa Cristina de Moura; GOMES, Roberta; GARCIA, Valéria Reani Rodrigues. **LGPD Aplicada.** 1. ed. São Paulo: Atlas, 2021. 362 p. ISBN 978-85-97-02692-4. *E-book*.

ISO. **ABOUT US**. [S. l.], 2021. Disponível em: https://www.iso.org/about-us.html. Acesso em: 3 mar. 2022.

JOHNSON, Dave. **What is software?** A guide to all of the different types of programs and applications that tell computers what to do. [S. l.], 26 mar. 2021. Disponível em: https://www.businessinsider.com/what-is-software?r=US&IR=T. Acesso em: 3 mar. 2022.

JUSTIA. **Planned Parenthood of Southeastern Pa. v. Casey, 505 U.S. 833 (1992).** [S. l.], 2022. Disponível em: https://supreme.justia.com/cases/federal/us/505/833/. Acesso em: 3 mar. 2022.

JUSTIA. **The Reporters Committee for Freedom of the Press, et al., Appellants, v. United States Department of Justice, et al. (two Cases), 816 F.2d 730 (D.C. Cir. 1987).** [S. l.], 2022. Disponível em: https://law.justia.com/cases/federal/appellate-courts/F2/816/730/137852/. Acesso em: 3 mar. 2022.

LA ROSA, Alexander. **Log Monitoring**: not the ugly sister. [S. l.], 8 fev. 2018. Disponível em: https://web.archive.org/web/20180214153657/https://blog.pandorafms.org/log-monitoring/. Acesso em: 3 mar. 2022.

MINIWATTS MARKETING GROUP. **TOP 20 COUNTRIES WITH THE HIGHEST NUMBER OF INTERNET USERS**. [S. l.], 2020. Disponível em: https://www.internetworldstats.com/top20.htm. Acesso em: 2 mar. 2022.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos, 1948.** Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 31 mai. 2021.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Pacto Internacional sobre Direitos Civis e Políticos, 1966.** Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 31 mai. 2021.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais:** Comentários à Lei n. 13.709/2018 - LGPD. 2. ed. São Paulo: Saraiva Educação, 2020. 136 p.

SOLOVE, Daniel J. **Understanding Privacy.** Cambridge: Harvard University Press, 2020. 272 p. ISBN 978-0674027725. E-book.

TEIXEIRA, Tarcisio. **LGPD e E-Commerce**. 2. ed. São Paulo: Saraiva Jur, 2021. 332 p. *E-book*.

UOL SEGURANÇA DIGITAL. **O que são cookies e como eles podem me prejudicar?** [S. l.], 26 jun. 2013. Disponível em: https://seguranca.uol.com.br/antivirus/dicas/curiosidades/o-que-sao-cookies-e-como-eles-podem-me-prejudicar.html#rmcl. Acesso em: 3 mar. 2022.

WORLDPAY FROM FIS**. The Global Payments Report.** [S. l.], 2020. Disponível em: https://worldpay.globalpaymentsreport.com/en/download. Acesso em: 31 maio 2021.