UNIVERSIDADE DO ESTADO DO RIO GRANDE DO NORTE
FACULDADE DE DIREITO

RAFAELA ALVES DE ALBUQUERQUE

A DIGNIDADE DA PESSOA HUMANA NA PROTEÇÃO DE DADOS PESSOAIS E SENSÍVEIS: UMA ANÁLISE À LUZ DA CONSTITUIÇÃO FEDERAL DE 1988 E A LEI Nº 13.709/2018

MOSSORÓ
2021

RAFAELA ALVES DE ALBUQUERQUE

A DIGNIDADE DA PESSOA HUMANA NA PROTEÇÃO DE DADOS PESSOAIS E SENSÍVEIS: UMA ANÁLISE À LUZ DA CONSTITUIÇÃO FEDERAL DE 1988 E A LEI Nº 13.709/18

Monografia apresentada à Universidade do Estado do Rio Grande do Norte – UERN – como requisito obrigatório para obtenção do título de Bacharel em Direito.

Orientadora: Profa. Me. Veruska Sayonara de Góis

MOSSORÓ
2021

RAFAELA ALVES DE ALBUQUERQUE

A DIGNIDADE DA PESSOA HUMANA NA PROTEÇÃO DE DADOS PESSOAIS E SENSÍVEIS: UMA ANÁLISE À LUZ DA CONSTITUIÇÃO FEDERAL DE 1988 E A LEI Nº 13.709/18

Monografia apresentada à Universidade do Estado do Rio Grande do Norte – UERN – como requisito obrigatório para obtenção do título de Bacharel em Direito.

BANCA EXAMINADORA

_____

Profa. Me. Veruska Sayonara de Góis

UNIVERSIDADE DO ESTADO DO RIO GRANDE DO NORTE

_____

Prof.

UNIVERSIDADE DO ESTADO DO RIO GRANDE DO NORTE

_____

Prof.

UNIVERSIDADE DO ESTADO DO RIO GRANDE DO NORTE

Catalogação da Publicação na Fonte.

Universidade do Estado do Rio Grande do Norte.

S729t Albuquerque, Rafaela Alves de. A DIGNIDADE DA PESSOA HUMANA NA PROTEÇÃO DE DADOS PESSOAIS E SENSÍVEIS: UMA ANÁLISE À LUZ DA CONSTITUIÇÃO FEDERAL DE 1988 E A LEI Nº 13.709/18/ Rafaela Alves de Albuquerque. - Mossoró, 2021. 60p.

Orientador(a): Profa. Me. Veruska Sayonara de Góis.
Monografia (Graduação em Direito). Universidade do Estado do Rio Grande do Norte.

1. Lei Geral de Proteção de Dados. 2. Constituição Federal de 1988. 3. Dignidade Humana. 4. Responsabilidade Civil. I. GÓIS, Veruska Sayonara de. II. Universidade do Estado do Rio Grande do Norte. III. Título.

O serviço de Geração Automática de Ficha Catalográfica para Trabalhos de Conclusão de Curso (TCC´s) foi desenvolvido pela Diretoria de Informatização (DINF), sob orientação dos bibliotecários do SIB-UERN, para ser adaptado às necessidades da comunidade acadêmica UERN.

Ao meu irmão Cláudio Alves de Albuquerque, que me deu forças para correr atrás dos meus sonhos e acreditar que sou capaz de conquistar o mundo, meu amor é e sempre será seu, meu Dinho.

AGRADECIMENTOS

Imperioso se faz realizar o agradecimento expresso ao maior provedor e o que me mostra a cada segundo a beleza da vida, assim como me proporciona a força para superar cada dificuldade. Obrigada Deus, por tantas bênçãos que me são concedidas diariamente.

Aos meus pais, Cláudio e Fábia, que me geraram, criaram e me formaram para eu ser capaz de realizar todos os meus sonhos. Vocês me mostram o sentido do mais puro amor em cada abraço, cada sorriso e até mesmo nos momentos de ser chamada atenção. Sem vocês nada seria possível. Vocês são meu tudo.

Daniel, obrigada por ser tão compreensível, companheiro e justo.

Fernanda, sua amizade constante me trouxe forças em momento de desespero, alegria em momentos tristes e determinação em momentos desafiadores.

Claudinho, sinto sua presença e seu amor todos os dias. Lembro-me de quando você me disse: “você vai conquistar tudo que quiser”, com tanta fé, que eu acreditei também.

Aproveito para agradecer a todos os meus familiares, em especial Cristina, Renato, Isabel, Flávio e Silvio.

Regina, sua amizade me é um balsamo calmante em meio a tempestade. Obrigada por ser tão presente, carinhosa, atenciosa e tão compreensível. Laços de sangue se tornam quase insignificantes em vista de nosso laço de alma.

A Laura, que foi a melhor amizade que a faculdade de direito da UERN me proporcionou e que me apoiou todos os dias desde então, em momentos difíceis ou apenas em risadas necessárias. Que seja a amizade de uma vida.

Professora Veruska, a senhora foi uma das presenças mais marcantes e significantes em todo meu curso. Mais que apenas um exemplo de profissional, a senhora se tornou um exemplo de vida. Obrigada por me acompanhar desde o primeiro período, até o último. Se fez presente quando eu precisei, me apoiou em momentos de dor e me orientou além do mundo acadêmico, mas para toda uma vida. Palavras não descrevem o carinho e orgulho que tenho da senhora, como ser humana. Obrigada por tudo.

Gregório Vieira, nossas brincadeiras e risadas sempre despertavam o que ha de melhor em mim.

A Carlos Henrique, por ter sido sempre compreensível nos meus momentos de dificuldade.

Mariana Cardoso, Rafaella Reis, Myrelle Leal, vocês são o sopro de vida e força que distância alguma consegue separar de mim. Começou no colégio, fica para a eternidade.

Obrigada por cada palavra e momento. Por cada mensagem, cada preocupação e por serem sempre essa vinha de luz em minha vida.

RESUMO

O emergente desenvolvimento tecnológico e a era digital em uma sociedade *hiperconectada* trouxeram desafios para o ordenamento jurídico, no intuito de resguardar, dentre outras questões, o fluxo de informação em um contexto de necessária proteção ao uso de dados e os direitos fundamentais de seu titular. As redes sociais e as modificações advindas dessas alterações promoveram um ambiente de desafios constantes para a imposição de limites para a manipulação de dados e o resguardo a privacidade, intimidade e dignidade humana. Dentro desse ambiente, existe a problemática do consentimento a ser dado de maneira válida, específica e expresso, assim como uma possível responsabilização civil em vista do uso indevido de dados. Nesse contexto, esta monografia aborda aspectos e norteadores da proteção de dados pessoais, enfocando na dignidade humana, o direito digital e a doutrina da responsabilidade civil. Além disso, trata-se de uma pesquisa histórica classificada como qualitativa e quantitativa, combinando elementos da literatura e dados quantitativos, a partir da visão conceitual. O resultado do projeto demonstra a necessidade do ordenamento jurídico interpor mecanismos eficientes para promover a dignidade humana do indivíduo através da sua proteção de dados pessoais, evitando o uso indevido destes, assim como determinando sanções para o caso de vazamento e uso indevido.

Palavras-chave: Lei Geral de Proteção de Dados. Constituição Federal de 1988. Dignidade Humana. Responsabilidade Civil.

ABSTRACT

The emerging technological development and the digital age in a *hyperconnected* society brought challenges to the legal system, in order to safeguard, among other issues, the flow of information in a context of data use and the fundamental rights of its holder. Social networks and the changes arising from these changes promoted an environment of constant challenges to the imposition of limits on data manipulation and the safeguarding of privacy, intimacy and human dignity. Within this environment, there is the issue of consent to be given in a valid, specific and express way, as well as possible civil liability in view of the misuse of data. In this context, this monograph addresses fundamental legal aspects and guidelines for the protection of personal data, focusing on human dignity, digital law and the doctrine of civil liability. Furthermore, it is a historical research classified as qualitative and quantitative, combining elements from the literature and quantitative data, based on the conceptual view. The result of the project demonstrates the need for the legal system to interpose efficient mechanisms to promote the human dignity of the individual through the protection of personal data, preventing their misuse, as well as determining sanctions in the case of leakage and misuse.

Keywords: Lei Geral de Proteção de Dados. Constituição Federal de 1988. Human dignity. Civil responsability.

LISTA DE SIGLAS

ADI	Ações Diretas de Inconstitucionalidade
ANDP	Autoridade Nacional de Proteção de Dados
IBGE	Instituto Brasileiro de Geografia e Estatísticas
LGPD	Lei Geral de Proteção de Dados
MP	Medida Provisória
PEC	Proposta de Emenda Constitucional
STF	Supremo Tribunal Federal

SUMÁRIO

1 INTRODUÇÃO

O desenvolvimento tecnológico alterou a forma como ocorrem os processos sociais e a sociedade como um todo. O Direito, enquanto ciência social, passa a conviver com o fenômeno tecnológico e surge a necessidade de adequar-se a uma sociedade *hiperconectada*. Assim, a dignidade da pessoa humana enquanto princípio fundamental deve ser respeitada a partir de um novo conceito de uso, armazenamento e transferência de dados na sociedade contemporânea.

A regulamentação da proteção de dados pessoais está diretamente relacionada com o processo de globalização, que com o avanço tecnológico, passou a exigir um maior controle a partir da dependência do fluxo de dados para o seu próprio funcionamento.

Nesse contexto, ganha notoriedade os dados pessoais e sensíveis, principalmente considerando que estes passam a ser um valioso ativo no mundo pós-moderno. Desse modo, torna-se essencial saber como, por quem e com qual finalidade estes dados estão sendo utilizados, e se os direitos fundamentais estão sendo respeitados.

Diante disso, elegeu-se como objetivo geral para esse trabalho, analisar criticamente os usos dos dados pessoais e sensíveis à luz da Constituição Federal de 1988 e a Lei nº 13.709/18 (Lei de proteção de dados pessoais), além de empreender a defesa e consolidação dos direitos e garantias fundamentais do cidadão, o que a reveste de notória legitimidade aos seus propósitos.

Pretende-se verificar, ainda, a problemática do consentimento e suas vertentes dentro de uma sociedade baseada em dados, analisando o recente posicionamento do Supremo Tribunal Federal (STF) a respeito dos dados pessoais como direito fundamental, assim como a responsabilidade civil em meio ao uso indevidos destes dados, considerando o ordenamento jurídico brasileiro. O intuito maior é entender como se pode impor o controle de dados por parte do Estado, em prol da dignidade humana do titular, inibindo formas de violação de direitos fundamentais.

Sob o ponto de vista metodológico, trata-se de um estudo bibliográfico, que recorrerá a fontes secundárias, tais como livros e artigos, de natureza descritiva, recurso a fontes históricas, bem como a análise de dados colhidos de relatórios e matérias jornalísticas, o que faz do presente estudo uma análise de natureza quanti-qualitativa.

Em relação ao aspecto estrutural, no primeiro capítulo trazem-se breves considerações acerca da declaração e reconhecimento dos direitos fundamentais, em especial da dignidade da pessoa humana e sua relação com o uso irrestrito de dados pessoais.

No segundo capítulo aborda-se a questão do consentimento válido, tendo em vista que, por diversas vezes o consentimento dado é apenas fictício, sendo que o próprio titular de dados não tem real ciência de como se dará o uso de seus dados, terceiros que terão acesso e o real controle sobre os meios utilizados de segurança na rede.

Já no terceiro capítulo, apresenta-se uma análise de recente julgado do STF em torno da proteção de dados pessoais, assim como a questão da responsabilidade civil para indenizar os danos causados aos titulares ou mesmo a sociedade em uso indevido de dados, a partir da legislação brasileira sobre o tema, em especial a Lei Geral de Proteção dos Dados (LGPD).

2 A RELAÇÃO ENTRE O PRINCÍPIO CONSTITUCIONAL DA DIGNIDADE DA PESSOA HUMANA E DA PRIVACIDADE COM O USO IRRESTRITO DE DADOS

Faz-se imperioso delimitar bases para a compreensão dos requisitos essenciais da dignidade da pessoa humana, um conceito abstrato que norteia todo o ordenamento jurídico brasileiro.

Hannah Arendt (2017) ao tratar do tema em seu livro *A Condição Humana*, trouxe a relação entre a *vita activa* e a condição humana, designando que a atividade humana estava fundamentada em trabalho, obra e ação. Cada uma delas corresponderia a uma condição básica da vida humana. Para esta renomada escritora, a condição humana do trabalho é a própria vida. Na mesma perspectiva concorda Silva (2017, p. 93-94):

> A pluralidade é a condição da ação humana porque somos todos iguais, isto é, humanos, de um modo tal que ninguém jamais é igual a qualquer outro que viveu, vive ou viverá. Todas as três atividades e suas condições correspondentes estão intimamente relacionadas com a condição mais geral da existência humana: o nascimento e a morte, a natalidade e a mortalidade. O trabalho assegura não apenas a sobrevivência dos indivíduos, mas a vida em espécie. A obra e seu produto, o artefato humano, conferem uma medida de permanência e durabilidade à futilidade da vida mortal e ao caráter efêmero do tempo humano. A ação, na medida em que se emprenha em fundar e preservar corpos políticos, cria a condição para a lembrança [*remembrance*], ou seja, para a história. [...] A condição humana compreende mais que as condições sob as quais a vida foi dada ao homem. Os homens são seres condicionados, porque tudo aquilo com o que eles entram em contato torna-se imediatamente uma condição de sua existência. O mundo no qual transcorre a *vita activa* consiste em coisas produzidas pela atividades humanas; mas as coisas que devem sua existência exclusivamente aos homens constantemente condicionam, no entanto, os seus produtores humanos.

Pode-se afirmar, portanto, que tudo que mantenha uma relação com a vida do indivíduo consiste em um caráter da condição humana. Tudo que adentra ao mundo humano, por si só, torna-se parte da condição humana. Desse fato decorre a necessidade de proteção dos mais diversos setores, entre eles, a tecnologia e o uso de dados.

A tecnologia influi diretamente em parte do aspecto da vida do mundo contemporâneo. A maior parte da atividade humana desempenhada tem, em algum aspecto, influência tecnológica. Porém, essa influência deve ser observada e controlada, sem limitar completamente o desenvolvimento, de maneira a resguardar a dignidade humana.

O uso das tecnologias e, consequentemente, de dados, faz parte da capacidade humana em transformar o ambiente ao seu redor otimizando, assim, os meios para obter resultados mais vantajosos, menos onerosos e, de certo modo, informações privilegiadas.

Por outro lado, sabe-se que o ordenamento jurídico é norteado basicamente por normas (regras e princípios, segundo uma classificação bastante aceita), que conforme elucida Arendt (2017, p. 212):

> [...] são preceitos que tutelam situações subjetivas de vantagem ou de vínculo, ou seja, reconhecem, por um lado, a pessoa ou a entidades a faculdade de realizar certos interesses por ato próprio ou exigindo ação ou abstenção de outrem, e, por outro lado, vinculam pessoas ou entidades à obrigação de submeter-se às exigências de realizar uma prestação, ação ou abstenção em favor de outrem. Os princípios são ordenações que se irradiam e imantam os sistemas de normas, são [como observam Gomes Canotilho e Vital Moreira] 'núcleos de condensações' nos quais confluem valores e bens constitucionais.

Nessa perspectiva, a Constituição Federal de 1988 declara invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, em seu art. 5º, X (BRASIL, 1988), direitos diretamente relacionados a ideia de dados.

Sendo assim, o intenso desenvolvimento das tecnologias no mundo globalizado e a consequente complexidade de utilização de dados pessoais e sensíveis, em um mundo *hiperconectado*, acaba se mostrando poderosa ameaça à privacidade e intimidade dos indivíduos, bem como salienta Silva (2017, p. 182):

> O amplo sistema de informações computadorizadas gera um processo de esquadrinhamento das pessoas, que ficam com sua individualidade inteiramente devassada. O perigo é tão maior quanto mais a utilização da informática facilita a interconexão de fichários com a possibilidade de formar grandes bancos de dados que desvendem a vida dos indivíduos, sem sua autorização e até sem seu conhecimento. A Constituição não descurou dessa ameaça. [...] A violação a privacidade, portanto, encontra no texto constitucional remédios expeditos. Essa violação, em algumas hipóteses, já constitui ilícito penal. Além disso, a Constituição foi explícita em assegurar, ao lesado, direito a indenização por dano material ou moral decorrente da violação da intimidade, da vida privada, da honra e da imagem das pessoas, em suma, do direito à privacidade.

Assim, é possível fazer menção ao contexto do mundo globalizado e suas consequências multidimensionais, entre elas, o uso irrestrito de dados pessoais e sensíveis. O avanço da integração tecnológica reconfigurou o desenho mundial e de suas culturas. Por isso que o estudo da história e da cultura é de vital importância para a proteção de se adentrar, inconscientemente, em duas propensões opostas, extremas e negativas, quais sejam: acreditar

que as sociedades não podem mudar, ou acreditar que elas podem mudar facilmente pela imposição da vontade de alguém. Na leitura de Schwartzman (2004, p. 115):

> Mas a pesquisa a experiência dos últimos séculos e a grande quantidade de pesquisas e estudos desenvolvidos para entender e explicar os diferentes destinos das pessoas sob ataque de desenvolvimento capitalista e os avanços da tecnologia são os últimos recursos que temos para lidar com os desafios antigos e novos que precisamos enfrentar.

Sabe-se que a globalização teve um importante papel na penetração das sociedades nacionais pelos mais diversos tipos de redes, levando desenvolvimento e tecnologia em um ímpeto nunca antes imaginado. Todavia, tal desenvolvimento vem atrelado a uma série de desavenças, sendo a proteção social e os direitos humanos uma preocupação de suma importância para resguardar a dignidade humana na utilização desse avanço de novas tecnologias.

Nesse aspecto, existem basicamente duas visões acerca da proteção social e os direitos humanos no mundo globalizado, que podem ser percebidos pela elucidação de Fonseca (2021, p. 39):

> Existem duas formas de pensar sobre a proteção social e os direitos humanos, uma procurando se apoiar na sabedoria e na experiência de instituições tradicionais, a outra tentando utilizar interpretações racionais sobre a natureza humana como fundamento do que deveriam ser os direitos humanos básicos. Tipicamente, os que aderem à primeira visão tendem a olhar para as sociedades como um todo, em lugar de indivíduos isolados, e evitam julgar instituições e tradições especificas a partir de normas abstratas, derivadas de sua própria cultura. Antropólogos comprometidos com a interpretação e a coerência interna das culturas costumam adotar essa visão, conscientes dos efeitos devastadores da introdução de valores e comportamentos exógenos nas sociedades tradicionais. No outro extremo, a visão universalista, tipicamente moderna, considera que algumas formas de conhecimento, comportamento e expressão são melhores que outras, e que é possível definir, em abstrato, como a sociedade deveria ser organizada para maximizar os direitos e potenciais humanos. Nessa perspectiva, os seres humanos teriam uma natureza universal e direitos também universais, independentemente de culturas e épocas históricas. No campo específico dos direitos humanos, é possível acompanhar a abordagem racional através de uma linhagem notável de filósofos racionalistas, desde Emmanuel Kant a Amartya Sem e John Rawls, cada qual tratando de definir a seu modo, o que é o comportamento moral, o que é a justiça e qual a melhor forma de organizar a sociedade para que a ética e a justiça prevaleçam.

O empasse que pode ser observado é que enquanto as empresas de tecnologia são multinacionais, os estados procuram enfrentar as questões em nível nacional. O respeito ao princípio basilar da dignidade da pessoa humana vem sendo sedimentado ao longo do ordenamento jurídico brasileiro após a Constituição Federal de 1988. Está ocorrendo à

sedimentação na percepção de cada indivíduo e sua obrigação moral, sendo essa conscientização tem contribuído de forma decisiva para lhe conferir alcance geral.

2.1 A DIGNIDADE HUMANA E O DIREITO À PRIVACIDADE

Percebe-se que a primazia humana e, consequentemente, da dignidade da pessoa humana é uma resposta à crise sofrida pelo excessivo positivismo jurídico do século XX, que justificou acontecimentos como o fascismo, nazismo e a ditadura militar brasileira, cometendo as mais diversas atrocidades, sem contemplar o mínimo vital humano.

No cenário brasileiro, a Constituição de 1988 representou um marco jurídico de institucionalização de direitos e garantias fundamentais, como assim leciona Piovesan (2008, p. 49):

> O texto demarca a ruptura com o regime autoritário militar instalado em 1964, refletindo o consenso democrático "pós ditadura". Introduz o texto constitucional avanço extraordinário na consolidação das garantias e direitos fundamentais, situando-se como documento mais abrangente e pormenorizado sobre os direitos humanos jamais adotados no Brasil. A Carta de 1988 destaca-se como uma das Constituições mais avançadas do mundo no que diz respeito à matéria. [...] Dentre os fundamentos que alicerçam o Estado Democrático de Direito brasileiro destacam-se a cidadania e dignidade da pessoa humana (art. 1º, incisos II e III). [...] Neste sentido, o valor da dignidade da pessoa humana impõe-se como núcleo básico e informador de todo ordenamento jurídico, como critério e parâmetro de valoração a orientar a interpretação e compreensão do sistema constitucional.

A luz desta concepção, pode-se inferir que o valor da cidadania e dignidade da pessoa humana, bem como o valor dos direitos e garantias fundamentais vem a constituir os princípios constitucionais de maior suporte ao sistema jurídico brasileiro, sendo seu principal referencial de justiça.

Piovesan (2008, p. 52) afirma ainda, que "é no valor da dignidade humana que a ordem jurídica encontra seu próprio sentido, sendo seu ponto de partida e seu ponto de chegada, na tarefa de interpretação normativa".

Do mesmo modo, Bonavides (2002, p. 233) expõe que "nenhum princípio é mais valioso para compendiar a unidade material da Constituição que o princípio da dignidade da pessoa humana".

Pode-se afirmar, então, que a dignidade da pessoa humana é princípio que unifica e centraliza todo o sistema normativo, assumindo especial prioridade. Portanto, o uso de dados

deve ser, assim como todo o ordenamento jurídico, baseado em escolhas que garantam e observem a dignidade da pessoa humana como norte.

O intuito é resguardar o interesse público e privado, sim. Mas, acima de qualquer outra questão, deve ser resguardada a intimidade, a privacidade do indivíduo, em todos os setores, incluindo o de uso de dados.

Segundo Sarlet (2011), a dignidade é qualidade integrante e irrenunciável da própria condição humana, devendo ser reconhecida, respeitada, promovida e protegida. Não poderá ser criada, concedida ou retirada, por tratar-se de algo inerente a cada ser humano.

Tratando dessa percepção, Sarlet (2011, p. 23) então complementa:

> [...] não se deverá olvidar que a dignidade – ao menos de acordo com o que parece ser a opinião largamente majoritária – independe das circunstâncias concretas, já que inerente a toda e qualquer pessoa humana, visto que, em princípio, todos – mesmo o maior dos criminosos – são iguais em dignidade, no sentido de serem reconhecidos como pessoas – ainda que não se portem de forma igualmente digna nas suas relações com seus semelhantes, inclusive consigo mesmos. Assim, mesmo que se possa compreender a dignidade da pessoa humana – na esteira do que lembra José Afonso da Silva – como forma de comportamento (admitindo-se, pois, atos dignos e indignos), ainda assim, exatamente por constituir – no sentido aqui acolhido – atributo intrínseco da pessoa humana (mas não propriamente inerente à sua natureza, como se fosse um atributo físico!) e expressar o seu valor absoluto, é que a dignidade de todas as pessoas, mesmo daquelas que cometem as ações mais indignas e infames, não poderá ser objeto de desconsideração. Aliás, não é outro o entendimento que subjaz ao art. 1º da Declaração Universal da ONU (1948), segundo o qual "todos os seres humanos nascem livres e iguais em dignidade e direitos. Dotados de razão e consciência, devem agir uns para com os outros em espírito e fraternidade", preceito que, de certa forma, revitalizou e universalizou – após a profunda barbárie na qual mergulhou a humanidade na primeira metade deste século – as premissas basilares da doutrina kantiana. [...] Assim sendo, temos por dignidade da pessoa humana a qualidade intrínseca e distintiva reconhecida em cada ser humano que o faz merecedor do mesmo respeito e consideração por parte do Estado e da comunidade, implicando, neste sentido, um complexo de direitos e deveres fundamentais que assegurem a pessoa tanto contra todo e qualquer ato de cunho degradante e desumano, como venham a lhe garantir as condições existenciais mínimas para uma vida saudável, além de propiciar e promover sua participação ativa e co-responsável nos destinos da própria existência e da vida em comunhão com os demais seres humanos, mediante o devido respeito aos demais seres que integram a rede da vida.

Por essa perspectiva, ao desenvolver o tema da privacidade e a proteção de dados, Doneda (2020) explana que essa preocupação é própria do tempo hodierno, sendo seu conceito relacionado às necessidades diversas, como a busca da igualdade, da liberdade de escolha, do anseio de não ser discriminado, entre outros. Além disso, a privacidade estaria intimamente ligada à personalidade e ao seu desenvolvimento, em uma complexa teia de ideias.

Portanto, entende-se que a garantia da privacidade como direito fundamental é pressuposto de elementos essenciais para a consubstanciação de requisitos mínimos para a dignidade humana, que implica, consequentemente, na necessidade de conhecer uma nova estrutura de poder vinculada a essa arquitetura informacional.

Sobre isso, Doneda (2020, p. 35-36) explica:

> Uma das formas para compreender essa estrutura é a verificação do papel da tecnologia e de como utilizá-la para uma eficaz composição jurídica do problema da informação. Há de se verificar como o desenvolvimento tecnológico age sobre a sociedade e, consequentemente, sobre o ordenamento jurídico; há de se considerar o potencial da tecnologia para imprimir suas próprias características ao meio sobre o qual se projeta – e não somente para ressaltar as possibilidades latentes nesse meio. Entra em cena, portanto, a tecnologia como elemento dotado de características próprias, abrindo a discussão em torno do que seria a "vontade da técnica". [...] a "vontade da técnica" penetrou em muitas instâncias da vida cotidiana, moldando-as segundo seus padrões, em uma lógica segundo a qual haveria claras vantagens: uma maior eficiência, rapidez ou mesmo uma frequentemente aludida infalibilidade das novas soluções tecnológicas. No entanto, as consequências técnicas podem ser diversas, conforme sejam examinadas no âmbito das situações patrimoniais ou no das não patrimoniais; talvez por conta de sua própria interdependência com a tecnologia. Assim, no momento que ruía o mito que relacionava aprioristicamente o progresso tecnológico com o bem-estar, abriu-se o leque de situações não patrimoniais sobre as quais a tecnologia poderia ter fortes implicações, causando, primeiramente, insegurança. [...] Se não por outros motivos, para não descurar dos mecanismos que deram origem a essa sua "excessiva" abrangência – que, de uma maneira geral, continuam atuais, mas, por serem tão frequentemente enunciados em forma de hipérbole, correm o risco de banalização.

Nesse sentido, deve ser feito uma análise a respeito do uso das tecnologias e sua projeção na problemática informacional, e os impactos em âmbito legal. O desenvolvimento tecnológico imprime novas características sobre o ordenamento jurídico e a própria sociedade, necessitando de uma adaptação a chamada "vontade da técnica", que seria, como explanado acima, as implicações do uso da tecnologia no cotidiano.

Assim, a tecnologia pode dar origem ou incentivar tendências, influenciando significativamente na dinâmica da sociedade. O papel da tecnologia em imprimir suas próprias características ao meio sobre o qual se projetou, como um elemento dotado de características próprias e penetrando em diversas instâncias do mundo cotidiano, é o que seria a chamada "vontade da técnica".

Tal ponto merece destaque em decorrência dos problemas relacionados à privacidade causada por esta "vontade da técnica", ao momento em que se chegou ao marco inicial de maturação da relação entre técnicas e valores presentes no ordenamento jurídico. Isso porque,

não há mais uma possibilidade tão clara de se escolher ou ter ciências de que tecnologias então sendo utilizadas e quais aspectos da vida estão sendo expostos.

A privacidade, por si só, já passou a ser relacionada com uma série de interesses e valores no mundo contemporâneo, que modificou substancialmente o seu perfil. Vê-se nesse caso que, a evolução tecnológica e a forma como adentra na privacidade dos indivíduos reforçou a necessidade de funcionalização da proteção da privacidade, e consequentemente a proteção de dados.

Esse fato pode ser constatado a partir do desenvolvimento de diversos mecanismos legais com o intuito de tentar trazer a coexistência de novas tecnologias e dos vários direitos fundamentais, como o marco da Lei Geral de Proteção de Dados (LGPD).

O ordenamento jurídico brasileiro contempla a proteção da pessoa humana como o seu valor máximo e a privacidade como um direito fundamental, como forma de concretizar a atuação de tais direitos, em meio as novas tecnologias. Tem-se, portanto, o papel do ordenamento jurídico na promoção e defesa dos valores fundamentais, em um cenário de determinação tecnológica, como bem assenta Doneda (2020, p. 54-55):

> O direito é a estrutura responsável por disciplinar a realização das escolhas relacionadas à técnica. O mundo que se afigura aos olhos do jurista pode representar um problema a mais entre tantos – não raro um problema que é deixado de lado, tal o trabalho necessário de atualização e pesquisa em áreas além da estritamente jurídica. A tecnologia, potente e onipresente, propõe questões e exige respostas do jurista. Os reflexos dessa dinâmica são imediatos para o direito, pois esse deve se mostrar apto a responder à novidade proposta pela tecnologia com a reafirmação de seu valor fundamental – a pessoa humana – ao mesmo tempo que fornece a segurança necessária para que haja a previsibilidade e segurança devidas para a viabilidade das estruturas econômicas dentro da tábua axiológica constitucional. O verdadeiro problema não é saber sobre o que o direito deve atuar, mas sim de como interpretar a tecnologia e suas possibilidades em relação aos valores presentes no ordenamento jurídico, mesmo que isso signifique uma mudança nos paradigmas do instrumental jurídico utilizado. [...] Alguns dilemas que hoje se apresentam com bastante frequência ao jurista, desde a utilização de técnicas de manipulação genética para os mais variados fins até as implicações do processamento automatizado de dados pessoais, dão mostras da importância do direito privado em face da difícil situação em que a tecnologia deixou várias categorias tradicionais do direito, que não encontram mais a sua tradicional razão de ser refletida na realidade dos fatos. Assim, apresenta-se o direito civil como o espaço ideal para a aplicação de fórmulas de adequação desses interesses à hierarquia axiológica constitucional em harmonia com as possibilidades tecnológicas; fatores que justificam a necessidade da aplicação de uma racionalidade não-sistêmica, voltada para a "concretude da vida". O surgimento da rede internet, por exemplo, decididamente alargou as possibilidades de comunicação e fez emergir um grande número de questões ligadas à privacidade. O impacto que a rede proporcionou, porém, já se encontrava de certa forma incubada em tecnologias anteriores, que provocaram fenômenos assemelhados e que, se hoje podem até parecer pálidos, devem ser considerados em relação ao que representaram à sua época – afinal, são justamente impressões como essas que o suceder das gerações costuma apagar da memória de uma sociedade. Assim, o telégrafo e o telefone, como instrumentos de comunicação bidirecional, ou

> mesmo o rádio e a televisão contribuíram cada um deles para formar a consciência de que representavam um encurtamento das distâncias, do fim de limites antes intransponíveis e, consequentemente, de uma interação mais frequente entre as pessoas, elementos que estão no âmago das questões relacionadas com privacidade.

Nesse contexto, destaca-se que o direito civil possui um ilustre papel na tarefa de criar estruturas jurídicas de respostas capazes de promover a garantia de direitos fundamentais, em meio ao uso de novas tecnologias, sendo estas utilizadas na plenitude de seu potencial, mas estabelecendo, igualmente, um perfil na intricada tarefa de ser instrumento para a atuação de liberdades individuais, ao mesmo tempo em que assegura direitos fundamentais a ela ligadas.

Outrossim, pode-se auferir que, por mais difícil que seja cristalizar a problemática da privacidade em uma única realidade, "é, no entanto, razoavelmente natural constatar que ela sempre foi diretamente condicionada pelo estado da tecnologia em cada época e sociedade" (DONEDA, 2020. p. 57).

Entende-se, desta forma, que cabe ao jurista a tarefa de atualizar os parâmetros interpretativos sobre a relação de desenvolvimento tecnológico e a pessoa humana, harmonizando a autonomia privada e os elementos garantidores de direitos fundamentais. Porém, não se pode deixar de perceber que a trajetória do direito à privacidade reflete tanto uma mudança de perspectiva da tutela da pessoa, quanto a sua adequação às novas tecnologias de informação, conforme salienta Doneda (2020, p. 93):

> Não basta pensar na privacidade nos moldes de um direito subjetivo, a ser tutelado conforme as conveniências individuais, nem da privacidade como uma "predileção" individual, associada basicamente ao conforto e comodidade. A própria noção da privacidade como algo de que um cidadão respeitável poderia abrir mão (ou que ao menos se esperasse isto de um cidadão honesto e de bons costumes), a presumida "transparência de quem não tem nada a temer", deixa de fazer sentido dada a crescente complexidade das situações que tais arroubos podem desencadear e das suas consequências para os cidadãos. Uma esfera privada, dentro da qual a pessoa tenha condições de desenvolver a própria personalidade, livre de ingerências externas, ganha hoje ainda mais importância: passa a ser pressuposto para que a pessoa não seja submetida a formas de controle social que, em última análise, anulariam sua individualidade, cerceariam sua autonomia privada (para tocar em um conceito caro ao direito privado) e, em última análise, inviabilizariam o livre desenvolvimento de sua personalidade.

Nessa perspectiva, a privacidade passa a assumir uma posição de destaque na proteção a direitos fundamentais, como a dignidade da pessoa humana, devendo ser tomada como elemento indutor da autonomia, cidadania e demais pressupostos para uma sociedade democrática moderna, assumindo um caráter relacional, associando a própria personalidade com as outras pessoas e o mundo exterior.

Assim, o real interesse da tutela da privacidade é a aplicação de mais um plano da dignidade da pessoa humana, podendo compreender a tutela da informação fornecida, recebida e utilizada em determinada situação.

Como já fora visto, a tecnologia influi diretamente em parte do aspecto da vida do mundo moderno, e a maior parte da atividade humana desempenhada tem, em alguma abordagem uma influência tecnológica. Entretanto, esse comando deve ser observado e controlado, sem cingir o desenvolvimento, de maneira a resguardar a dignidade humana.

Pelo que se pode afiançar, tudo que mantenha uma relação com a vida humana consiste em um caráter da condição humana. O que possa embrenhar-se ao mundo humano, torna-se parte da condição humana. Do exposto, decorre a necessidade de proteção dos mais diversos setores, entre eles, a tecnologia e o uso de dados.

2.2 A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018) dispõe sobre tratamento de dados de pessoas naturais, tanto por meio físico, quanto por meio digital, reconhecendo a finalidade da tutela desses dados/informações para a proteção de direitos, como os da liberdade de expressão, privacidade, autodeterminação informativa e livre desenvolvimento da personalidade.

Após ser discutida por mais de dez anos, a referida lei foi aprovada garantindo a transparência total no tratamento, uso de dados pessoais e coletas de informações dos consumidores por meio de empresas públicas e privadas brasileiras.

A legislação contribui nesse caso para que os cidadãos tenham mais poder sobre as informações disponibilizadas, o que inclui nome completo e CPF, dados de compras, curtidas, localizações registradas *online*, bem como buscas em sites de pesquisa trazendo a baila à garantia do § 1° do artigo 43 do Código do Consumidor que prevê o acesso às informações existentes em registros, fichas e dados pessoais de consumo arquivados sobre eles, incluindo suas fontes (BRASIL, 1990).

Toda essa proteção veio com a mudança tecnológica e seu impacto nas consequentes alterações culturais sofridas na sociedade. A LGPD começa e desenvolver a consciência de que os dados são bens cuja coleta, armazenamento e utilização são tutelados pelo ordenamento jurídico pátrio, criando direitos, deveres e responsabilidades para as partes.

Como parte do processo para constituir maior segurança a proteção dos dados, veio à publicação do Decreto nº 10.474/2020, que aprovou a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados, remanejando e transformando cargos em comissão e funções de confiança, estabelecendo a aprovação e a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados – ANPD.

A LGPD não visa apenas proteger a privacidade dos titulares de dados, mas os direitos fundamentais de liberdade e privacidade, assim como o livre desenvolvimento da personalidade da pessoa natural. Na análise de Mulholland (2020, p. 43 e 44):

> Em 14 de agosto de 2018, foi sancionada a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD). O Brasil somou-se assim ao grupo de mais de 128 países que adotam a criação de uma lei geral como forma de melhor estruturar a proteção de dados. A própria nomenclatura da Lei revela alguns componentes importantes para o entendimento do seu contexto, alcance e objetivos. Ao se afirmar como uma lei sobre "proteção de dados pessoais", o texto confirma a lógica de que só se protege aquilo que está ameaçado. E qual seria então a necessidade de se protegerem dados pessoais por meio de uma transformação legislativa? Vive-se tempos em que dados (pessoais) fazem girar novos modelos de negócios. Esses dados estão essencialmente ligados a aspectos da personalidade de seus titulares. São elementos que identificam as pessoas, revelando suas identidades, preferências e rotinas. Da mesma forma, o interesse por acesso a estes dados vem gerando uma série de situações em que falhas de segurança permitem que terceiros possam coletar e usar os dados pessoais de terceiros para as mais distintas finalidades. Tratam-se de casos de vazamento de dados pessoais, que constantemente figuram no noticiário, expondo como especialmente empresas e governos podem estar vulneráveis a ataques e como essas violações atingem um número crescente de indivíduos. Outro fator que motivou a edição da LGPD foi a aprovação, na Europa, de um novo regulamento geral de proteção de dados (conhecido como GDPR – *General Data Protection Regulantion*). Os preparativos para a entrada em vigor deste regulamento em 2018 mobilizaram empresas, governos, sociedade civil e academia. Inúmeras práticas precisaram ser revistas para se adequar ao novo modelo em vigor na Europa, gerando ainda importantes impactos extraterritoriais. O GDPR ampliou direitos dos titulares de dados pessoais, definiu novas responsabilidades e com isso efetivamente inseriu o debate sobre proteção de dados pessoais no centro das atenções no Brasil. O fato é que hoje o compartilhamento de dados ocupa um papel de destaque nas mais diversas relações.

Pelo exposto, o novo instrumento jurídico nasce para chancelar a toda pessoa física ou jurídica, o direito de resistir à violação do que lhe é próprio, cujo objeto é a integridade moral do titular.

Desta feita, se o aparato jurídico anota que se alguém sofrer intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, ou, ainda, ataques à sua honra e reputação, o Estado deverá oferecer institutos legais para proteger e, se

necessário, reparar o dano. Pode-se afirmar, portanto, que a LGPD no Brasil, é a salvaguarda destes direitos fundamentais.

Ademais, a lei reconhece a efetivação e promoção de Direitos Humanos Fundamentais como justificativa para a tutela dos dados pessoais. Tendo em vista a caracterização da pessoa como um fim em si mesmo, toda e qualquer manifestação legislativa deve ter como finalidade a promoção do homem e de seus valores.

Dessa forma, o ordenamento jurídico deve se utilizar dos ramos em que alcançam a utilização da tecnologia para versar a garantia dos princípios constitucionais em meio a autonomia privada e a autodeterminação informacional. Tem-se claramente o papel do direito civil em dar cabo a esse intuito por meio de ações protetivas e estabelecer critérios para uso e análise de dados, dentro das relações privadas e especificidades das novas relações, como observa Mulholland (2009, p. 67-68):

> O Direito civil é chamado a dar concretude a este princípio (dignidade da pessoa humana) por meio de uma atuação protetiva. É por meio da específica caracterização da pessoa e da consideração de suas qualidades que se dará a verdadeira – no sentido de justa e equitativa – tutela da pessoa em suas relações privadas. Diferentemente do conceito de indivíduo, igual ao outro em todos os seus aspectos e, portanto, devendo ser tratado de maneira igualitária, o conceito de pessoa permite ao ordenamento, por meio de normatização ou de trabalho hermenêutico desempenhado pela doutrina e magistratura, a possibilidade de estabelecer tratamentos desiguais de acordo com a qualidade que cada pessoa desempenha numa relação privada.

Obsoleta se faz a restrição de dados ao arcaico pensamento daqueles que restringe esses aos cadastros governamentais, de modo que, no contexto do desenvolvimento tecnológico, existe uma grande dificuldade em restringir e quantificar os dados, não existindo, por sua vez, dados insignificantes.

O direito fundamental a proteção de dados não diz respeito ao dado em si, mas sim ao titular destes. Os efeitos dessa proteção, alinhado ao conceito de autodeterminação informativa, demonstra o duplo efeito da proteção de dados no ordenamento jurídico brasileiro: de um lado existe a dimensão subjetiva da intervenção do Estado no espaço pessoal do indivíduo, por outro lado, em uma dimensão objetiva, ela estabelece um dever de atuação estatal em estabelecer condições para garantir o exercício e gozo desse direito.

Com a vigência da LGPD, a regulação dos dados pessoais deixa de ser fragmentada. Como estatuto mais abrangente de determinado setor da vida em sociedade, a LGPD é verdadeiro microssistema. Sua interpretação deve guardar coerência com as demais normas

infraconstitucionais e com os institutos do sistema, de modo a materializar as normas constitucionais.

A autodeterminação informativa objetiva assegurar que os dados sejam utilizados pelas pessoas certas, para os propósitos corretos. A autodeterminação individual pressupõe, dessa forma, que o indivíduo esteja garantido da liberdade de decisão a serem procedidas ou omitidas, evitando ser inibido substancialmente em sua liberdade de planejar ou decidir com autodeterminação.

Nesse sentido, o direito à autodeterminação informativa se constitui na faculdade que toda pessoa tem de exercer, de algum modo, o controle de seus dados pessoais, sendo-lhe garantido o direito de decidir se a informação pode, ou não, ser objeto de tratamento por terceiro, bem como ter acesso a esses dados e cancelar, se assim achar pertinente, a sua utilização.

O tratamento de dados promoveu importantes mudanças no fenômeno humano. Pelo lado positivo, esse tratamento trará formas de produção mais eficientes e desenvolvimento tecnológico. Porém, pelo lado negativo, as relações humanas tornam-se ainda mais assimétricas, pois, tendo o controle tecnológico, o agente de tratamento se coloca em uma situação de superioridade.

Assim, o reconhecimento de que os dados pessoais são de propriedade do seu titular e decorrem de uma série de direitos fundamentais, assim como a necessidade de assegurar os direitos de seu titular na perspectiva da personalidade e dignidade da pessoa humana se faz de suma importância. Pois, os dados assumiram uma relevância inimaginável, sendo seu tratamento responsável por uma nova dinâmica social.

Significa dizer que o tratamento de dados passou a fazer parte no processo de produção, mas ele não se restringe ao aspecto econômico. A importância do tratamento de dados foi evidenciada com o surgimento das inovações tecnológicas nas últimas décadas, permitindo uma análise de uma gigantesca quantidade de informações.

Os dados e seu tratamento consistem, por conseguinte, no alicerce do avanço tecnológico que repercutirá em todas as atividades da sociedade contemporânea, e fazendo parte, assim, da indústria do conhecimento.

Na era da informação, dados são a matéria prima de muitos e promissores negócios. Porém, a ausência de uma cultura de proteção de dados parece fazer com que boa parte dos titulares de dados ainda não tenha se dado conta do impacto que o uso indevido destes pode ocasionar na vida privada e no seu direito a privacidade, sendo então importantes ações de

que estimulem a educação digital que sensibilizem para a questão. O atual desenvolvimento tecnológico proporciona e exige, simultaneamente, volumoso tratamento de dados.

Tratando desse contexto, Martins (2021, p. 396-397) entende que,

> Embora a proteção de dados pessoais esteja chamando muita atenção nos últimos anos, a superexposição no ambiente virtual ainda é preocupante. Em uma sociedade hiperconectada, diferentes aspectos da vida são compartilhados com os seguidores, muitos deles absolutamente desconhecidos. São compartilhados fotos da comida, dos lugares visitados, da casa, dos filhos, dos animais de estimação, do time de futebol favorito, do local de trabalho, da academia, do café preferido, entre outros hábitos. Isso deixa rastros enormes sobre o indivíduo, que podem ser utilizados para a oferta de produtos e serviços cada vez mais personalizados, mas também podem ser usados para golpes, fraudes e discriminações dos mais variados matizes. E depois que esses dados são expostos, mesmo que posteriormente se queira retirá-los da rede, nem sempre isso era possível.

O avanço do direito à privacidade se desenvolve a cada momento, no intuito de abranger aspectos da sociedade moderna, como o direito ao esquecimento, ao livre desenvolvimento da personalidade e a proteção de dados.

Porém, apesar do inegável desenvolvimento tecnológico e avanço nos meios de produção em decorrência da melhoria do tratamento de dados, não se pode esquecer seu aspecto negativo, devendo ser estabelecido processos cautelosos para assegurar o direito de seu titular. Sobre isso, Bioni (2020, p. 170) detalha:

> O tratamento de dados, porém, possui seu aspecto negativo. Como qualquer atividade humana, traz-se externalidades positivas e negativas. Se, por um lado, o tratamento de dados é imprescindível para o desenvolvimento econômico e tecnológico; por outro, cria-se o risco de violação dos dados pessoais dos seres humanos. Ao longo de suas vidas, as pessoas vão deixando rastro de informações, que dizem muito a seu respeito, em suas atividades cotidianas, sendo que a tecnologia atual permite capturá-los, trata-los e chegar-se a uma conclusão que pode ser utilizada contra a vontade ou até mesmo em prejuízo do dono do dado. Da mesma forma que se testemunhou em outras épocas surgirem relações sociais assimétricas tais como proprietário/não proprietário, empregador/empregado e fornecedor/consumidor, o tratamento de dados está forjando uma nova relação social assimétrica entre o controlador e o titular de dados. E, nesta nova relação social, o titular dos dados vem ser a parte mais vulnerável, seja por não possuir os meios tecnológicos, seja por desconhecer seu funcionamento, a merecer uma tutela especial do ordenamento jurídico. [...] O grande desafio da Sociedade contemporânea será em lograr êxito em regulamentar a atividade de tratamento de dados com a manutenção de sua externalidade positiva, ou seja, o desenvolvimento econômico e tecnológico; e, ao mesmo tempo, mitigar a sua externalidade negativa, ou seja, violação de dados pessoais. Por isso, os ordenamentos jurídicos vigentes, seja o europeu, seja americanos ou o brasileiro, visam a proteção do dado pessoal da pessoa humana, ou seja, apenas dos dados que estejam vinculados a uma pessoa. Posto de outra forma, o ponto de equilíbrio entre desenvolvimento tecnológico e a tutela da pessoa humana assenta-se na proteção de dados pessoais. O tratamento de dados, sejam ou não pessoais, é uma atividade que incorporará definitivamente no cotidiano das pessoas, empresas e Estados; trazendo, como não poderia ser diferente,

> repercussões no mundo jurídico a demandar a releitura de conceitos, institutos e princípios.

A imensurável coleta de dados pessoais, bem como a enorme capacidade de processamento desses dados não deve devassar a intimidade, a honra ou a imagem de seu titular, motivo pelo qual se faz indispensável que a proteção de dados pessoais seja realizada em harmonia com o desenvolvimento econômico, tecnológico e os dizeres constitucionais.

Por envolverem o centro do interesse do ordenamento jurídico, os dados pessoais, por fazerem menção a pessoa humana, e não apenas ao patrimônio, merecem o tratamento jurídico próprio inaugurado pela LGPD, de maneira a mitigar ou atenuar a externalidade negativa dessa atividade, nesse caso, por meio da disponibilização de normas para a proteção dos dados pessoais.

O elemento fundamental do dado é a possibilidade de identificação de seu titular. O intuito assenta-se na proteção da pessoa humana, tendo em vista que está é a real titular de direitos e deveres. Assim, a principal garantia para proteção efetiva dos dados pessoais está no dever do sigilo do agente de tratamento.

A proteção de dados pessoais é um direito autônomo, advindo da personalidade, que não se confunde com a privacidade ou intimidade. O intuito é conceder ao seu titular a autonomia e controle, na medida do possível, de seus próprios dados.

Com a magnitude da capacidade de processamento de dados, a autodeterminação será o elemento crucial para que os demais direitos tenham uma matriz axiológica sempre voltada aos melhores interesses dos titulares de dados pessoais, sendo fundamental para o livre desenvolvimento da personalidade e garantia de condições mínimas de dignidade, conforme e verá a seguir.

Destarte, a LGPD tem por objetivo a proteção dos direitos fundamental de liberdade, privacidade e do livre desenvolvimento da personalidade, ante o tratamento de dados pessoais realizado por pessoas ou empresas, reconhecendo tratar-se de novo fenômeno intrinsicamente relacionado à Era Digital. O que implica dizer que a passadio de dados passou a fazer parte no processo de produção, e a importância desse tratamento foi demonstrada com o surgimento das inovações tecnológicas nas últimas décadas, o que gerou a análise de um grande número de informações. Ou seja, o alicerce do avanço tecnológico que repercutirá nas relações da sociedade hodierna.

3 OS LIMITES DA AUTODETERMINAÇÃO INFORMACIONAL E SUA INFLUÊNCIA NO CONSENTIMENTO E NA UTILIZAÇÃO DE DADOS PESSOAIS E SENSÍVEIS

O surgimento do direito à autodeterminação informativa está intimamente ligado à própria história da proteção da personalidade como direito fundamental, na medida em que se desenvolveu como desdobramento do direito ao livre desenvolvimento da personalidade, ganhando relevo no momento em que o uso de dados pessoais e sensíveis abriga não apenas o direito à liberdade, mas os próprios limites estabelecidos pelo princípio da dignidade humana.

Com as inovações tecnológicas, uma série de novos desafios surgiu, fazendo com que o ordenamento jurídico necessitasse se adequar aos seus desdobramentos. A ideia perpassa pelo compreensão de criar uma nova abordagem capaz de constituir uma proteção de direito fundamental orientada para a informação, resultando, assim, na autodeterminação informativa, dando direito ao cidadão de decidir quais informações individuais ele fornece, a quem e sob quais circunstâncias.

As novas condições tecnológicas e sociais requerem o desenvolvimento continuado da interpretação dos direitos fundamentais para garantir a proteção de indivíduos na sociedade de informação. Assim, percebe-se que todo e qualquer processamento eletrônico de dados pode acarretar em riscos para a personalidade do indivíduo.

De toda sorte, se torna decisiva a concepção que não mais existiriam dados insignificantes nas circunstâncias modernas do processamento automatizado de dados, já que todos os dados pessoais estariam abrangidos no âmbito de proteção do direito à autodeterminação informativa.

De forma expressa, a LGPD veda consentimentos genéricos. Não basta o chamado consentir, mas deve pressupor um consentir qualificado. Tem que ser livre, informado e inequívoco. É com essas qualificações que o seu art. 5º, XII, estabelece ser o consentimento: “[...] manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada” (BRASIL, 2018).

O contexto inicial em torno da demanda regulatória da proteção de dados pessoais surge, segundo Bioni (2021), basicamente com a formação do Estado Moderno e após a Segunda Guerra Mundial, momento em que a máquina administrativa percebe que as informações pessoais de seus cidadãos são úteis para planejar e coordenar suas ações para um crescimento ordenado, através da viabilização tecnológica.

A partir dessa nova faceta do Estado e a ciência computacional que estava a se desenvolver, revolucionando completamente a quantidade e qualidade do processamento de dados, é que surge o contexto da primeira geração de leis de proteção de dados, nascendo da preocupação com o processamento dos dados pessoais dos cidadãos na conjuntura da formação do Estado Moderno. Bioni (2021, p. 171) discorre sobre esse momento:

> Naquela época, a saída regulatória foi focar na própria tecnologia que deveria ser domesticada e orientada pelos valores democráticos. Temia-se a emergência da figura orwelliana do Grande Irmão, que poderia sufocar a liberdade do cidadão com uma vigilância ostensiva. Optou-se, então, por controlar a criação desses bancos de dados por meio da concessão de autorizações para o seu funcionamento. Em suma, o que marca a primeira geração de proteção dos dados pessoais é o seu foco na esfera governamental, bem como na premissa em se estabelecer normas rígidas que domassem o uso da tecnologia. Todavia, o processamento de dados transcendeu a esfera governamental, o que aumentou a quantidade de atores e, simetricamente, o número de bancos de dados a serem regulados-autorizados. Esse novo cenário exigiu uma nova estrutura normativa.

Porém, percebe-se que seria inviável a estratégia reguladora de uma única e centralizada base de dados, sendo diluída pela ideia de bancos dispersos no plano estatal e privado. Surge, assim, a segunda geração de leis de proteção de dados pessoais, reformando o ideal regulatório anterior em que incumbia ao Estado licenciar a criação e o funcionamento de todos os bancos de dados, transferindo para o próprio titular de dados o dever de protegê-los (BIONI, 2021).

A segunda geração, portanto, seria o marco inicial para que o indivíduo pudesse ter juntamente a autonomia privada, o controle de suas informações pessoais, pois até a primeira geração, esse controle era centralizado no Estado, conforme explica Bioni (2021, p. 120):

> A segunda geração de leis de proteção de dados pessoais é caracterizada por uma mudança do âmago regulatório. Preocupa-se não somente com as bases de dados estatais, mas, também, com as da esfera privada. A figura do Grande Irmão (uma única e centralizada base de dados) é diluída pela de Pequenos Irmãos (bancos de dados dispersos no plano estatal e privado). Com isso, percebe-se que seria inviável a estratégia regulatória anterior em que incumbia ao Estado licenciar a criação e o funcionamento de todos os bancos de dados. A segunda geração de leis transfere para o próprio titular dos dados a responsabilidade de protegê-los. Se antes o fluxo das informações pessoais deveria ser autorizado pelo Estado, agora cabe ao próprio cidadão tal ingerência que, por meio do consentimento, estabelece as suas escolhas no tocante à coleta, uso e compartilhamento dos seus dados pessoais. [...] Destaca-se, nesse sentido, o referencial teórico de Alan Westin que compreendia a privacidade como a "reivindicação dos indivíduos, grupos e instituições de determinar, por eles mesmos, quando, como e em qual extensão suas informações pessoais seriam comunicadas aos outros". Dá-se ênfase à autonomia do indivíduo em controlar o fluxo de suas informações pessoais. A amplitude desse papel de protagonismo do indivíduo na proteção dos dados pessoais é o divisor de águas para a terceira geração de leis. Nesse estágio, as normas de proteção de dados pessoais

> procuraram assegurar a participação do indivíduo sobre todos os movimentos dos seus dados pessoais: da coleta ao compartilhamento. Alcançar-se-ia, assim, o êxtase da própria terminologia da "autodeterminação informacional", pois, com tal participação, possibilitar-se-ia que o sujeito tivesse um controle mais extensivo sobre as suas informações pessoais. Não por outra razão, Viktor Mayer-Schoneberger elege a analisada decisão da Corte Constitucional alemã como emblemática para a terceira geração das leis de proteção de dados pessoais, em que pese, como já destacado, tal julgado ter focado também na criação de deveres para quem coleta e processa dados pessoais, cuja abordagem é complementar e, em certa medida, minimiza o protagonismo do titular das informações pessoais.

Pode-se afirmar, portanto, que, a partir da segunda geração de leis de proteção de dados, as reinvindicações dos indivíduos de como e em qual situação suas informações pessoais seriam utilizadas, dando ênfase em sua autonomia e protagonismo, começou a ganhar forma. É nesse momento em que começam os questionamentos acerca da efetividade das leis de proteção de dados vigentes no momento, ao redor do mundo.

Esse protagonismo impulsionou o início da terceira geração de leis, em que a proteção de dados procurou assegurar a participação do indivíduo sobre a criação de deveres para quem coleta e processa dados pessoais, na própria terminologia da "autodeterminação informacional", partindo do pressuposto da possibilidade do sujeito ter um controle sobre suas informações pessoais.

Ao mesmo tempo, conforme explana Bioni (2021), a quarta geração veio para cobrir essas deficiências das gerações de leis anteriores. Assim, a disseminação de autoridades independentes para a aplicação das leis de proteção de dados pessoais, bem como de proposição normativa, relativizaram o ponto central da problemática do consentimento, permanecendo, nesta geração, como um ponto marcante da trajetória de proteção de dados.

Percebe-se que em todas as gerações normativas de proteção dos dados assinala uma preocupação central com a perspectiva do consentimento e do titular de dados como seus pontos vetores centrais.

Essas questões puderam ser comprovadas com maior facilidade em vista do desenvolvimento econômico e social, trazendo novas searas a tecnologia de informação e, consequentemente, da capacidade de processamento de dados pessoais. Esse desenvolvimento econômico veio atrelado a necessidade de proteção da privacidade pessoal do indivíduo.

A autodeterminação informacional seria, assim, o controle que o cidadão tem sobre seus dados pessoais, como, por exemplo, o poder do titular de emendar, retificar ou excluir seus dados se assim lhe for conveniente. Para Bioni (2021, p. 120):

> De um lado, a diretriz normativa da autodeterminação informacional permaneceu intacta, mas com a ressalva de que novas tecnologias emergiram e, com isso, a coleta e uso dos dados estavam cada vez mais complexos e menos transparentes. Seria necessário investigar meios que reduzissem essa opacidade e, por conseguinte, garantissem aos indivíduos controle sobre suas informações. (...) De outro lado, ainda se buscava fazer ajustes em termos de interoperabilidade legal entre os países membros. E, nesse sentido, mais do que haver uniformidade normativa, o processo de revisão aponta para a necessidade de ações coordenadas para a aplicação e a fiscalização das leis de proteção de dados pessoais, por ser isto também elemento crucial para o livre fluxo informacional trasnfronteiriço.

A tentativa de operacionalizar o consentimento qualificado (livre, informado, inequívoco e específico), é uma das mais marcantes características do progresso geracional das leis de proteção de dados pessoais, em decorrência da dificuldade do controle efetivo das informações pelo titular dos dados, em face do controlador/operador.

Em todos os momentos, a maior dificuldade era o consentimento livre, específico e informado, realizado, preferencialmente, de maneira prévia à coleta e processamento dos dados pessoais. Conforma, justamente, com a ideia de que o titular de dados pessoais deve possuir o controle de suas informações, resguardando, assim, seus direitos fundamentais, como a sua dignidade humana, o direito a intimidade, privacidade, dentre outros.

Evidentemente, a LGPD provoca importantes alterações no setor público e privado, a partir do momento em que demanda adequação das atividades atualmente praticadas, em consonância com a proteção humana.

Pode-se afirmar que, em um contexto contemporâneo no qual os dados são compartilhados quase que espontaneamente e em grandes volumes, é de suma importância que o legislador pátrio desenvolva mecanismos com o objetivo de proteger a liberdade, privacidade e livre desenvolvimento da pessoa natural. Mulholland (2020, p. 46) aponta que:

> [...] um dado, atrelado à esfera de uma pessoa, pode se inserir dentre os direitos de personalidade. Para tanto, ele deve ser adjetivado como pessoal, caracterizando-se como uma projeção, extensão ou dimensão do seu titular. E, nesse sentido, cada vez mais, as atividades de processamento de dados têm ingerência na vida das pessoais. Hoje vivenciamos em uma sociedade e uma economia que se orientam e movimentam a partir desses signos identificadores do cidadão. Trata-se de um novo tipo de identidade e, por isso mesmo, tais dossiês digitais devem externar informações corretas para que seja fidedignamente projetada a identidade do titular daquelas informações. Isso acaba por justificar dogmaticamente a inserção dos dados pessoais na categoria dos direitos da personalidade.

Nesse sentir, o direito é apenas um dos meios diretos que influencia e sofre, diretamente, a influência do desenvolvimento. Mas, em épocas de desenvolvimento tecnológico e utilização maciça de dados, a eficácia da lei não pode, nem deve, ser

renunciada. Essa eficácia deve estar atrelada aos novos desafios que surgem juntamente as características especiais que a tecnologia atribui nas relações e na sociedade como um todo.

As tecnologias e infraestruturas digitais, muitas vezes, são utilizadas de forma transnacional e em rede global, em face ao desenvolvimento tecnológico e a própria globalização, como tratado no capítulo anterior. Isso também se aplica aos inúmeros serviços prestados com tecnologia digitalizada.

Porém, existe uma notória dificuldade no ordenamento jurídico em encontrar um ponto de partida para a intervenção regulatória e estabelecer limites na autonomia privada e o próprio desenvolvimento tecnológico. Nesse sentido, é de suma importância o estabelecimento de mecanismos que propiciem e resguardem o indivíduo como pessoa humana, como "ser", não apenas um dado.

3.1 A AUTONOMIA DO TITULAR DE DADOS

Sabe-se que o direito precisa estar em constante adequação às novas dificuldades sociais. Hodiernamente, as ideias tradicionais sobre privacidade e publicidade foram desgastadas, sendo necessária a proteção específica da privacidade e intimidade, assim como entende Riem-Hoffmann (2021, p. 54):

> As ideias tradicionais sobre a privacidade e publicidade estão se desgastando, e a necessidade de proteção específica de privacidade está até sendo questionada em alguns casos, como por apoiadores do chamado movimento pós-privacidade. Acima de tudo, fenômeno de dissolução de fronteiras podem levar a consideráveis flancos abertos na proteção jurídica, na medida em que – como é habitual – a lei está ligada ao estabelecimento de fronteiras, por exemplo, regionalmente (seja no âmbito nacional ou comunitário), e na medida em que também é limitada em seu escopo. Em princípio, a legislação transnacional ou globalmente aplicável, como direito internacional, também está disponível. Seu âmbito geográfico de aplicação pode ser amplo. O direito internacional, entretanto, está objetivamente relacionado apenas a setores individuais – por exemplo, o direito comercial mundial a questões individuais de direito autoral – e muitas vezes é limitado em sua força vinculativa e sancionabilidade.

Em relação à proteção de dados pessoais, a LGPD faz parte da proteção legal da autonomia. Para isso, parte do pressuposto que, para que determinado dado pessoal ou sensível possa ser usado por terceiros, é necessário o consentimento do seu titular.

A grande problemática, contudo, diz respeito a esse consentimento ser considerado válido e estabelecer limites que não interfiram diretamente no desenvolvimento tecnológico, muitas vezes um universo a parte da realidade.

A autonomia pode ser tida como uma concretização da proteção à dignidade humana e da proteção à personalidade e, como explica Riem-Hoffmann (2021), ela é feita principalmente sob a forma de proteção da autodeterminação informacional, em frente as quase infinitas possibilidades de coleta de dados e posterior processamento. Segundo Riem-Hoffmann (2021, p. 73, 74 e 75):

> No que diz respeito à proteção de dados pessoais, a lei de proteção de dados faz parte da proteção legal da autonomia. É uma concretização da proteção da dignidade humana e da proteção da personalidade, especialmente sob a forma da autodeterminação informacional. [...] Há muitas possibilidades de coleta de dados e posterior processamento pelas autoridades privadas e públicas. [...] A lei de proteção de dados é uma abordagem tradicional – embora de conteúdo restrito – à proteção de interesses legais e, portanto, também a limitação do uso do poder. O objetivo é o "processamento", ou seja, em particular a coleta, armazenamento e outros usos de dados pessoais. A este respeito, uma proibição com reserva de permissão se aplica, em princípio. A proibição é violada se uma disposição legal permitir essas atividades ou se a pessoa interessada tiver consentimento.

Assim, pode-se afirmar que, salvo disposição legal em contrário, a grande problemática para a legalidade do levantamento, processamento e armazenamento de dados está no consentimento da pessoa em causa no seu direito. Esse consentimento pode até ser dado como um ato isolado, porém, na maior parte dos casos deve ser tido como condição geral para a ocorrência do negócio jurídico.

Nestes termos, Riem-Hoffmann (2021. p. 76) situa que:

> O caráter voluntário do consentimento é um elemento importante para a proteção da autonomia dos usuários. Entretanto, se determinados serviços são praticamente indispensáveis aos usuários por questões profissionais e pessoais importantes – por exemplo, para atuar no mundo do trabalho ou nas autoridades públicas ou para a participação social na comunicação - e se não existem serviços concorrentes de qualidade comparável, os usuários não têm praticamente outra escolha senão dar seu consentimento. O pressuposto de que eles dão seu consentimento voluntariamente é, então, ficção. O Tribunal Constitucional Alemão também identificou este dilema e o formulou do seguinte modo: "Em todas as áreas da vida, serviços básicos para o público em geral estão sendo cada vez mais prestados por empresas privadas, muitas vezes poderosas, com base em extensas coletas de dados pessoais e medidas de processamento de dados. Os indivíduos dificilmente terão outra escolha senão a de revelar em grande medida seus dados pessoais para aas empresas, caso não queiram ser excluídos desses serviços básicos. Diante da capacidade de manipulação, reprodução e de possibilidade de divulgação praticamente ilimitada dos dados, tanto em termos de tempo como de espaço, bem como sua imprevisível capacidade de recombinação em procedimentos e processamento não transparentes por meio de algoritmos incompreensíveis, os indivíduos podem se tornar amplamente dependentes ou ficar impostos a condições contratuais impositivas". Ainda que aqui não se trate dos pressupostos para a validade de um consentimento do usuário, a importância das circunstâncias citadas devem ser levadas em consideração para a avaliação da natureza voluntária de um consentimento. Também é importante para a

> validade de um consentimento saber se a coleta e o processamento de dados pelo fornecedor estão relacionados em conteúdo ao uso pretendido.

Assim, pondera dizer que, quando se trata do consentimento, não basta por si só a existência deste. Na verdade, é imprescindível que o consentimento seja voluntário e consciente para que produza efeitos no mundo jurídico. Essa é uma das maiores dificuldades com a utilização de dados em massa: conscientizar o titular de dados de quais são os dados que vão ser utilizados, para quê e o obter seu consentimento consciente e voluntário.

Ocorre que, em detrimento da dependência tecnológica para obter serviços e produtos cotidianos, dependendo da necessidade do usuário em utiliza-lo e não existindo serviços concorrentes, o usuário praticamente se vê coibido a dar seu consentimento, em prol de ver atendidas suas necessidades. Ou seja, os indivíduos dificilmente tem escolha em não dar seu consentimento, posto pelo receio de ser excluído de determinado serviço.

Importante se faz mencionar que, apesar de não ser requisito fundamental, algumas situações devem ser analisadas em relação à validade do consentimento, de acordo com o binômio necessidade/utilidade, assim como se mostra razoável esperar comportamento distinto do usuário naquela situação, muitas vezes impostas pelo controlador de dados.

Outra problemática real e constante está no fato do titular realmente ter conhecimento dos motivos que os dados estão sendo utilizados, sua relação com o uso pretendido e a compreensão sobre a coleta e processamento de seus dados. Em verdade, é bastante comum que o consentimento de empresas muitas vezes vá além da obrigação de proteção de dados no que diz respeito aos dados necessários ao processamento dos seus serviços.

De toda sorte, não é raro que as empresas exijam consentimento para o uso de outros dados, algumas vezes até mesmo obtendo o “consentimento” de repassa-lo a terceiros ou a fazer aproveitamento de dados e imagens. No modelo de negócios, supostamente gratuitos, os dados são o pagamento; e o consentimento, um suposto consenso obtido em bases muito desiguais.

O consentimento abre a possibilidade prática e normativa para que os controladores possam invadir o direito pessoal do titular dos dados e de terceiros, sem que estes, necessariamente, estejam cientes disso e possam se proteger. A dimensão do problema traz a real necessidade de proteção da privacidade e dos dados pelo ordenamento jurídico, como forma de resguardar o indivíduo e até mesmo a coletividade.

Pelo entendimento de Riem-Hoffmann (2021, p. 82):

> A exigência de consentimento também é frequentemente utilizada pelas empresas não só para lidar com questões de proteção de dados, mas também para renunciar à validade de algumas das obrigações legais impostas as empresas, reduzindo assim a proteção legal dos usuários. Isso se aplica, por exemplo, ao âmbito de proteção ou a responsabilidade por direitos autorais, mas também à redução da proteção legal ao designar uma jurisdição ou sistema jurídico estrangeiro como exclusivamente decisivo para disputas legais.

Ocorre que problemas de proteção adequada de interesses legalmente significativos estão intimamente atrelados ao universo além da proteção da personalidade. A proteção de dados é fundamentalmente importante, tanto no ponto de vista individual, como coletivo, para que haja condições efetivas para a participação social em desenvolvimento tecnológico e social, sem comprometimento a direitos fundamentais.

Perante essas considerações, a LGPD se trata de uma iniciativa normativa para garantir maior efetividade e segurança ao consentimento do titular dos dados. A questão maior não é afirmar a inutilidade do consentimento atual, longe disso, mas sim a necessidade de revisar o seu protagonismo frente a proteção de direitos fundamentais do titular de dados.

3.2 DAS INSUFICIÊNCIAS NO PARADIGMA DO CONSENTIMENTO

Em face da complexidade e transitoriedade das novas tecnologias, que rapidamente se tornam obsoletas, tem-se que o consentimento do titular dos dados, em frente a suas limitações cognitivas, pode afetar e comprometer a qualidade desse consentimento. Sobre essa problemática, Doneda (2021, p. 79) leciona que:

> A primeira insuficiência enfrentada pelo paradigma do consentimento advém de sua abordagem quanto ao seu próprio titular de dados e seu processo cognitivo-decisório. É que, sob tal ótica, esse indivíduo é guiado pela maximização de seus interesses em face dos custos e benefícios envolvidos em consentir, ou não, com os termos que lhe são apresentados. Assim, caso esteja munido de amplo conhecimento acerca do que é feito com seus dados pessoais, poderá sopesar os custos envolvidos para sua personalidade e contrapô-los diante dos benefícios trazidos, por exemplo, pela utilização de um serviço *on-line.* Por conseguinte, tomará uma decisão sobre o que consentir e o que não consentir na Internet, em seu melhor interesse, após ler os termos de privacidade disponibilizados, por exemplo. Partindo desses premissas, o seguinte procedimento se tornou comum: (i) informar o titular de dados pessoais acerca de quais dados estão sendo coletados e como eles serão usados (*notice*); em seguida, (ii) permitir com que ele detenha o poder de decidir se aceita, ou não, os referidos usos de seus dados pessoais (*consent*). Com base nas informações disponibilizadas, portanto, pressupõe-se que o indivíduo está apto a tomar decisões racionais, embasadas e efetivamente autônomas.

Entende-se, pois, que não basta apenas o consentimento com as informações que lhe foram apresentadas, mas as informações disponibilizadas devem ser de fácil compreensão, de maneira a evitar o excesso de informação que possa vir a ser prejudicial e sobrecarregue a cognição do titular dos dados acerca do uso dos dados em questão. Sobre essa questão, Doneda (2021, p. 73-74) analisa:

> "Li e aceito os termos." Ao navegar pela Internet, é bastante comum se deparar com essa frase ao fim de um longo texto, com letras pequenas e linguagem técnica. Não por acaso, estudos têm indicado que muitos usuários não leem esses termos e, quando o fazem, acabam por não o entender ou levam um tempo significativo para tanto. Mais que isso, caso o usuário concorde com os termos apresentados, é comum que sua única opção seja a de não desfrutar de produtos e serviços *on-line*. Entretanto, assim fazendo, acaba enfrentando elevados custos sociais na medida em que esses produtos e serviços penetram, cada vez mais, a vida social e as dinâmicas político-econômicas dos cidadãos para o Estado, com empresas privadas e com a comunidade que estão inseridas. Ao longo das últimas cinco décadas, muitas das discussões relacionadas à regulamentação da privacidade e da proteção de dados pessoais destinaram bastante foco em torno do consentimento expressado pelo titular de dados. Nesse sentido, não é exagero afirmar que o consentimento tem figurado como instrumento regulatório central e núcleo de legitimidade prática desse regime protetivo. Ele é lido, ainda, como expressão de autonomia individuais e do controle do titilar dos dados em torno dos seus direitos de personalidade, contudo sem inviabilizar o livre fluxo desses dados, elemento relevante para uma série de atividade econômicas e até mesmo para a elaboração de políticas públicas.

Percebe-se com clarividência que a insuficiência do consentimento é real e palpável na tarefa de tutelar a privacidade e de proteger os dados, e o próprio consentimento individual, em face da limitação cognitiva, se vê comprometido em decorrência dos vários conceitos técnicos e jurídicos, assim como a extensão e complexidade dos textos, que dificultam a real compreensão pelo titular de dados, obtendo um consentimento expresso, mas inadequado para conferir autonomia e proteção aos dados.

Doneda (2021, p. 81) ainda destaca outra insuficiência do consentimento:

> A segunda insuficiência vivenciada pelo paradigma do consentimento advém da desconsideração da assimetria de poderes existente na relação entre titular dos dados pessoais e os agentes responsáveis pelo tratamento desses dados. É que, sob essa perspectiva, o consentimento do indivíduo se apresenta como base legitimadora para praticamente toda operação de tratamento de dados, independentemente das assimetrias existentes quanto ao poder de barganha das partes, o que poderia prejudicar a tomada de uma decisão realmente livre e autônoma. Ocorre que, não rara as vezes, o titular dos dados pessoais se encontra em situação de vulnerabilidade nessa relação contratual eletrônica. Primeiro, pois, como já dito, os termos das políticas de privacidade podem ser demasiadamente complexos e abstratos, impossibilitando uma compreensão mais transparente a respeito do concreto emprego dos dados. Segundo, porque vários desses termos negociais se baseiam em uma lógica binária "*take it or leave it*": consentir ou não consentir, sem outras opções. Entretanto, ao não consentir, o custo é o de não desfrutar o serviço

> almejado, *v.g.*, o uso de uma rede social ou de um aplicativo *on-line.* Dessa forma, mesmo estando exposto a tamanhos riscos, o titular dos dados pessoais pode acabar realizando seu consentimento com base em proveitos, tais como: a conexão com suas amizades, a disponibilidade doe meios de comunicação em tempo real, a possibilidade de ouvir música e assistir filmes, etc. Assim, muitas vezes esse consentimento é meramente aparente, sendo questionável sua contribuição para o objetivo de proteger o titular dos dados. Portanto, coloca-se em dúvida o grau concreto pelo qual ele reflete a *autonomia decisória* desse titular.

Apesar da relevância do consentimento e que na prática ele realmente é dado de maneira expressa, sua validade deve ser plenamente questionada. Isso ocorre porque, a desigualdade de poderes e a dependência dos serviços pela sociedade impõem ao titular de dados à necessidade de aceitar e dispor do uso de seus dados, pois, se assim não o fizer, se verá excluído daquele serviço ou daquele produto.

A autonomia decisória do titular está comprometida, pois o consentimento dado não é contrapartida de sua vontade, mas um pressuposto da necessidade de uso de determinada rede social ou aplicativo, por exemplo. O titular se encontra, na maioria das vezes, em vulnerabilidade, se percebendo obrigado a dar o consentimento para não se ver excluído de determinada situação.

Os riscos são aceitos, pois, não existe outra possibilidade: ou se dá o consentimento e tira proveito daquele serviço ou bem quase essencial para o desenvolvimento da vida social, ou não se dá e se vê excluído destes. Perante isso, afirma-se, então, que o consentimento na maioria das vezes é apenas aparente, uma ficção, pois o indivíduo carece de autonomia decisória para se proteger dos possíveis perigos e danos a sua personalidade. Sobre uma terceira insuficiência, Doneda (2021, p. 82) apresenta:

> A terceira insuficiência de uma visão centrada no consentimento advém de sua menor capacidade de oferecer respostas aos desafios decorrentes da "massificação da produção, coleta, armazenamento, tratamento e compartilhamento de dados pessoais". Apesar do nome sugestivo, a proteção de dados não se volta exclusivamente aos dados em si. O seu enforque protetivo está no *titular* desses dados: quem arcará com os riscos e com as eventuais consequências prejudiciais do uso de seus dados pessoais. Nesse sentido, o papel regulatório é mais amplo: disciplinar a *informação* gerada a partir do processamento e do tratamento dos dados pessoais, em um devido contexto. São as informação extraídas a partir desses dados, que essencialmente formarão a representação virtual do indivíduo na sociedade. Os dados precisam ser processados e organizados para a extração dessas informações. A partir delas, por exemplo, são geradas decisões ou interpretações que podem ampliar ou reduzir as oportunidades do titular do mercado, formatar sua "imagem" perante os setores públicos e privados, bem como desenvolver sua personalidade dentro da comunidade digital.

As novas tecnologias, atreladas ao potencial significativamente exponencial de agregação de informações, gera um risco eminente ao titular dos dados. Ressalta-se que a proteção aqui deve ser realizada em prol do titular, o efetivo e real detentor dos direitos da personalidade inerente aos dados, não aos dados propriamente, que figuram como uma parte que pode gerar danos a esses direitos.

A massificação dos processos de coleta e armazenamento de dados configuram um patente desafio ao proteção ao titular de dados, tendo em vista que disciplinar informações geradas a partir do processamento e tratamento de dados se torna um negócio extremamente lucrativo e representativo perante a sociedade.

O tratamento dos dados pessoais não pode ser visto como algo estético, e seu consentimento não deve ser realizado apenas ficticiamente. A criação de detalhados perfis a respeito dos dados coletados pode criar sérios riscos a personalidade, e podem ser utilizados para práticas e operação com os mais diversos fins, gerando grande insegurança jurídica.

Com a grande capacidade de informação processada, é improvável que, sem as políticas adequadas, as decisões tomadas pelo titular de dados tenha a validade que realmente deveriam haver, tendo em vista que o consentimento dificilmente contemplará todas as vertentes necessárias para sua real validade.

Assim, não se trata de limitar o desenvolvimento tecnológico ou o tratamento de dados, como também não faria jus abandonar o consentimento individual. É nesse ponto especialmente, que a LGPD deve atuar, para criar mecanismos, como instrumento protetivo, para avaliar a capacidade de efetivar essa proteção a partir do contexto particular em que está inserido. A responsabilidade pela proteção de dados pessoais em um complexo ambiente digital deve ser compartilhada, não podendo ficar restrita ao gerenciamento individual do titular por meio exclusivo do seu consentimento.

O art. 5º, XVII, da LGPD prevê a necessidade de elaborar os relatórios de impacto à proteção de dados, quando “os processos de tratamento de dados pessoais” possam “gerar riscos às liberdades civis e aos direitos fundamentais”, devendo não apenas descrever esses processos, como também apresentar “medidas, salvaguardas e mecanismos de mitigação” dos riscos identificados (BRASIL, 2018).

Ocorre que, abordagens preventivas devem ser combinadas com considerações éticas e limites jurídicos sobre as formas de coletas, uso e tratamento de dados, assim como o consentimento. O intuito é não permitir que, no paradigma do consentimento, os ideais de autonomia e de direitos individuais assumam contornos meramente formais, desconsiderando

questões como contexto do consentimento envolvido. A decisão do titular deve ser de livre vontade, tornando questionável, em alguns contextos, a sua capacidade de consentir.

Convém observar que a LGPD condiciona e legitimidade e a legalidade do tratamento de dados à observância da boa-fé (art. 6º, caput), vedando que ele ocorra "mediante vício de consentimento" (art. 8º, §3º) ou que tenha "fins discriminatórios, ilícitos ou abusivos" (Art. 6º, IX) (BRASIL, 2018).

Pela compreensão de Doneda (2021, p. 82):

> O intuito é *adequar* o consentimento à finalidade do tratamento, porém não de forma rígida, mas sim de acordo com o contexto em que inserido. Nesse equilíbrio, a própria natureza dos dados é levada em consideração. Casos enquadrados como sensíveis, a análise e do tratamento ocorre a partir de parâmetros mais rígidos quanto à sua forma e à sua finalidade. Enseja-se, assim, maior cautela na própria formação dos bancos de dados, pretendendo garantir qualidade, exatidão, clareza e atualização dos elementos que os compõe.

Desta feita, apesar do dado em si ser o protagonista e ponto de referência regulatória para a disciplina da proteção de dados pessoais, é preciso pensar no contexto em que está inserido. Não se trata, apenas, de limitar irrestritamente o tratamento de dados ou abandonar o consentimento individual como mecanismos protetivo, mas sim de avaliar a sua real capacidade para efetivar essa proteção a partir com contexto em que está inserido.

A garantia da autodeterminação informativa é de suma importância na proteção de dados pessoais e, consequentemente, dos direitos fundamentais atrelados a esses. Essa autodeterminação, contudo, somente poderá ser concretizada quando considerados os limites resultantes dos fenômenos da informação, tecnologia e contexto social em que estão inseridas e, muitas vezes, impossibilitam a tomada de uma decisão livre pelo indivíduo.

Desse modo, uma proteção de dados pessoais precisa ser muito além de garantias formais limitadas ao consentimento individual, sendo necessário assegurar os pressupostos materiais dessa proteção, de maneira a consubstanciar um ambiente apto para o indivíduo configurar suas relações informacionais.

Observa-se que o legislador se preocupou em considerar todos os aspectos que poderiam abranger a LGPD, entretanto, conforme já exposto, uma questão nevrálgica é o aspecto do consentimento em face da limitação cognitiva, dado as questões técnicas e jurídicas, extensão e complexidade dos textos e, por assim dizer, dificultar a compreensão do texto pelo titular dos dados, o que faria o "consentimento" inadequado pra conferir autonomia e proteção.

4 A RESPONSABILIDADE CIVIL ADVINDA DO USO IRRESTRITO DE DADOS E A PROTEÇÃO CONSTITUCIONAL DOS DADOS PESSOAIS: RUMO A UM DIREITO FUNDAMENTAL AUTÔNOMO

O desenvolvimento tecnológico promoveu uma reorganização na forma de geração, distribuição e acesso a dados. Informação, mais que nunca, se tornou riqueza. A atividade econômica gerada a partir da troca de informações, cruzamento de dados e controle de fluxo de transmissão promoveu um novo ambiente social.

A partir desse novo paradigma social, houve a eminente necessidade de adequar a sociedade e o ordenamento jurídico para promover uma maior proteção aos direitos fundamentais atrelados ao titular dos dados, estes tidos hoje como núcleo gerador de riquezas, poder e status.

Surgiu, portanto, a necessidade de adequar o aparato jurídico para regular as novas relações derivadas dessa economia baseada na produção, controle e distribuição de informação. Os aspectos civis e constitucionais relativos a proteção da intimidade e privacidade restam muito mais complexo, bem como a regularização do amplificado escopo das novas ferramentas digitais.

De suma importância a correta distribuição dos riscos e responsabilidade próprios da atividade de controle de informação, sendo relevante para propiciar o melhor aproveitamento econômico da distribuição de dados, inibindo a concentração de benefícios em prol daqueles que invadem, sem a devida validade jurídica, os direitos de outrem.

O Brasil delimitou o assunto a partir de duas normas norteadoras: o Marco Civil da Internet, em vigor desde 2014, e a Lei Geral de Proteção de Dados, cuja vigência se deu em setembro de 2021, com algumas ressalvas para as sanções dos artigos 52, 53 e 54, que entraram em vigor em 1º de agosto de 2021, nos termos da Lei nº 14.010/2020.

O intuito é resguardar o cidadão, este como detentor de direitos e deveres fundamentais, dos danos decorrentes da atividade econômica que se utiliza de dados pessoais como insumo para o desenvolvimento econômico. Porém, a versatilidade dos dados na sociedade contemporânea estabelece um grande desafio na capacidade e efetividade de defesa de valores constitucionais.

A manipulação de informação gera grande desenvolvimento econômico e tecnológico, nunca antes imaginado. Porém, ela também está atrelada a diversos fatores de riscos, como ataques informacionais terroristas ou espionagem industrial, por exemplo.

Do ponto de vista individual, os prejuízos sofridos na esfera dos direitos a personalidade por aqueles que tiveram seus dados violados se torna cada vez mais complexo e cotidiano. Danos individuais podem ser utilizados para facilitar fraudes, assedio ou atrair retaliações. Tal risco na esfera individual atrai a necessidade de parâmetros de proteção e controle, tendo em vista a hipossuficiência e vulnerabilidade do indivíduo em frente às organizações complexas que detém o controle das informações.

Sem o amparo jurídico para invocar a proteção estatal, o cidadão não encontrará meios para defender seus direitos individuais pertinentes ao tratamento de dados pessoais. A sociedade caminha para maior uso de dados pessoais e maior integração, muitas vezes submetidas a ordenamentos jurídicos distintos e com diferentes perspectivas acerca dos direitos e deveres individuais.

É a responsabilização inerente à quebra dos deveres da atividade de tratamento de dados como mecanismo da atividade empresarial e forma de proteção as garantias constitucionais, advindo do novo paradigma de tratamento de informações e fluxo de dados na sociedade.

Com efeito, a LGPD, visando a facilidade de acesso e o não vazamento de dados, assim como as transformações entre os indivíduo e a sociedade em decorrência do processamento cibernético, estabeleceu tanto multas administrativas quanto a possibilidade de reparação civil por danos, consoante explica Magalhães (2021, p. 52-53):

> O artigo 42 estabelece expressamente a reparação por dano patrimonial, moral, individual ou coletivo, em razão da violação à legislação de proteção de dados pessoais. Em seguida, no artigo 44, a Lei alarga a possibilidade de reconhecimento de irregularidades sempre que o tratamento não observar a legislação ou mesmo quando serviço não atender à expectativa de segurança, a qual pode ser determinada de maneira ampla, porque o legislador optou pela técnica legislativa do *numerus apertus*, ou seja, a Lei não elenca expressamente todas as hipóteses, apenas indica algumas circunstâncias, à guisa de ilustração, para orientar os limites do conceito de segurança esperada. Dessa forma, esse dispositivo engendra amplos debates acerca da regularidade do tratamento de dados. À primeira vista, a exegese literal aponta para ser irregular a atividade apenas por deixar de observar o uso de técnicas disponíveis na segurança dos dados pessoais como, por exemplo, as exigidas pelo artigo 14, do Decreto 8.771/16, que regulamentou o MCI. Todavia, a imputação e responsabilidade dependerão da ocorrência de dado e da interpretação sistemática do conjunto de obrigações impostas para o tratamento de dados. As técnicas de segurança evoluem muito rapidamente e os protocolos de segurança são estabelecidos por parâmetros técnicos. Logo, por exemplo, apenas a inobservância de determinada técnica de segurança ainda não disseminada no mercado por si só não deverá acarretar a atribuição de irregularidades. Ocorre que, muitas empresas, ante a existência de custos para implementação de segurança, simplesmente não adotam os padrões técnicos exigidos e as boas práticas recomendadas.

Tem-se, portanto, que a efetividade da LGPD e a consequente responsabilidade civil pelo uso e vazamento indevido de dados pessoais dependerão da capacidade do sistema de impor as regras de proteção.

Em verdade, a noção e possibilidade dos dados serem considerados objetos de propriedade não é recente, mas só foi realmente explorado no ordenamento jurídico brasileiro com o advento da LGPD.

A valorização econômica dos dados pessoais e da informação, de um modo geral, assim como o desenvolvimento tecnológico e as novas proporções tomadas frente às novas possibilidades de afluxo de dados coletados, gerou a preocupação relativa à possibilidade de controlar a transmissão a terceiros dos dados coletados por quem originalmente os captou, sem o consentimento ou ciência do seu titular.

Isso ocorre, dentre outros fatores, pois informações relacionadas a dados sensíveis, como dados genéticos, relacionados à saúde, à vida sexual e a preferências, podem ser extremamente significativas para encontrar e desenvolver conteúdo adequado para o público em questão. Conhecendo melhor o público, se pode desenvolver melhor estratégias de vendas, situação altamente valorizada em uma sociedade de consumo.

Nesse sentido, os dados sensíveis começam a ser tratados como essencial para desenvolvimento de perfis de venda e estratégicas políticas, por exemplo, em que dados são utilizados para manipular as informações e promover conteúdo mais relevante e propício à aceitação.

O tratamento de dados pessoais sensíveis deve ser precedido de cautelas maiores, com especial atenção aos princípios e direitos dos titulares, uma vez que eventual incidente de segurança com esses tipos de dados pode trazer consequências mais gravosas aos seus direitos e liberdades.

Conforme explana o art. 5º da LGPD, a principal diferença entre o tratamento de dados pessoais e dados pessoais sensíveis é que nessa última, como regra, a base legal aplicada é o consentimento, de forma específica e destacada, para finalidades específicas. Assim, consoante Mulholland (2020, p. 180):

> [...] dois fatores têm contribuído primordialmente para a defesa, em sede doutrinária, de que dados pessoais são objetos de propriedade: a insuficiência da responsabilidade civil para apresentar soluções a problemas modernos como a prática de *profiling*, sem o consentimento do titular de dados, e a necessidade de recorrer ao direito de sequela, atributo do direito de propriedade e dos direitos reais, na intenção de reaver dados indevidamente transmitidos a terceiros.

Porém, cumpre observar que, quando o legislador brasileiro afirma que “toda pessoa natural tem assegurada a titularidade de dados pessoais” (BRASIL, 2018), este claramente assegura a realidade de cada indivíduo ter o poder de disposição e controle de seus dados. Considerando estes bem jurídicos, atribui os dados à pessoa natural à qual estão atrelados.

Assim, o uso deve ser sempre previamente consentido, o que justifica a restrição presente no art. 10 da LGPD, no que concerne ao uso secundário, a restrição em situações absolutamente excepcionais, baseadas no interesse legítimo do controlador e do titular.

O caso de responsabilização civil decorre, portanto, do dano causado pelas práticas indevidas que venha a determinar a medida da indenização, não apenas o uso indevido por si só. Pela explanação de Mulholland (2020, p. 187):

> Diante da opção do legislador de atribuir os dados, na qualidade de bem jurídico, ao seu titular, é importante observar que, relativamente aos aspectos patrimoniais decorrentes de seu uso não autorizado, a tutela a lhes ser conferida em tal hipótese não estará respaldada na responsabilidade civil, como ocorreria em caso de divulgação indevida de dados que pudesse abalar a reputação de uma pessoa e assim causar-lhe danos morais ou materiais. A reflexão é relevante por ser o dano, nas hipóteses que dão ensejo à responsabilidade civil, “o elemento que determina a medida da indenização”. O problema enfrentado antes do advento de leis como o GDPR ou a LGPD era a dificuldade de se demonstrar a ocorrência de dados em caso como os que envolvem a prática de *profiling* ou de uso secundários de um modo geral. Com efeito, sendo o titular de tal bem jurídico a pessoa física de quem os dados foram coletados, a sua tutela patrimonial não está fundada na responsabilidade civil. A utilização dos dados para fins diversos dos autorizados pelo titular poderá, eventualmente, acarretar um enriquecimento ilícito por parte de que os processos ou transmite a terceiros. Em tais hipóteses, não se exige – ao contrário do que ocorre no âmbito da responsabilidade civil – uma efetiva diminuição no patrimônio da vítima, bastando que alguém enriqueça à sua custa capaz de justificar tal enriquecimento, nos termo do art. 885 do Código Civil.

Consequentemente, a opção adotada pelo legislador brasileiro no art. 17 da LGPD denota a intenção de refletir que o os dados pessoais estão totalmente vinculados ao seu titular, assegurando seu exercício ao direito resguardado de modo direto e imediato, no âmbito da propriedade.

Já o art. 42 da LGPD instituiu a obrigação de reparação de danos, patrimoniais ou extrapatrimoniais, que tenham nexo causal com a atividade de tratamento de dados. Como contraponto, o art. 43, por sua vez, instituiu causas de exclusão da responsabilidade dos agentes de tratamento de dados pautadas pela quebra do nexo de causalidade entre os elementos do dano e do risco.

Por sua vez, o inciso II do art. 43 previu a exclusão da responsabilização do agente caso comprove que atuou em conformidade com a legislação pertinente, levando a

interpretação que o cumprimento da LGPD e demais normas específicas sobre o tema eliminaria o risco da atividade a fim de afastar o dever de indenizar. Sobre isso, Kavasaki (2021, p. 433-434) resume:

> Em suma, a LGPD, lei geral aplicável à atividade de tratamento de dados, sem prejuízo a outras leis especiais, adotou a Teoria do Risco para fundamentar uma responsabilidade objetiva nas operações de tratamento de dados. Sua redação complementa a construção principiológica dos demais diplomas aplicáveis, como o Código de Defesa do Consumidor e o Marco Civil da Internet, especificando as operações de coleta e tratamento, direitos, garantias e deveres, de maneira a balancear a economicidade das aplicações de Internet com o direito de privacidade de seus usuários.

A proteção de dados pessoais consiste, como já informado, em um dos mais sensíveis desafios que o direito contemporâneo enfrenta em decorrência do extraordinário avanço tecnológico verificado nas últimas décadas, assim como as inúmeras dificuldades em estabelecer limites que não dificultem o bem estar proporcionado a esse desenvolvimento, mas sem atingir negativamente os direitos fundamentais diretamente ligados ao indivíduo.

A consequência para o tratamento irregular de dados pessoais e seu uso indevido ou vazamento, então, está mais para a inobservância da legislação que recorde a violação da proteção de dados, dando ensejo a responsabilidade civil.

Tem-se que seria provável que o que deve ser punido, nessa esfera, é a não adequação a norma, não apenas a questão do vazamento de dados em si, que muitas vezes pode acontecer independentemente de medidas de segurança implantada ou não. Na leitura de Schreiber (2021, p. 329):

> Entre a conduta do operador ou do controlador na atividade de tratamento de dados pessoais e o dano sofrido pelo titular deve-se, para que haja responsabilização, estabelecer uma relação de causalidade. Trata-se de noção indispensável à configuração do dever de indenizar, consubstanciada no liame que liga a conduta do agente ao dano sofrido pela vítima. O nexo causal (relação de causa e consequência) é originariamente um conceito lógico, e não jurídico. Todavia, a fim de se evitar "*super-resposabilização*", a ciência jurídica tem historicamente procurado qualificar o nexo causal, restringindo a relação de causalidade que é aceita pelo direito como apta a produzir a obrigação de indenizar.

Assim, deve-se sempre estar presente o nexo causal para que seja consubstanciado o dever de indenizar derivado da responsabilização civil. A conduta do operador na atividade de tratamento de dados pessoais deve-se estar ligada a relação de causa e consequência, para que assim realmente seja imposta a obrigação de indenizar.

De toda sorte, os direitos dos titulares de dados pessoais foram reconhecidos pelo ordenamento jurídico brasileiro, devendo ser efetivados. A materialização de sua eficácia depende da capacidade de impor as obrigações estabelecidas. Um dos fundamentos primordiais seriam a responsabilização civil e seus efeitos benéficos para a imposição da norma, tratando-se de incentivo para a adequação ao ordenamento.

Nesse sentido, Magalhães (2021, p. 94-95) pontua que:

> Assim, a responsabilidade do agente de dados na LGPD é objetiva, fundada no risco inerente a atividade normalmente desenvolvida. Porém, quando o agente demonstrar que o risco era inevitável, porque adotadas todas as medidas necessárias exigidas pelas boas práticas do mercado e pela Autoridade Nacional, não acarretará a indenização a seus usuários. O titular de dados que entabula relacionamento com o controlador assume posição análoga ao consumidor de produtos potencialmente nocivo à segurança, regulado no artigo 9º do CDC, ou seja, há responsabilidade objetiva do fornecedor em função dos riscos do serviço, mas não se avança para a teoria do risco integral. Evidentemente que a responsabilidade objetiva em face de terceiro sem relação com o agente de tratamento de dados irá ensejar a indenização em qualquer situação. Porém, tal hipótese, no caso da atividade de tratamento de dados, será resolvida sem o recurso à responsabilidade objetiva, uma vez que o agente de tratamento não pode armazenar dados sem o consentimento do titular. O dano nesses casos será decorrente do ato ilícito porque a conduta é expressamente vedada pelo artigo 7º, I, 7, §5º, da LGPD.

A responsabilidade civil poderá incidir no tratamento de dados pessoais sempre que o controlador descumprir os deveres de proteção e cuidados impostos. Analisando diretamente a LGPD, percebe-se que não se requer a menção de culpa dos agentes de tratamento para a responsabilização, pois se trata de risco inerente a atividade, devendo acarretar a assunção da responsabilidade aos respectivos empreendedores.

4.1 O SUPREMO TRIBUNAL FEDERAL, A MEDIDA PROVISÓRIA Nº 954/2020 E A PROPOSTA DE EMENDA À CONSTITUIÇÃO (PEC) Nº 17/2019

O Supremo Tribunal Federal (STF), em maio de 2020, proferiu uma decisão histórica para o desenvolvimento de dados pessoais no Brasil. O Plenário da Suprema Corte referendou a Medida Cautelar concedida pela Ministra Rosa Weber, relatora das Ações Diretas de Inconstitucionalidade (ADIs) 6.387, 6.388, 6.389, 6.390 e 6.393.

Desse modo, o Tribunal suspendeu a eficácia da Medida Provisória 954/2020 a qual, em seu art. 2º, *caput*, determinava que empresas de telecomunicações compartilhassem com o Instituto Brasileiro de Geografia e Estatística (IBGE) nome, número de telefone e endereço de seus consumidores de telefonia móvel e fixa.

A decisão é de suma importância para o direito brasileiro, pois reconhece o direito fundamental à proteção de dados como direito autônomo, extraído a partir de leitura sistemática do texto constitucional brasileiro.

O caso concreto trata-se da Medida Provisória nº 954, editada pelo governo brasileiro em 17 de abril de 2020. Estava presente em seu corpo, mais especificamente no art. 2º, que:

> As empresas de telecomunicação prestadoras do STFC e do SMP deverão disponibilizar à fundação IBGE, em meio eletrônico, a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas (BRASIL, 2020).

Logo em seguida, continua no § 1.º do mesmo dispositivo, afirmando que os dados pessoais seriam utilizados "direta e exclusivamente pela fundação IBGE" com a finalidade de construir "a produção estatística oficial", por meio da realização de "entrevista em caráter não presencial no âmbito de pesquisas domiciliares." (BRASIL, 2020).

Quatro partidos políticos (PSB, PSDB, PSol e PCdoB) e o Conselho Federal da OAB ajuizaram as ADIs alegando a contrariedade da norma em face dos requisitos formais exigidos pela Constituição (art. 62, *caput*) e alguns direitos fundamentais, tais como dignidade da pessoa humana, inviolabilidade da intimidade e da vida privada, além da violação expressa da *autodeterminação informativa.* A inicial acentual a necessidade de se tutelar expressamente o direito fundamental a proteção de dados.

As ADIs defendiam, basicamente, haver vícios de inconstitucionalidade na MP, sendo os argumentos apresentados: a) o caráter extremamente genérico da redação normativa empregada para medidas que poderiam restringir direitos fundamentais; b) a referida exigência da norma era desproporcional em vista dos dados necessários para a pesquisa e os requisitados; c) a ausência de regulamentação quanto aos mecanismos de segurança de informações utilizados e a falta de previsão sobre o relatório de impacto à proteção de dados pessoais.

Em verdade, existia um grau de abstração muito elevado nas obrigações impostas pela MP, sem ser devidamente tratado as garantias de segurança nos dados tratados, que por si só, no ordenamento jurídico brasileiro, já possui um grande déficit institucional na proteção de dados no Brasil.

A linha argumentativa ("b") prevaleceu no Supremo Tribunal Federal e, no dia 24 de abril de 2020, a Ministra Relatora, Rosa Weber, suspendeu a Medida Provisória com o seguinte fundamento:

> "Não se subestima a gravidade do cenário de urgência decorrente da crise sanitária nem a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento. O seu combate, todavia, não pode legitimar o atropelo de garantias fundamentais consagradas na Constituição." (BRASIL, Supremo Tribunal Federal. ADI nº 6387. Rel. Min. Rosa Weber, Decisão Monocrática, j. 24/04/2020, DJe 28/04/2020, p. 12).

A Ministra Rosa Weber trouxe o conceito de "dado pessoal" e sua adequação a tutela constitucional de modo ampliado, na decisão liminar do caso em comento, trouxe o seguinte argumento:

> O art. 2º da MP nº 954/2020 impõe as empresas prestadoras de Serviço Telefônico Fixo Comutado – STFC e do Serviço Móvel Pessoal – SMP o compartilhamento, com a Fundação Instituto Brasileiro de Geografia e Estatística – IBGE, da relação de nomes, números de telefone e endereços de seus consumidores, pessoas físicas ou jurídicas.
>
> Tais informações, relacionadas a identificação – efetiva ou potencial – de pessoa natural, configuram dados pessoais e integram, nessa medida, o 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). Sua manipulação e tratamento, desse modo, hão de observar, sob pena de lesão a esses direitos, os limites delineados pela proteção constitucional. (...) Decorrência dos direitos de personalidade, o respeito a privacidade e à autodeterminação informativa foram positivados, no art. 2º , I e II, da Lei n. 13.709/2018 (LGPD), como fundamentos específicos da disciplina da proteção de dados (BRASIL, Supremo Tribunal Federal. ADI nº 6387. Rel. Min. Rosa Weber, Decisão Monocrática, j. 24/04/2020, DJe 28/04/2020, p. 8).

É de suma importância reconhecer que a decisão do STF apresenta-se como um rumo importante na proteção de dados no Brasil, pois apesar de se tratar de decisão liminar, representa um verdadeiro avanço e evolução em relação à jurisprudência anterior do STF em relação a proteção de dados, expressa em julgados como o RE nº 418.416-8/SC, Relator Min. Sepúlveda Pertence, 10/05/2006, e o HC nº 91.867/PA, Relator Min. Gilmar Mendes, 24/04/2012.

A interpretação constitucional conferida foi a de que qualquer dado que leve a identificação de uma pessoa, seja ele pessoal ou sensível, merece a proteção constitucional, estabelecendo, assim, uma maior abertura da tutela constitucional, podendo aplica-la a tal direito fundamental em uma multiplicidade de casos envolvendo coleta, armazenamento, processamento e transmissão de dados pessoais.

Cabe ressaltar, ainda, que o plenário do STF referendou a liminar concedida, nos dias 6 e 7 de maio de 2020, a partir do placar de 10 votos favoráveis.

O Ministro Luís Roberto Barroso resumiu a questão informando que o caso concreto demonstrava a necessidade de se estabelecer um delicado equilíbrio. De um lado, a importância da obtenção e do fluxo de dados pessoais para não apenas a customização de produtos e serviços no mercado privado, como também a formulação de políticas públicas empiricamente informadas. De outro lado, o potencial lesivo que o fluxo de dados inadequados ou o seu vazamento poderia trazer grande violação a dignidade e personalidade dos indivíduos.

> "Portanto, a dualidade que se coloca, aqui, nesta ação é precisamente essa: uma tensão entre a importância dos dados no mundo contemporâneo e os riscos para a privacidade que a sua malversação representa para todos nós." (BRASIL, Supremo Tribunal Federal. ADI nº 6387. Rel. Min. Luis Roberto Barroso, Acórdão. j. 24/04/2020, DJe 28/04/2020).

A Ministra Carmen Lúcia salientou que *"não existem dados insignificantes"* ou neutros. Dessa maneira, o Tribunal ultrapassou o discurso que não haveria problema no compartilhamento de dados como nome, endereço, e número de telefone, uma vez que estes estariam abrangendo informações da vida íntima dos envolvidos.

O Ministro Luiz Fux destacou a centralidade do tema da proteção de dados em face da manutenção da democracia, uma vez que dados aparentemente "insignificantes" podem ser utilizados para distorcer até mesmos processos eleitorais.

> "o recente escândalo envolvendo a Cambridge Analytica revelou como modelos de negócios são rentabilizados pela análise de dados a alertou como seu uso indevido pode lesar (...) a própria democracia" (BRASIL, Supremo Tribunal Federal. *ADI n. 6387*. Rel. Min. Rosa Weber, Plenário, j. 06 e 07.05.2020)

Segundo o Ministro Gilmar Mendes, o conteúdo desse direito fundamental exorbita àquele protegido pelo direito à privacidade, pois não se limita apenas aos dados íntimos ou privados. Ao contrário, refere-se a qualquer dado que identifique ou possa identificar um indivíduo.

Temos, portanto, a importância da formulação de políticas públicas empiricamente informadas, dentro da necessidade de obtenção e do fluxo de dados pessoais sem gerar prejuízo à dignidade e a personalidade dos indivíduos.

Apesar de essa decisão ter tratado de um caso concreto em que verse uma situação de risco de ingerência abusiva do Estado, parece adequado. Guardada as devidas especificidades aplicáveis a esfera privada, poderá ser utilizada analogamente dentro das relações entre

particulares, a partir da irradiação de preceitos fundamentais constitucionais nas cláusulas gerias do direito civil, assim como sua adequação a LGPD.

Pode-se concluir que o amplo acesso aos dados pessoais exige, no mínimo, intervenção legislativa em relação à coleta ou transferência, a partir da previsão de medidas e critérios de intervenções que sejam proporcionais a restrição deste direito fundamental.

Em sentido análogo, no ano de 2019, foi proposta perante o Senado Federal a Proposta de Emenda Constitucional (PEC) nº 17/2019, cujo principal objetivo é inserir o direito à proteção de dados pessoais no art. 5º da Constituição Federal de 1988, reconhecendo, dessa maneira, a proteção de dados como direito fundamental.

A PEC também continha a competência legislativa exclusiva da União para inserir matéria de proteção de dados, com a ajuda da instituição do órgão fiscalizador sobre a proteção de dados no Brasil, a Autoridade Nacional de Proteção de Dados (ANDP).

Caso seja aprovada, a inserção da proteção de dados pessoais no rol do art. 5º da Constituição, por si só, representa um desenvolvimento positivo para a proteção de dados como fundamental a dignidade humana e livre exercício da cidadania, resguardando o interesse do particular e a privacidade numa sociedade em extremo desenvolvimento tecnológico.

O reconhecimento da proteção de dados pessoais como direito fundamental na Constituição Federal representa a positivação de um entendimento jurisprudencial já existente com o julgamento da ADI nº 6.387 pelo STF, proferindo decisão colegiada elevando a proteção de dados pessoais ao nível de direito fundamental autônomo no direito brasileiro.

A aprovação da PEC, portanto, reforçaria a validade do direito fundamental à proteção de dados, que contaria com previsão específica na Constituição Federal, sendo importante ressaltar que o reconhecimento da proteção de dados pessoais como direito fundamental implica em melhores perspectivas de efetivação desse direito.

Atualmente, a PEC foi aprovada na Câmara dos Deputados com sugestão de algumas alterações, devendo retornar para o Senado Federal para que sejam realizadas as devidas correções.

4.2 A RESPONSABILIDADE CIVIL NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Hodiernamente existe um amplo debate internacional sobre a importância da proteção de dados pessoais e os riscos inerentes à sua má utilização. A proteção de dados pessoais vem a ser, em realidade, um sensível desafio que o ordenamento jurídico mundial precisa enfrentar, em decorrência do avanço tecnológico das últimas décadas.

No ordenamento jurídico brasileiro, a norma reguladora pioneira em tratar a respeito do armazenamento, uso e transferência de dados pessoais é a Lei nº 13.709/2018, que encontra seu fundamento na Constituição Federal de 1988, mais precisamente em seu art. 5º, X. O direito à privacidade abrange não apenas à vida do indivíduo, mas também a proteção de seus dados pessoais.

A LGPD assegura ao titular de dados pessoais um amplo rol de direito (art. 18), além de disciplinar diversos aspectos do processo de tratamento de dados pessoais, sendo inegável a preocupação do legislador em conferir respeito maior aos titulares dos dados, resguardando seus direitos fundamentais.

> A responsabilidade civil pode ser definida, sinteticamente, como o campo do direito civil que se ocupa dos danos sofridos na vida social. Historicamente erigida em torno da noção de ato ilícito e, em especial, do seu elemento subjetivo (culpa), a responsabilidade civil era compreendida como um mecanismo de sanção àquilo que Paul Esmein chegou a definir como "péché juridique" ("pecado jurídico"). [...] Em total sintonia com essa trajetória histórica da responsabilidade civil, a LGPD determinou no *caput* do seu art. 42: "O controlador ou operador que, em razão do exercício de atividade do 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". O dispositivo suscita diversas questões que merecem redobrada atenção ao intérprete. Em primeiro lugar, salta aos olhos a pluralidade de espécies de danos expressamente apanhadas pela norma: "dano patrimonial, moral, individual ou coletivo". O dano, que constitui figura nuclear da responsabilidade civil, é tradicionalmente conceituado como a lesão a um interesse juridicamente protegido. O dano patrimonial é entendido como a lesão a um interesse jurídico passível de valoração econômica. O dano moral, por sua vez, deve ser compreendido como a lesão a um interesse jurídico atinente à personalidade humana. Ambas as noções foram construídas a partir de uma perspectiva estritamente individual: lesão ao patrimônio ou à dignidade de uma pessoa específica.

A própria vítima do uso indevido de dados pessoais é o seu próprio titular, ao ter seu direito a privacidade, intimidade e dignidade humana violada, o que desenvolve o seu direito a indenização pelo abalo moral sofrido. Porém, a LGPD abrange essa esfera de proteção, de modo a abranger seu titular, os danos materiais sofridos e até mesmo a própria coletividade.

A esfera de incidência da responsabilidade civil da LGPD sobre qualquer dano decorrente do uso irrestrito de dados pessoais não é demarcada apenas pelo interesse lesado,

ou por uma especial condição de lesão, mas sim o ato lesivo decorrente do exercício da atividade de tratamento de dados pessoais.

A vinculação do conceito de dados pessoais (art. 5º, I) como "informações relacionadas a pessoa natural identificada ou identificável" (BRASIL, 2018) traz o propósito de tutelar os dados pessoais como manifestação específica a pessoa humana e suas respectivas dimensões de proteção.

Existe uma notória discussão a respeito do regime de responsabilidade civil instituída pela LGPD. O art. 42 não alude, em sua literalidade, a culpa, o que poderia indicar uma responsabilidade objetiva. Porém, o mesmo artigo não faz menção expressa da expressão "independente de culpa", como presente no Código de Defesa do Consumidor (art. 12, *caput*, e 14, *caput*) e o Código Civil (art. 927, parágrafo único, e 931).

Nesse sentido, Schreiber (2021, p. 328) destaca:

> Pode-se afirmar, em outras palavras, que não há uma resposta unívoca a indagação sobre a espécie de responsabilidade civil que vigora no âmbito da LGPD. Tal como ocorre no Código de Defesa do Consumidor e, também, no Código Civil, ambos os regimes de responsabilidade civil – subjetivo e objetivo – convivem na legislação de proteção de dados pessoais. Dentre as hipóteses de responsabilidade subjetiva, o legislador destacou, por meio do parágrafo único do art. 44, a hipótese de ausência de adoção das medidas protetivas indicadas no art. 46, mas isso não afasta outros casos de responsabilidade civil objetiva, decorrentes do tratamento de dados pessoais que não fornaça a segurança que pode esperar o titular dos referidos dados, à luz das circunstâncias indicadas nos incisos do art. 44 da LGPD. [...] Em suma, apesar da redação confusa, pode-se concluir que convivem na LGPD dois regimes distintos de responsabilidade civil: a responsabilidade subjetiva e responsabilidade objetiva. É, de resto, o que ocorre no Código Civil, no qual convivem as cláusulas gerais de responsabilidade subjetiva (art. 186 c/c art. 927, *caput*) e objetiva (art. 927, parágrafo único), bem como no Código de Defesa do Consumidor (responsabilidade objetiva nos arts. 12, *caput*, e 14, *caput*, por exemplo; e responsabilidade subjetiva no art. 14, §4º), sendo certo que esses dois diplomas legislativos parecem ter guiado, acertadamente, as opções do legislador especial na disciplina de dados pessoais.

A responsabilidade subjetiva surge, portanto, independente ou não da presença da culpa, requisito indispensável para caracterizar a responsabilidade objetiva. Ocorre que, ambas as espécies de responsabilidade civil em comum a aferição de nexo de causalidade entre a conduta do operador ou do controlador na atividade de tratamento de dados pessoais e o próprio dano sofrido pelo titular.

> No que diz respeito especificamente ao tratamento de dados pessoais, a questão da causalidade pode ser tornar especialmente complexa. O vazamento de dados pessoais em uma sociedade de informações ocorre, muitas vezes, por meio de sucessivas transferências ou apropriações de dados que, mesmo em casos de investigação policial, se tem dificuldade em reconstituir. A fonte originária de dados

> pessoais expostos indevidamente nem sempre é passível de identificação (*trackable*) e o caminho percorrido pelos dados pessoais frequentemente restará demonstrado mais a título de efetiva probabilidade que de certeza matemática. Aqui, desempenha papel relevante o mecanismo de inversão do ônus da prova contemplado expressamente pela LGPD (SCHREIBER. 2021. p. 329 e 330).

Por fim, ressalta-se que, em que pese à previsão de diversos institutos vocacionados à prevenção de danos, a real efetividade da lei dependerá dos instrumentos voltados à reparação dos danos eventualmente causados, resguardando, assim, a dignidade humana do titular de dados, assim como as obrigações legais do controlador e operador, nos seus limites legais.

Assim, o propósito de tutelar os dados pessoais como manifestação específica a pessoa humana e suas respectivas dimensões de proteção, traz a eminente necessidade de instrumentos adequados a proteção desse direito fundamental.

5 CONSIDERAÇÕES FINAIS

Para trazer à tela o tema enunciado neste trabalho “A dignidade da pessoa humana na proteção de dados pessoais e sensíveis, com análise à luz da Constituição Federal de 1988 e a Lei nº 13.709/18”, evocou-se primeiramente a Carta Magna, que subsidia a discussão dentro do espectro da dignidade da pessoa humana.

Partiu-se do pressuposto de que a Constituição Federal de 1988 declara invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, em seu art. 5º, X (BRASIL, 1988). Esses princípios nortearam todo o trabalho desenvolvido, assim como a dignidade da pessoa humana.

A ser assim, é fato que hodiernamente os desafios de um mundo *hiperconectado* constitui poderosa ameaça à privacidade e intimidade dos indivíduos. Estas mudanças surgem com o fenômeno da Globalização, sendo que o acesso à tecnologia de maneira maciça fez aproximar uma variedade de serviços virtuais, sejam para compras, ambientes sociais, financeiros e outros.

Ao longo das últimas cinco décadas, o tema da proteção de dados pessoais ganhou considerável espaço nas discussões no universo jurídico, bem como nas agendas reguladoras e empresariais. Nesse período, várias mudanças tecnológicas ocorreram e, por conseguinte, alteraram estruturalmente as dinâmicas relacionadas ao tratamento a ao fluxo de dados pessoais no mundo, assim como seus usos e finalidade, gerando violação a dignidade humana, privacidade e intimidade do indivíduo.

É possível compreender que a dignidade da pessoa humana é princípio que unifica e centraliza todo o sistema normativo, assumindo especial prioridade no ordenamento jurídico pátrio. Pode-se, inclusive, afirmar que este princípio norteia toda a rede normativa do Brasil. Portanto, o uso de dados deve ser, assim como todo o ordenamento jurídico, baseado em escolhas que garantam e observem a dignidade da pessoa humana como norte.

Com enfoque no tema, surgiu a eminente necessidade do regramento do tema em vista do uso arbitrário de dados, sem o devido controle, ferindo assim, princípios primordiais do ordenamento jurídico. Assim, foi sancionada a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18), que tem como garantia a transparência total no tratamento, uso de dados pessoais e coletas de informações dos consumidores por meio de empresas públicas e privadas brasileiras. Esse novo instrumento jurídico nasce para chancelar a toda pessoa física ou jurídica, o direito de resistir à violação do que lhe é próprio, cujo objeto é a integridade moral do titular.

O reconhecimento de que os dados pessoais são de propriedade do seu titular e decorrem de uma série de direitos fundamentais, assim como a necessidade de assegurar os direitos daquele na perspectiva da personalidade e dignidade da pessoa humana é de caráter primordial para resguardar a sociedade em um universo baseado em dados, tendo em vista que estes assumiram uma relevância inimaginável, sendo seu tratamento responsável por uma nova dinâmica social.

Desta feita, a proteção de dados pessoais começou a ser vista como um direito autônomo, advindo da dignidade da pessoa humana, proteção a personalidade, privacidade e intimidade, concedendo, na medida do possível, controle dos dados ao próprio titular destes.

No capítulo "Os limites da autodeterminação informacional e sua influência no consentimento e na utilização de dados pessoais sensíveis", se observou primariamente que as novas condições tecnológicas e sociais requerem o desenvolvimento continuado da interpretação dos direitos fundamentais para garantir a proteção de indivíduos na sociedade de informação.

Assim, percebe-se que todo e qualquer processamento eletrônico de dados pode acarretar em riscos para a personalidade do indivíduo, motivo que necessita que o posicionamento do ordenamento jurídico para impor meio coercitivos de controle e uso de dados.

É a partir deste novo ordenamento jurídico que o Estado e o Direito Digital desenvolvem mecanismos que passam a revolucionar a discussão a cerca da quantidade e a qualidade do processamento de dados, de onde emerge o contexto da primeira geração de leis de proteção de dados dentro do Estado Moderno.

De toda sorte, a autodeterminação informacional ganha uma maior perspectiva de atuação em frente ao controle que o cidadão tem sobre seus dados pessoais, como, por exemplo, o poder do titular de emendar, retificar ou excluir seus dados se assim lhe for conveniente.

Dentro do que trata a LGDP, há uma lacuna que ainda precisa de tratamento, pois, não basta apenas o consentimento com as informações que lhe foram apresentadas acerca do uso dos dados em questão.

O próprio consentimento individual se vê comprometido em decorrência dos vários conceitos técnicos e jurídicos, assim como extensão e complexidade dos textos, que dificultam a real compreensão dos termos de uso pelo titular de dados, obtendo um consentimento expresso, mas inadequado para conferir autonomia e proteção aos dados.

Percebe-se que a massificação dos processos de coleta e armazenamento de dados configura um patente desafio a proteção ao titular de dados, tendo em vista que disciplinar informações geradas a partir do processamento e tratamento de dados se torna um negócio extremamente lucrativo e representativo perante a sociedade.

É imperioso observar que ao legislador se preocupou em considerar todos os aspectos que poderiam abranger a LPDG, entretanto, a questão nevrálgica é o aspecto do consentimento em face da limitação cognitiva, dado as questões técnicas e jurídicas, extensão e complexidade dos textos e, por assim dizer, dificultar a compreensão do texto pelo titular dos dados.

Assim, a LGPD deve atuar para criar mecanismos, para avaliar a capacidade de efetivar essa proteção, a partir do contexto particular em que está inserido. A responsabilidade pela salvaguarda de dados pessoais em um complexo ambiente digital deve ser compartilhada, não podendo ficar restrita ao gerenciamento individual do titular por meio exclusivo do seu consentimento, pois já foi comprovado que, na maior parte das vezes, ele apresenta apenas um caráter formal.

Em outro capítulo se tratou sobre “A responsabilidade civil advinda do uso irrestrito de dados e a proteção constitucional dos dados pessoais, rumo a um direito fundamental autônomo”. A exposição recaiu sobre a necessidade de adequar o aparato jurídico para regular as novas relações derivadas dessa economia baseada na produção, controle e distribuição de informação.

O Brasil delimitou o assunto a partir de duas normas norteadoras: o Marco Civil da Internet e a Lei Geral de Proteção de Dados – LGPD, cuja vigência se deu em setembro de 2021, com algumas ressalvas para as sanções dos artigos 52, 53 e 54, que entraram em vigor em 1º de agosto de 2021, nos termos da Lei 14.010/2020.

A distribuição correta dos riscos e responsabilidade próprios da atividade de controle de informação é relevante e deve oferecer o melhor aproveitamento econômico da distribuição de dados e dificultar a concentração de benefícios em prol daqueles que investem, sem a devida validade jurídica, os direitos de outrem.

A obrigação de responder pelas ações próprias ou dos outros, poderá incidir no tratamento de dados pessoais sempre que o controlador descumprir os deveres de proteção e cuidados impostos.

Considerando todo o exposto, conclui-se em tela com o posicionamento do STF, quando, publicou decisão acerca da Medida Provisória nº 954/2020 com ênfase na proteção constitucional de dados pessoais como direito fundamental autônomo.

Dessa forma, pode-se afirmar que o vazamento de informações gera direito a indenização pelo dano causado, nem sempre sendo necessário que se comprove a culpa daquele que era responsável pela guarda dos dados compartilhado. O tema ainda é controverso nos tribunais, sendo cedo para afirmar qual entendimento irá prevalecer na jurisprudência.

Em conformidade com o exposto, cumpre ressaltar que apesar do dado em si ser o protagonista e ponto de referência regulatória para disciplina da proteção de dados pessoais, é preciso pensar no contexto em que está inserido. Não se trata, apenas, de limitar irrestritamente o tratamento de dados ou abandonar o consentimento individual como mecanismos protetivo, mas sim de avaliar a sua real capacidade para efetivar essa proteção a partir com contexto em que está inserido.

Para superar essas insuficiências, tendências contemporâneas de materialização da proteção de dados apresentam-se como soluções interessantes, tornando-a mais responsiva tanto aos riscos gerados pelo tratamento como aos obstáculos concretos de uma decisão livre e autônoma.

Nesse sentido, a garantia da autodeterminação informativa, incluída em uma política de responsabilidade civil, é de suma importância para objetivar a proteção de dados pessoais e, consequentemente, a dignidade humana. Uma proteção de dados pessoais efetiva precisa ir além da garantia meramente formal do consentimento individual. É preciso assegurar os pressupostos materiais dessa proteção para se construir um espaço de liberdade no qual o indivíduo esteja apto a configurar as suas relações informacionais.

REFERÊNCIAS

ARENDT, Hannah. **A condição humana.** 13 ed. Rio de Janeiro: Forense Universitária. 2017.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** a função e os limites do consentimento. Rio de Janeiro. Forense. 2021.

BONAVIDES, Paulo. **Teoria Constitucional da Democracia Participativa.** São Paulo: Malheiros, 2001.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 18 set. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 14 ago. 2021.

BRASIL. **Lei nº 8.078, de 11 de Setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 28 set. 2021.

BRASIL. **Lei nº 10.406, de 10 de Janeiro de 2002**. Institui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 28 set. 2021.

BRASIL**. Medida Provisória nº 954**, de 17 de Abril de 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. Acesso em: 27 set. 2021.

BRASIL, Supremo Tribunal Federal. **ADI nº 6387.** Rel. Min. Rosa Weber, Decisão Monocrática, j. 24/04/2020, DJe 28/04/2020. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629. Acesso em: 28 set. 2021.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais elementos da formação da Lei Geral de Proteção de Dados.** São Paulo: Thomas Reuters Brasil. 2020.

FONSECA, Edson Pires da. **Lei Geral de Proteção de Dados Pessoais – LGPD.** Salvador: Editora Juspodivm. 2021.

KAVASAKI, Fujie. **Empresas e a Implementação da Lei Geral de Proteção de Dados.** Coordenador Tarcísio Teixeira. Salvador: JusPodivm. 2021.

MAGALHÃES, Marcus Abreu. **Responsabilidade Civil por Danos Pessoais.** Orlando: Ambra University Press. 2021.

MARTINS, Fernando Ono. **Empresas e a Implementação da Lei Geral de Proteção de Dados**. Salvador: Juspodivm. 2021.

MENDES, Laura Schertel. FONSECA, Gabriel Campos Soares da. **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense. 2021.

MULHOLLAND, Caitlin. **A responsabilidade civil por presunção de causalidade.** Rio de Janeiro: GZ Editora, 2009.

MULHOLLAND, Caitlin. **A LGPD e o novo marco normativo no Brasil.** Porto Alegre: Arquipélago. 2020.

PIOVESAN, Flávia. **Direitos Humanos, o Princípio da dignidade Humana e a Constituição Brasileira de 1988.** Leituras Complementares de Direito Constitucional. Direitos Humanos e Direitos Fundamentais. 3 ed. Salvador: Juspodivm. 2008.

SARLET, Ingo Wolfgang. **Dignidade da Pessoa Humana e Direitos Fundamentais na Constituição Federal de 1988**. Porto Alegre: Livraria do Advogado. 2011.

SCHREIBER, Anderson. **Tratado de proteção de dados pessoais.** Rio de Janeiro. Forense. 2021.

SCHWARTZMAN, Simon. **Pobreza, exclusão social e modernidade:** uma introdução ao mundo contemporâneo. São Paulo: Augurium Editora, 2004.

SILVA, José Afonso. **Curso de Direito Constitucional Positivo.** 40 Ed. São Paulo: Malheiros, 2017.

SOUZA, Carlos Affonso; MAGRANI, Eduardo; CARNEIRO, Giovana. **A LGPD e o novo marco normativo no Brasil.** Porto Alegre: Arquipélago. 2020.

RIEM-HOFFMANN, Wolfgang. **Teoria Geral do Direito Digital.** Transformação Digital. Desafio para o Direito. Rio de Janeiro: Forense. 2021.