UNIVERSIDADE DO ESTADO DA BAHIA

MARCOS AURÉLIO DE MELO

AS CONTROVÉRSIAS ENTRE A LGPD (LEI Nº 13.709/2018) E AS MEDIDAS DE SEGURANÇA DA INFORMAÇÃO EM FACE DA INVIOLABILIDADE DA INTIMIDADE, DA HONRA E DA IMAGEM DAS PESSOAS

JUAZEIRO

2022

MARCOS AURÉLIO DE MELO

AS CONTROVÉRSIAS ENTRE A LGPD (LEI Nº 13.709/2018) E AS MEDIDAS DE SEGURANÇA DA INFORMAÇÃO EM FACE DA INVIOLABILIDADE DA INTIMIDADE, DA HONRA E DA IMAGEM DAS PESSOAS

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do grau de Bacharel em Direito no curso de Direito da Universidade do Estado da Bahia – UNEB, Campus III, Juazeiro, Bahia.

Orientador: Ivanildo Almeida Lima

JUAZEIRO

2022

MARCOS AURÉLIO DE MELO

AS CONTROVÉRSIAS ENTRE A LGPD (LEI Nº 13.709/2018) E AS MEDIDAS DE SEGURANÇA DA INFORMAÇÃO EM FACE DA INVIOLABILIDADE DA INTIMIDADE, DA HONRA E DA IMAGEM DAS PESSOAS

UNIVERSIDADE DO ESTADO DA BAHIA

Data de aprovação: ___/____/_____

_____
Ivanildo Almeida Lima (UNEB)

_____
Paulo de Tarso Duarte de Menezes (UNEB)

_____
Pedro Henrique Matos Souza de Santana (UNEB)

JUAZEIRO

2022

AGRADECIMENTOS

Ao professor Reginaldo Gomes da Silva, que deu início à orientação deste Trabalho de Conclusão de Curso com dicas valiosas. Ao professor Ivanildo Almeida Lima, pela continuidade da orientação, trazendo à baila comentários pertinentes à temática, discussão salutar e sugestões de artigos apropriados ao desenvolvimento da argumentação. De ambos levarei comigo o exemplo de dedicação à análise e compreensão apropriadas do Direito.

Ao colega Rafael Vitória do Nascimento pela parceria na trajetória profissional e acadêmica, um autêntico jaguaririense, literato e poeta nato, águia que alçará voos altaneiros no Direito. É imperioso destacar os colegas Warley Gonçalves e José Guilherme pela dedicação e empenho nos trabalhos acadêmicos em conjunto, jovens advogados de envergadura propícia a grandes feitos no mundo jurídico.

Dedico este trabalho a minha família – Camila, Ester e Levi – pela paciência e confiança ao longo da jornada acadêmica. Certamente os desafios foram superados com a cooperação de vocês.

"Aqueles que sabem sobre nós têm muito poder sobre nós.”

Finn Brunton & Helen Nissenbaum

“A privacidade, disse ele, era uma coisa muito valiosa. Todos queriam um lugar onde pudessem estar sozinhos ocasionalmente.”

George Orwell

RESUMO

A Tecnologia da Informação e as possibilidades de comunicação proporcionadas pelo avanço da Internet trouxeram significativas controvérsias quanto ao tratamento de dados. A Lei Geral de Proteção de Dados (Lei 13.709/18) apresenta-se como um importante marco no ordenamento jurídico pátrio e como um instrumento efetivo de funcionalização da tecnologia de dados à proteção da pessoa humana, em especial no que pertine às informações sensíveis dos usuários de serviços *on-line* e aplicações diversas, tendo como base o viés constitucional da inviolabilidade da intimidade, honra e imagem. O entendimento adequado do alcance dos princípios que norteiam o tratamento de dados é fundamental para dirimir as controvérsias nesse contexto.

Palavras-chave: Tratamento de dados; Inviolabilidade; Privacidade; LGPD.

ABSTRACT

Information Technology and the possibilities of communication provided by the advancement of the Internet have brought significant controversies regarding the treatment of data. The General Law of Data Protection (Law 13.709/18) presents itself as an important milestone in the Brazilian legal system and as an effective instrument to functionalize data technology to protect the human being, especially regarding sensitive information of users of online services and various applications, based on the constitutional bias of the inviolability of intimacy, honor and image. The adequate understanding of the scope of the principles that guide the treatment of data is fundamental to settle controversies in this context.

Keywords: Data processing; Inviolability; Privacy; LGPD.

SUMÁRIO

INTRODUÇÃO 9

1. CAPÍTULO 1 11
1.1 CONTORNOS SOCIAIS E HISTÓRICOS 11
1.2 PRIVACIDADE DE DADOS PESSOAIS 13
1.3 PRINCÍPIOS APLICÁVEIS 15
1.4 TRATAMENTO DE DADOS SENSÍVEIS 20
1.5 CONTROVÉRSIA JURÍDICA 20
1.6 OBSERVAÇÕES SOBRE PRIVACIDADE E LGPD 22

2. CAPÍTULO 2 26
2.1 FUNDAMENTOS CONSTITUCIONAIS DO DIREITO À PRIVACIDADE 26
2.2 A EMENDA CONSTITUCIONAL Nº 115/2022 32
2.3 LEGISLAÇÃO CORRELATA SOBRE A TEMÁTICA 36
2.4 BIG DATA E A INTERNET DAS COISAS 41

3. CAPÍTULO 3 45
3.1 CONTROVÉRSIAS DA LEI GERAL DE PROTEÇÃO DE DADOS 45
3.2 DADOS X INFORMAÇÃO X CONHECIMENTO 45
3.3 UTILIZAÇÃO DE COOKIES 47
3.4 O CONSENTIMENTO DO USUÁRIO 49
3.5 INCIDENTES DE SEGURANÇA DE DADOS PESSOAIS 55
3.6 LEGÍTIMO INTESSE DO CONTROLADOR 58
3.7 ANONIMIZAÇÃO E PSEUDOMINIZAÇÃO DE DADOS PESSOAIS 62

CONSIDERAÇÕES FINAIS 66
REFERÊNCIAS 72

INTRODUÇÃO

A vigência e amplitude da Lei Geral de Proteção de Dados – LGPD (Lei 13.709/2018) tem causado perplexidade para muitas empresas que precisam se adaptar ao novo sistema legal. Ao estabelecer os parâmetros legais de proteção de dados pessoais, a legislação busca garantir o mandamento constitucional de proteção à intimidade, à honra e à imagem das pessoas. Numa sociedade marcada pela forte presença das redes e mídias sociais, a ênfase na segurança da informação é condição indispensável para que não haja exposição de dados sensíveis de clientes e possíveis fraudes por terceiros inescrupulosos.

Adotando a terminologia apresentada no início do século por Zygmunt Bauman (2001), a “modernidade líquida” é a fase atual da história na qual o que antes era sólido tornou-se liquefeito. Não existe estabilidade nos acordos firmados entre as pessoas, pois é um tempo marcado pela efemeridade das relações e construtos sociais, sendo eficazes somente enquanto forem convenientes. Sendo assim, enfatiza-se a importância da cautela com que os dados digitais das pessoas devem ser tratados. Justifica-se a pesquisa em favor deste aspecto garantista que a LGPD busca implementar, regendo as relações digitais de modo que a intimidade, a honra e a imagem das pessoas não se tornem liquefeitas ao sabor dos humores dos conglomerados econômicos ou poderes governamentais.

Neste diapasão, apresenta-se como problemática a existência de controvérsias entre as medidas de segurança da informação e a própria Lei Geral de Proteção de Dados, no que tange ao aspecto de salvaguardar a intimidade, honra e imagem das pessoas. Num mundo cada vez mais globalizado, tecnológico e informacional, as pessoas são representadas por bytes, arquivados em vários bancos de dados na rede mundial de computadores. Sendo assim, os cadastros feitos em lojas virtuais ou bancos digitais devem ser utilizados com parcimônia pelas empresas responsáveis pela guarda destes dados pessoais, em razão da previsão constitucional no Inciso X do Art. 5º da Constituição Federal que aponta a garantia de inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, e ainda assegura o direito a pedir indenização pelo dano material ou moral decorrente de sua

violação. Nessa esteira, surgem algumas controvérsias justificáveis e injustificáveis para aplicação da Lei Geral de Proteção de Dados, possibilitando a investigação acurada sobre tais controvérsias.

O homem na modernidade líquida tem sido reduzido aos cadastros informacionais e os dados sensíveis pessoais podem ser utilizados de modo leviano por empresas com práticas abusivas. Nota-se ainda a perspectiva de monetização de controle e fiscalização governamentais. A explicitação dos critérios que favorecem e dificultam a aplicabilidade da LGPD serve como ferramenta para diagnóstico de pontos em que a legislação de proteção de dados pode ser aperfeiçoada. Justifica-se a problematização deste tema de pesquisa com base nas divergências entre cientistas de dados e juristas no que pertine aos fundamentos da inviolabilidade da intimidade, honra e imagem frente aos ditames legais que regem a matéria de segurança da informação no Brasil.

A ocorrência de inúmeras fraudes no tocante ao pagamento do Auxílio Emergencial pela Caixa Econômica Federal, em razão da pandemia de Covid-19, revela o lado obscuro da proteção de dados pessoais. Ainda se faz necessário maior investimento em mecanismo de segurança da informação que viabilizem e assegurem a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações. Neste sentido, o poder governamental precisa apontar direcionamentos em face do que estabelece a Lei Geral de Proteção de Dados Pessoais, em especial no que toca a imagem, honra e intimidade das pessoas.

Portanto, o presente trabalho de conclusão de curso tem por objetivo explicitar as controvérsias que existem na seara da proteção de dados em correlação com os direitos civis garantidos pela Carta Magna brasileira, considerando o que dispõe a LGPD (Lei 13.709/18), os fundamentos constitucionais sobre privacidade, inviolabilidade da intimidade, imagem e honra das pessoas bem como as medidas de segurança de informação adequadas tecnicamente em consonância com a Lei Geral de Proteção de Dados. A metodologia baseou-se em densa pesquisa bibliográfica sobre a temática em periódicos e livros sobre proteção de dados e afins.

Capítulo 1

1.1. CONTORNOS SOCIAIS E HISTÓRICOS

Na história do homem, é marcante a premente necessidade da utilização de informação para o desenvolvimento social e cultural. De fato, a informação é indispensável para a comunicação entre as pessoas e as diferentes sociedades estabelecidas pelos seres humanos. Sendo assim, o tratamento que é direcionado à informação ou à qualidade bruta de dados perpassou por um processo evolutivo que se confunde com a própria conscientização do homem em suas interações sociais. Com o avanço da história, o tratamento jurídico com respeito à intimidade, honra e imagem das pessoas também foi sendo aperfeiçoado para preservar direitos no âmbito da privacidade e foro íntimo de cada indivíduo. Neste sentido, André Luís Martins Bezerra e Paul Hugo Weberbauer (2019) asseveram que um dos maiores avanços recentes na comunicação humana é a popularização da Internet e a revolução tecnológica de massas trazida por ela.

Frise-se ainda que, com o desenvolvimento da Internet, a esfera de privacidade do indivíduo foi sendo reduzida em razão da avalanche de dados pessoais que trafega na rede mundial de computadores a cada instante. Na atual era digital, a proteção da pessoa humana relaciona-se umbilicalmente com os dados pessoais, especialmente os dados sensíveis, que potencializam atos de discriminação e desigualdade. Ademais, o uso da internet e das redes sociais como plataformas da comunicação digital proporcionou rápido avanço de propagação da informação. Como afirma Manuel Castells (2013), em seu livro Redes de Indignação e Esperança, a comunicação digital é multimodal, permitindo a referência constante a um hipertexto global de informações. Para o autor, “os seres humanos criam significado interagindo com seu ambiente natural e social, conectando suas redes neurais com as redes da natureza e com as redes sociais.” (CASTELLS, 2013, p. 40). Portanto, a multimodalidade é característica intrínseca à atual era informacional, proporcionando um acelerado processo de digitalização de dados e disseminação de informações, que muitas vezes extrapolam limites e violam princípios de proteção à privacidade pessoal.

Poderosas empresas, fortes conglomerados econômicos e governos de Estados detêm dados pessoais de usuários de seus serviços, tais como documentos de identificação, problemas de saúde, histórico escolar, experiência profissional, quantidade de filhos, dentre outros. Tornou-se a marca indelével do nosso tempo a adoção do modelo empresarial e governamental em rede global, utilizando-se dos protocolos de Internet como meios de armazenagem, tratamento e difusão das informações. Ainda, na obra Sociedade em Rede, o autor Manuel Castells (2011) reverbera a ideia do capitalismo informacional, que tem um apego de busca constante e crescente pelo desenvolvimento tecnológico e maior capacidade de processamento de informações por parte das empresas e governos. Neste cenário, necessário se faz examinar amiúde quais os reflexos das novas tecnologias da informação na privacidade individual, especialmente naqueles direitos fundamentais que são albergados constitucionalmente. A forte influência da tecnologia, em especial por conta da conectividade contínua, marca a sociedade hodierna, na qual tudo gira em torno da coleta e da aplicação de dados para os mais diversos fins – o que impõe uma releitura dos caminhos pelos quais se pode zelar pelo direito fundamental à intimidade, honra e imagem pessoal (FALEIROS, 2019). Num mundo cada vez mais conectado, marcado pelas redes sociais, transações on-line e modelos de negócio em nuvem, é importante acrescentar que a grande circulação dos dados pessoais no meio intangível da Internet "facilita o acesso de terceiros a todas as informações necessárias para praticar qualquer ação, inclusive crimes praticados por cibercriminosos." (GERMANI D'AVILA; SILVA; ARAÚJO, 2020, p. 30).

Conforme demonstrado por Alexandre C. Mantovani e Fabiano Menke (2019), a proteção dos dados pessoais foi alçada à condição de direito fundamental autônomo na Carta dos Direitos Fundamentais da União Europeia[1], e atualmente possui estreita relação com a proteção da dignidade da pessoa humana, dos direitos da personalidade e da privacidade, pelo potencial lesivo do tratamento de dados pessoais envolvido. Sobressai a relevância de se avaliar a Lei Geral de Proteção de Dados –

[1] Artigo 8º. Protecção de dados pessoais. 1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação. Carta dos Direitos Fundamentais da União Europeia (2000/C364/01). Disponível em: <http://www.europarl.europa.eu/charter/pdf/text_pt.pdf >. Acesso em 22.06.2021

LGPD (Lei 13.709/18) e seus reflexos à luz da Constituição Federal de 1988 no que tange à preservação da intimidade, honra e imagem das pessoas. Busca-se compreender a Lei Geral de Proteção de Dados como um importante marco jurídico, que se evidencia um potencial instrumento de funcionalização da tecnologia à proteção da pessoa humana, em especial no que pertine a informações sensíveis.

1.2. PRIVACIDADE DE DADOS PESSOAIS

Atualmente, prevalece o paradigma da sociedade informacional, em que os dados e informações assumem papel de destaque para o dinamismo da vida em rede. Com este pano de fundo, urge a necessidade de proteção dos dados pessoais, radicado fundamentalmente no direito à privacidade, tendo em vista a capacidade que o tratamento inadequado dos dados pode trazer à lume aspectos íntimos e privados dos titulares. Nota-se que evolução tecnológica em escala global, aliada com a integração econômica e social, bem como o aumento do intercâmbio de dados entre entes públicos e privado, trouxeram novos desafios em matéria de proteção de dados pessoais. Ademais, a privacidade dos usuários de redes sociais e e-mails gratuitos está continuamente exposta a diversas e significativas ameaças. Neste contexto, digno de nota é o papel que a legislação desempenha, apontando direcionamentos que buscam efetivar direitos decorrentes do princípio régio da dignidade da pessoa humana, presente em praticamente todo o ordenamento jurídico brasileiro. Assim, reputa-se crucial para o equilíbrio das tensões sociais, agora em rede informacional, que haja a devida valoração e sanção das práticas errôneas.

Mesmo em data anterior à publicação da LGPD, Tatiana Malta Vieira (2007, p. 30) já defendia que o direito à privacidade consiste em um “direito subjetivo de toda pessoa não apenas de constranger os outros a respeitaram sua esfera privada, mas também de controlar suas informações de caráter pessoal resistindo às intromissões indevidas provenientes de terceiros. ” Ainda é importante asseverar que o direito à privacidade é um desdobramento do direito da personalidade, cujo fundamento está tanto da Constituição Federal de 1988 (art. 5º, incisos X, XI e XII), quanto na legislação infraconstitucional. O direito à privacidade “implica em um dever geral de abstenção que comporta a autodeterminação do indivíduo tanto na determinação do que faz

parte da sua privacidade quanto do que deseja compartilhar" (MANTOVANI; MENKE, 2019, p. 20). Desse modo, exsurge como pináculo da privacidade a autodeterminação do indivíduo quando ao que deseja ou não compartilhar, restringindo conforme queira o consentimento referente aos seus dados pessoais.

Com base na doutrina de Maria Helena Diniz, fundamenta-se que a vida privada envolve forma exclusiva de convivência. Nesta toada, o direito à vida privada tem como conteúdo estrutural a permissão de resistir à devassa na esfera pessoal, gerando uma conduta negativa de todos, ou seja, o respeito à privacidade (DINIZ, 2016). Essa percepção envolve a privacidade do indivíduo intrinsicamente ligada à valoração principiológica da personalidade humana em seu contexto social, dentro do espectro digital e multifacetado de proteção de dados que compõe o atual cenário. O direito civil brasileiro tem entendido os direitos de privacidade e consentimento digital como decorrentes lógicos do direito da personalidade. Neste sentido, salienta-se que o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais.

A privacidade é comumente relacionada a uma ideia de exclusividade da esfera individual, ou seja, o ser humano tem uma esfera de sua personalidade que decidiu não revelar, caso queira assim. Insta salientar que a privacidade foi incorporada à Declaração Universal dos Direitos Humanos no artigo 12, que traz a seguinte redação: "Ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem ataques à sua honra e reputação. Todos os seres humanos têm direito à proteção da lei contra interferências ou ataques." Considerando que a privacidade pessoal foi elevada à condição de direito humano fundamental, José Faleiros (2019, p.187) expõe que "a delimitação de marcos regulatórios voltados especificamente à tutela de contingências relacionadas ao uso da Internet é uma tendência inescapável na sociedade da informação".

Natalia Melo de Moura e Cristiniana Freire (2019) apontam que a Constituição Federal resguarda o direito à privacidade de modo estritamente relacionado com o direito à vida, à dignidade da pessoa humana e à liberdade, pressupostos norteadores do Estado Democrático de Direito. Ademais, o direito à privacidade tem como

desiderato a proteção da esfera íntima dos indivíduos de intromissões externas não permitidas, seja pelo Estado ou por terceiros, sempre primando pelo exercício da personalidade de forma livre e digna. Nesse trilhar, a autora aponta também que a pessoa humana detém a faculdade de ter resguardado o seu espectro de existência no mundo físico e subjetivo de interferências internas não autorizadas, tendo como base o viés de proteção institucional e legal que reveste o direito à privacidade (MOURA; FREIRE, 2019). Defendem os autores José L. M. Faleiros e João Victor Rozatti Longhi (2019, p. 189) que “a privacidade é, sem dúvidas, tema de relevância ímpar para o estudo dos efeitos jurídicos experimentados na sociedade da informação. ”

Dados e informações pessoais têm se tornado fonte de vantagens para os seus detentores, sejam vantagens pessoais ou econômicas. O armazenamento e uso adequado dessas informações é fator primordial para o equilíbrio das relações sociais, num mundo cada vez mais conectado. Diego Coelho e Alberto Nogueira Junior (2020) argumentam que o interesse das corporações em obter informações relaciona-se com o princípio da eficiência e do controle social. Assim, pesquisas e censos são realizados para obtenção de maior conhecimento sobre a população e consequente aumento de seu poder de controle sobre os indivíduos.

1.3. PRINCÍPIOS APLICÁVEIS

Em sequência, explicita-se a relevância de alguns termos para o presente estudo. Na Lei Geral de Proteção de Dados (Lei nº. 13.709/18) está assentado que todo dado pessoal tem importância e valor. Conforme asseveram Tefé e Viola (2020), adotou-se um conceito amplo de dado pessoal, sendo definido como informação relacionada a pessoa natural identificada ou identificável. Frise-se que o fato de o indivíduo ser identificado ou identificável afasta do âmbito de proteção dessas normas os dados anonimizados, que são uma espécie de antítese do dado pessoal (FALEIROS, 2019). No entanto, conforme alerta Bioni (2015, p. 17), “partindo do pressuposto que dados anônimos são sempre reversíveis, eles sempre terão o potencial de identificar alguém.” São igualmente considerados como dados pessoais, para as finalidades da Lei 13.709/18 aqueles utilizados para formação do perfil

comportamental de determinada pessoa natural, se esta puder ser identificada. Com base nestes pormenores, a Lei Geral de Proteção de Dados estabelece que qualquer pessoa que proceda o tratamento de dados pessoais, seja ela natural ou jurídica, de direito público ou privado, inclusive na atividade realizada nos meios digitais, deverá ter uma base legal para fundamentar os tratamentos de dados que realizar. Tal premissa tem por objetivo “proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (Lei 13.709/18, art. 1º).

A finalidade da coleta dos dados não pode prescindir de base legal justificada, devendo, portanto, ser previamente conhecida. Essa diretriz diz respeito à relação entre os dados colhidos e a finalidade perseguida pelo agente, conforme preceitua expressamente o Art. 6º da LGPD, que aponta a necessidade de realização do tratamento de dados “para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades”. Exsurge do texto legal que não há margem para utilização indiscriminada dos dados pessoais com finalidade desvirtuada do que foi originalmente acertado mediante consentimento do titular dos dados.

O conceito de consentimento reveste-se de fundamental relevância, tendo em vista que a observância ou violação da privacidade e intimidade estará estritamente relacionada com a manifestação primeva de vontade do titular dos dados pessoais. Considerando a importância do domínio da pessoa sobre seus dados pessoais, a LGPD instituiu um sistema com carga principiológica elevada, com destaque ao consentimento do indivíduo. A própria Lei Geral de Proteção de Dados define consentimento como a “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada” (Art. 5º, inciso XII da Lei 13.709/18). O consentimento do titular apresenta-se no Art. 7º da Lei 13.709/18 como a primeira possibilidade para a realização do tratamento de dados. Nesse caso, o consentimento “deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular” (Art. 8º, Lei 13.709/18).

Convém destacar, portanto, que a finalidade de coleta ou tratamento dos dados tem uma robusta conexão com o consentimento do titular, o que é condição

indispensável para a preservação da intimidade, honra e imagem pessoal no ambiente cibernético. Apontam Teffé e Viola (2020) que a omissão do titular não tem o condão de liberar o consentimento, tendo em vista que somente atos positivos revelam claramente a real manifestação de vontade, como, por exemplo, por meio de click em botão, marcação de opção em caixa (que deve vir desmarcada) ou gravação confirmando a aceitação. Neste trilhar, conforme argumentam Sousa e Tavares Silva (2021) o consentimento se apresenta como aspecto mais delicado para o tratamento dos dados pessoais, considerando que a circulação sobre o processamento, transmissão e compartilhamento dos dados e informações dependem da vontade do titular, o que a própria Lei 13.709/18 denomina de autodeterminação informativa (art. 2º, inciso II).

Outra disposição relevante da Lei 13.709/18 afirma que o consentimento poderá ser revogado a qualquer momento, mediante manifestação expressa do titular, por procedimento gratuito e facilitado, conforme disposto no §5º, do art. 8º, da Lei Geral de Proteção de Dados. Imperioso destacar ainda o teor do § 6º do Art. 7º, que afirma que eventual dispensa da exigência do consentimento do titular não desobrigará os agentes do tratamento das demais obrigações previstas pela LGPD, especialmente da observância dos princípios gerais e da garantia dos direitos do titular. Resta consubstanciada a louvável intenção do legislador visando a proteção dos direitos do titular dos dados pessoais ao eliminar a ausência de consentimento como motivo para a utilização espúria dos dados pessoais. Em consonância com a proteção do hipossuficiente, esses dispositivos legais revelam a preocupação do legislador com a participação do indivíduo no fluxo de suas informações (TEFFÉ; VIOLA, 2020).

Com base em estudos e pesquisas acerca do tema da privacidade no atual cenário de hiperconectividade, Eduardo Magrani (2019) considera que o princípio do consentimento usado como meio principal para permitir o uso dos dados pessoais não tem se mostrado eficaz. Variados abusos praticados pelas empresas nos termos de uso de aplicativos ou sistemas têm sido praticados de forma recorrente, o que resulta inevitavelmente, na violação dos direitos de personalidade, em especial no tocante à proteção da honra e imagem prevista no texto da Carta Magna brasileira. Os dispositivos onipresentes conectados à Internet, em especial os smartphones, são

capazes de coletar diversos dados do usuário (por exemplo, a localização por GPS) e armazená-los não somente em uma memória local do dispositivo como também na nuvem da empresa que os idealizou ou de terceiros, sem que o usuário saiba. Não se sabe também como os dados são armazenados e tratados, o que tem gerado uma preocupação constante com a segurança da informação (MAGRANI, 2019).

Neste sentido, expressa-se como relevante e necessária a preservação do princípio da transparência, que tem como enfoque principal a possibilidade de o titular ter acesso às informações sobre a realização do tratamento dos dados e seus controladores. A Lei 13.709/18, no art. 10, em seu § 2º, prevê que o controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse. Aos titulares dos dados devem ser garantidas informações claras, precisas e facilmente acessíveis sobre o tratamento e sobre os respectivos agentes de tratamento, resguardados os segredos industriais e comerciais. Portanto, a utilização de jargões técnicos que dificultam o entendimento por parte de pessoas leigas não se coaduna com o propósito do princípio da transparência, pois o que se procura garantir é que as pessoas possam compreender do que se trata a informação correspondente, considerando que é imprescindível que o titular saiba o que ocorrerá com os seus dados após tratados (PESTANA, 2020).

Corrobora com essa argumentação o que prevê o dispositivo legal sob análise, Lei 13.709/18, no art. 44, quanto aponta que o tratamento de dados pessoais será considerado irregular quando não observar a legislação pertinente ou quando não fornecer a segurança necessária para o titular considerando o modo de realização do tratamento de dados, o resultado e os riscos bem como as técnicas disponíveis no momento da realização. A partir desses elementos, o titular poderá identificar se estão sendo observados os dispositivos da lei e o princípio da transparência no tratamento de seus dados e tomar as medidas necessárias para garantir a efetividade de seus direitos. Em adição, com fulcro no princípio da transparência, o titular poderá optar ou rejeitar um determinado produto ou serviço que opera mediante coleta de dados, inclusive por meio de consentimento específico para escolher certo tipo de tratamento realizado pelo controlador ou operador (SOARES, 2019).

Afigura-se relevante destacar o princípio do livre acesso, previsto no art. 6º, inciso IV, da LGPD, pelo qual é garantida aos titulares “consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais” (Lei 13.709/18). Em decorrência desse princípio, os titulares de dados pessoais têm assegurado o acesso aos seus dados pessoais tratados pelo controlador, isto é, podem exigir do controlador cópia dos dados pessoais de sua titularidade que sejam objeto de tratamento pelo controlador. Ainda o titular pode exigir que dados pessoais tidos como desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei Geral de Proteção de Dados sejam anonimizados, bloqueados ou eliminados. Gustavo Tepedino (2020) destaca que esse direito deriva do princípio da necessidade, previsto no artigo 6º, inciso III, da LGPD, pelo qual se garante a “limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados” (Lei 13.709/18).

1.4. TRATAMENTO DE DADOS SENSÍVEIS

Considerando a temática da proteção de dados pessoais em sua amplitude, destacam-se as diferenças de tratamento estabelecidas para dados que são considerados sensíveis. A definição de dados sensíveis alinha-se com a essência deste trabalho de pesquisa, cuja ênfase está nas controvérsias entre as medidas de segurança da informação que fundamentam a inviolabilidade da intimidade, da honra e da imagem das pessoas e a Lei Geral de Proteção de Dados. Intimidade, honra e imagem são conceitos subjetivos que influenciam e garantem a personalidade do ser humano, albergando os valores pessoais, espirituais, bem como informações que dizem respeito à origem raça, cor, sexo, hábitos de vida, entre outros.

Segundo o art. 5º, inciso II, da Lei nº 13.709/18, dados sensíveis versam sobre origem racial ou étnica, convicção religiosa, opinião política e filiação a sindicato ou a organização de caráter religioso, filosófico ou político. Acrescentem-se à lista os dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos. Pela relevância dessas informações do ponto de vista dos direitos e liberdades fundamentais da pessoa humana, a violação de dados sensíveis propicia riscos significativos para seu

titular. Salientam, com razão, Teffé e Viola (2020) que o tratamento espúrio desses dados pode resultar em discriminação do titular, devendo, portanto, ser protegidos de forma ainda mais rígida.

A Lei Geral de Proteção de Dados, no Art. 11, dispensa a necessidade de consentimento do titular para tratamento dos dados sensíveis em algumas hipóteses, tais como: o tratamento compartilhado de dados necessários à execução, pela Administração Pública, de políticas públicas previstas em leis ou regulamentos; a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; a proteção da vida ou da incolumidade física do titular ou de terceiros; e garantia da prevenção à fraude e à segurança do titular. Percebe-se que a Lei 13.709/18 trouxe à tona situações *sui generis* que reclamam do Poder Público uma medida protetiva ao cidadão, considerando a urgência e necessidade de utilização dos dados para o bem do indivíduo enquanto integrante do tecido social. Como será discutido, há controvérsias nestas situações excepcionadas, mesmo considerando um controle ainda mais rígido dos dados considerados sensíveis, inclusive mediante técnicas de anonimização por algoritmos e técnicas de Inteligência Artificial.

Imperioso observar que o Estado é o detentor de grande quantidade de dados de seus cidadãos, incorrendo também numa responsabilização ainda maior perante o uso desvirtuado das informações armazenadas. Conforme assevera Diego Damasceno Coelho (2020, p. 87) o uso de informações sensíveis “pode auxiliar na adoção de medidas profiláticas e preventivas, bem como no controle de epidemias, mas jamais tais informações devem ser utilizadas para justificar atitudes discriminatórias e desiguais.”

1.5. CONTROVÉRSIA JURÍDICA

A título exemplificativo das controvérsias jurídicas que envolvem a temática, importante destacar o julgamento da Ação Direta de Inconstitucionalidade – ADI 6387 MC-REF/DF. Essa ADI buscou atacar a edição da Medida Provisória nº 954/2020. Restou assentado que o tratamento e a manipulação de dados pessoais devem

observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. A Medida Provisória nº 954/2020 tinha como objetivo determinar que as operadoras de telefonia fixa (ou Serviço Telefônico Fixo Comutado –STFC) e de comunicações móveis (ou Serviço Móvel Pessoal–SMP) disponibilizassem à Fundação Instituto Brasileiro de Geografia e Estatística (IBGE) suas bases de dados, com a relação dos nomes, números de telefone e endereços de seus usuários, para que, no período da pandemia do coronavírus (Covid-19), as estatísticas oficiais produzidas pela instituição pudessem ser formuladas a partir de entrevistas não presenciais, preservando a integridade física de seus pesquisadores. A Ministra Rosa Weber, atuando como relatora, deferiu medida liminar para suspensão da Medida Provisória 954/2020, tendo em visa que a MP não previa exigência alguma quanto aos mecanismos e procedimentos para assegurar o sigilo, a higidez e o anonimato dos dados compartilhados. Em síntese, não satisfazia as exigências que exsurgem do texto constitucional no tocante à efetiva proteção de direitos fundamentais dos brasileiros. Mesmo em tempos de pandemia, não se pode flexibilizar direitos de modo arbitrário, configurando-se inoportuna a necessidade de se combater um mal sanitário com a prática por demais nociva de violação da privacidade de dados pessoais sem balizas claramente delineadas.

O artigo 17 da Lei Geral de Proteção de Dados (Lei 13.709/18) prevê expressamente que “toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei”. Depreende-se do dispositivo legal que os dados pessoais são de titularidade da pessoa natural a quem dizem respeito, e, portanto, não pertencem aos agentes de tratamento. Conforme argumenta Bezerra (2020, p. 80) torna-se temerário “esperar que a regulação da internet e da proteção de dados pessoais, em um Estado Democrático de Direito, dependa exclusivamente da vontade política de qualquer um dos Poderes da República”. O Poder Executivo através da publicação de medidas provisórias e decretos pode extrapolar para o autoritarismo e fomentar a invasão de privacidade. No sentido oposto, os princípios da governança da Internet idealizam a construção de um ambiente digital democrático, universal, colaborativo e que atenda às necessidades de todos os setores sociais (BEZERRA,

2020). A violação de balizas constitucionais que asseguram a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, conforme previsto no Art. 5º, inciso X da CF/1988, é questão que merece atenção e debate contínuos, sob pena de termos uma sociedade marcada pela devassidão cibernética.

Verifica-se que o legislador inseriu na Lei Geral de Proteção de Dados a garantia de direitos previstos na Constituição Federal, considerando a estreita vinculação entre a titularidade dos dados pessoais e os direitos fundamentais da liberdade, da intimidade e da privacidade. Conforme argumentam Viviane Maldonado e Renato Ópice Blum (2020) não há desvinculação dos dados pessoais da pessoa de seu titular quando aqueles passam a ser tratados pelo controlador ou pelo operador. Mesmo que o titular disponibilize irrestritamente os seus dados pessoais por meio de consentimento, permanece com ele a plena titularidade, em liame indissociável.

1.6. OBSERVAÇÕES SOBRE A PRIVACIDADE E LGPD

É oportuno considerar que a privacidade, enquanto direito fundamental pertencente ao indivíduo, pugna pela completa proteção dos dados pessoais. Para esse desiderato, a Lei 13.709/18 afirma quais os direitos assegurados aos titulares dos dados, além de descrever várias regras protetivas atreladas aos princípios da transparência e da finalidade, como forma de garantir seu pleno exercício (MALDONADO; BLUM, 2020).

Em face dos ditames legais e constitucionais que se impõem, faz-se necessário que as empresas e governos aprimorem seus mecanismos de governança. Em síntese, “a governança é um sistema que conduz, monitora e motiva as empresas e estreita a relação entre sócios, conselho de administração, diretoria, órgãos de fiscalização e demais partes interessadas.” (GERMANI D’AVILA; SILVA; ARAÚJO, 2020, p. 83). A Lei Geral de Proteção de Dados em seu artigo 50, § 3º, dispõe acerca da criação de regras de boas práticas e governança nas empresas, que devem ser publicadas, atualizadas e acessíveis aos interessados, com reconhecimento e ampla divulgação. Deste modo os controladores e operadores de dados, nos termos do disposto no caput do artigo 50 da LGPD, respeitando suas competências, podem

elaborar regras de boas práticas e governança em relação ao tratamento de dados, em especial “as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais” (Lei 13.709/18).

Considerando esse contexto, ao realizar tratamento de dados pessoais, torna-se imprescindível a implementação de medidas técnicas e administrativas que são capazes de efetivamente proteger os dados de acessos não autorizados, perda, destruição, alteração ou divulgação indevida, assim como prevenir quaisquer incidentes que possam causar danos aos titulares dos dados, especialmente aqueles fundados na intimidade, privacidade, honra e imagem da pessoa humana. Com base no princípio universal na dignidade da pessoa humana, o cidadão possui o direito de determinar o fluxo de suas informações na sociedade. Dessa forma, o princípio da autodeterminação informacional garante ao cidadão o livre desenvolvimento da sua personalidade (FALEIROS, 2019).

Por oportuno, impõe-se considerar que o Poder Público deve atuar no sentido de disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população, de tal forma que possa garantir ao indivíduo a capacidade de controle e disposição sobre as próprias informações que dizem respeito à sua personalidade. Sobreleva-se a importância de ações educativas sobre a proteção de dados, visto que essa tutela dos direitos da pessoa humana justifica-se no próprio ordenamento jurídico, não sendo possível olvidar a responsabilidade do próprio cidadão em conhecer o regramento legal, especialmente a Lei de Acesso à Informação (Lei n. 12.527/11), o Marco Civil da Internet (Lei n. 12.965/14) e a Lei Geral de Proteção de Dados (Lei. 13.709/18). Esses dispositivos legais apresentam o arcabouço de prerrogativas e garantias que visam dar concretude à questão da inviolabilidade da intimidade, honra e imagem da pessoa, conforme disposto no texto da Constituição Federal de 1988. Nesta esfera, a LGPD figura como um marco divisor na questão do tratamento de dados pessoais por empresas ou pelo Poder Público, ensejando responsabilidades e deveres que devem ser atendidos para a preservação incólume da vida privada das pessoas que fazem uso dos serviços e aplicações de Internet ou cadastros em bancos de dados de caráter privado ou público.

Revela-se necessário considerar a responsabilização prevista na Lei 13.709/18 para danos causados em decorrência da coleta ou tratamento de dados com medidas ou finalidades destoantes do regramento. Determina o art. 42 da Lei Geral de Proteção de Dados que “o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo”. Conforme aduz Humberto Lima (2021, p. 143), “a Lei estabelece dois requisitos para a responsabilização judicial: a) a provocação de um dano e b) a irregularidade do tratamento. ” Explica-se que uma operação de tratamento de dados pessoais será considerada irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar.

O autor aponta ainda que tanto o dano patrimonial quanto o moral serão indenizáveis. Nessa esteira, o dano patrimonial resulta de prejuízos materiais sofridos em face da violação indevida de dados do titular, geralmente associados a golpes em contas bancárias ou utilização fraudulenta de cartão de crédito. Na esfera do dano moral, geralmente a violação da privacidade afeta negativamente a imagem e a honra do titular ou faz nascer uma série de transtornos decorrentes do vazamento ou utilização indevida dos dados. Neste caso, não se trata de um mero dissabor da vida em sociedade, cabendo reparação civil nos termos estabelecidos na legislação pertinente ao tema (LIMA, 2021).

Observa-se que as controvérsias entre as medidas de segurança da informação que fundamentam a inviolabilidade da intimidade, da honra e da imagem das pessoas e a LGPD (Lei Nº 13.709/ 2018), tangenciam a própria questão da responsabilização civil e administrativa por danos sofridos. Sobressai da presente análise teórico-conceitual que, de um lado tem-se o Estado e conglomerados econômico-empresariais com enorme poderio na operacionalização de dados pessoais, e o do outro apresenta-se pessoa natural titular dos dados como hipossuficiente, que almeja a não violação da sua intimidade com fulcro nos ditames constitucionais que estão presentes na Carta Magna de 1988.

Há na Lei Geral de Proteção de Dados (Lei 13.709/18) algumas incongruências e excepcionalidades que requerem análise mais detida, por exemplo, no tocante à

questão controversa sobre transferência de dados pessoais constantes de bases de dados do Poder Público a entidades privadas. Constitui-se relevante a investigação e prevenção de fraudes e irregularidades, bem como a segurança e a integridade do titular dos dados, desde que vedado o tratamento pelo Governo e empresas para outros propósitos não declarados. Neste sentido, o princípio da finalidade talvez seja o principal regulador das atividades de tratamento de dados pessoais. Afinal, para que os dados pessoais sejam tratados pelos operadores ou controladores deve ficar claro ao titular dos dados qual é o propósito legítimo, específico e explícito da coleta de seus dados (PESTANA, 2020).

As controvérsias entre as medidas de segurança da informação que fundamentam a inviolabilidade da intimidade, da honra e da imagem das pessoas e a LGPD, giram em torno dos princípios aplicáveis ao tratamento de dados pessoais do titular, especialmente os princípios da finalidade e da transparência. Importante diagnosticar precisamente se a operação e tratamento realizado com os dados, em face das medidas de segurança necessárias, viola os princípios e por consequência a personalidade nos aspectos da intimidade, honra e imagem. Neste sentido, conclui Lima (2021, p. 131) que são requisitos essenciais para a boa governança de dados: “confiança, transparência e participação, tendo como objetivo estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular”.

Capítulo 2

2.1. FUNDAMENTOS CONSTITUCIONAIS DO DIREITO À PRIVACIDADE

A noção geral de privacidade já estava inserida no ordenamento jurídico brasileiro antes da promulgação da Lei Geral de Proteção de Dados, uma vez que já constavam na própria Constituição Federal de 1988 as diretrizes sobre esta temática. O artigo 5º, inciso X, já estabelecia a garantia da inviolabilidade da vida privada e da intimidada no rol dos direitos e garantias fundamentais. Danilo Doneda observa, no entanto, que existia um grau significativo de permissividade concernente à utilização de informações pessoais no Brasil, mesmo em razão de determinações constitucionais como o artigo 5º, inciso XII, que trata sobre a inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas (DONEDA, 2019). Isto se deve ao fato que os tempos mudaram com o surgimento de novos meios de intercomunicação e com o crescimento vertiginoso das transações *on-line* feitas por intermédio da rede mundial de computadores.

Com o passar dos anos e aprimoramento das tecnologias informacionais, estabeleceu-se como essencial a promoção e a proteção ampla das informações pessoais e privacidade, como direitos fundamentais responsáveis pela concretização do livre desenvolvimento da personalidade, das liberdades individuais e coletivas e da não discriminação. Conforme argumenta Maimone (2022), a proteção de dados pessoais passou a ter importância fundamental no cenário da sociedade da informação, a ponto de ser necessário que surjam “mecanismos aptos a afastarem ou mitigarem o risco de violação, uma vez que esta ensejaria consequências nocivas a diversos fatores da pessoa humana e ao Estado Democrático de Direito. ”

A pauta da proteção de dados pessoais não é um debate meramente incidental no atual contexto jurídico brasileiro. Em verdade foi desenvolvida ainda na fase do processo constituinte, do qual resultou a Constituição Federal de 1988, pioneira mundialmente ao contemplar a chamada ação de Habeas Data. À luz do artigo 5º, inciso LXXII, da CF e do art. 7º da Lei nº 9.507/1997, o habeas data destina-se a assegurar o acesso a informações relativas, pertinentes, intrínsecas à própria pessoa

do impetrante, ou seja, dados pessoais íntimos, personalíssimos, constantes de cadastros ou bancos de dados, com o objetivo precípuo de conhecê-los e/ou retificá-los. Sobre este remédio constitucional, o Supremo Tribunal Federal já estabeleceu que a ação de *habeas data* busca a proteção da privacidade do indivíduo contra abuso no registro e/ou revelação de dados pessoais falsos ou equivocados (STF, Tribunal Pleno, HD 90 AgR, Rel. Min. Ellen Gracie, DJe 19-03-2010).

Com o advento e implementação da rede mundial de computadores, houve uma vasta ampliação das relações negociais que passam a ser realizadas de forma digital, utilizando a alta informatização, uso de assinatura eletrônica, compras on-line no e-commerce, geolocalizadores, operações financeiras, redes sociais, celulares, dispositivos digitais, perfil de compras, entre outros meios, por causa dos significativos avanços vinculando tecnologias e relações negociais. As novas tecnologias demonstram a preocupação central em relação à confiabilidade, no sentido de assegurar as relações negociais deste imensurável contexto digital. Neste amplo leque de transações, os dados pessoais são considerados moeda bastante valiosa, tornando imprescindível a tutela jurídica das demandas complexas do ecossistema digital (DINIZ, 2020).

A perda de privacidade como resultado da violação de dados pessoais pode causar discriminação ilegal, exposição indesejada, preconceito religioso, preconceito étnico, sofrimento emocional, perda financeira, transações falsas com cartão de crédito, dentre outros prejuízos à pessoa humana. A violação de privacidade dos dados digitais pode causar uma ameaça aos direitos, liberdades e escolhas. Como exemplo, as pessoas de má índole que buscam tomar empréstimo de um banco em nome de terceiros cujos dados foram violados. Ou então criminosos condenados que querem escapar da mácula de seus registros, gerando inconvenientes por não conseguirem mais recolocação no mercado após vazamento de dados do histórico prisional. Diante de tal cenário, imperioso que o ordenamento jurídico estabeleça parâmetros legais para o tratamento e disponibilização de dados pessoais.

Conforme argumentam Scoble e Israel (2014), neste cenário turbulento de enorme quantidade de dados que circulam nas redes de corporações, aplicações de Internet ou sites governamentais, “cinco forças tecnológicas favorecem uma

tempestade perfeita: dispositivos móveis, mídias sociais, big data, sensores e serviços baseados em localização.” No livro *Age of Context – Mobile, Sensors, Data and the Future of Privacy* (2014), os autores afirmam que essas cinco forças estão mudando a experiência de qualquer pessoa como comprador, cliente, paciente, espectador ou viajante online. Todas essas cinco forças – celular, mídia social, dados, sensores e localização – desfrutam atualmente de um ciclo virtuoso: a adoção rápida destas tecnologias reduz os preços, o que, por sua vez, gera mais incremento das forças, o que completa o ciclo, reduzindo ainda mais os preços das transações digitais.

O homem moderno está inserido em uma economia movida e orientada pelo uso de dados pessoais. Sabe-se, com certeza, que a cada dia novas tecnologias são desenvolvidas e desafiam a dogmática jurídica. Em face das enormes transformações pelas quais o mundo passa, importante considerar que está em curso uma verdadeira revolução do cliente, na qual o mundo está sendo remodelado pela convergência de tecnologias de nuvem social e dispositivos móveis. A combinação dessas tecnologias nos permite conectar tudo de maneira instantânea e redireciona drasticamente a maneira como o trabalho e a vida funcionam. É importante frisar que num Estado democrático regido pelo Direito, a proteção de dados pessoais precisa ter garantias legais para evitar quaisquer arbítrios. O objetivo é trazer segurança jurídica às relações e interações nos ambientes digitais que afetem direta ou indiretamente a dignidade da pessoa humana ao fornecer dados para sistemas múltiplos e aplicações variadas.

Para os autores Fornasier e Knebel (2021) há a ascensão de uma nova mercadoria, que não é fruto necessariamente do trabalho industrial: a mercadoria dos dados que tem como base as plataformas de redes sociais. Nessas plataformas os usuários entregam seus dados em troca de serviços anunciados como gratuitos, mas que são transformados em mercadoria pelas empresas responsáveis pela sua oferta no mercado. Desta forma, o chamado “capitalismo de vigilância”, definido por Shoshana Zuboff (2019), gera uma consequência em destaque: “a formação de mercados de comportamentos futuros, ou seja, da mercantilização dos dados com o objetivo de prever e determinar comportamentos. ” A pesquisadora entende que as tecnologias de informação digital são adequadas e usadas para coletar dados comportamentais em larga escala sobre os usuários de serviços, que são apenas

parcialmente necessários e usados para melhorar produtos e serviços. É importante delinear essa ênfase atual da exploração dos dados pessoais como fim em si mesmo, a fim de ressaltar que o direito à proteção de dados precisa ser entendido como essencial à manutenção do próprio Estado constitucional de Direito. Os meios digitais e as redes sociais trazem serviços funcionais e relevantes para as pessoas, mas ao mesmo tempo os interesses corporativos acabam prevalecendo, resultando então numa verdadeira digitalização da vida em rede.

A Constituição Federal de 1988 foi promulgada com uma carga principiológica bastante significativa no quesito de preservação da dignidade da pessoa humana em variados aspectos, inclusive no que diz respeito à privacidade e inviolabilidade da imagem e honra das pessoas. Esta ênfase ganha novos contornos na era informatizada na qual o cidadão está inserido no atual momento, em que a mineração de dados é uma relevante mercadoria para a economia mundial numa dinâmica de atividades complexas e de pouca transparência (WEST, 2019). Diante deste cenário tecnologicamente efervescente, não é prudente esperar que os conglomerados econômicos que utilizam a Internet como meio negocial se pautem apenas pela ética. Confiar somente em princípios éticos dificilmente estará de acordo com a responsabilidade do Estado em fornecer garantias. Considerando-se os riscos associados à digitalização em geral e ao uso da Inteligência Artificial em particular, é indispensável uma lei do Poder Público, ou ao menos um direito pelo qual o Estado possa impor sanções em razão de violações ou vazamentos de dados na rede mundial de computadores ou em sistemas internos de empresas ou órgãos públicos (WOLFGANG, 2021).

Para Bruno Bioni, há fortes conexões entre o princípio da dignidade da pessoa humana e o direito fundamental à proteção dos dados pessoais, mesmo com aspectos compreensivos diversos no âmbito das diferentes ordens jurídicas. O autor destaca que “os dois principais pontos de contato, todavia, são o princípio autonômico (autodeterminação) e os direitos de personalidade, representados pelo direito (de natureza geral) ao livre desenvolvimento da personalidade” (BIONI, 2019). Neste contexto sobrelevam-se os direitos especiais à privacidade e à autodeterminação informativa, igualmente conectados entre si, mas que não esgotam o leque de alternativas. Para o autor, é sabido que nem todo direito fundamental tem um

fundamento direto e um conteúdo em dignidade, mas no caso do direito à proteção dos dados pessoais, o princípio da dignidade da pessoa humana pode e deve ser acionado (BIONI, 2019). Importa considerar a elevada importância dos dados pessoais na constituição do indivíduo na atual sociedade informacional. Ademais, a dignidade da pessoa humana passa a adquirir novos contornos, perpassando pela evolução tecnológica e sociológica da espécie humana e as suas consequências nas diversas relações econômicas no tecido social.

Na perspectiva objetiva dos direitos da pessoa humana, insta salientar o reconhecimento do dever de proteção do Estado, no sentido de que a este incumbe zelar, inclusive preventivamente, pela proteção dos direitos fundamentais dos indivíduos. É imprescindível que o enfoque geral de efetivação dos direitos basilares funcione também contra as agressões provindas de particulares e até mesmo de outros Estados. Define-se, assim, a eficácia irradiante dos direitos fundamentais, visto que os valores por eles exprimidos devem se expandir em todo o ordenamento jurídico, o que abarca também uma abrangência de tais parâmetros na esfera das relações jurídicas entre atores privados. No tocante ao direito fundamental à proteção de dados pessoais, os parâmetros garantidores da sua eficácia sustentam-se também no princípio da dignidade da pessoa humana. Para muitos juristas, muito mais ainda do que um princípio, a dignidade da pessoa humana erige-se à condição de um verdadeiro metaprincípio e identifica um espaço de integridade moral a ser assegurado a todas as pessoas nas diversas relações jurídicas no contexto das interações sociais.

O Supremo Tribunal Federal já vinha reconhecendo o direito à proteção de dados pessoais como direito fundamental autônomo, com fulcro nos princípios constitucionais da dignidade da pessoa humana, da privacidade e intimidade. Destaca-se a autodeterminação informativa e a necessidade de concretizar permanentemente o compromisso com a renovação da força normativa da Constituição em face dos riscos gerados pelo avanço tecnológico. Por exemplo, a Medida Cautelar na ADPF 695/DF, do relator Min. Gilmar Mendes, decisão em sede de liminar de 24.06.2020. Ficou assegurado que a matéria afeta ao compartilhamento de dados entre órgãos e instituições do Poder Público possui extrema relevância para a proteção do direito constitucional à privacidade, situando-se como garantia

elementar de qualquer sociedade democrática contemporânea. O relator salientou em seu voto que o Poder Público de modo geral deve assumir o ônus de apresentar uma justificativa constitucional para qualquer intervenção que de algum modo afete a autodeterminação informacional dos cidadãos.

Na mesma toada desta decisão proferida, igualmente reconhecendo um direito fundamental autônomo à proteção de dados implicitamente positivado, tem-se a ADI 6.387/DF, da relatora Min. Rosa Weber. Nesta importante decisão restou assentado que “o cenário de urgência decorrente da crise sanitária deflagrada pela pandemia global da COVID-19 e a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento não podem ser invocadas como pretextos para justificar investidas visando ao enfraquecimento de direitos e atropelo de garantias fundamentais consagradas na Constituição.” Ademais, a ministra Rosa Weber asseverou que “eventuais restrições ao direito à privacidade, à proteção de dados e à autodeterminação informativa podem e devem ocorrer, posto inexistir direitos absolutos, mas sempre orientadas por parâmetros constitucionais e legais”.

O julgamento da ADI 6.387/DF foi um marco pois tornou expressa a tutela dos dados pessoais como direito fundamental. Ademais o julgamento levou em conta a importância da proteção de dados para a própria manutenção do regime democrático brasileiro, tendo em vista que em todo o mundo há uma crescente preocupação em relação ao aumento da vigilância estatal e a limitação das liberdades individuais. Ficou assentado que não existem dados pessoais neutros ou insignificantes e que a proteção de dados possui dimensão subjetiva (a defesa do titular dos dados) e uma dimensão objetiva, qual seja ao dever de proteção por parte do Estado. Sendo assim, tanto a ação quanto a omissão estatal no quesito privacidade dos dados devem ser rigorosamente controlados.

O Conselho Federal da OAB propôs Ação Direta de Inconstitucionalidade questionando o Decreto nº 10.046/2019. A ADI 6649/DF foi distribuída por prevenção ao Ministro Gilmar Mendes, relator da ADPF 695/DF, que também aborda questões associadas à privacidade, proteção de dados pessoais, compartilhamento de dados pela Administração Pública e constitucionalidade daquele decreto. A ADI defende a

inconstitucionalidade do Decreto por violação do artigo 84, incisos IV e VI, ‘a’, da Constituição Federal (CF), e violação direta dos artigos 1º, *caput*, inciso II e 5º, *caput* e incisos X, XII e LXXII, da CF. O Decreto 10.046/2019, da Presidência da República, dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.

Restou evidenciado, assim, que o Estado só pode realizar tratamentos de dados dentro do âmbito de competência determinado pela legislação vigente e pelos princípios que regem a Administração Pública. Ademais, a Lei 13.709/2018 não autoriza a integração e compartilhamento irrestrito de bases de dados de forma *a priori*, sem levar em conta a finalidade e o contexto em que se insere o tratamento. Qualquer açodamento feito às custas da privacidade pessoal é deletério para o sistema protetivo constitucional da dignidade da pessoa humana, considerando ainda todos os mecanismos de salvaguarda da intimidade e honra dos cidadãos.

2.2. A EMENDA CONSTITUCIONAL Nº 115/2022

Como resultado de debates intensos em torno da temática, em 10 de fevereiro de 2022 foi publicada a Emenda Constitucional 115, que acrescentou o inciso LXXIX ao rol de direitos fundamentais do Art. 5º da Constituição Federal, assegurando, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. Com este avanço, o direito à proteção dos dados pessoais foi inserido no bojo dos direitos fundamentais protegidos constitucionalmente. Ademais, foi atribuída à União a competência material exclusiva do tema, com a inserção do inciso XXVI no Art. 21, para organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei. Ainda, a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais foi assegurada, com o acréscimo do inciso XXX, no Art. 22 da CF/1988. Note-se, no entanto, que já estava consolidada a necessidade de se reconhecer a proteção de dados como direito fundamental autônomo a partir da interpretação, sobretudo, da proteção da inviolabilidade, da intimidade e da privacidade das pessoas.

A garantia dada pela Emenda Constitucional nº 115 para a proteção de dados pessoais repercute de modo a estabelecer status normativo superior em relação a toda legislação brasileira. Nesse diapasão, consolida-se a condição de direito fundamental autônomo, com âmbito de proteção próprio, independentemente da existência de outros direitos fundamentais, como o direito à privacidade. Acrescenta-se ainda o status de cláusula pétrea à proteção de dados, não podendo sofrer nenhuma alteração ou revogação posterior, nem mesmo por Proposta de Emenda à Constituição (PEC). Ressalta-se ainda a aplicabilidade imediata aos casos concretos, o que dispensa qualquer regulamentação posterior para que o direito seja assegurado. A LGPD funciona então como vetor normativo infraconstitucional que direciona as ações institucionais para salvaguardar o direito à proteção de dados, agora expressamente previsto na Carta Magna do Brasil. A Lei 13.709/2018 é considerada um grande avanço para o ordenamento jurídico pátrio, mas não se pode negar que já existia um microssistema de proteção de dados com base em legislação esparsa e no próprio Código de Defesa do Consumidor.

A inserção da proteção de dados pessoais no rol do artigo 5º da Constituição é um avanço civilizacional bastante positivo, pois implica no reconhecimento de que a proteção de dados pessoais é hoje uma garantia essencial para o livre exercício da cidadania. Considerando o contexto revolucionário das mídias digitais e redes sociais, a ascensão da proteção de dados pessoais ao nível de direito fundamental se faz indispensável na atualidade. A decisão do STF de maio de 2020 e a efetiva inserção da proteção de dados pessoais no artigo 5º (inciso LXXIX) da Constituição Federal pela Emenda Constitucional 115/2022 são uma grande conquista da cidadania na era informacional.

A mesma Emenda Constitucional nº 115 fixou a competência privativa da União para legislar sobre o tema, bem como para organizar e fiscalizar a proteção e o tratamento de dados pessoais. Tal fixação de competência busca evitar a fragmentação da regulação sobre proteção de dados pessoais por meio de diversas leis estaduais e municipais, o que poderia resultar em insegurança jurídica decorrente de diferentes interpretações das disposições da Lei Geral de Proteção de Dados Pessoais, bem como de abordagens legislativas conflitantes sobre a temática. Ademais, busca-se garantir a possibilidade de declaração de inconstitucionalidade de

leis e propostas legislativas dos Estados e Municípios sobre a proteção de dados pessoais.

Conforme assevera Sarlet e Caldeira (2019), o modelo informacional alterou a gramática cultural da sociedade, o que traz à tona novos conflitos judiciais e requer uma análise a partir do princípio da dignidade da pessoa humana, dos direitos humanos e fundamentais previstos na maioria das constituições. Convém salientar que a proteção de dados visa assegurar a própria pessoa humana, principalmente no tocante ao livre desenvolvimento de sua personalidade e, em particular, por meio da garantia da sua autodeterminação informacional. Considerando a relevância dos dados pessoais, os estudiosos da temática, a exemplo de Sarlet e Caldeira (2019), sustentam que “os dados e a informação ocupam um lugar de destaque e de importância para a sociedade, sendo considerados o verdadeiro petróleo da era digital.”

Assevera-se, neste contexto, que o direito à proteção de dados pessoais no ordenamento jurídico brasileiro, mesmo antes da Emenda Constitucional nº 115/2022, já era considerado um direito fundamental implícito. Vejamos o quadro abaixo, que traz o inciso X e o inciso LXXIX recentemente incluído no Art 5º da CF/1988, conhecido como rol não taxativo de direitos fundamentais previstos no Brasil:

Inciso X do Art. 5º da CF/1988	Inciso incluído pela EC nº 115/2022
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;	LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

Percebe-se que o Art. 5º, inciso X da Constituição estabelece a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas. No mesmo sentido, a Lei nº 13.709/18 (LGPD) dispõe sobre o tratamento de dados pessoais visando à proteção dos direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural. Em seu voto magistral na ADPF 695/DF, Gilmar Mendes (2019) pontifica que “o direito à privacidade, em sentido mais estrito, conduz à pretensão do indivíduo de não ser foco da observação por terceiros, de não ter os

seus assuntos, informações pessoais e características particulares expostas a terceiros ou ao público em geral". Agora, com a inserção do inciso LXXIX no art. 5º não há maiores debates sobre o reconhecimento do direito à proteção de dados pessoais como direito fundamental da pessoa humana. Agora trata-se de um direito fundamental explicitamente previsto.

Releva-se pertinente destacar que, de acordo com a própria CF/1988, no Art. 60, § 4º, não pode ser objeto de deliberação qualquer proposta de emenda à Constituição tendente a abolir os direitos e garantias individuais (inciso IV). Sendo assim, o direito à proteção de dados pessoais constitui-se cláusula pétrea, o que robustece o arcabouço normativo que envolve a temática de segurança de dados. O impedimento de que o Poder Legislativo apresente propostas de emenda que venha suprimir ou reduzir a proteção constitucional conferida a esse direito, é mais uma garantia para o respeito à dignidade da pessoa humana e inviolabilidade da vida privada.

O princípio da legalidade é estabelecido no art. 37 da Constituição Federal, um dos princípios basilares da Administração Pública. Este princípio tem por objetivo restringir a atuação do Estado somente dentro de parâmetros claramente permitidos por lei. Da leitura harmônica do princípio constitucional com o disposto na LGPD, conclui-se que as hipóteses para compartilhamento de dados pela Administração Pública devem estar embasadas em fundamentos normativos que estabeleçam finalidades específicas para esse tipo de tratamento. Não cabe ao Estado, utilizando-se de suas prerrogativas constitucionais, tornar-se arbitrário e atropelar os ditames legais para beneficiar-se dos dados pessoais de que dispõe.

Importante ressaltar que o Estado pode utilizar-se de meios idôneos para a coleta, ordenamento e análise de dados, usando-os na identificação de possíveis ameaças à segurança, na prestação de serviços sociais e na governança da população. Porém, quando o procedimento é feito sem observância do direito fundamental à proteção dos dados pessoais e ao alvedrio da legislação infraconstitucional, resulta em enormes prejuízos para a soberania estatal e a manutenção da democracia. Num Estado democrático de direito, a afronta aos direitos fundamentais das pessoas é um agravador natural das tensões sociais que podem

implodir as estruturas de poder que sustentam a Democracia. No contexto atual, a pessoa humana está no centro das atenções em questões relacionadas à privacidade de dados, e, portanto, sua autonomia deve ser protegida, cabendo ao Estado o ônus de efetivar esse direito fundamental.

Pelo presente estudo, percebe-se que o sigilo de dados tem status constitucional, portanto, com proteção assegurada mesmo antes mesmo do advento da Lei n. 13.709/2018, sobretudo porque contava também com o reforço legal instituído pelo Marco Civil da Internet – Lei 12.965/2014. Com o advento da EC nº 115/2022, tanto o direito à proteção aos dados pessoais nas interações digitais como o direito à privacidade constam expressamente no rol dos direitos fundamentais da Lei Maior. Assim, em razão de violações a disponibilização de dados pessoais existe potencial de danos irreparáveis à intimidade, honra, imagem e ao sigilo da vida privada de muitos indivíduos. Neste sentido, é imprescindível que as empresas e órgãos públicos têm o dever de zelar pela segurança e sigilo dos dados de seus usuários, prestar informações adequadas e possuir sistemas de detecção antifraude internos e externos, em que devem aprimorar os sistemas de segurança para coibir transações suspeitas.

2.3. LEGISLAÇÃO CORRELATA SOBRE A TEMÁTICA

Oportuno ressaltar que, na esfera da infraconstitucionalidade, em especial no Código Civil brasileiro, a abordagem sobre a temática da proteção da privacidade recebe especial atenção. Como exemplo, destacam-se os artigos 21 e 186 do Código Civil brasileiro tratam, respectivamente, sobre a inviolabilidade da vida privada e sobre a base da responsabilidade civil por violação e por dano, em face de ação ou omissão voluntária, negligência ou imprudência do agente. Além disso, a Lei 10.406/2002 dedica os Artigos 11 ao 21 para a proteção dos direitos da personalidade, tais como os direitos à identidade, ao próprio corpo, ao nome, à imagem e à honra. Importante destacar que a responsabilidade civil tem previsão nos artigos 186, 187, 389 e seguintes, e 927 e seguintes do Código Civil Brasileiro (CCB), sendo um resultado do descumprimento de uma obrigação, mas com esta não se confunde.

Importante ressaltar que o Direito brasileiro prevê o princípio da boa-fé como princípio aplicável ao negócio jurídico (Art. 422 do Código Civil pátrio). Fundamenta-se a boa-fé na ideia de fidelidade no agir, isto é, a conduta de uma parte feita com honestidade, correspondendo à confiança depositada pela outra parte. A Lei nº 13.709, de 14/8/2018, insere a boa-fé como um dos princípios a serem observados para a atividade de tratamento de dados pessoais (art. 6º, caput). Muito embora a navegação na Internet por si só não se constitua um negócio jurídico *ipsis literis,* razões de ordem pública e de interesse social justificam a salvaguarda dessa atividade, proporcionando uma regra implícita de conduta (boa-fé objetiva) que as partes deverão ter a respeito do uso e tratamento de dados, em face de circunstâncias do caso concreto.

Configura-se extremante relevante o impacto do princípio da boa-fé objetiva para a análise e solução de casos concretos que tenham por objeto o legítimo interesse ou, ainda, o autoconsentimento informado. O respeito à privacidade e intimidade, com o correspondente tratamento adequado dos dados pessoais embasado na boa-fé, é fator preponderante para o efetivo exercício da liberdade individual nos meios digitais. Sendo assim, a pessoa cujos dados vieram a ser utilizados ou tratados sem que a sua legítima expectativa fosse observada, deve ter tutela garantida quanto à responsabilização civil. Conforme leciona Patrícia Peck Pinheiro (2020): “o espírito da lei foi proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, trazendo a premissa da boa-fé para todo o tipo de tratamento de dados pessoais.”

Segundo Sergio Cavalieri Filho (2012) “só se cogita de responsabilidade civil onde houver violação de um dever jurídico e um dano”. A responsabilidade civil opera a partir do ato ilícito, com o surgimento da obrigação de indenizar, que tem por finalidade colocar a vítima na situação em que estaria sem a ocorrência do fato danoso, isto é, fazer retornar ao *status quo ante*. A responsabilidade do art. 186 consubstancia a responsabilidade civil subjetiva, na qual se exige a verificação e comprovação de uma conduta culposa, que efetivamente provocou a ocorrência de um prejuízo, vinculados por um nexo de causalidade. No atual cenário de inovação tecnológica e avanço da Internet, solidifica-se a responsabilidade civil digital, aplicada especialmente à violação da privacidade dos dados pessoais.

A responsabilidade pelos danos causados pelo tratamento irregular de dados se encontra disciplinada em capítulo próprio da Lei 13.709/2018 (Seção III, cap. VI). Com respeito aos danos causados em razão do tratamento indevido de dados pessoais, Bruno Miragem (2021) argumenta que é necessário que se compreenda a "existência de um dever de segurança imputável ao segurador como agente de tratamento de dados (controlador ou operador de dados), que é a segurança legitimamente esperada daqueles que exercem a atividade em caráter profissional. " Sendo assim, é imperioso considerar que há presunção que os agentes de tratamento tenham a expertise suficiente para assegurar a integridade dos dados e a preservação da privacidade de seus titulares. No entanto, a violação dos dados pessoais, por si só, não gera o dano moral presumido.

Bruno Miragem (2021) assevera que a "responsabilidade dos agentes de tratamento decorre do tratamento indevido ou irregular dos dados pessoais do qual resulte o dano." Sendo assim, faz-se necessário a comprovação de falha do controlador ou do operador caracterizando, por conseguinte, o nexo causal do dano. As condições de imputação de responsabilidade do controlador e do operador pelos danos decorrentes do tratamento indevido dos dados serão: a) a identificação de uma violação às normas que disciplinam o tratamento de dados pessoais; e b) a existência de um dano patrimonial ou extrapatrimonial (moral) ao titular dos dados. Impende considerar que não pode haver responsabilidade civil sem dano, que deve ser certo, a um bem ou interesse jurídico, sendo necessária a prova concreta dessa lesão. Para o surgimento do dever de indenizar, faz-se necessário aferir se o vazamento de dados resultou efetivamente em algum dano à pessoa (MIRAGEM, 2021).

A civilista Maria Helena Diniz (2005) assevera que "a personalidade é que apoia os direitos e deveres que dela irradiam, é objeto de direito, é o primeiro bem da pessoa, que lhe pertence como primeira utilidade, para que ela possa ser o que é". Neste diapasão, nota-se que a privacidade é a expressão mais ampla do espectro da vida humana e de sua personalidade, tornando-se um refúgio impenetrável para a coletividade. Assim, considera-se privado tudo aquilo que é reservado do público ou exclusivo do particular. Afirma-se também que a privacidade carrega o sentido de um direito de estar só ou de ter uma vida longe dos holofotes de terceiros.

Conforme aponta Renato Afonso Gonçalves em artigo “Evolução e cenário atual da Proteção De Dados Pessoais”, citado no livro Direito em Debate organizado por Maria Helena Diniz (2020), “dos pressupostos da dignidade da pessoa humana e dos direitos da personalidade, surge a imperiosa proteção dos dados de caráter pessoal, ou um direito à proteção de dados pessoais.” Torna-se inevitável, portanto, reconhecer que os dados pessoais expressam o espectro de privacidade, intimidade e dignidade da pessoa, desembocando no conceito de autodeterminação informativa, positivada como princípio fundamental na LGPD, Art. 2º, inciso II. A autodeterminação informativa é entendida como o poder e controle que cada cidadão tem sobre seus próprios dados pessoais.

O Marco Civil da Internet (Lei 12.965/2014) buscou estabelecer princípios, garantias, direitos e deveres para o uso da Internet no Brasil. No seu Art. 7º, há expressa previsão que o acesso à internet é essencial ao exercício da cidadania, e que deve ser assegurado ao usuário o direito da inviolabilidade da intimidade e da vida privada, com a respectiva proteção e indenização pelo dano material ou moral decorrente de sua violação. Quanto aos dados pessoais, a sua proteção foi destacada como princípio para o uso da Internet no Brasil, no Art. 3º, inciso III. Ao usuário de Internet foi conferido o direito de sigilo dos seus dados pessoais, bem como a garantia de informação e a prerrogativa de autorizar as operações de “coleta, uso, armazenamento e tratamento” (art. 7º, VII a X). Este arcabouço normativo estabelece colunas estruturantes da proteção de dados pessoais em razão da preservação da intimidade, honra e imagem das pessoas.

A Lei 13.709/2018 institui princípios a serem observados na matéria de proteção de dados, estipulados no rol exemplificativo do Artigo 6º, e que contempla a o princípio da boa-fé, delineado e consolidado no espectro do Direito Civil. A ausência da boa-fé e tutela da confiança por parte de algumas empresas, que por livre arbítrio, oportunizam vazamento de cadastros de usuários, utilizam seus produtos para influenciar consumidores, dentre outras variáveis, trazendo com tais ações, responsabilização civil por danos patrimoniais ou morais aos prejudicados. Neste sentido, a tutela da confiança, embasada na boa-fé, torna-se inafastável no comércio digital, cabendo à legislação apontar as sanções cabíveis para os casos de violação de dados pessoais. As empresas devem instituir ou rever a forma como recolhem,

manipulam, armazenam e processam dados pessoais, assegurando a consolidação da confiabilidade dessas empresas perante consumidores e clientes, visto que “toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade”, nos termos do Art. 17 da Lei 13.709/2018.

O Código de Defesa do Consumidor é aplicável nas relações jurídicas relativas à Internet quando estiver caracterizada a relação de consumo, por meio de critério subjetivo, isto é, a existência de um fornecedor e de um consumidor. Por outro giro, surge a questão da inclusão em bancos de dados e cadastros de consumidores, que está prevista no art. 43 do CDC, que pode gerar conflito com o direito à intimidade, ferindo a proteção de dados pessoais, no tocante ao consentimento e autodeterminação informativa da pessoa. Maimone (2022) aponta que eventuais vazamentos de dados por fornecedores podem representar um acidente de consumo e, assim, “ensejar a incidência dialógica de diplomas legais (como a LGPD), ainda que ausente relação de consumo, uma vez que as vítimas do evento danoso se equiparam a consumidores” (conforme o art. 17 do Código de Defesa do Consumidor).

Ainda, conforme o § 2.º do art. 42 da Lei n. 13.709/2018, o juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados pessoais quando for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa. Portanto, percebe-se a influência da inversão do ônus da prova, já consagrada pelo CDC (art. 6.º, inc. VIII). O art. 43 da LGPD preceitua que os agentes de tratamento de dados só não serão responsabilizados quando provarem: a) que não realizaram o tratamento de dados pessoais que lhes é atribuído; b) que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou c) que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros. Neste diapasão, forçoso reconhecer que a responsabilidade civil envolve não só cumprir a legislação vigente, é preciso proativamente prevenir a ocorrência de danos decorrentes do mau uso ou do tratamento inadequado de dados pessoais.

Nota-se que a Lei Geral de Proteção de Dados não declara expressamente qual deve ser a espécie de responsabilidade civil a ser aplicada. Não há indícios diretos da aplicabilidade de uma conduta negligente, imperita ou imprudente (subjetiva); bem como não há indícios de responsabilização independente da culpa (objetiva). Qualquer conclusão perpassa por um exercício de interpretação feito pelos operadores do Direito.

No entanto, importante frisar que o Art. 45 da LGPD aponta que quando o tratamento de dados se dá em situações de relação de consumo, aplica-se o Código de Defesa do Consumidor: “As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente”. O CDC é claro quanto à adoção do instituto da relação civil objetiva, conforme se observa nos artigos 12, 13, e 14 deste importante diploma legal. O que se conclui é que sempre que o titular dos dados for enquadrado como consumidor poderá valer-se da responsabilidade objetiva para pleitear o seu direito.

Maria Celina Bodim Moraes (2019) afirma que “o sistema de responsabilização civil da LGPD, previsto nos artigos 42 a 45 da Lei nº.13.709/2018, mostra-se especialíssimo, configurando-se como a principal novidade da lei.” Considerando o princípio da responsabilização e prestação de contas do inciso X do Art. 6º da Lei, o legislador teve como objetivo prevenir e evitar a ocorrência dos danos decorrentes do tratamento de dados. Esse conceito de prestação de contas inaugura um novo sistema de responsabilidade proativa, isto é, o agente de tratamento de dados deve comprovar a boa-fé e transparência na adoção das melhores práticas de governança e proteção de dados, bem como a observância dos requisitos legais previstos, mesmo antes da ocorrência de qualquer dano.

2.4. BIG DATA E A INTERNET DAS COISAS

A criação de bancos de dados é uma prática antiga e bancos de dados digitais já existem há um bom tempo. Nos tempos hodiernos, a revolução digital proporcionada pela Internet e pelos computadores interconectados em rede transformou radicalmente o que se entendia como banco de dados. As diversas aplicações e sistemas de inteligência artificial que efetuam mineração de dados são

cada vez mais robustas e precisas, analisando em fração de segundos uma gama de dados que outrora seria impossível por conta das limitações operacionais. Por exemplo, as empresas de cartões de crédito registram e analisam vastas quantidades de dados com informação sobre hábitos e ações financeiras pessoais para tentar detectar fraudes e identificar tendências de compra dos consumidores (MARTÍNEZ-ÁVILA; SOUZA; GONZALEZ, 2019).

Para Martínez-Ávila, Gonzalez e Souza (2019), muito além da perspectiva meramente quantitativa dos dados sob análise em variadas plataformas e sistemas, as “técnicas de análise de Big Data podem ser vistas, em uma perspectiva metodológica, como um conjunto de métodos de análise que incorpora uma diversidade de conhecimentos, técnicas de programação e tecnologias”. Desta forma, o conhecimento adquirido com a combinação de diferentes dados é fundamental para a ampliação de conhecimentos e para o sucesso econômico das empresas e agências governamentais que utilizam as tecnologias digitais. As finalidades são diversas tais como análises, previsões, consultas, decisões de produção, estratégias de negócios definição de perfis, etc. Neste sentido, a utilização de dados massivos, por vezes sem a permissão livre e esclarecida dos usuários, apresenta desafios à ciência e à vida cotidiana, especificamente para o universo jurídico.

A partir do uso de técnicas avançadas de correlação de dados, os analistas, valendo-se da Inteligência Artificial, podem efetuar pesquisas variadas em enormes quantidades de dados, em tempo bastante reduzido, prevendo comportamentos, situações e eventos de modos inimagináveis. Assim, segundo Wolfgang (2022) o termo *Big Data* refere-se a situações em que as tecnologias digitais são direcionadas para “lidar com grandes e variadas quantidades de dados e às várias possibilidades de combinação, avaliação e processamento desses dados por autoridades privadas e públicas em diferentes contextos.”

O autor ainda destaca cinco características que são utilizadas para identificar Big Data, conhecidas como os cinco “Vs”. As possibilidades de acesso a enormes quantidades de dados digitais (*High Volume*), de diferentes tipos e qualidade, assim como diferentes formas de coleta, armazenamento e acesso (*High Variety*), e a alta velocidade do seu processamento (*High Velocity*). O uso da inteligência artificial em

particular torna possível novas e altamente eficientes formas de processamento de dados, bem como a verificação de sua consistência e garantia de qualidade (*Veracity*). Além disso, os Big Data são objeto e base de novos modelos de negócios e de possibilidades para diversas atividades de valor agregado (*Value*) (WOLFGANG, 2022). Salienta-se, por oportuno, que os desafios que se impõem na questão do tratamento de dados e proteção às garantias fundamentais de privacidade e intimidade são ainda mais gigantescos quando se trata de Big Data. A legislação brasileira é um avanço considerável para a temática, mas ainda se faz necessário ampliar o escopo de fundamentação técnica para aplicabilidade das normas de modo eficaz.

De acordo com Eduardo Magrani (2018), a internet das coisas (*internet of things*, IoT) é um termo que está diretamente relacionado com aumento da comunicação entre máquinas por meio da Internet, “perpassando pelo desenvolvimento de diversos utensílios, além de microdispositivos, como sensores que, dispostos das mais diversas maneiras para captar dados a partir de seu ambiente, tornam-se partes integrantes da internet.” Nesta seara, também importa garantir os direitos fundamentais de privacidade e a proteção de dados com base na LGPD, ao mesmo tempo em que não se criem barreiras às inovações tecnológicas.

Ampliando o conceito, Eduardo Magrani (2018) assevera que a internet das coisas pode ser entendida como um “ambiente de objetos físicos interconectados com a internet por meio de sensores pequenos e embutidos, criando um ecossistema de computação onipresente (ubíqua), voltado para a facilitação do cotidiano das pessoas”. Esse ecossistema tecnológico introduz uma diversidade de soluções funcionais nos processos de interação homem-máquina no dia a dia, o que possibilita maior aproveitamento do potencial das conexões em rede. Sendo assim, a Internet tem se tornado mais do que um meio para entregar mensagens de uma pessoa a outra ou para a busca de informações que estão disponibilizadas on-line.

Ressalta-se que o desafio lançado pelo salto tecnológico e paradigmático da internet das coisas não é de pequena monta. Considerando-se a fragmentação e a multiplicação das fontes de dados (incluindo dados pessoais), a concessão de variados graus de autonomia a elementos dispostos pela rede e a crescente

dificuldade de separar a internet do próprio cotidiano, o quadro se torna bastante desafiador no tocante ao adequado tratamento de dados. Afinal, computadores, sensores e objetos interagem uns com os outros e processam dados em um contexto de hiperconectividade, gerando um volume significativo de informações de usuários destes dispositivos.

Para Magrani (2018), “o avanço da hiperconexão depende do aumento de dispositivos que enviam e recebem as informações de usuários” e, consequentemente, “quanto maior o número de dispositivos conectados, mais dados são produzidos”. O crescimento exponencial de “coisas” conectadas à internet com capacidade para compartilhar, processar, armazenar e analisar um volume enorme de dados entre si une o conceito de *IoT* ao de *Big Data*. Neste diapasão, observa-se que *Big Data* significa, em suma, que tudo o que fazemos, tanto online como *offline*, deixa vestígios digitais. Com a utilização massiva de dispositivos interligados, os vestígios digitais de usuários são produzidos incessantemente, inclusive ao dormir, como, por exemplo, por meio dos relógios digitais que medem batimentos cardíacos, o tempo e qualidade do sono. Sistemas de automação residencial cada vez mais modernos já permitem que o usuário, antes mesmo de chegar à sua residência, programe os dispositivos para abrir os portões, desligar alarmes, preparar o banho quente, colocar música ambiente e alterar a temperatura da casa. Certamente a combinação entre objetos inteligentes e Big Data já alterou significativamente a maneira como vivemos e continuará trazendo inovações para o cotidiano (MAGRANI, 2018).

O autor Eduardo Magrani (2018) faz um alerta com relação à segurança dos dados, afirmando que “ainda não há um consenso entre os fabricantes de produtos de IoT e que os próprios desenvolvedores ainda não têm uma noção completa do que é realmente necessário em termos de segurança”. Busca-se equacionar essa falta de segurança dos dispositivos por meio de testes de vulnerabilidade em softwares e sistemas e também pela conscientização dos usuários da importância de sempre manter seus dispositivos atualizados. Quando se trata de Internet das coisas, uma série de pormenores de segurança devem ser levados em consideração, como gestão de armazenamento, servidores e redes de *data center*, considerando-se o grande fluxo de dados.

Capítulo 3

3.1. CONTROVÉRSIAS DA LEI GERAL DE PROTEÇÃO DE DADOS

Evidentemente, após a abordagem teórico-conceitual feita nos capítulos anteriores, torna-se necessário partir para uma análise da Lei Geral de Proteção de Dados (Lei 13.709/18) sob o ponto de vista de suas controvérsias e também de suas deficiências. Nota-se, por oportuno, que a LGPD representa um avanço importante no que tange à segurança de dados pessoais, mas é forçoso reconhecer que há desafios que precisam ser encarados para a modernização e aplicabilidade adequada da Lei 13.709/18.

Neste diapasão, o presente trabalho doravante busca elencar as principais controvérsias ou assuntos que geram divergência de entendimento dentro do campo teórico de proteção de dados, privacidade e inviolabilidade de aspectos da personalidade humana. Serão abordados temas relevantes que são fundamentais à aplicabilidade da Lei Geral de Proteção de Dados, quais sejam: a diferença conceitual entre dado, informação e conhecimento, a utilização de cookies, o consentimento do usuário, incidentes de segurança de dados pessoais, legítimo interesse do controlador e anonimização ou pseudonimização de dados pessoais.

A argumentação a seguir tem como ponto fulcral os aspectos que, em tese, podem gerar controvérsias a respeito da correta aplicabilidade da LGPD dentro do contexto para o qual ela foi pensada e elaborada.

3.2. DADO X INFORMAÇÃO X CONHECIMENTO

De início, destaca-se que a Lei Geral de Proteção de Dados não faz clara distinção entre dos conceitos de dados e informação. A proteção de dados por vezes é utilizada como sinônimo de segurança da informação, o que se constitui numa atecnia. O Art 5º, inciso I, da Lei, define dado pessoal como sendo a informação relacionada a pessoa natural identificada ou identificável. Ao definir o dado anonimizado, a LGPD aponta que é o dado relativo a titular que não possa ser identificado. É comum se dizer que os dados são o ativo e o legado do século 21, da

“Era da Informação”. Na área da Ciência da Informação, têm-se três conceitos chave devido a sua importância, a saber: dados, informação e conhecimento. Frise-se que a Lei de Acesso à Informação (LAI) também não foi precisa na abordagem dos conceitos, definindo que “informação são os dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato” (Art. 4º, I, Lei 12.527/2011).

Para a Ciência da Informação, dado e informação são conceitos distintos, apesar de existir uma certa gradação entre eles, dentro de uma escala que considera o fator temporal. Conforme Ricardo Barreto (2019), “o dado gera a informação que, por sua vez, leva ao conhecimento, refletido finalmente em inteligência aplicada no resultado de eventos futuros.” O autor Bruno Ricardo Bioni (2021) assevera que o dado é o estado primitivo da informação, pois não é algo *per si* que acrescente conhecimento. Na opinião do renomado autor, “dados são simplesmente fatos brutos que, quando processados e organizados, se revertem em algo inteligível, podendo ser deles extraída uma informação” (BIONI, 2021).

Em outras palavras, dados podem ser concebidos como símbolos não interpretados que possuem natureza formal, podendo ser reproduzidos e transmitidos mediante determinadas operações computacionais. Portanto, para o devido processamento, os dados dependem de um meio técnico-físico (hardware) e não apenas assumem forma semântica, que se distingue da informação por eles processada.

Informações, por seu turno, são elementos de teor semântico delimitado obtidos em determinado contexto social, mediante observações, comunicações ou dados e para posterior utilização. Para tanto, há a necessidade de um processo interpretativo com clara atribuição de sentido aos dados coletados. Assim, embora informações sejam contidas e veiculadas mediante dados, com estes não se confundem, porquanto dependem (daí não terem natureza puramente formal como os dados) do contexto de sua utilização.

Em suma, os dados são geralmente concebidos como a matéria-prima para a informação, que é concebida como matéria-prima para o conhecimento. Conforme assevera Marcel Leonardi (2019), dados bem utilizados e processados permitem

análises informacionais profundas e conhecimento integrado que beneficiam toda a sociedade. Segundo o autor, “a análise inteligente de dados é um dos principais impulsionadores da economia atual e do crescimento futuro” – e isso só se faz possível mediante o emprego correto de técnicas de mineração dos dados, que possibilitem a geração de informação com sentido apurado e conhecimento adequado para melhor tomada de decisões das empresas.

Assim, pondera-se que deveria ter sido aplicada uma melhor técnica na elaboração da Lei Geral de Proteção de Dados, no que concerne a termos apropriados ao contexto da ciência informacional, que engloba diferentes nuances para explicar o que se define como dado e informação e, por consequência, o conhecimento produzido. Essa falha teria sido evitada se houvesse uma assessoria qualificada para apontar as diferenças de conceito antes da matéria ser posta em votação.

3.3. UTILIZAÇÃO DE COOKIES

Outro fator bastante controverso na Lei Geral de Proteção de Dados é a ausência de menção expressa aos *cookies.* Segundo Felipe Palhares (2020), “*cookies* são pequenos arquivos de texto que são armazenados no dispositivo do usuário (cliente) e que são deixados pelo servidor web antes que o ciclo da comunicação se encerre.” Nesses arquivos constam pequenas partes de dados que são compartilhados quando um dispositivo visita ou utiliza os serviços on-line. Assim, toda vez que o usuário acessa novamente o mesmo website, os cookies inicialmente armazenados são lidos pelo servidor *web*, possibilitando a execução mais rápida de várias funcionalidades e acompanhar o comportamento do usuário na página.

As informações coletadas, geralmente o nome do site que o originou, o tempo de navegação e um valor gerado aleatoriamente, são interpretadas e executadas pelos portais na Internet, o que possibilita o reconhecimento do usuário e identificação futura de seus interesses e necessidades. O usuário pode revogar a sua autorização quanto à utilização dos cookies, por meio de alteração das configurações de seu navegador de preferência. Contudo, de acordo com as configurações executadas,

certas funcionalidades dos serviços *on-line* poderão não funcionar da maneira ideal, bem como aspectos de segurança da informação podem ser prejudicados.

Verifica-se, desse modo, que os cookies podem armazenar diversas informações sobre os hábitos de utilização da internet do usuário, desde os links que foram clicados, os produtos que foram comprados, os termos que foram pesquisados, a região em que vive o usuário, e tantos outros dados valiosos para uma segmentação de publicidade, que vão muito além dos objetivos de meramente viabilizar algumas funcionalidades específicas da página visitada (PALHARES, 2020).

A controvérsia sobre a utilização de cookies gira em torno da autorização dada pelo usuário. Os cookies geralmente são armazenados sem o conhecimento ou consentimento expresso dos usuários; eles levantam preocupações adicionais de privacidade na medida em que capturam e transmitem dados sobre usuários individuais. Essas informações podem incluir as pesquisas que os usuários executaram, as informações de identificação que eles divulgaram (por exemplo, para se registrar e fazer *logon* em um determinado serviço), seus padrões de navegação ao visitar um site e o comportamento do “fluxo de cliques” (ou seja, em quais links eles clicaram enquanto navegavam na Web).

Além disso, empresas terceiras de publicidade usam *cookies* para compilar informações sobre o comportamento on-line dos usuários quando eles visitam vários sites que dependem da mesma rede de anúncios para exibir propagandas direcionadas. Importa ressaltar que o fato de terceiros terem acesso aos cookies, bem como a identificação precisa desses terceiros, são aspectos que devem ser informados ao usuário, no sentido de garantir que o tratamento de dados seja justo e transparente (PALHARES, 2020).

O simples fato de um *website* incluir um aviso genérico sobre a utilização de *cookies* dentro de sua política de privacidade é considerado insuficiente para caracterizar um ato de efetiva exposição da informação, uma vez que a vasta parcela dos usuários não se importa com as Políticas de Utilização de Cookies dos sites visitados, que são escritas com linguagem excessivamente técnica e exorbitam da capacidade de leitura de muitos. De fato, o usuário médio não conhece a verdadeira lógica por trás da tecnologia dos *cookies* nem mesmo do que ela é capaz. *Cookies*

são ferramentas poderosas capazes de monitorar o comportamento *on-line* do usuário, e, conforme a sua configuração, registrar todos os sites que foram visitados pelo usuário, os produtos que foram incluídos no seu carrinho, os sites em que o usuário é um cliente e que tenha realizado *login*, as informações dos formulários que tenham sido preenchidos pelo usuário, dentre outros.

Cookies de rastreamento (os chamados supercookies) são baixados em um navegador web para rastrear o comportamento e atividade *on-line* de uma pessoa. Como os *cookies* de rastreamento são usados para coletar informações sem a autorização do usuário, eles representam uma ameaça real à privacidade online. *Cookies* de rastreamento, como cookies de terceiros, não são usados para melhorar a experiência, mas para acompanhar a atividade do cliente em determinados sites. De fato, os cookies são ferramentas invasivas e poderosa que possibilitam o direcionamento de informações específicas que influenciam o comportamento do usuário, direcionando-o inclusive a adquirir um determinado produto ou serviço.

Recentemente, a Autoridade Nacional de Proteção de Dados (ANPD) emitiu recomendação à Secretaria de Governo Digital (SGD/ME) para a adequação do Portal Gov.BR às disposições da Lei Geral de Proteção de Dados Pessoais (LGPD). A recomendação propõe adequações em relação ao tratamento de dados pessoais decorrente da coleta de cookies no Portal Gov.br. Argumenta-se na recomendação que os sites do portal Gov.br precisam disponibilizar botão de fácil visualização, que permita rejeitar todos os cookies não necessários e desativar cookies baseados no consentimento por padrão (opt-in). De fato, a ANPD busca implementar melhorias quanto à privacidade no que tange ao rastreamento de dados e configuração de *cookies*.

3.4. O CONSENTIMENTO DO USUÁRIO

No Brasil, a Lei Geral de Proteção de Dados constitui-se um marco normativo protetivo do titular de dados pessoais, sujeito de direito capaz de fornecer seus dados pessoais comportamentais por meio de um processo de consentimento. De acordo com o art. 7º, inciso I, da LGPD, o uso de dados pessoais só pode ser realizado

mediante o fornecimento de consentimento pelo titular. Este consentimento deve consistir em uma “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada” (art. 5º, inciso XII). Isso significa que o usuário deve ser capaz de controlar seus dados sem coação física ou moral, a fim de que a autodeterminação informacional seja livre e verdadeira. Na LGPD, o consentimento do titular dos dados é considerado elemento essencial para o tratamento, regra excepcionada nos casos previstos no art. 11, inciso II, da Lei 13.709/2018.

O consentimento, apesar de ser somente uma das hipóteses de tratamento, figura como protagonista da grande maioria das leis de proteção de dados ao redor do mundo. Isso porque a complexidade em se estabelecer um sistema que possibilite a regulação de autorizações e proibições sobre o tratamento de dados levou os sistemas de proteção de dados a adotarem uma política que aumentou a carga participativa do indivíduo na autodeterminação de suas informações pessoais (SOLOVE, 2013)

No tocante ao consentimento, Patrícia Peck Pinheiro (2016) explica que os chamados Termos de Uso e Política de Privacidade “são uma espécie de contrato de adesão eletrônico para o uso da aplicação, atribuindo direitos e obrigações ao internauta e ao provedor, inclusive a autorização para tratamento de dados pessoais.” Ocorre que a redação costuma ser excessivamente longa, visualmente homogênea e com vocabulário excessivamente técnico, o que acaba tornando incompreensível em razão da hipossuficiência da pessoa que se utiliza dos serviços digitais disponíveis na Internet. A tecnicidade dos Termos de Uso e Política de Privacidade acaba por torna-los de difícil assimilação, o que acaba inviabilizando o real consentimento do usuário.

Eduarto Magrani (2018) pondera que “o modelo de consentimento do usuário como elemento central para a permissão do uso de seus dados pessoais tem se mostrado ineficaz” considerando algumas incongruências contidas nos termos de uso dos provedores de serviços on-line. Diante da ineficácia do modelo de consentimento e da ficção de crer que tal consentimento é livre e esclarecido, surge a necessidade de buscar modelos mais eficientes como o *privacy-by-design*, no qual os princípios fundamentais de privacidade devem ser aplicados em todo o processo de

desenvolvimento de um sistema. Desta forma, busca-se observar o princípio da finalidade desde a concepção da solução tecnológica para a validade do uso e tratamento de dados, em harmonia com as especificidades trazidas pela Lei 13.709/2018.

O consentimento do titular de dados é a forma mais conhecida do tratamento legal de dados e deve ser livre e realizada do modo mais consciente possível, ou seja, o titular deve ter pleno conhecimento de quais dados estão sendo captados e exatamente para qual fim ele será utilizado, o qual perfaz a inequivocabilidade do consentimento (TEIXEIRA E ARMELIN, 2019). Os dados pessoais coletados somente devem ser utilizados para cumprir com as finalidades específicas informadas ao titular no ato de consentimento, conforme preceitua o Art. 11, inciso I da LGPD. Ademais, a eliminação dos dados pessoais tratados também deve contar com o consentimento do titular, mediante requerimento expresso do titular ou de representante legalmente constituído ao agente de tratamento. Conforme aponta Danilo Doneda (2019), “na esteira do direito geral de personalidade, o direito à autodeterminação informativa proporciona ao indivíduo o controle sobre suas informações. ” É justamente essa deliberação própria sobre os dados pessoais que o consentimento objetiva assegurar.

Nessa esteira, de acordo com Danilo Doneda (2019), “o consentimento compreende um poder conferido à pessoa de modificar sua própria esfera jurídica, com base na expressão de sua vontade. ” Frisa-se que o consentimento para o tratamento de dados pessoais pode se apresentar como um procedimento aparentemente inócuo, no entanto as consequências podem ser pouco nítidas e difíceis de serem identificadas. O consentimento para o tratamento de dados pessoais relaciona-se com uma série de elementos da própria personalidade, e por isso mesmo, tal consentimento há de ser revogável e a sua caracterização como ato jurídico unilateral tem por meta reforçar essa revogabilidade (DONEDA, 2019).

A questão controversa reside justamente na abrangência do consentimento do titular de dados pessoais. Neste ponto, destaca-se a insuficiência do consentimento na árdua tarefa de tutelar plenamente a privacidade e de proteger os dados pessoais dos cidadãos frente aos desafios contemporâneos trazidos, por exemplo, pela ascensão do Big Data e da IoT.

Os autores Laura Schertel Mendes e Gabriel Fonseca no artigo “Proteção de dados para além do consentimento: tendências contemporâneas de materialização”, destacam três pontos que elucidam as insuficiências do consentimento como foco regulatório:

> (i) as limitações cognitivas do titular dos dados pessoais para avaliar os custos e benefícios envolvidos quanto aos seus direitos de personalidade; (ii) as situações em que não há uma real liberdade de escolha do titular como, por exemplo, em circunstâncias denominadas de “*take it or leave it*”; e (iii) as modernas técnicas de tratamento e análise de dados a partir de Big Data que fazem com que a totalidade do valor e a possibilidade de uso desses dados não sejam completamente mensuráveis no momento em que o consentimento é requerido. (MENDES; FONSECA, 2020, p. 7-8)

Dos pontos destacados acima depreende-se que há necessidade de melhor compreensão por parte do usuário sobre as implicações de sua decisão de consentir com a coleta e tratamento de seus dados pessoais. Questiona-se sobre a real capacidade de o titular dos dados pessoais avaliar adequadamente os riscos e prejuízos que podem ser gerados a partir do seu consentimento online. Muitas vezes, os usuários nem se dão ao trabalho de ler as “Políticas de Privacidade” ou “Informações sobre o Uso de Dados” que são apresentadas nas páginas da Internet. A LGPD é expressa ao afirmar que “é vedado o tratamento de dados pessoais mediante vício de consentimento” (Art. 8º, § 3º).

Os autores reforçam ainda que existe uma flagrante assimetria de poderes na relação entre o titular dos dados pessoais e os agentes responsáveis pelo tratamento desses dados, resultando numa óbvia vulnerabilidade do usuário de serviços informatizados. Vários sites adotam a lógica binária nas relações online, isto é, consentir ou não consentir. Ocorre que, ao não consentir, o usuário não poderá desfrutar do serviço almejado, por exemplo, o uso de uma rede social ou de um aplicativo para celular. Questiona-se, com razão, em que se fundamenta a autonomia decisória do indivíduo, já que a opção de não consentir gera inconvenientes e a opção de consentir é um risco assumido com base no princípio da boa-fé. Neste aspecto, Laura Mendes e Gabriel Fonseca (2020) argumentam que “o consentimento é meramente uma ficção, uma vez que o indivíduo carece de efetiva autonomia decisória para se proteger dos possíveis perigos e danos à sua personalidade. ”

Ademais, considerando que informações extraídas a partir dos dados pessoais estabelecem a representação virtual do indivíduo na sociedade em rede, num cenário marcado pelo *Big Data*, o tratamento dos dados pessoais não pode ser visto como algo estático. A combinação de dados manipulada por Inteligência Artificial e algoritmos torna possível extrair novas informações totalmente descoladas da finalidade original que ensejou o consentimento para coleta e tratamento desses dados. Dados considerados simples ou irrelevantes como idade, altura, nacionalidade, endereços de residência e de trabalho, podem servir de insumo para correlações, predições e ranqueamentos a respeito da personalidade do titular dos dados pessoais ou de determinados grupos sociais, a depender das combinações matemáticas realizadas por algoritmos.

Conforme lição de Gustavo Tepedino (2020) é importante que a interpretação do consentimento seja feita restritivamente, de modo a impedir que o agente estenda a autorização do tratamento dos dados para outros meios além daqueles pactuados, para momento posterior, para fim ou contexto diverso ou, ainda, para pessoas distintas daquelas informadas ao titular. Assim, revela-se necessário que mudanças significativas sejam implementadas tanto na maneira pela qual o consentimento é apresentado nos Termos e Políticas de Uso, como também no desenho e arquitetura das plataformas.

No atual contexto normativo relacionado com a privacidade de dados, os usuários devem estar em condições de consentir de forma livre e informada em relação ao recebimento de anúncios ou publicidade comportamental na Internet, independentemente do acesso às redes sociais. As boas práticas institucionais e o cumprimento integral da LGPD no que tange ao consentimento deve ser o objetivo primário dos setores público e privado, considerando a autodeterminação informativa como princípio nuclear da privacidade. Ressalte-se ainda que o titular do bem jurídico precisa ter acesso às informações necessárias e suficientes para avaliar corretamente a situação e a forma como seus dados serão tratados (TEPEDINO, 2020). Deve ainda ser assegurada a observância ao princípio da finalidade, uma vez que a validade do consentimento se relaciona com a efetivação do tratamento de dados para propósitos legítimos, específicos, explícitos e informados ao titular, não sendo permitido nenhum tratamento posterior de forma incompatível com esses fins.

Necessário salientar que o consentimento poderá ser revogado a qualquer momento, mediante manifestação expressa do titular, por procedimento gratuito e facilitado. A Lei 13.709/2018 estabelece que “o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.” Neste sentido Gustavo Tepedino (2020) também observa que “a possibilidade de revogação incondicional do consentimento tem como base a autodeterminação em relação à construção da esfera privada e na proteção da personalidade”.

Outro problema relativo ao consentimento é que os usuários são instados a tomar decisões racionais sobre o compartilhamento de dados individuais isoladamente, no entanto é bastante problemático saber como seus dados podem ser agregados no futuro. Suponha que um indivíduo forneça um inócuo dado em um ponto no tempo, pensando que ele ou ela não está revelando nada sensível. Em outro momento, a pessoa revela dados igualmente não sensíveis. Inesperadamente, esses dados podem ser combinados e analisados para revelar fatos sensíveis sobre a pessoa. A pessoa nunca divulgou esses fatos nem previu que eles seriam descobertos, mas a agregação dos dados, por meio de técnicas de Inteligência Artificial e mineração de dados pode deduzir informações extensas sobre uma pessoa determinada. Em outras palavras, pequenos pedaços de dados inócuos podem dizer muito em combinação. Daniel J. Solove (2013) refere-se a isso como o “efeito de agregação”.

A dificuldade com o efeito de agregação é que ele torna quase impossível gerenciar os dados pessoais. A variedade de novas informações que podem ser colhidos da análise de dados existentes e os tipos de previsões que podem ser feitas a partir da combinação desses dados são muito vastos e complexos, e estão evoluindo muito rapidamente. Torna-se uma tarefa hercúlea para os usuários de sistemas informacionais avaliarem completamente os riscos e benefícios envolvidos quando oferecem o consentimento. Para favorecer que uma pessoa tome uma decisão racional sobre o compartilhamento de dados, essa pessoa precisaria ter uma compreensão da gama de possíveis danos e benefícios para fazer uma análise de custo-benefício (SOLOVE, 2013).

É de se notar que a autogestão da privacidade requer que as pessoas avaliem o dano potencial normalmente quando os dados são coletados inicialmente. No entanto, por várias razões, é imensamente desafiador envolver-se nessa análise de custo-benefício para o futuro. Daniel J. Solove (2013) destaca que muitos danos à privacidade são de natureza cumulativa: “as pessoas podem concordar com muitas formas de coleta, uso e divulgação de dados por um longo período de tempo, e os efeitos nocivos só podem emergir posteriormente mediante a combinação dos dados.” Esta é uma controvérsia que a Lei Geral de Proteção de Dados não soluciona de modo eficaz: os danos causados por violações de privacidade podem se desenvolver gradualmente ao longo do tempo, mas decisões sobre privacidade devem ser tomadas individualmente, isoladamente e com antecedência. Conforme Patricia Peck Pinheiro (2020), o consentimento do titular ao tratamento de seus dados pessoais “não deve lhe onerar de forma alguma, por isso as informações coletadas não devem ser utilizadas em prejuízo do titular.”

Em suma, o instrumento do consentimento apresenta-se como questionável para garantir a autonomia decisória do indivíduo quanto aos seus dados pessoais, considerando a autodeterminação informacional. Essa observação, no entanto, não aponta para a plena renúncia do consentimento como instrumento protetivo. Em face do poderio tecnológico ao dispor das empresas e serviços governamentais on-line, não se pode ignorar a condição de vulnerabilidade do usuário de serviços digitais, no entanto deve-se buscar mecanismos para aperfeiçoamento dos fundamentos e alcance do consentimento do titular dos dados pessoais.

3.5. INCIDENTES DE SEGURANÇA DE DADOS PESSOAIS

Mesmo com todo desenvolvimento tecnológico e investimento em segurança dos últimos anos, notícias sobre vazamentos de dados pessoais ocorrem com relativa frequência. A Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) deixou algumas lacunas neste assunto e delegou o estabelecimento de parâmetros e procedimentos à Autoridade Nacional de Proteção de Dados pessoais. Este pode ser um vetor de controvérsias significativas, considerando que a edição de atos normativos infralegais às vezes ficam aquém ou vão além do propósito da Lei.

Existem três importantes princípios da segurança da informação que fornecem os fundamentos para categorias de incidentes de segurança: confidencialidade, integridade e disponibilidade. Conforme elucida Maria Luciano (2019), “os incidentes de confidencialidade abrangem as ocorrências em que há uma divulgação ou acesso acidental ou não autorizado a dados pessoais.” No que concerne aos incidentes de integridade, nota-se algum tipo de alteração acidental ou não autorizada dos dados. Por fim, nos incidentes de disponibilidade há a perda de acesso ou destruição, acidental ou não autorizada, desses dados. Obviamente, tais categorias não são estanques, podendo haver ocorrências que pertençam a mais de uma categoria. O grave cenário de desafio à segurança da informação faz com que as legislações de proteção de dados procurem estabelecer obrigações mais rígidas aos controladores (LIMA, 2021).

A LGPD estabelece que as medidas de segurança técnicas e administrativas “deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução” (art. 46, § 2º). Afigura-se a noção da segurança por design (*security by design*). Desta forma, as medidas de segurança devem abranger tanto o planejamento do tratamento quanto o tratamento em si e se protrair após o término do tratamento, por força do art. 47 da LGPD. Essa previsão legal precisa ser aplicada com acurácia respeitando-se as melhores e mais modernas práticas de governança de dados.

Segundo Alexandre Fernandes Moraes (2010), “a Segurança da Informação pode ser definida como um processo de proteger a informação do mau uso tanto acidental como intencional, por pessoas internas ou externas à organização”. Em se tratando de redes de computadores, considera-se como vulnerabilidade ou falha de segurança um bug de sistema operacional ou aplicação, como em um servidor Web ou no Windows, o que pode acarretar problemas nos serviços de banco de dados da organização.

É importante destacar que o dever de proteção de dados expresso na LGPD se relaciona com o dever geral de qualidade da prestação de serviço do fornecedor previsto no CDC, o que inclui necessariamente uma infraestrutura computacional de rede adequada para o tratamento de dados pessoais dos usuários de aplicações, bem como o dever de segurança das plataformas que operacionalizam tais serviços. Sob

este enfoque, todas as vezes que utilizamos a Internet para procurar ou disponibilizar informações estamos sujeitos a riscos diversos, uma vez que a Internet é uma enorme rede pública sujeita a ataques.

Como reflexo dos princípios da transparência, da segurança e da prevenção (art. 6º, incisos VI, VII e VIII), qualquer incidente de segurança envolvendo dados pessoais que possa acarretar risco ou dano relevante aos titulares deverá ser comunicado pelos controladores à Autoridade Nacional e ao próprio titular interessado (art. 48, LGPD). De acordo com Maria Luciano (2019), “o grau de risco pode variar ao longo do tempo, tendo-se em vista as inovações tecnológicas e o estado da arte das medidas de segurança e mitigação de riscos disponíveis no mercado. ” Ademais, na avalição do risco envolvido no incidente torna-se imprescindível considerar as especificidades da ocorrência: natureza do incidente, a natureza e o volume dos dados e a gravidade das consequências que o incidente acarretará aos titulares. Neste cenário, compete aos agentes de tratamento avaliar se o risco colocado ao titular pelo incidente é alto o suficiente para ensejar a notificação da ocorrência. Ainda se faz necessário realizar justificação plausível para os casos em que decidir-se por não comunicar o incidente à autoridade nacional ou ao titular.

Para a autora Maria Luciano (2019) um fator de controvérsia é que “a LGPD adota a nomenclatura ‘incidente de segurança’ sem, contudo, defini-la.” Apesar de não apresentar definição explícita, a norma parece convergir com a GDPR ao estabelecer, em seu art. 46, a adoção de medidas visando “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”.

Outro ponto controverso é que, ao contrário do GDPR europeu, que prevê prazo de 72 horas, a LGPD apenas prevê o dever de o controlador comunicar, em prazo razoável, à Autoridade Nacional e ao titular sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos dados pessoais. Neste ponto falhou a lei brasileira (13.709/2018) pois não há elementos para a definição de prazo razoável, que possivelmente ficará ao encargo de regulamento da Autoridade Nacional, o que gera bastante insegurança jurídica e dificuldades sob o ponto de vista prático e de cunho operacional.

Ressalta-se que é importante delimitar o conteúdo normativo da expressão “incidente de segurança”. Isso perpassa necessariamente por avaliação de risco que considera as especificidades de cada caso, da natureza dos dados e dos indivíduos envolvidos. Além disso demanda um compromisso ainda mais intenso com a transparência das atividades de tratamento de dados e prestação de contas. Nota-se que, após a ocorrência do incidente, a avaliação do “risco ou dano relevante aos titulares” transcende inclusive o caráter mais genérico e hipotético dos relatórios de impacto (LUCIANO, 2019). De acordo com o art. 5º, inciso XVII, da LGPD, o relatório de impacto à proteção de dados é uma “documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação desses riscos. ”

De toda a discussão sobre a temática, depreende-se que a segurança e a prevenção de incidentes são premissas centrais para a tutela jurídica dos dados pessoais. Nesse sentido, a Lei prescreve aos agentes de tratamento a adoção de medidas 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 difusão. A LGPD exorta os operadores e controladores a estabelecer regras e procedimentos internos de governança corporativa em proteção de dados (art. 50), objetivando a mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. Nota-se que é de importância fundamental a definição do que sejam incidentes de segurança no âmbito da LGPD e adoção de procedimentos de gestão de crise e de proteção aos direitos e liberdades dos cidadãos.

3.6 LEGÍTIMO INTERESSE DO CONTROLADOR

Outro ponto de controvérsia na legislação protetiva de dados diz respeito ao conceito bastante elástico de legítimo interesse. A Lei 13.709/18 aponta que o tratamento de dados poderá ser realizado quando necessário visando atender aos “interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados

pessoais". Portanto, o legítimo interesse é hipótese legal que tem como objetivo possibilitar o tratamento de dados dos titulares, vinculados ao âmbito de atividades desenvolvidas pelo controlador e que encontrem justificativa plausível e legítima.

Essa questão é bastante discutível, considerando quão difícil é a delimitação de interesse legítimo à luz da gama de possibilidades interpretativas no mundo atual marcado pela cibernética e Inteligência Artificial. Os interesses legítimos são mais flexíveis e podem, em princípio, aplicar-se a qualquer tipo de tratamento para qualquer finalidade razoável. O art. 37 da LGPD destaca que o controlador e o operador devem manter registro das operações de tratamento de dados que realiza, "especialmente quando baseado no legítimo interesse". Esse cuidado do legislador aponta para uma necessidade de cautela ainda maior quando se utiliza o legítimo interesse como fundamento para o tratamento de dados. Ademais, no que concerne ao legítimo interesse do controlador ou de terceiros, as balizas de aplicação ainda precisam ser devidamente delineadas por regulação da Autoridade Nacional de Proteção de Dados (ANPD).

O autor Marcel Leonardi anota que o controlador deve realizar um teste triplo, ao decidir utilizar o legítimo interesse como base legal de tratamento. Esse teste é conhecido internacionalmente como avaliação de legítimo interesse (em inglês, Legitimate Interests Assessment – LIA):

> (i) teste da finalidade: identificação de qual é o interesse legítimo e se esse interesse legítimo é próprio ou de terceiros; (ii) teste da necessidade: demonstração de que o tratamento dos dados pessoais é necessário para alcançar esse interesse legítimo; e (iii) teste da proporcionalidade: balanceamento desse interesse legítimo com os direitos e as liberdades fundamentais do titular que exijam a proteção dos dados pessoais. (LEONARDI, 2019)

Impende ressaltar que o uso do legítimo interesse como base legal para o tratamento de dados pessoais gera um ônus argumentativo maior quanto ao princípio da finalidade visando evitar seu uso indiscriminado. Nos dizeres de Ricardo Bioni (2021) "a arquitetura normativa do legítimo interesse apresenta-se como uma nova e potencialmente mais flexível base legal para o tratamento de dados, mas por outro lado impõe ônus argumentativo por quem dele se vale".

O art. 7º, IX, da LGPD que trata sobre o legítimo interesse como base deve ser lido em consonância como todo o art. 10, que detalha a sua operacionalização. O legítimo interesse apresenta-se como uma base legal mais flexível, dinâmica e exatamente por isso requer o uso constante da técnica de balanceamento entre os interesses do titular, de terceiros e do controlador, além de considerar as garantias e liberdades individuais. Frise-se que, nos casos de tratamento de dados lícito por razões de interesse legítimo de um controlador ou de terceiro, o titular dos dados terá, ainda assim, com base em razões preponderantes e legítimas relacionadas com a sua situação específica, o direito de se opor ao tratamento dos seus dados pessoais.

Bioni também (2020) destaca o legítimo interesse como o requisito de conciliação entre a proteção de direitos e liberdades fundamentais e o livre desenvolvimento econômico. No entanto, enfatiza que a atividade de tratamento de dados não deve ser opaca, considerando que o legítimo interesse prescinde o consentimento do usuário. Pelo contrário, o dever de transparência é incrementado e reforçado, sendo franqueado ao cidadão o poder de tomada de decisão para se opor a um determinado tratamento de dados (*opt-out*), por considerar incompatibilidades com as suas legítimas expectativas. *Opt-out*, explica-se, é um termo técnico em inglês que faz referência à revogação do consentimento feito pelo titular de dados.

Percebe-se, portanto, que o assunto é controverso justamente por conta deste necessário e difícil sopesamento entre os interesses do controlador e de terceiros e os interesses que dizem respeito ao titular dos dados. Ainda assim o controlador deve adotar ações que mitiguem os riscos do titular dos dados, por exemplo a anonimização dos dados, buscando-se minimizar as incertezas decorrentes deste ponto controverso da LGPD.

A análise deste ponto controverso quanto ao tratamento de dados mostra que em determinadas operações a balança tende a estar em desequilíbrio por fugir das legítimas expectativas do titular dos dados, o que acaba impactando de forma negativa a própria autodeterminação informativa do titular. Por exemplo, algumas empresas verificam qual é o modelo do computador que está conectado ao site para, a partir de tal informação, exercer precificação dinâmica, colocando preços maiores para pessoas que têm computadores de marcas mais caras. São situações diversas

em que as operações realizadas pelos algoritmos possuem enorme potencial de impactar negativamente o poder de tomada de decisão do usuário para a aquisição de um produto. Assim, a volição do indivíduo é drasticamente afetada e manipulada por mecanismos de Inteligência Artificial.

Bioni (2021) argumenta que “a principal salvaguarda nesses casos é a adoção de mecanismos de transparência que permitam ao titular dos dados se opor a tal tipo de tratamento (*opt-out*)”. Quanto mais fácil for a implementação e o exercício do *opt-out,* ofertando ao titular a livre escolha para revogar seu consentimento dado anteriormente, maior também é a possibilidade de o legítimo interesse ser considerada como uma base legal válida. Ressalte-se que o princípio da transparência é um verdadeiro pilar da Lei nº 13.709/2018, resultando até mesmo na nulidade do consentimento requerido, quando “as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca” (Art. 9º, §1º).

O Considerando 47 da GDPR (General Data Protection Regulation) aponta que a existência de um interesse legítimo requer uma avaliação cuidadosa, em especial se “o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados pessoais são recolhidos, que esses poderão vir a ser tratados com essa finalidade.” Observa-se, na prática, que esse exercício preditivo por parte do titular é demasiadamente desafiador, considerando os algoritmos autômatos e diversos mecanismos de IA, Big Data e IoT que operacionalizam os dados a serem tratados.

Tendo como base o princípio da *accountability* (prestação de contas), argumenta-se que os controladores de dados precisam demonstrar a sua responsabilidade em balancear seus interesses diante dos titulares por meio de registros especificamente documentados, cuja previsão está no Art. 37 da LGPD. O dever de registro das atividades de tratamento de dados reforça o princípio da transparência, sendo exercido por intermédio de um teste de proporcionalidade que pondera entre os interesses dos controladores de dados e as medidas tomadas para a salvaguarda dos direitos do titular. O registro é feito em um documento intitulado “Legitimate Interest Assessment (LIA)” ou “Avaliação de Legítimo Interesse”. O ônus argumentativo é suportado pelo controlador, devendo demonstrar que existe real

legitimidade de seu interesse para a coleta e tratamento de dados do titular em razão da finalidade e necessidade apropriadas.

A divulgação do nome completo e outros dados de pessoas vacinadas contra a Covid-19, por força de leis municipais, não está em harmonia com a proteção constitucional à intimidade e à privacidade que decorre exatamente do artigo 5º, inciso X, da Constituição Federal, e agora do novo inciso LXXIX, acrescentado por força da Emenda Constitucional 115/2022. Questiona-se qual o legítimo interesse que fundamentaria tal divulgação, haja vista que a exposição de nomes e dados pessoais pode ter o efeito inibidor de desestímulo à vacinação contra o novo coronavirus. Qualquer iniciativa que envolva a utilização de dados pessoais para enfrentar a pandemia deve ser feita com prudência, transparência e obediência aos ditames legislativos sobre a temática. Frise-se que a proteção de dados é uma expressão de liberdade e dignidade da pessoa humana, e como tal, não se deve admitir num Estado Constitucional de Direito que os dados pessoais sejam usados de modo a transformar um indivíduo em objeto sob constante vigilância. É o que podemos denominar de “panóptico digital”, que entra em rota de colisão com os princípios da LGPD, em especial o princípio da finalidade cujo propósito é realização de tratamento de dados para propósitos legítimos, específicos e informados ao titular.

3.7. ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO DE DADOS PESSOAIS

O Art. 5º, inciso III da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2028) define dado anonimizados como o “dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento” e o inciso XI define anonimização como a “utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo”. O artigo 18, IV, da LGPD, apresenta como direito do titular dos dados pessoais a obtenção, junto ao controlador, da anonimização de dados desnecessários ou excessivos.

Por seu turno, o artigo 12 da LGPD estabelece que os dados anonimizados "não serão considerados dados pessoais, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido." Depreende-se do texto legal que a anonimização de dados pessoais é uma espécie de exclusão do vínculo da informação com a pessoa a qual se refere, cujo objetivo é diminuir os riscos presentes no tratamento dos dados armazenados.

No que diz respeito à pseudonimização, o artigo 13º, no parágrafo 4º, dispões que "pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro". Neste caso as relações adicionais para identificar os dados são mantidas em um banco à parte, com a possibilidade de maior liberdade de manipulação, desde que seja preservada a privacidade dos titulares da informação. Em suma, impossível não considerar que os dados anonimizados ou pseudonimizados continuam sendo dados pessoais, apenas, em tese, com maior garantia técnica quanto à sua privacidade.

A questão controversa trazida à baila reside justamente na possibilidade de reversão da anonimização ou da pseudonimização por terceiros, mediante "esforços razoáveis", cuja determinação, nos termos do § 1º do próprio artigo 12, "deve levar em consideração fatores objetivos, tais como custo e tempo necessários, de acordo com as tecnologias disponíveis." O problema é que já existem estudos científicos que comprovam a relativa facilidade com que essa reversão pode ser realizada, utilizando-se técnicas avançadas de mineração de dados ou algoritmos inteligentes que decifram procedimentos de anonimização. Segundo Rircardo Maffeis e Daniel Guariento (2020), há pesquisas sobre aprendizagem de máquina (*machine learning*) que apontam "a probabilidade de um indivíduo específico ser reidentificado a partir de bancos de dados anonimizados, ainda que incompletos."

Maffeis e Guariento (2020) concluem que as "técnicas tradicionais de anonimização podem não ser suficientes para manter-se aderente às regras de privacidade de dados de normas como a General Data Protection Regulation – GDPR." Nessa toada, há de considerar que a mesma realidade preocupante se coloca

para o Brasil, já que a LGPD foi bastante inspirada na GDPR e traz dispositivos bem parecidos com respeito à tutela da anonimização de dados pessoais.

Conforme aborda Moisés Simões, em artigo publicado no site do Serpro – Serviço Federal de Processamento de dados, o que se coloca é que dados anonimizados ou pseudonimizados só podem ser considerados como seguros enquanto não passarem por processos de reversão, por meios próprios ou mediante ação espúria de terceiros. Ademais, importante destacar que bases de dados anonimizados ou pseudonimizados "não são imunes a consultas com cruzamento de informações e identificação de padrões, ou que adotam engenharias sociais distintas e informações externas. " (SIMÕES, 2019).

Com a evolução cada vez mais acelerada das técnicas computacionais de banco de dados, cresce exponencialmente a dificuldade em garantir a efetiva anonimização de dados pessoais. Neste sentido, é salutar que a anonimização seja realizada por empresa independente (e não internamente pelo controlador) e mediante a "utilização continuada de técnicas de última geração, que sejam constantemente atualizadas, mantendo o estado da arte" (MAFFEIS; GUARIENTO, 2020).

O imbróglio que se apresenta neste contexto é a necessidade de se garantir a realização de uma anonimização segura e ao mesmo tempo eficaz para evitar que os dados, muito embora anonimizados, sejam considerados dados pessoais à luz do artigo 12 da LGPD, ao mesmo tempo sem riscos evidentes para a reversão em dados pessoais identificáveis. Para tal desiderato, torna-se imprescindível que haja um massivo investimento em modernas técnicas criptográficas e de mascaramento de dados, proporcionando mecanismos de garantia efetiva da privacidade.

Atualmente, é importante frisar que, com o volume, complexidade e velocidade dos chamados Big Data, surge a necessidade de ferramentas analíticas mais precisas e de desempenho exponencial para correlacionar e interpretar a gama de dados disponíveis. Por meio de correlações realizadas por algoritmos de inteligência artificial e com técnicas de aprendizagem de máquina, já é possível identificar pessoas com um nível de acurácia cada vez maior. Cada vez mais, o titular de dados está numa

situação de vulnerabilidade algorítmica diante dos avanços computacionais proporcionados pela indústria da Internet.

O que se pode esperar de conglomerados econômicos que buscam cada vez maior controle sobre sua carteira de usuários, com as possiblidades quase infinitas de manipulação dos dados e categorização das informações úteis para as empresas? A resposta a esta pergunta é deveras oportuna, visto que, mesmo com o arcabouço jurídico protetivo da privacidade de dados no Brasil trazido pela Lei 13.709/2018 e pela Emenda Constitucional nº 115/2022, ainda permanecem incertezas quanto aos procedimentos efetivos e seguros de ordem técnico-operacional utilizados no tratamento adequado dos dados pessoais. Na complexa tarefa de análise e manipulação de dados reverberam-se os ideais de autonomia e de empoderamento individual, que muitas vezes assumem contornos meramente formais. Torna-se questionável a validade do consentimento dado pelo usuário em razão do patente desconhecimento das intricadas situações que envolvem anonimização e pseudonimização de dados pessoais.

CONSIDERAÇÕES FINAIS

Não há como negar que a inovação tecnológica proporcionada pela Internet e pelos ecossistemas digitais, em especial diante da popularização dos *smarthphones*, criou um ambiente de incertezas quanto à consolidação dos direitos de personalidade humana, com destaque para a questão da privacidade pessoal. Considerando que o mundo on-line por vez é até mais intenso que o mundo real, é imprescindível que um arcabouço legar proporcione o ambiente jurídico propício para a continuidade das inovações tecnológicas sem menosprezo das garantias fundamentais da pessoa humana nesse contexto digital.

Neste cenário a Lei Geral de Proteção de Dados (Lei 13.709/2018) tem como intuito primário, como visto neste trabalho, enaltecer a dignidade da pessoa humana por meio de instrumentos que afastem a equiparação do homem a um valor medido em dados pessoais disponibilizados na Internet. Medidas eficazes devem ser adotadas por empresas e governos no sentido de reduzir prejuízos advindos da atividade informacional em rede, no tocante a minimizar os potenciais efeitos danosos derivados do rápido avanço da tecnologia sobre a privacidade do indivíduo. A discussão perpassa necessariamente por questões éticas que devem reger as relações no ambiente digital, especialmente quanto à transparência e boa-fé, ao mesmo tempo em que as empresas e governos investem em mecanismos de proteção de dados mais modernos e eficientes.

Ao longo deste trabalho, o assunto referente à carga principiológica contida na LGPD foi apresentado com o propósito de estabelecer as balizas para averiguação das práticas corriqueiras quanto ao tratamento de dados pessoais. A própria LGPD é exaustiva em apresentar princípios que devem ditar os rumos da privacidade on-line, garantindo aos cidadãos que suas informações pessoais não sejam violadas indevidamente ou utilizadas para propósitos diversos do que foi consentido. Neste diapasão, percebe-se uma ênfase bastante forte do legislador em fundamentar a proteção de dados pessoais em direitos humanos, no livre desenvolvimento da personalidade, na dignidade e no exercício da cidadania pelas pessoas naturais. Obviamente o desafio da implementação da Lei 13.709/2018 não se resume ao mero

entendimento dos princípios e fundamentos de sua existência, mas deve ser traduzido na prática em ações modeladoras de comportamento adequado das empresas e órgãos públicos, objetivando maior segurança às organizações e aos titulares dos dados.

A questão da gestão do risco destaca-se como um fator deveras relevante para as empresas no que se refere à implementação da LGPD. A fim de evitar judicialização de demandas envolvendo responsabilidade civil por danos causados, as organizações precisam identificar e reduzir os riscos relacionados ao tratamento de dados, por meio de planejamento rígido e medidas de *compliance* atualizadas. Um plano emergencial para incidentes de vazamento de dados também é essencial quando qualquer evento adverso afete direta ou indiretamente a tríade de segurança da informação: confidencialidade, integridade e disponibilidade dos dados. Ademais, a ANPD precisa estabelecer parâmetros coerentes para definição do que é “prazo razoável” para a comunicação de um vazamento de dados, considerando que um prazo em aberto gera enormes incertezas para as empresas que operam enormes quantidades de dados.

É um questionamento relevante se a Lei Geral de Proteção de Dados de fato trouxe um empoderamento ao titular de dados. Considerando as controvérsias envolvendo a LGPD em face das medidas de segurança da informação, em especial o consentimento do usuário, vislumbra-se ainda um cenário difícil para o pleno gozo do direito fundamental da autodeterminação informativa. Observa-se que o usuário médio de redes sociais ou consumidor on-line geralmente não atenta para as implicações de um mero clique no botão “Aceitar e Continuar” quanto solicitado por um determinado website. Os dados do usuário podem sofrer diversos tratamentos mediante algoritmos inteligentes e combinações matemáticas, muitos nem sequer consentidos inicialmente. Conclui-se, neste aspecto, que é temerário afirmar que Lei Geral de Proteção de Dados garantiu efetivamente um caráter protetivo ao titular de dados, considerando a vulnerabilidade diante de conglomerados econômicos poderosos que atuam na Web.

Outro ponto importante no debate da LGPD é a realidade do uso de *cookies* que são inegavelmente onipresentes no ambiente *on-line.* A utilização de cookies deve continuar se expandindo, principalmente em alguns modelos de negócio que

dependem de sistemas de rastreamento ou monitoramento do comportamento do usuário, como aqueles de publicidade direcionada. Percebe-se que, apesar da recente entrada em vigor da Lei 13.709/2018, cookies que se enquadram nessa categoria continuam sendo amplamente disparados por websites brasileiros sem qualquer observância aos ditames legais. O que se pode concluir é que vários *cookies* continuam sendo instalados no navegador do usuário sem o seu consentimento prévio e qualificado, pois o aviso sobre cookies é bastante genérico e na maioria das vezes não informa ao usuário quais dados serão coletados. Mudar este cenário é uma tarefa bastante intricada e desafiadora, pois o mercado tem dificuldades de compreender cookies como dados pessoais. Exige-se das empresas e de governos que haja maior transparência nas tratativas a respeito do armazenamento de *cookies* nos dispositivos dos usuários, com respeito às funcionalidades, finalidades, período de retenção, e terceiros que terão acesso. É imprescindível entender o funcionamento dessa ferramenta, seus riscos à privacidade dos usuários e como adequá-los ao contexto de proteção de dados no ordenamento jurídico brasileiro. Ademais, os titulares de dados, PROCONs, Ministérios Públicos, SENACON e a própria ANPD devem cobrar do mercado adequação à legislação, em especial quanto à submissão aos princípios e fundamentos da LGPD.

É sabido que as operações de tratamento de dados pessoais possuem riscos inerentes. O desafio é identificar esses riscos, compreender e avaliar o seu impacto e assim buscar mecanismos protetivos que possam mitiga-los, preservando os direitos de personalidade dos titulares. É oportuno salientar que os riscos podem ser reduzidos, retidos, evitados ou transferidos, mas dentro do escopo da LGPD é necessário averiguar com atenção o que se propõe diante dos chamados incidentes de segurança. No mundo da informática, computação em nuvem, inteligência artificial e algoritmos autônomos, necessário se faz que a legislação seja mais expansiva ao apresentar que critérios fundamentam a ocorrência de incidentes de segurança. Um vazamento de dados bancários de um cliente, por exemplo, por pontual que seja, ainda assim revela um risco que não foi devidamente averiguado. Mesmo que os dados não sejam utilizados indevidamente ou que não sejam dados sensíveis, prevalece a necessidade de se identificar e reportar aos responsáveis o incidente ocorrido. Neste aspecto, conclui-se que é possível valer-se das ferramentas previstas na LGPD para adoção de medidas que visem ao gerenciamento de riscos. Importante

destacar que as empresas que não possuem um planejamento de Governança de Proteção de Dados precisam de uma fiscalização mais incisiva da ANPD, com base em orientações claras de como os riscos e incidentes de segurança podem sem melhor avaliados. Assim, busca-se pavimentar um caminho interdisciplinar para a compreensão da temática à luz da LGPD, observando os paradigmas e metodologias que enxergam os incidentes de segurança sob o enfoque dos direitos e garantias dos titulares de dados pessoais.

Com relação ao legítimo interesse para o tratamento de dados, convém ressaltar que a adoção deste permissivo legal requer uma avaliação cuidadosa e argumentação mais robusta por parte do controlador ou terceiros, objetivando maior aderência ao princípio da finalidade do tratamento. Conclui-se que os controladores, ao realizar o enquadramento em legítimo interesse, precisam fundamentar sua análise conforme explicado pelo (LIA - Legitimate Interests Assessment) que será parte integrante do Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Sobre este ponto, o melhor entendimento do artigo 10, parágrafo 3º, da LGPD, é que sempre seja elaborado o RIPD no caso de tratamento de dados pessoais baseado em legítimo interesse, visto que a ANPD pode solicitar a qualquer tempo esse relatório. A conjuntura complexa que envolve a definição do que seja legítimo interesse em suas variadas aplicações, faz surgir a importância de se demonstrar que o tratamento de dados pessoais é necessário para alcançar a finalidade proposta, em perfeito equilíbrio com os interesses, direitos e liberdades do titular. O controlador deve levar em consideração se os titulares esperam razoavelmente que seus dados pessoais sejam tratados em acordo com as suas expetativas nas circunstâncias específicas. Em outras palavras, o legítimo interesse não deve resultar apenas do arbítrio do controlador ou de terceiros, mas transitar em harmonia com a legítima expectativa do titular, que precisa também ser respeitada à luz dos ditames protetivos insculpidos na Lei Geral de Proteção de Dados.

No tocante à anonimização ou pseudonimização de dados pessoais, a LGPD assegura que um conjunto de dados é considerado anonimizado quando não permite a reidentificação do titular dos dados. Ademais, o conjunto de dados anonimizado está resguardado da aplicação de sanções pela Autoridade Nacional de Proteção de Dados (ANPD). No entanto, em caso de reidentificação dos dados as punições da

LGPD são aplicáveis, o que faz surgir a necessidade de gestão e governança da segurança da informação muito bem avaliada e estruturada para preservação da privacidade dos titulares. Observa-se na atualidade uma evolução cada vez mais acelerada das técnicas computacionais que possibilitem a anonimização ou pseudonimização de dados pessoais, porém os recursos tecnológicos que possibilitam a reversão também avançam exponencialmente. Urge, portanto, que as empresas e governos invistam em técnicas seguras de anonimização somada a uma forte estratégia na gestão de riscos (governança da informação), objetivando a proteção do ativo relacionado ao conjunto de dados. Imperioso considerar que as medidas de segurança e decisões estratégicas relacionadas à privacidade dos usuários devem ser administradas tanto nos repositórios em que se encontram as os dados originais como nos que se encontram os dados anonimizados. Surge a preocupação quanto à reversibilidade dos dados anonimizados sem consentimento dos titulares, o que acarreta afronta aos princípios da transparência e boa-fé previstos na LGPD.

Para trabalhos futuros, deve-se considerar que a LGPD não tratou de alguns assuntos pertinentes. Apesar de representar uma legislação com fundamentos teóricos importantes (tendo como base o GPDR europeu), a Lei 13.709/2018 não trouxe regulamento em matérias importantes como: dados pessoais em relações trabalhistas, tratamento de dados em investigações criminais e infrações administrativas, direito ao esquecimento, biotecnologia, perfirização, videovigilância, subcontratação, aspectos técnicos de segurança, conduta e certificação digital, documentos públicos e certificação digital, tratamento de dados feito por entidades religiosas, entre outros assuntos. Estes temas podem até ser regulamentados pela Autoridade Nacional de Proteção de Dados, mas é imprescindível o debate sério sobre o conteúdo e abrangência deles.

Com a evolução das tecnologias digitais surgem também novos deveres que devem estar harmonizados com a LGPD. São necessárias medidas amplas de transparência, também em relação à publicidade on-line e aos algoritmos utilizados para recomendar conteúdo aos usuários. Ademais configura-se como urgente a elaboração de um processo de cooperação inovador entre os atores que lidam diretamente com proteção de dados (encarregado, operador, controlador, ANPD) para

garantir uma aplicação eficaz da legislação. É oportuno que sejam estabelecidas novas obrigações para plataformas muito grandes (Google, Amazon), que precisam tomar medidas baseadas em risco para prevenir abusos nos seus sistemas *on-line*, bem como precauções de proteção dos usuários para que seus conteúdos não sejam apagados erroneamente das plataformas.

Conclui-se, pelas observações e discussões deste trabalho, que a Lei Geral de Proteção de Dados é uma lei aberta, propositalmente lacunosa, com algumas incertezas e de pontos deixados sem definição clara e específica pelo Poder Legislativo, pendentes de regulamentações futuras por parte da ANPD, que se tornou recentemente uma autarquia de natureza especial por meio da Medida Provisória (MPV) nº 1.124, de 13 de junho de 2022. Com essa Medida Provisória, a Autoridade Nacional de Proteção de Dados terá maior autonomia para o desempenho de suas competências legais, inclusive quanto à gestão administrativa do órgão.

Portanto, há um longo caminho a ser percorrido para a adequação às normas de proteção de dados, além de uma maior transparência com relação os processos que envolvem o tratamento de dados do titular. Fica evidente que a legislação não consegue abranger os vários ramos de negócios que envolvem proteção de dados, considerando a complexidade e as diferentes formas com que cada modelo de negócio trata dados. Será imprescindível que o órgão regulador responsável (ANPD) crie regulamentações específicas para atender determinados setores do mercado *on-line*, sem destoar do propósito basilar da LGDP, qual seja a preservação da dignidade da pessoa humana ainda que nos meios digitais.

Com o fito de regulamentar as relações entre pessoas e algoritmos, o Direito precisa se adaptar aos novos contornos sociais e fáticos que revestem a hodierna sociedade digital. De todo modo, é inconteste que ocorra um equilíbrio entre o direito à privacidade pessoal e o desenvolvimento de novos produtos e serviços (inovação tecnológica), considerando que os avanços da Internet, dos Big Data e IoT, estabelecem um caminho sem ponto de retorno.

REFERÊNCIAS

BARRETO, Ricardo. **Dados, informação, conhecimento e inteligência.** Disponível em: <https://www.ricardobarreto.com/blog/index.php/2019/09/14/dados-informacao-conhecimento-e-inteligencia/> Acesso em: 28.05.2022.

BAUMAN, Zygmunt. **Modernidade Líquida.** Rio de Janeiro: Editora Jorge Zahar, 2001.

BEZERRA, André Luís Martins; WEBERBAUER, Paul Hugo (Orient.). **A Lei 13.709/18 e os novos desafios da proteção de dados pessoais e identidade.** Faculdade de Direito do Recife - CCJ - Universidade Federal de Pernambuco - UFPE - Recife, 2019. Disponível em: <https://repositorio.ufpe.br/handle/123456789/36323> Acesso em 27.06.2021.

BIONI, Bruno Ricardo. **Xeque-mate: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil.** São Paulo: GPoPAI/USP, 2015. Disponível em: <https://bit.ly/2RXzhDB> Acesso em: 29.06.2021.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento.** São Paulo: Editora Forense, 2019. Edição digital.

BIONI, Bruno Ricardo. **Legítimo Interesse: aspectos gerais a partir de uma visão obrigacional.** In: Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018: Lei Geral de Proteção de Dados (LGPD).** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 30.06.2021.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade (ADI) nº 6.387 MC-REC /DF.** Relatora: Ministra Rosa Weber. Disponível em: <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629>. Acesso em: 30.06.2021.

CARVALHO, Victor Miguel Barros de. **O Direito fundamental à privacidade ante a monetização de dados pessoais na internet: apontamentos legais para uma perspectiva regulatória.** Dissertação (Mestrado em Direito) - Centro de Ciências Sociais Aplicadas, Universidade Federal do Rio Grande do Norte, Natal, 2018. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/510/384>. Acesso em 28.06.2021.

CASTELLS, Manuel. **A sociedade em rede: economia, sociedade e cultura.** vol. 1 - 6ª edição. São Paulo: Paz e Terra, 2011.

_____. **Redes de indignação e esperança: movimentos sociais na era da Internet.** 2ª edição revista e atualizada. São Paulo: Jorge Zahar, 2013.

COELHO, Diego Henrique Damasceno; JUNIOR, Alberto Nogueira (Orient.). **Regime jurídico da proteção de dados pessoais e a implementação da Lei nº 13.709/2018 no Brasil: a reafirmação de direitos humanos e constitucionais.** Dissertação de Mestrado. Universidade Federal Fluminense – UFF – Rio de Janeiro, 2020. Acesso em 28.06.2021.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro: Teoria Geral do Direito Civil**. 33ª ed. Volume 1. São Paulo: Saraiva, 2016.

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados.** São Paulo: Edição digital do Kindle, 2019.

FALEIROS, José Luiz de Moura; LONGHI, João Victor Rozatti. **Estudos Essenciais de Direito Digital.** LAECC. Uberlândia: Edição do Kindle, 2019.

FILHO, Sergio Cavalieri. **Programa de Responsabilidade civil.** 10. ed. São Paulo: Atlas, 2012.

FORNASIER, Mateus de Oliveira; KNEBEL, Noberto Milton Paiva. **O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados na Lei Geral de Proteção de Dados.** Revista Direito e Práxis, junho, 2020. Disponível em: <https://www.e-publicacoes.uerj.br/index.php/revistaceaju/article/view/46944/33907> Acesso em: 04.04.2022.

GERMANI D'AVILA, Ana Vitória; SILVA, Bruna Fabiane; ARAÚJO, Thiago Volpi de. **LGPD: muito além da Lei: Uma análise do direito em conjunto com a segurança da informação.** Edição do Kindle, 2020.

LEONARDI, Marcel. **Legítimo Interesse.** Revista do Advogado. ANO XXXIX, Nº 144. Novembro, 2019.

LIMA, Humberto Alves de Vasconcelos. **A Tutela Jurídica dos Dados Pessoais no Brasil: Estudo sistemático da Lei Geral de Proteção de Dados**. 2ª Edição independente. São Paulo: Edição do Kindle, 2021.

LUCIANO, Maria. **Vazamentos de dados na LGPD: em busca do significado de "incidentes de segurança".** Revista do Advogado, Ano XXXIX, nº 144. Novembro, 2019.

MAFFEIS, Ricardo; GUARIENTO, Daniel Bittencourt. **A efetividade da anonimização de dados pessoais.** Disponível em: <https://www.migalhas.com.br/coluna/impressoes-digitais/319519/a-efetividade-da-anonimizacao-de-dados-pessoais>. Acesso em 14.06.2022.

MAGRANI, Eduardo. **Entre Dados e Robôs: Ética e Privacidade na Era da Hiperconectividade.** Rio de Janeiro: Arquipélago Editorial, 2019.

MAGRANI, Eduardo**. A internet das coisas**. Rio de Janeiro: FGV Editora, 2018.

MAIMONE, Flávio Henrique Caetano de Paula. **Responsabilidade civil na LGPD: efetividade na proteção de dados** - Indaiatuba, SP: Editora Foco, 2022. ePUB

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de Dados comentada [livro eletrônico]** – 2. ed. rev., atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2020.

MANTOVANI, Alexandre Casanova; MENKE, Fabiano (Orient.). **O consentimento na disciplina da proteção dos dados pessoais: uma análise dos seus fundamentos e elementos.** Dissertação de Mestrado - Universidade Federal do Rio Grande do Sul. Faculdade de Direito. Programa de Pós-Graduação em Direito – Porto Alegre, 2019. Disponível em: <https://www.lume.ufrgs.br/handle/10183/203810> Acesso em 30.06.2021.

MENDES, Gilmar Ferreira. **Curso de direito constitucional**, 14. ed. rev. e atual. São Paulo: Saraiva Educação, 2019.

MENDES, Laura Schertel; FONSECA, Gabriel C. Soares. **Proteção de dados para além do consentimento: Tendências contemporâneas de materialização.** Revista Estudos Institucionais, v. 6, n. 2, p. 507-533, maio/ago. 2020.

MIRAGEM, Bruno. **Responsabilidade Civil.** Barueri: Grupo GEN, 2021. 9788530994228. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994228/. Acesso em: 03 mai. 2022.

MOURA, Natalia Mirella Melo de; FREIRE, Cristiniana Cavalcanti (Orient.). **A efetivação do direito à privacidade digital e proteção de dados no Brasil.** Faculdade de Direito do Recife - CCJ - Universidade Federal de Pernambuco - UFPE - Recife, 2019. Disponível em: <https://repositorio.ufpe.br/handle/123456789/37121> Acesso em 26.06.2021.

MORAES, Alexandre Fernandes. **Segurança em Redes - Fundamentos.** São Paulo: Editora Saraiva, 2010. 9788536522081. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788536522081>. Acesso em: 30 mai. 2022.

PALHARES, Felipe**. Temas atuais de proteção de Dados.** São Paulo: Thomson Reuters Brasil, 2020.

PESTANA, Márcio. **Os princípios no tratamento de dados na Lei Geral da Proteção de Dados Pessoais.** Revista Consultor Jurídico, 25 de maio de 2020. Disponível em: <https://www.conjur.com.br/2020-mai-25/marcio-pestana-principios-tratamento-dados-lgpd>. Acesso em: 28.06.2021.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD)** – 2. ed. – São Paulo: Saraiva Educação, 2020. Edição do Kindle.

SARLET, G. B. S.; CALDEIRA, C. **O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana.** Revista civilistica.com, v. 8. n.1. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/411. Acesso em: 03.05.2022.

SCOUBLE, Robert; ISRAEL, Shel. **Age of Context: Mobile, Sensors, Data and The Future of Privacy.** First Edition – Patrick Brewster Press, 2013. Kindle Edition.

SIMÕES, Moisés. **Anonimização e pseudonimização são o suficiente?** Disponível em: <https://bit.ly/3Qlon9K> Acesso em: 14.06.2022.

SOARES, Pedro Silveira Campos. **A questão do consentimento na Lei Geral de Proteção de Dados.** Revista Consultor Jurídico, 11 de maio de 2019. Disponível em: <https://www.conjur.com.br/2019-mai-11/pedro-soares-questao-consentimento-lei-protecao-dados>. Acesso em 28.06.2021.

SOLOVE, Daniel J. **Introduction: Privacy self-management and the consent dilemma. Harvard Law review.** V. 126, p. 1880-1903, 2013. Available from: <https://harvardlawreview.org/wp-content/uploads/pdfs/vol126_solove.pdf> Acesso em: 24.05.2022.

SOUSA, R. P. M. de; TAVARES DA SILVA, P. H. **Proteção de dados pessoais e os contornos da Autodeterminação Informativa.** Informação e Sociedade: Estudos, [S. l.], v. 30, n. 2, 2020. DOI: 10.22478/ufpb.1809-4783.2020v30n2.52483. Disponível em: <https://periodicos.ufpb.br/ojs2/index.php/ies/article/view/52483>. Acesso em: 26.06.2021.

TEFFÉ, C. S. de; VIOLA, M. **Tratamento de dados pessoais na LGPD: estudo sobre as bases legais.** Revista civilistica.com, v. 9, n. 1, p. 1-38, 9 de maio 2020. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/510> Acesso em 28.06.2021.

TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei Geral de Proteção de Dados Pessoais: comentado artigo por artigo.** Salvador: Editora JusPodivm, 2019.

TEPEDINO, Gustavo**. Lei geral de proteção de dados pessoais e suas repercussões no Direito brasileiro [livro eletrônico].** 2. ed. - São Paulo: Thmoson Reuters Brasil, 2020.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação, efetividade desse direito fundamental diante dos avanços da tecnologia da informação.** Porto Alegre: Sergio Antonio Fabris Editor, 2007.

WOLFGANG, Hoffmann-Riem. **Teoria Geral do Direito Digital.** Barueri: Grupo GEN, 2021. 9786559642267. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786559642267>. Acesso em: 26.04.2022.