Pontifícia Universidade Católica
do Rio de Janeiro

Rafaela Sartore Furquim

A proteção dos dados pessoais como um direito fundamental autônomo: boas práticas de *compliance* frente ao Capitalismo de Vigilância

Dissertação de Mestrado

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Mestrado Profissional em Direito Civil Contemporâneo e Prática Jurídica da PUC-Rio.

Orientadora: Prof.ª Caitlin Mulholland

Rio de Janeiro,
Abril de 2023

Pontifícia Universidade Católica
do Rio de Janeiro

Rafaela Sartore Furquim

A proteção dos dados pessoais como um direito fundamental autônomo: boas práticas de *compliance* frente ao Capitalismo de Vigilância

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Mestrado Profissional em Direito Civil Contemporâneo e Prática Jurídica da PUC-Rio.

Prof.ª Caitlin Mulholland
Orientadora
Departamento de Direito – PUC-Rio

Prof.ª Ana de Oliveira Frazão
UNB

Prof. Carlos Affonso Pereira de Souza
PUC-Rio

Rio de Janeiro, 18 de abril de 2023.

Rafaela Sartore Furquim

Graduada em Direito pela Universidade Cândido Mendes – Centro (UCAM) em 2003. Pós-graduada em Direito Empresarial e Gestão de Negócios na Vez do Mestre/UCAM em 2008. Curso de especialização IAG Master em desenvolvimento Gerencial – ONS na PUC/RJ em 2014. Pós-graduada em Direito Digital – EBRADI 2021. Advogada.

Ficha Catalográfica

Furquim, Rafaela Sartore

A proteção dos dados pessoais como um direito fundamental autônomo: boas práticas de *compliance* frente ao capitalismo de vigilância / Rafaela Sartore Furquim; orientadora: Caitlin Mulholland. – 2023.

105 f.; 30 cm

Dissertação (mestrado)–Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Direito, 2023.

Inclui bibliografia

1. Direito – Teses. 2. Proteção de dados Pessoais. 3. Lei Geral de Proteção de Dados Pessoais. 4. Capitalismo de vigilância; 5. *Compliance*. 6. ANPD.

CDD: 340

Para meus tesouros
Gustavo, Arthur e Antonio.

Agradecimentos

À minha orientadora, Caitlin Mulholland, por ter aceitado o meu convite e me dado a oportunidade de aprender sobre esse tema que tanto me moveu nos últimos dois anos e cujos ensinamentos foram fundamentais para o meu amadurecimento acadêmico;

Ao meu marido, Gustavo Furquim, que me apoiou e me incentivou nesse projeto e, sem dúvida nenhuma, por cuidar dos nossos filhos para que eu pudesse me dedicar e dar tudo de mim nesse estudo;

Ao meu pai Eros Sartore, que mesmo sem estudo formal, é uma das pessoas mais inteligentes que já conheci e seu legado foi me ensinar a amar a leitura e os estudos como fonte de conhecimento e crescimento contínuos;

E à minha mãe, Silene Vieira Sartore, que mais uma vez me apoiou com amor e generosidade em mais um projeto importante da minha vida.

Resumo

Furquim, Rafaela Sartore. **A proteção de dados pessoais como um direito fundamental autônomo:** boas práticas de *compliance* frente ao Capitalismo de vigilância. Orientadora: Mulholland, Caitlin. Rio de Janeiro, 2023. 105 p. Dissertação (Mestrado em Direito) – Departamento de Direito, Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2023.

Em razão do desenvolvimento tecnológico das últimas décadas, a sociedade contemporânea passou por profundas mudanças que deram origem, segundo Shoshana Zuboff, ao Capitalismo de vigilância. Diante deste cenário, o presente estudo tem por objetivo analisar os reflexos desse fenômeno no ordenamento jurídico brasileiro que justificaram a promulgação da Emenda Constitucional 115/22 e da Lei Geral de Proteção de Dados, constituindo um modelo regulatório híbrido, fortemente baseado em princípios, no qual, além de estabelecer obrigações para os agentes de tratamento, cria um ambiente de incentivo à adoção de boas práticas e de governança. Para tanto, será analisado como o *compliance* de dados pode ser um eficiente instrumento para promover, na prática, a adoção dos princípios da LGPD e da regulação já existente da ANPD em prol uma cultura de proteção de dados no Brasil.

Palavras-chave

Proteção de dados Pessoais; Lei Geral de Proteção de dados pessoais; Capitalismo de vigilância; *compliance;* ANPD.

Abstract

Furquim, Rafaela Sartore. **Personal Data protection as a fundamental right itself: *compliance* guidelines against the Surveillance capitalism**. Supervisor: Mullholand, Caitlin. Rio de Janeiro, 2023. 105 p. Master's Dissertation - Department of Law, Pontifical Catholic University of Rio de Janeiro

The technological development of recent decades, contemporary society has faced profound changes that have given rise, according to Shoshana Zuboff, to Surveillance Capitalism. Therefore, this study aims to analyze the impacts of surveillance capitalism in the brazilian legal system that justified the promulgation of Constitutional Amendment 115/22 and the Brazilian General Data Protection Law (LGPD), based on the strong principled on a hybrid regulatory model in which, in addition to establishing obligations for treatment agents, creates an environment that encourages the adoption of good practices and governance. This way, it will be analyzed how data compliance can be an efficient instrument to promote, in practice, the adoption of the LGPD principles and the ANPD regulation in a data protection culture in Brazil.

Keywords

Personal data protection; Brazilian General Data Protection law; Surveillance capitalism; compliance; ANPD.

Sumário

O pressuposto da vulnerabilidade aos perigos depende mais da falta de confiança nas defesas disponíveis do que do volume ou da natureza das ameaças reais.

Zygmunt Bauman

1 INTRODUÇÃO

Em 2017, o jornal *The Economist*[1] afirmou: "os dados são o novo petróleo"[2]. Essa expressão passou a ser muito utilizada para fazer referência ao fenômeno gerado pelos avanços tecnológicos e seus impactos sobre os dados pessoais na sociedade contemporânea. Em que pese algumas críticas quanto à popular comparação, sem dúvidas, serviu para chamar atenção da sociedade para a ordem econômica, por meio da qual os dados pessoais se tornaram a principal engrenagem.

Ao longo dos últimos trinta anos, o avanço da Tecnologia da Informação e Comunicação (TIC) teve como base diversos fatores, dentre eles, a disseminação de computadores pessoais, a *internet*, os *smartphones*, o *e-commerce*, redes sociais, dentre outras inovações que propiciaram significativas alterações sociais, modificando e criando formas de interações no ambiente digital.

Esse contexto é marcado pela excessiva coleta e acumulação de dados no ambiente digital, contudo, logo se descobriu que os dados pessoais são potencialmente valiosos e disponíveis, já que são cedidos gratuitamente em troca de serviços ou facilidades para os seus usuários. A falta de consciência dos impactos decorrentes desse novo modelo, aliada à criação de grandes bases de dados (*Big data*), propiciou uma escalada quantitativa e qualitativa da sua operacionalização e circulação, na medida em que passaram a ser o vetor da economia do século XXI.[3]

Esse cenário foi caracterizado por Shoshana Zuboff como Capitalismo de vigilância, que o definiu da seguinte forma:

> 1. Uma nova ordem econômica que reivindica a experiência humana como matéria-prima para práticas comerciais dissimuladas de extração, previsão e vendas; 2. Uma lógica parasítica na qual a produção de bens e serviços é subordinada a uma nova arquitetura global de modificação de comportamento; 3. Uma funesta mutação do capitalismo marada por concentrações de riqueza, conhecimento e poder sem precedentes na história da humanidade; 4. A estrutura

[1] Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em 07 fev. 2023.

[2] "Vistos como o novo petróleo, os dados são hoje insumos essenciais ara praticamente todas as atividades econômicas e se tornaram, eles próprios, objeto de crescente e pujante mercado. Não é sem razão que se cunhou a expressão *data-driven economy*, ou seja, economia movida a dados, para designar o fato de que, como aponta Nick Srnicek, o capitalismo do século XXI passou a centrar-se na extração e no uso de dados pessoais." (FRAZÃO, 2020, p. 24).

[3] No mesmo sentido, com o avanço dos algoritmos dos sistemas de informação, criou-se um ambiente propício para uma guinada significativa de ordem quantitativa e qualitativa no processo de coleta, acumulação e mineração dos dados. (BIONI, 2021, p. 32-33).

> que serve de base para a economia de vigilância; 5. Uma ameaça tão significativa para a natureza humana no século XIX e XX; 6. A origem de um novo poder instrumentário que reivindica domínio sobre a sociedade e apresenta desafios surpreendentes para a democracia de mercado; 7. Um movimento que visa impor uma nova ordem coletiva baseada em certeza total; 8. Uma expropriação de direitos humanos críticos: uma destituição da soberania dos indivíduos. (ZUBOFF, 2020, p. 7).

A análise qualitativa dos dados realizada *Big data* e *Big analysis* oferece aos agentes que os detém, profundo conhecimento acerca dos indivíduos e de grupos sociais, notadamente sobre suas tendências e predileções. Enquanto prendem a atenção do usuário, coletam inúmeras informações e comportamentos *online* que são processados e analisados com o objetivo de extrair padrões e definir conteúdo que será oferecido pelos agentes aos usuários na rede, manipulando e direcionando suas escolhas.

Em seu livro *Privacidade é Poder*, Carissa Véliz salienta que o uso dos dados pessoais como fonte de sustentação na economia baseada em dados pode ser bastante nocivo às pessoas. Para ilustrar essa afirmação, comparou-o ao amianto que, no princípio, era considerado uma grande descoberta por ser matéria-prima valiosa mineirada a baixíssimo custo, mas, no entanto, foi posteriormente constatado seu alto potencial tóxico desse material (VÉLIZ, 2021, p. 129-137). Da mesma forma que o amianto, os dados pessoais são coletados em abundância e a baixo custo, e ambos com alto potencial de gerar grandes lucros. Contudo, vale ressaltar que, diferentemente do amianto, o uso dos dados pessoais somente se torna nocivo se houver violação a direitos humanos já consagrados.

Com efeito, comparação da referida autora remete a possibilidade de usar indiscriminadamente dados pessoais, interferindo não só em aspectos da privacidade dos titulares, no sentido mais tradicional de vida privada e intimidade, mas principalmente, na sua capacidade de controlá-los, ferindo direitos fundamentais como liberdade e livre desenvolvimento da pessoa humana.

Adicionalmente, o uso desregulado dos dados pessoais que circulam na rede pode impactar, não apenas os indivíduos, mas também grupos sociais[4], e sob essa perspectiva coletiva, ampliar esse possível efeito nocivo de restrição de liberdades.

[4] No livro *Privacidade é Poder*, a autora explica o aspecto coletivo da privacidade frente a possibilidade da tecnologia de realizar o perfilamento comportamental de uma pessoa por meio de conexões com outras. Assim, mesmo que um indivíduo autorize por meio do consentimento o uso dos seus próprios dados, a partir deles é possível traçar o perfil de pessoas a ele conectada (VÉLIZ, 2021, p. 111-112).

Vale ressaltar, mesmo que a proteção de dados não se restrinja ao meio de circulação (físico ou digital), sem dúvidas, as ferramentas tecnológicas existentes são fator preponderante que desperta a preocupação de como os dados pessoais são utilizados na sociedade contemporânea.

Em vista disso, para se construir uma regulação acerca da proteção de dados pessoais não se pode levar em consideração apenas a privacidade. Em verdade, deve-se buscar a efetiva tutela da pessoa, considerando as várias formas de controle existentes e contra a discriminação, tudo isso com a finalidade de assegurar a integridade de aspectos fundamentais de própria liberdade pessoal (DONEDA, 2021, p. 24).

Nesse contexto, seguindo outras legislações sobre o tema, com especial inspiração no Regulamento Geral de Proteção de Dados europeu (GDPR), em 14 de agosto de 2018 foi instituída a Lei nº 13.709, a Lei Geral de Proteção de Dados (LGPD), que regula o tratamento dos dados pessoais definindo princípios e obrigações dos agentes, com fundamento na proteção de direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural.

Poucos anos depois, em 10 de fevereiro de 2022, foi promulgada a Emenda Constitucional 115 que inseriu o direito à proteção de dados pessoais no rol dos direitos fundamentais, ao incluir o inciso LXXIX no artigo 5º.

Assim, a importância do marco legislativo brasileiro está relacionada ao reconhecimento de que os dados pessoais necessitam de proteção especial na sociedade de vigilância. Afinal, correspondem a todas as informações relacionadas à pessoa natural identificada ou identificável (artigo 5º, I LGPD) e, como tal, devem ser assegurados todos os direitos fundamentais conferidos ao seu titular.

Na perspectiva de proporcionar maior eficácia à proteção de dados pessoais, a lei brasileira adotou modelo intermediário entre a regulação clássica, ou seja, por meio da criação de direitos, deveres e sanção (comando-controle), e o modelo da autorregulação, que consiste na adoção de boas práticas e governança que assumem papel de regular o mercado, impondo verdadeiras regras sociais de adesão voluntária.

Desse modo, foi adotada na LGPD a corregulação, que conjuga a disposição expressa de objetivos e fundamentos que orientam a aplicação dos princípios e regras contidos na lei, atribuindo ao titular diversos direitos e, ao mesmo tempo,

autorizando o tratamento dos dados pessoais pelos agentes, desde que devidamente justificado em alguma das bases legais e em deveres de prestação de contas para monitoramento pela Autoridade Nacional de Proteção de Dados (ANPD).

Assim, a lei, fundamentalmente principiológica e promocional da proteção de dados pessoais, evita que sanções sejam o único meio de coibir ilicitudes, já que lesões decorrentes do tratamento de dados são irreparáveis e podem ser potencializadas pela TIC quantitativamente (o dano pode atingir uma coletividade) e qualitativamente (hipóteses de violação a direitos mais sutis, impossibilitando que o titular reconheça um eventual dano).

Desta forma, a lei cria um ambiente regulatório de incentivo à adoção de boas práticas de governança, formuladas para serem adequadas aos modelos de negócio dos agentes e com vistas à promoção de uma cultura de proteção dos dados, como um propósito estratégico da organização e, principalmente, associado aos riscos existentes na atividade desempenhada.

Com base nisso, busca-se com esse estudo, compreender o *compliance* como uma valiosa ferramenta a ser utilizada na função de apoiar a governança corporativa no estabelecimento de políticas e práticas internas para atendimento aos propósitos da LGPD.

Para tanto, o estudo perpassa pela compreensão da evolução da tutela à privacidade e a noção do direito à proteção de dados, para verificar como a LGPD, através dos seus fundamentos e princípios, promove a adoção, por parte dos agentes de tratamento, de boas práticas de governança de dados pessoais tendo a ANPD com principal ator na verificação da adequação de tais práticas.

Nesse sentido, o primeiro capítulo aborda o contexto do capitalismo de vigilância e seus reflexos que culminaram na necessidade de evolução protetiva dos dados pessoais. O segundo capítulo, após a contextualização legislativa histórica, para o melhor entendimento da distinção entre privacidade e proteção de dados pessoais, e o exame dos fundamentos e princípios contidos na LGPD para compreender como contribuem para uma abrangente proteção de dados no Brasil. Por fim, no terceiro capítulo, procura-se demonstrar a importância do *compliance* para o efetivo cumprimento à LGPD, estimulando os agentes na busca de soluções adequadas de conformidade com a lei, e o papel da ANPD fomentando o uso correto dos dados pessoais.

Vale informar que, para efeitos deste estudo, que apesar de a proteção de dados pessoais não se restringir à esfera digital, conforme dispõe o artigo 1º da LGPD, a abordagem será estritamente na perspectiva das Tecnologia da Informação e Comunicação. Fica também excluída da análise, o aprofundamento das bases legais autorizativas para o tratamento de dados.

Por fim, cumpre indicar que metodologia utilizada foi a análise crítica da literatura jurídica e legislações e regulações contemporâneas sobre a proteção de dados pessoais e privacidade.

2 A TECNOLOGIA E O CAPITALISMO DE VIGILÂNCIA

2.1 Contexto da transformação tecnológica

O avanço tecnológico é capaz de realizar profundas transformações na sociedade, seus impactos exponenciam o modo de viver e, com isso, estabelece novos relacionamentos, formas de trabalho, circulação de bens e serviços dentre outras inovações disruptivas. De maneira marcante na história, esse fenômeno foi observado com a criação das máquinas à vapor, no século XVIII, com o uso da energia no século XIX e a invenção da internet no século XX, que culminaram nas Revoluções Industriais cujos reflexos geraram profundas transformações na economia mundial, criando modelos sociais.

Nas últimas décadas, em transformação semelhante, a partir do surgimento de práticas inovadoras, como as redes sociais, massificação da *internet* e do comércio eletrônico, a humanidade vem sendo impactada, de maneira global, nos mais diversos aspectos sociais, econômicos e políticos.

Esse fenômeno foi percebido por Klaus Schwab que o denominou de Quarta Revolução Industrial[5], caracterizada pela fusão entre a esferas física, digital e biológica, notadamente marcada pelo avanço tecnológico nos campos da TIC, *Internet* das coisas (IoT), inteligência artificial (IA) e robótica.

Schwab (2018) chama atenção para o avanço tecnológico das últimas décadas que está mudando profundamente a economia e o modo de viver, transformando consideravelmente a humanidade, tal como as Revoluções Industriais precursoras.

Há poucas décadas, o armazenamento de dados e informações eram feitos em papéis e arquivos físicos, cuja organização demandava esforço e espaço. Com a crescente digitalização, esses mesmos papéis passaram por um processo de desmaterialização e se tornaram *bytes*, que são arquivados em pastas virtuais. Com uma pesquisa simples na ferramenta de busca é possível encontrar qualquer arquivo ou informação de maneira rápida e eficaz.

[5] Em janeiro de 2016, no Fórum Econômico Mundial ocorrido em Davos, Klaus Schwab no seu discurso trouxe o conceito de Quarta Revolução Industrial caracterizada pelo fim dos limites entre os mundos físico, biológico e digital, ou seja, na nova era, todos esses fatos se interligam de tal forma que não é mais possível identificá-los separadamente isso decorre do uso massivo da tecnologia em todos os campos da vida humana.

Atualmente, não são somente papeis arquivados no meio digital. Há muitos outros dados que são constantemente coletados e arquivados, sujeitos a análises por programas automatizados, que podem não só rastreá-los como cruzá-los. Todo tipo de dado é registrado, inclusive dados pessoais. A esse fenômeno chama-se "datificação" dos dados.

Ao usar um *smart watch*, dados físicos tangíveis são transformados em dados digitalizados que, por sua vez, são usados em benefício do próprio usuário, como controlar rotas de exercícios físicos, pressão arterial etc. Mas, por outro lado, esses mesmos dados são coletados e submetidos às análises por sistemas automatizados bastante complexos que definem o perfil deste usuário, classificam sua saúde e que podem ser utilizados para outros propósitos muito diferentes daqueles que motivam o uso do dispositivo. Ou seja, são processadas informações e delas extraídas diversas outras finalidades que não são de interesses do titular, nem estão vinculados aos propósitos do produto.

Outro exemplo, são os assistentes pessoais, como a *Alexa* da *Amazon*, a *Siri* da *Apple*, e tanto outros equipamentos que, além das funcionalidades do próprio equipamento, paralelamente receptam dados dos usuários e os convertem em informações úteis para outros objetivos.

Dispositivos que usam TIC tem se tornado cada vez mais ubíquos no cotidiano em razão dos diversos benefícios (como rapidez e eficiência) para seus usuários e, paralelamente, coletam e processam de dados pessoais, transportando para o digital diversos aspectos da pessoa de maneira contínua, gratuita e, principalmente, sem que o usuário sequer se dê conta de que seus dados estão sendo tratados com finalidades econômicas.

Atualmente, vive-se em uma sociedade na qual a informação é o elemento gravitacional da economia, concebendo a chamada economia movida a dados. Logo, no mundo globalizado, a informação assume valoroso papel ao reorganizar a dinâmica social, semelhante ao que as máquinas a vapor fizeram outrora.

2.2 Capitalismo de Vigilância

Cunhada por Shoshana Zuboff, a expressão "capitalismo de vigilância" se refere a um novo modelo de capitalismo decorrente das mudanças promovidas pelo

avançado ferramental tecnológico da atualidade, que monitora e extrai informações em todos os aspectos da vida humana, com a finalidade de explorar dados pessoais para exercer controle e obter lucro.

Esse ambiente, sustentado pela vigilância ininterrupta, criou um modelo de "superávit comportamental", no qual os dados servem ao mesmo tempo para aprimorar o serviço oferecido, bem como para outras finalidades como, por exemplo, o uso em publicidade direcionada.

A massificação do uso de celulares e dispositivos inteligentes de uso pessoal conectados à internet alavancaram a fusão entre os ambientes *on-line* (digital) e *off-line* (físico). Atualmente, pessoas estão cada vez mais conectadas e seus comportamento em rede, rastreados. Assim, dados relativos à localização geográfica, pressão arterial, tempo de leitura de uma mensagem, quantidade de interações com determinadas pessoas; tudo pode ser monitorado e traduzido para análise do perfil comportamental do usuário, inclusive sentimentos, tornando-o transparente perante o agente de tratamento.[6]

Estabelece, desse jeito, uma relação assimétrica entre as organizações que usam dados pessoais e os indivíduos, que são usuários dos serviços ou produtos, e ao mesmo tempo, fornecem a matéria-prima da qual os agentes obtém lucro.

Essa dinâmica consagra uma nova forma de capitalismo, descrita por Shoshana Zuboff como capitalismo de vigilância:

> O capitalismo de vigilância reivindica de maneira unilateral a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais. Embora alguns desses dados sejam aplicados para o aprimoramento de produtos e serviços, o restante é declarado como superávit comportamental do proprietário, alimentando avançados processos de fabricação conhecidos como "inteligência de máquina" e manufaturado em produtos de predição que antecipam o que um determinado indivíduo faria agora, daqui a pouco e mais tarde. (ZUBOFF, 2020, p. 18-19).

A autora constata que "[...] o capitalismo industrial transformava as matérias-primas da natureza em mercadorias, já o capitalismo de vigilância reivindica matéria da natureza humana para a feitura de uma mercadoria nova [...]" (ZUBOFF, 2020, p. 115).

[66] Sobre publicidade direcionada como tônica dos modelos de negócios na internet, ver BIONI, Bruno. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021, p. 14-31.

Nesse mesmo sentido, Bruno Bioni assevera que consumidor passa a ter uma posição ativa na relação de consumo, para além da tradicional passividade, ao que chama de "*prossumer"*, uma fusão entre os termos consumidor e produtor (BIONI, 2021, p. 13).

De maneira sem precedentes, algoritmos altamente complexos são utilizados, por exemplo, por empresas pioneiras como *Facebook* e *Google*, e muitas outras empresas que usam da tecnologia para serem capazes de depreender informações com alto grau de precisão e utilizá-las para as finalidades perseguidas pelos seus negócios.

Originalmente, o Google foi criado para se tornar uma ferramenta de conteúdo e disseminação de conhecimento (ZUBOFF, 2020, p. 80). Contudo, após estudos internos realizados a partir do material que era coletado por meio das pesquisas dos seus usuários, percebeu-se que era possível traduzi-los em pensamentos, sentimentos e interesses que, ao mesmo tempo, retroalimentava a contínua aprendizagem dos seus algoritmos por meio de processos de *feedbacks* de aperfeiçoamento.

O grau de acerto na relevância da busca demostrava que era possível predizer os interesses e tendências dos usuários. Note-se que no momento inicial, as informações comportamentais eram utilizadas tão-somente para o interesse do próprio usuário, de fato servindo como forma de aperfeiçoamento dos serviços.

A grande guinada ocorreu quando o *Google* passou a utilizar informações comportamentais para publicidade direcionada, treinando os algoritmos para fornecer serviços e produtos que eram de interesse dos próprios usuários. Então, os custos com publicidade foram reduzidos e ao mesmo tempo, alterou a lógica inicial do seu serviço de buscas.

Cedendo às pressões dos seus investidores para obter mais lucro, o Google colocou fim à reciprocidade entre os serviços e usuários, passou então a utilizar os resultados das predileções dos usuários com a finalidade de compatibilizá-los (*matching*) com publicidade direcionada. Os dados coletados que não tinham utilidade direta para o aperfeiçoamento dos serviços passaram a ser vendidos, transformados em "superávit comportamental" (ZUBOFF, 2020, p. 92), ou seja, um resíduo de informação que poderia servir para obtenção de lucro. A novidade foi

copiada por outras empresas e, atualmente, se tornou um dos fatores elementais do capitalismo de vigilância.

Na fase primária do capitalismo de vigilância, apenas a propaganda estava relacionada com as buscas do usuário, não havia, nesse estágio, nenhum componente que fosse capaz de alterar suas tendências ou comportamentos. Mas não foi por muito tempo.

Do mesmo modo que o Google, o Facebook obtém lucros altos em razão dessa dinâmica. Ele se fortaleceu e disseminou como uma ferramenta social, na qual qualquer um, e todos ao mesmo tempo, podem interagir e expor seu cotidiano, suas ideias, maneira de viver e encoraja a expressão de opiniões pessoais e o empoderamento do indivíduo.

Contudo, por trás do seu serviço, há algoritmos eficazes para coletar, selecionar e processar informações das mais variadas possíveis, direta e indiretamente, por meio da tradução de comportamentos *on-line* dos seus usuários, traçando perfis que podem ser utilizados para a manipulação de condutas.

Em 2012, para avaliar a efetividade da alteração de comportamento em razão do conteúdo digital, o *Facebook* realizou um experimento para avaliar a propensão de alterações no estado mental de cerca de 700 mil usuários. Para isso, analisou dois grupos, um que recebia postagens com mensagens positivas e outro recebia mensagens com postagens negativas. O estudo descobriu que usuários que receberam conteúdos positivos eram mais propensos a realizar no seu próprio feed postagens positivas.[7]

Analisando o fenômeno sob a perspectiva da sociedade da transparência, Byung-Chul Han compara a forte exigência por transparência artificialmente criada por um imperativo econômico, a um "panóptico digital do século XXI" para demonstrar, com base na teoria do panóptico de Benthan, que atualmente, vive-se em uma sociedade de múltiplos observadores, visto que os indivíduos estão sob onipresente supervisão e controle em todos os lugares (HAN, 2017, p. 106)[8].

Não há dúvidas que a TIC influencia no desenvolvimento econômico, quando substitui processos manuais ou semi-manuais para processos integralmente

[7] ALBERGOTTI, Reed. *WSJ*. s.d. https://www.wsj.com/articler/facebook-experiments-had-few-limits-1404344378 Acesso em 15 jan. 2023.
[8] De igual modo in RODOTÀ, Stefano. **A vida na sociedade de vigilância**. Tradução de Danilo Doneda e Luciana Cabral Doneda. p. 47.

executados por programas de computador, ou ainda, que propicia a criação de novos modelos de negócio com inovações revolucionárias, algumas benéficas, outras nem tanto, para a sociedade.

Por outro lado, toda essa inovação causou impactos relevantes para o ser humano, como indivíduo e como coletividade, e por essa razão precisam ser reavaliados sob a ótica ética-jurídica, sobretudo, demanda uma reflexão sobre o necessário equilíbrio entre o desenvolvimento tecnológico e proteção de direitos fundamentais eventualmente impactados de maneira que estes permaneçam no centro do ordenamento jurídico do Estado democrático de direito.

Os impactos supracitados estão revestidos na oferta de serviços e produtos, que sutilmente ameaçam direitos fundamentais como a liberdade. Quando o assinante da *Netflix*, ou qualquer outro *streaming*, assiste ao filme indicado de acordo com o seu perfil, em verdade, está delegando sua liberdade de escolha de qual o próximo filme será assistido. O algoritmo "ajuda" a tomar decisões que "julga" melhores para o usuário de acordo com suas tendências e comportamentos predecessores. Essas recomendações estão baseadas nos padrões identificados para este usuário em comparação com perfis semelhantes, compreendendo desejos ou tendências de determinado grupo de acordo com certas características.[9]

A escolha de um filme pode parecer um fato simplório, ou até benéfico, pois poupa o tempo de escolha do usuário e a chance de a recomendação ser satisfatória é grande. Contudo, a partir de um dado 'simples', é possível realizar cruzamento de dados para obter o perfilamento do usuário em outras instâncias da sua vida. Por isso, qualquer dado importa, desde que seja relacionado à pessoa natural. Além disso, cotidianamente fatos como esse fazem parte da vida conectada, de forma silenciosa e imperceptível, a autonomia pessoal está sendo, cada vez mais, delegada a algoritmos.

Discorrendo sobre esse assunto, Danilo Doneda reflete que "[...] a tecnologia aumenta as oportunidades de realizarmos escolhas que podem influir diretamente na nossa esfera privada [...]" (DONEDA, 2021, p. 23).

[9] Nas palavras de Mulholland e Frajhof (2020), "Atualmente, a aplicação de IA está cada vez mais inserida nos mais variados aspectos da vida contemporânea. Ela não apenas modula a percepção da realidade humana por meio do filtro bolha (PARISIER, 2011), mas também participa das nossas escolhas (Google) e preferencias musicais, cinematográficas (Netflix) e compras on-line, identificando e disponibilizando exatamente aquilo que estaríamos possivelmente interessados em ver, de acordo com o que já ouvimos, vimos e compramos em um passado recente."

Dados pessoais refinados e organizados de forma estruturada geram resultados com melhores predições, elevando a chance de acurácia da publicidade direcionada que se retroalimenta a cada navegação, e passam a ser mais acessadas pelos usuários e mais desejadas pelos agentes de publicidade. Nesse ciclo, os valores com publicidade são reduzidos, diminuído também o esforço para buscar novos clientes e produz mais eficácia na venda.

Aliás, ao avaliar tendências de um usuário, a publicidade direcionada também pode criar necessidades de consumo antes inexistentes, incentivando-o desnecessariamente.

Essa dinâmica, contudo, está para além do mercado de consumo, ao terceirizar às máquinas decisões humanas, delega-se a autonomia de escolha, não ao algoritmo, mas às empresas que detém a propriedade desse algoritmo.

No estudo realizado em 2014, Wu Youyou, Michal Kosinski e David Stillwell concluíram que:

> Ferramentas de avaliação de personalidade automatizadas, precisas e baratas podem afetar a sociedade de várias maneiras: as mensagens de marketing podem ser adaptadas às personalidades dos usuários; os recrutadores poderiam combinar melhor os candidatos com os cargos com base em sua personalidade; produtos e serviços poderiam ajustar seu comportamento para melhor corresponder aos personagens e mudanças de humor de seus usuários; e os cientistas poderiam coletar dados de personalidade sem sobrecarregar os participantes com longos questionários. Além disso, no futuro, as pessoas podem abandonar seus próprios julgamentos psicológicos e confiar em computadores ao tomar decisões importantes na vida, como escolher atividades, planos de carreira ou até mesmo parceiros românticos. É possível que tais decisões baseadas em dados melhorem a vida das pessoas.
>
> No entanto, o conhecimento da personalidade das pessoas também pode ser usado para manipulá-las e influenciá-las. Compreensivelmente, as pessoas podem desconfiar ou rejeitar as tecnologias digitais depois de perceber que seu governo, provedor de internet, navegador da web, rede social online ou mecanismo de pesquisa pode inferir suas características pessoais com mais precisão do que seus familiares mais próximos. Esperamos que consumidores, desenvolvedores de tecnologia e formuladores de políticas enfrentem esses desafios apoiando leis e tecnologias de proteção à privacidade e dando aos usuários controle total sobre suas pegadas digitais. (YOUYOU; KOSINSKI; STILLWELL, 2015, p. 1).

Alguns argumentos sobre o fim da privacidade no mundo digital foram utilizados, especialmente pelas partes que têm interesse em manter a extração e exploração dos dados. O discurso retórico se baseia na ideia quem não tem nada a esconder, não deveria se preocupar com a privacidade.

Esse mesmo argumento foi muito usado para justificar a realização de certas políticas públicas invasivas após 11 de setembro. Colocado desta forma, faz-se uma comparação valorativa entre a segurança nacional e a privacidade. Ocorre que, como demonstra Daniel Solove, o argumento é falho. Segundo o autor, é preciso entender o conceito de privacidade para dar o peso necessário e afastar retóricas desse gênero. Além disso, a privacidade não seria composta por elementos estritamente relacionados à vida privada e a intimidade, seu campo de atuação é mais amplo e conduz a impactos coletivos e como ela influência sobre interesses sociais maiores (SOLOVE, 2007, p. 745). A tecnologia da informação e comunicação contribui para uma nova forma de controle social, mais discreta, porque seus mecanismos de persuasão estão encrustados no cotidiano dos cidadãos sem que sejam percebidos, e mais penetrante, porque sua precisão decorre da análise de aspectos da sua personalidade.

Deve-se ter em mente que os algoritmos utilizados pelas TIC são modelos matemáticos e estatísticos elaborados por outro ser humano e que fazem análises probabilísticas.

Por serem projetados por humanos, os algoritmos são falíveis e podem carregar no seu código fonte vieses cognitivos dos seus programadores. Além disso, dependendo da base de dados utilizada na programação, vieses cognitivos e preconceitos arraigados na sociedade podem, inevitavelmente, ser replicados para o algoritmo, sendo uma nova fonte de discriminação. “Modelos são opiniões embutidas em matemática [...]” (O'NEIL, 2020, p. 35).

Logo, o ordenamento jurídico deve ser capaz de garantir a proteção à pessoa natural no seu aspecto físico e digital, considerando que, em razão do desenvolvimento tecnológico, tais aspectos não podem mais ser avaliados separadamente. Essa resposta se dá com a criação de uma regulação sobre o tratamento e o fluxo dos dados pessoais, que a rigor, são a base de tudo.

Vale lembrar que usar dados pessoais para fins empresariais ou para realização de políticas públicas é um ato lícito e, porque não dizer, necessário na realidade atual. Contudo, o que interessa para o ordenamento jurídico é estabelecer qual é a maneira correta, ética, assim como estabelecer os limites legais para seu uso, visando a proteção de valores fundamentais.

A famosa frase de Francis Bacon, “conhecimento é poder” continua atual. Curiosamente, a essência dos serviços prestados por grandes empresas de tecnologia da informação e comunicação consiste em acumular e produzir a maior quantidade de informações para catalogá-las e filtrá-las, produzindo conhecimento.[10]

O termo *gatekeepers* é usado para fazer referências à essas empresas que funcionam como os “guardiões dos portões” da *internet*, porque se comportam como verdadeiros editores dos conteúdos que chegam até os usuários.

Paradoxalmente, por ser a informação personalizada, a sensação do usuário é de liberdade de escolha dentre as vastas opções disponíveis na *internet*, mas o que acontece, de fato, é que ela é direcionada de acordo com os interesses dos *gatekeepers*.

Já se sabe que usuários da *internet* clicam em anúncios ou qualquer outro conteúdo movido por tendências e interesses pessoais e esse é o segredo dessas empresas que buscam conhecer cada vez mais seus usuários, às vezes melhor que ele mesmo, e a partir desse conhecimento, retroalimenta o interesse pelo seu conteúdo.

Os impactos negativos da sociedade baseada em dados já foram percebidos em casos como Cambrige Analytica[11], cuja experiência serviu para inferir quão nocivo pode ser o uso dos dados pessoais de maneira desregulada.

É por essa razão que Carissa Veliz afirma que “[...] viver em um mundo sem privacidade é perigoso [...]” (VÉLIZ, 2021, p. 23). Há diversos exemplos que já demonstram os resultados catastróficos do mal uso dos dados pessoais, impactando diretamente na democracia.[12]

[10] “A informação em si não é o que alavanca eficiência na atividade empresarial, mas o seu processamento-organização a ser transformado em um conhecimento aplicado.” (BIONI, 2021, p. 10-11).

[11] Cambridge Analytica foi uma empresa que utilizou algoritmos para predizer e influenciar comportamentos de milhares de cidadãos usuários do Facebook para supostamente ajudar Donald Trump a vencer as eleições presidenciais norte-americanas. A reportagem do The Guardian relata como o caso ocorreu. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Acesso em 29 jan. 2023.

[12] Shoshana Zuboff assim discorre “O estado de exceção declarado pelos fundadores do Google transformou o jovial Dr. Jekyll num impiedoso e forte Mr. Hyde, determinado a caçar sua presa em qualquer lugar, a qualquer hora, quaisquer que fossem os objetivos soberanos de cada indivíduo. O novo Google ignorava reivindicações de autodeterminação e não reconhecia limites a priori sobre o que poderia descobrir e tomar para si. Desprezava o conteúdo moral e jurídico dos direitos individuais de decisão e remoldava a situação transformando-a em oportunismo tecnológico e poder

O tratamento de dados pessoais tem natureza potencialmente invasiva e, como a Constituição brasileira tem como valor central a proteção da dignidade humana, a legislação a respeito dos dados pessoais deve ser ampla e dinâmica, evitando a existência de lacunas. Assim sendo, a legislação deve acompanhar as mudanças promovidas pelos avanços tecnológicos, no sentido de buscar, para o titular, uma proteção ampla, além da proteção da privacidade, protegendo-o de possíveis ameaças a direitos fundamentais, como a liberdade e cidadania.

Este capítulo teve a intenção de contextualizar a situação dos dados pessoais como *commodity* na sociedade da informação, cujas características assumem novos contornos delineados em uma nova forma de capitalismo.

Neste contexto, a partir da criação de novas relações, surgem conflitos sociais até então inexistentes e outras formas de poder sobre os quais o ordenamento jurídico deve reavaliar se as categorias jurídicas existentes atendem às novas necessidades, de modo que os direitos fundamentais permaneçam como o centro da sociedade democrática.

No capítulo a seguir, serão analisados os motivos pelos quais os dados pessoais, como projeções da personalidade no ambiente digital, merecem proteção para além da privacidade. Para isso, será realizada uma contextualização histórica das principais normas mundiais sobre o assunto, até a criação da lei brasileira de proteção de dados pessoais (LGPD) e sua abordagem principiológica.

unilateral. O novo Google assegura àqueles que são, de fato, seus clientes que fará tudo que for necessário para transformar a falta de clareza inerente ao desejo humano em fato científico. Este Google é a superpotência que estabelece seus valores e persegue suas metas acima e além dos contratos sociais aos quais outros precisam se submeter." (ZUBOFF, 2020, p. 101).

3 A CONSTRUÇÃO DA PROTEÇÃO DE DADOS NO BRASIL

3.1 Evolução legislativa no contexto mundial

A privacidade passou a ser protegida pelo ordenamento jurídico no período que se seguiu após a Segunda Guerra mundial, como um compromisso político dos Estados com as novas democracias ocidentais com relação aos direitos invioláveis das pessoas (PERLINGIERI, 2002, p. 36).

Assim, a proteção da dignidade da pessoa humana e outros direitos fundamentais surgiram como uma resposta protetiva aos cidadãos frente ao poder do Estado, e a privacidade nesse contexto, passou a ser um direito fundamental com estreita relação com a liberdade e a democracia.

Isso se deu em declarações internacionais de direitos, sendo a primeira em 1948, na Declaração Universal dos Direitos do Homem da Assembleia Geral das Nações Unidas que no seu artigo 12 dispôs: "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra essas intromissões ou ataques toda a pessoa, tem direito à proteção da lei [...]" (DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS, 1948, p. 1)[13].

Essa diretriz, difundida mundialmente, reconhecia a pessoa como titular de um direito fundamental à privacidade como a faculdade de controlar o acesso de terceiros à sua esfera privada.

A mesma direção foi seguida por outras normas sobre o tema, como a Convenção Europeia dos Direitos do Homem de 1950[14] e Convenção americana dos direitos do Homem (Carta de San José de 1969).[15]

[13] Disponível em: https://www.ohchr.org/en/human-rights/universal-declaration/translations/portuguese?LangID=por. Acesso em 31 jan. 2023.

[14] Art. 8º Direito ao respeito pela vida privada e familiar Toda a pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. Disponível em https://echr.coe.int/Documents/Convention_Instrument_POR.pdf. Acesso em 04 fev. 2023.

[15] Artigo 11. Proteção da honra e da dignidade. 1.Toda pessoa tem direito ao respeito de sua honra e ao reconhecimento de sua dignidade. 2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação. 3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas. Disponível em: https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm. Acesso em 04 fev. 2023.

Nessa época, foi determinante a constatação que o direito à privacidade, sob a ótica estritamente individualista, não abarcava os impactos coletivos prejudiciais à igualdade e cidadania que o tratamento de dados pessoais poderia causar na dinâmica de controle e poder.

Foi na Alemanha em 1970 com a Lei de Proteção de Dados do Estado de Hesse que houve uma resposta jurídica ao perfilamento decorrente de controle censitário realizado pelo Estado. Muito embora, naquela época o progresso tecnológico não fosse expressivo como atualmente, foi um poderoso passo ao reconhecer a proteção de dados como um direito humano fundamental e autônomo (SARLET, 2021, p. 14).

A partir desta lei, seguindo a mesma ótica, a Suécia em 1973 criou a Lei de Acesso à Informação, tendo sido esse passo precursor à proteção dos dados pessoais em ordenamento jurídico, seguida por outros países da Europa, e, posteriormente, o mesmo caminho adotado no Brasil. (PEIXOTO; ERHHARDT JÚNIOR, 2018, p. 38).

Em 1974, nos Estados Unidos, foi promulgada a *Pricavy act*[16] como instrumento jurídico para regular e proteger a privacidade e o uso indevido pelo Estado e terceiros de dados de identificação pessoal.[17]

A questão também foi observada em fóruns econômicos como a Organização de Cooperação e Desenvolvimento Econômico (OCDE) com a publicação do *Guidelines on the Protection of Principles and Trasnborder Flows of Personal Data* em 1980, tendo sido revisada posteriormente em 2013[18].

Mas foi em 1981, na Convenção de Estrasburgo nº 108 do Conselho Europeu, que se deu relevante passo na direção da proteção dos dados pessoais, para além da proteção à privacidade. O seu artigo 2º define como informação pessoal "qualquer informação relativa a uma pessoa singular identificada ou suscetível de identificação", consagrando o conceito que veio a ser considerado em regulações

[16] Disponível em: https://www.govinfo.gov/content/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf. Acesso em 04 jan. 2023.

[17] De acordo com Bruno Bioni e Rafael Zanatta, "[...] a aprovação do *Privacy Act* de 1974, na esteira do 'escândalo de Watergate', que custou a renúncia de Richard Nixon e expôs ao grande público um aparato de escutar ilegais e coleta de dados." (BIONI; ZANATTA, 2022, p. 14).

[18] A alteração de 2013, teve importante relevância ao incorporar práticas de gestão de risco, como fator de limitação e controle ao fluxo de dados, redefinindo suas diretrizes, contudo, originariamente serviu como guia para proteção de dados pessoais e privacidade no contexto de crescente fluxo de dados para estabelecer os pilares que seriam replicados em leis nacionais. Disponível em: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Acesso em 22 jan. 2023.

posteriores, qual seja, qualquer informação relativa à pessoa, merece proteção para assegurar importantes aspectos da personalidade.

Assim, a Convenção nº 108 teve significativo papel ao lançar novas diretrizes sobre a proteção de dados pessoais na Europa (SOUZA *et al.*, 2020), contudo, por sua natureza, consistia apenas em recomendações para que os países membros estabelecessem legislações próprias sobre essa matéria.

Tempos depois, com a evolução da tecnologia da informação e comunicação conjugado ao uso massivo da internet, os dados pessoais passaram a ser considerados bem jurídico relevante em virtude da imensa capacidade de fluxo de informação, o que jogou luzes na importância de criar mecanismos regulatórios mais efetivos e específicos para a proteção dos dados pessoais.

Em razão disso, em mais um passo evolutivo na regulação dos dados pessoais, o Conselho Europeu em 1995, concebeu a importante Diretiva 95/46/CE[19] que foi precursora do Regulamento Geral de Proteção de dados pessoais (GDPR).

Tal Diretiva tinha como objetivo de traçar convergências e uniformizar a coleta, tratamento e uso dos dados pessoais pelos estados membros da União Europeia e, tal a sua relevância, que transbordou o contexto europeu, contudo, por ser diretiva era apenas uma orientação para criação de leis nacionais.

O artigo 1º a Diretiva 95/36/CE estabelecia a "proteção das liberdades e direitos fundamentais das pessoas singulares e, em particular, o seu direito à privacidade que diz respeito ao tratamento de dados pessoais".

Em 2000, a Carta de Direitos fundamentais da União Europeia reconheceu o direito da proteção de dados como um direito autônomo, visto de forma apartada do direito à privacidade e com previsão em dois dispositivos diferentes, o artigo 7º dispõe sobre o respeito pela vida privada e familiar e, o artigo 8º, sobre a Proteção de dados pessoais.[20]

---

[19] Disponível em: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:pt:HTML. Acesso em 04 jan. 2023.

[20] Artigo 7º Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.
Artigo 8º 1. Todas as pessoas têm direito à proteção dos dados de caractere pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

Na Europa, a partir de discussões acerca da adoção de uma abordagem ampla e harmônica que contemplasse a proteção de dados como um direito autônomo, foi publicado o Regulamento Geral de Proteção de dados (GDPR) em 2016, impactando a nível global disposições sobre o tema e regulando de maneira contundente e com eficácia vinculante para os países membros da União Europeia.

Por meio do GDPR, apostou-se na instauração um sistema de corregulação, no qual os agentes possuem obrigações de documentação e registro dos processos e relatório de impacto; distanciando-se, no que foi possível, de uma abordagem de comando-controle, utilizada em caso de descumprimento das normas e violações a direitos fundamentais.

Feita essa breve análise das legislações, observa-se que no contexto europeu, privacidade e proteção de dados eram tratados conjuntamente e, somente após a maturação do tema, a proteção de dados passou a ser tratada como um direito autônomo.

De maneira diversa, nos EUA, a preocupação com a proteção de dados se deu mais acentuadamente nas relações entre particulares e os abusos advindos, especialmente, no contexto dos direitos dos consumidores. Além disso, nos EUA sua normatização se deu por meio de legislações estaduais esparsas. (PEIXOTO; ERHHARDT JÚNIOR, 2018, p. 42).

Não obstante, a partir das políticas governamentais adotadas pelos EUA em resposta aos atentados terroristas de 11 de setembro de 2001 e das revelações de Edward Snowden[21] em 2013, mostraram o quanto a sociedade pode ser monitorada e controlada com o emprego de tecnologia avançadas, uma verdadeira sociedade em permanente vigilância. Levando em conta esses fatos e das suas nefastas consequências, se tornou cada vez mais clara a necessidade de limitar os poderes dos agentes de tratamento (públicos e privados) frente aos possíveis abusos e violações a dignidade humana.[22]

No que diz respeito às diferenças entre o modelo regulatório dos EUA e da Europa, nota-se que seguiram por caminhos diversos. Enquanto os EUA seguiram

[21] Para esse tema, ver em SNOWDEN, Edward J. **Eterna vigilância**. Tradução Sandra Martha Dolinsky. São Paulo: Planeta do Brasil, 2019.

[22] Para melhor compreensão do *right to privacy* e sua característica como uma disciplina fragmentada, diferenciando-se dos rumos tomados na Europa, ver DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Op.cit., p. 223-256.

baseados fundamentalmente em três pilares: normas setoriais relativas à privacidade, uma abordagem consumerista e essencialmente baseada em princípios[23]; a Europa seguiu o caminho de um modelo baseado em leis gerais, com a influência de autoridades independentes para atuação na proteção dos dados pessoais.

Como visto, com o avanço da TIC, a potencialização quantitativa e qualitativa acerca do uso dos dados pessoais, tornou a proteção da privacidade insuficiente para proteger o livre desenvolvimento da personalidade, demonstrando a importância de regular juridicamente o tratamento de dados pessoais a partir da proteção de direitos fundamentais, como a liberdade, no âmbito do fluxo de informação.

Nesse sentido, a normatização da privacidade e da proteção de dados em termos globais, foram evoluindo na medida em que esses direitos se tornaram cada vez mais relevantes diante dos avanços tecnológicos.

Alguns autores[24] discorrem acerca das gerações de leis protetivas da privacidade e dos dados pessoais. Essa abordagem é interessante para verificar a evolução do entendimento acerca da privacidade e como a proteção de dados, se mostrou um direito novo e necessário perante os avanços da tecnologia e seus impactos sobre a sociedade. Para expressar essa análise, reporta-se nos parágrafos seguintes àquela realizada por Bruno Bioni.[25]

Segundo o referido autor, as legislações de primeira geração decorreram da constatação de que o processamento de dados pessoais massivo executado pelos Governos poderia se tornar nocivo aos cidadãos (BIONI, 2021). Naquele momento, a proteção pelo ordenamento jurídico teve como mote a regulação da própria tecnologia no sentido de impor limites rígidos ao poder derivado do seu uso.

As leis de segunda geração tiveram uma virada quando se verificou que o tratamento de dados passou a ser exercido também por entidades privadas, além dos Estados. Nesse momento, o consentimento se tornou a chave para a autorizar e legitimar o tratamento, mas não contemplava o que acontecia com os dados depois dele, permanecendo a insegurança jurídica relativa à proteção. Nesse processo de

[23] *Fair Information Practices Principles* (FIPP).
[24] Por exemplo Danilo Doneda. (DONEDA, 2021, p. 179-184).
[25] Bruno Bioni faz uma análise do estudo das gerações das leis no contexto do consentimento, originalmente elaborado por MAYER-SCÖNBERGER, Vikor. General development of data protection in Europe. Em AGRE, Philip; ROTENBERG, Marc (Org.). **Tecnology and privacy**: the new landscape. Cambrige: MIT Press, 1997 (BIONI, 2021, p. 113-117).

evolução, verificou-se que apenas o consentimento no momento da cessão dos dados era insuficiente para que o titular mantivesse o efetivo controle dos seus dados pois, há uma grande assimetria de poder entre o agente de tratamento e o titular, que muitas vezes cede seus dados pessoais em troca do serviço, ou facilidades, sem que tivesse a consciência dos possíveis impactos nefastos sobre seus direitos da personalidade.

Ainda segundo Bruno Bioni (2021), na terceira geração de leis deslocou-se o eixo da tecnologia para os dados, fazendo uma análise ampliada do conceito de dados pessoais e colocando o titular como protagonista da decisão de 'como' e 'o que fazer' com eles, enquanto perdurar o tratamento dos seus dados, conferindo ao titular a autodeterminação sobre seus dados. Essa foi uma significativa virada para que os direitos dos titulares fossem melhor protegidos, conferindo à proteção de dados uma autonomia com relação à tutela da privacidade.

As leis da quarta geração, por hora a última e na qual se encontra a LGPD, supriram algumas ineficiências das gerações anteriores, como quando relativiza o consentimento como fator central para legitimar o tratamento, ou quando considera que determinados dados, de natureza existencial (dados sensíveis) não podem ser livremente disponíveis pelos titulares. Adicionalmente, outro traço marcante nas leis de quarta geração, foi a criação de autoridades independentes para regular, orientar e controlar a aplicação das leis, bem como a incorporação de controles especiais dos dados, além do tradicional comando-controle (sancionatório).

Essa noção geracional das leis de proteção de dados pessoais conforma-se com o desenvolvimento de novas relações de poder frente ao uso e disseminação da tecnologia, e a forma com as quais os ordenamentos jurídicos tentam equilibrar os poderes entre as partes envolvidas, dando ao titular a proteção que lhe é devida.

3.2 Tutela da privacidade e a proteção de dados pessoais

Para melhor compreensão do atual estado da arte sobre a proteção e dados é necessário entender sobre desenvolvimento do conceito de privacidade e a estreita, mas distinta, relação entre os dois universos.

Privacidade trata-se de um conceito que se desenvolveu principalmente a partir do século XIX tendo evoluído até a concepção atual. Assim, percebe-se um

componente dinâmico em razão de como é percebida de maneira diversa em diferentes contextos sociais e culturas[26].

Nas culturas ocidentais, a necessidade de se afastar do convívio social e ter um ambiente recluso, era restrito à burguesia que tinha condições de ter propriedades nas quais era possível reservar-se em espaços privados para recolhimento, distantes da convivência social. Enquanto isso, nas classes menos privilegiadas, era comum moradias sem espaços privativos onde numerosas famílias conviviam e compartilhavam ambientes, onde a ideia de espaço privativo era quase inexistente (POSNER, 2010 *apud* PEIXOTO; EHRHADT JÚNIOR, 2018, p. 37).

Então, até século XIX a noção de privacidade era ligada à burguesia, sendo possível apenas para classes mais abastadas, porque até então, o entendimento sobre uma primitiva privacidade estava vinculada a um determinado espaço físico[27].

Nos Estados Unidos em 1890, Samuel D. Warren e Louis D. Brandeis escreveram prestigiado artigo sobre o tema (WARREN; BANDEIS, 1890). Nele, os autores se referem ao direito da privacidade como sendo o "direito de ser deixado só"[28]. Esse entendimento refletia à ideia de um direito autônomo do direito de liberdade pela relevância do seu conteúdo, uma vez que se trata do direito de controlar o acesso a sua esfera privada de intervenção de terceiros. Assim, de modo a agregar mais um componente à noção de privacidade: o aspecto psicológico da importância de estar só para que pudesse de forma livre, desenvolver a própria personalidade.

Deve ser levado em consideração que a privacidade para esses autores estava atrelada à época em que escreveram o estudo e, portanto, em meio ao início do uso de máquinas fotográficas e escândalos jornalísticos envolvendo artistas e pessoas influentes da alta sociedade. Consequentemente, eles se referem à privacidade sob aspectos relacionados à habitação (preservação), isolamento e tranquilidade e ao "[...] direito de escolher compartilhar ou não compartilhar com os outros as

[26] Estando ela (a privacidade) estreitamente ligada aos valores e projeções do homem em cada sociedade e, dentro de cada uma, aos diversos grupos sociais, essa tarefa reflete um forte conteúdo social e ideológico. (DONEDA, 2021, p. 129).

[27] Danilo Doneda, ao explicar sobre as raízes da privacidade, chama atenção quanto ao cuidado de relacionar privacidade com espaço físico, isso porque, em verdade, o que se pretende ao dar essa delimitação física, em verdade, é o raciocínio baseado na exclusão. (DONEDA, 2021, p. 111 e 122).

[28] A expressão '*right to be let alone*' foi cunhada pelo Juiz Cooley em *Cooley on Torts*, 2nd ed. p. 29 (WARREN; BANDEIS, 1890).

informações sobre sua vida privada, hábitos, atos e relações [...]*”* (PEIXOTO; EHRHARDT JÚNIOR, 2019, p. 37).

Com o passar do tempo e a partir do desenvolvimento de novas tecnologias, foram verificados outros impactos sobre a pessoa humana, notadamente sobre suas liberdades. Consequentemente, foi desenvolvida na Europa uma nova definição sobre privacidade que, segundo Stefano Rodotà (2008, p. 92), é “[...] o direito de manter o controle sobre suas informações [...]” e por meio desse controle, construir a própria esfera privada compreendida como “[...] aquele conjunto de ações, comportamentos, opiniões, preferências, informações pessoais, sobre as quais o interessado pretende manter um controle exclusivo [...]” (RODOTÀ, 2008, p. 92).

Esse pensamento decorre, da ampliação do que estaria contemplado na esfera privada da pessoa, assim, passa a ser considerado aquele conjunto de informações sobre uma pessoa e não apenas aquilo o que ela experencia na sua vida privada, mas também opiniões, seus interesses e tudo o mais que quer (e deve) manter sob seu controle.

Por esta razão, constata Stefano Rodotà (2008, p. 93) que a privacidade se desenvolveu dos aspectos primitivos relacionados a pessoa-informação-sigilo para agregar elementos de circulação e controle, pairando sobre a perspectiva pessoa-informação-circulação-controle.

De maneira geral, a privacidade vista sob esse ângulo, contempla elementos relacionados à proteção a vida privada e intimidade sob os quais deseja manter acesso restrito, mas também elementos como convicções, escolhas individuais e comportamentos que se vinculam à proteção das liberdades pessoais.

Caitlin Mulholland e Priscila Laterça explicam que a concepção tradicional de privacidade se relaciona com o direito de estar só e limitar o conhecimento de terceiros aquilo está no âmbito da vida privada. Contudo, na esteira da evolução da privacidade, tornou-se necessário visualizá-la como um elemento essencial para o exercício democrático de direito, a partir da expressão das liberdade de escolhas individuais (MULHOLLAND; LATERÇA, 2022, p. 142).

Do mesmo modo, Ana Frazão, apresentando uma espécie de linha evolutiva acerca do conceito da privacidade, reflete que a ideia inicial estava vinculada a privacidade e segredo, que em um segundo momento, foi ampliando para abarcar o controle da esfera privada e, atualmente, além dos aspectos anteriores, também

considera direitos e garantias fundamentais de liberdade, igualdade e democracia (FRAZÃO, 2020, p. 107).

Nessa perspectiva, conclui-se que a privacidade se relaciona com interesses de reserva e isolamento, mas também de construção da personalidade na medida em que deve ser assegurada a liberdade de escolha (DONEDA, 2021, p. 133).

Assim, a privacidade é uma proteção estática e negativa (RODOTÀ, 2008, p. 17), relacionada ao poder individual de controlar a esfera privada própria, delimitando interferências alheias e realizando livremente escolhas para garantir o desenvolvimento da personalidade.

No Brasil, a privacidade é tratada na Constituição Federal artigo 5º, X[29] relativo à vida privada e a intimidade, e no Código Civil artigo 21[30] ao referir à proteção da esfera privada conferida à pessoa contra interferência externa e proteção aos direitos da personalidade.

Incluem-se nesse conceito o direito a intimidade, vida privada, a honra e a imagem. Relativamente à intimidade e vida privada, Gilmar Mendes e Paulo Branco (2021, p. 18-19) ressaltam a linha tênue que diferencia tais conceitos sendo basicamente o primeiro, diz respeito a fatos, situações e acontecimentos que a pessoa deseja ver sob seu domínio exclusivo, sem compartilhar com qualquer outra pessoa e a vida privada, diz respeito ao ambiente familiar, gosto pessoal, preferências e outros aspectos que interessam exclusivamente o seu titular:

> A reclusão periódica à vida privada é uma necessidade de todo o homem, para a sua própria saúde mental. Além disso, sem privacidade, não há condições propícias para o desenvolvimento livre da personalidade. Estar submetido ao constante crivo da observação alheia dificulta o enfrentamento de novos desafios. A exposição diuturna dos nossos erros, dificuldade e fracassos à crítica e à curiosidade permanentes de terceiros, e ao ridículo público mesmo inibiria toda tentativa de autossuperação. Sem a tranquilidade emocional que se pode auferir da privacidade, não há muito menos como o indivíduo se autoavaliar, medir perspectivas e traças metas. (MENDES; BRANCO, 2021, p. 290).

[29] Art. 5º X, CF: São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano matéria ou moral decorrente de sua violação.
[30] Art. 21 Código Civil: A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

Quanto ao direto ao sigilo, os mesmos autores discorrem sobre discussão acerca da proteção constitucional ser voltada para a comunicação em si[31] e não relativa aos dados pessoais que são o conteúdo de correspondências e comunicações.

Independentemente de a discussão acerca do direito ao sigilo estar ou não na perspectiva da proteção à vida privada[32], é marcante é a constatação de que a proteção da inviolabilidade nesses casos, possui caráter negativo, de não interferência de terceiros que devem se abster de violar a privacidade alheia.

Note-se nesse contexto, que há uma lacuna quanto à proteção dos dados pessoais, que necessitam mais do que a mera abstenção, mas de uma tutela positiva que evite ou efetivamente previna a sua utilização abusiva.

Portanto, até chegar ao reconhecimento da proteção de dados como um direito autônomo no ordenamento jurídico, o caminho comumente adotado foi considerá-lo como um direito fundamental implícito, decorrente de outros direitos fundamentais, especialmente, do direito à privacidade (SARLET, 2021, p. 16). Mas vale ressaltar que essa concepção está superada.

Para conceber a proteção de dados como um direito autônomo, deve ser levado em consideração o aumento expressivo do fluxo de informação e, especialmente, as necessárias medidas propositivas protetivas à pessoa humana que garantam o adequado e seguro tratamento dos dados pessoais.

O núcleo das novas relações constituídas na sociedade da informação é o uso dos dados pessoais, que na acepção ampla adotada pela legislação brasileira, conceitua como sendo toda informação relativa a uma pessoa natural (artigo 5º, I da LGPD), identificada ou não, que não se limita apenas àquela que retrata características físicas, ou àquela como nome, endereço número de identificação ou telefônico, mas também àquela que possa reconhecer características da sua personalidade.

Ao transpor aspectos da pessoa física para o meio digital, permite-se a criação de um *avatar* da pessoa que corresponde não só aos seus aspectos físicos, mas

[31] Sobre esse tema ver julgado recorrentemente citado: STF, RE 418.416/SC, Rel. Min. Sepúlveda Pertence, 10/05/2006, publicado DJ 19/12/2006.

[32] Danilo Doneda discorre acerca das correntes de pensamento que tratam da inviolabilidade do sigilo da correspondência e das comunicações e a tendência, a partir da EC115/2022, de superar o entendimento dominante para que o conteúdo da comunicação, quando se tratar de dados pessoais, também esteja protegido. (DONEDA, 2021, p. 270-273).

também gostos, comportamentos, preferências, humor, rotinas e muito mais que, acumulados e tratados em bancos de dados, permitem traçar um perfil de identidade eletrônico desta pessoa.

A esse fenômeno, Stefano Rodotà chamou de corpo eletrônico:

> O "corpo eletrônico", o conjunto de informações que constroem a nossa identidade, é assim remetido ao corpo físico: a dignidade torna-se o liame forte para reconstruir a integridade da pessoa (Carta dos Direitos Fundamentais da União Europeia, art. 3º) , para evitar que a pessoa seja considerada uma espécie de "mina a céu aberto" onde qualquer pessoa possa alcançar qualquer informação e, assim, criar perfis individuais, familiares e grupais, tornando a pessoa objeto de poderes externos, que podem falsificá-la, construí-la em formas consistentes com as necessidades de uma sociedade de vigilância, de seleção social, de cálculo econômico. (RODOTÀ, 2017, p. 15).

De igual modo, Daniel Solove ressalta que a revolução digital é capaz de combinar diversos aspectos da pessoa, a partir de cruzamento de informações superficiais ou até mesmo incompletas, é possível criar uma *biografia digital* do indivíduo (SOLOVE, 2004, p. 44).

Portanto, a compreensão do que deve ser considerado dado pessoal precisa ser ampla, de modo que acomode todos os aspectos que venham a refletir na pessoa do seu titular, inclusive os frutos dos processamentos feitos por algoritmos[33].

A rigor, dado é o estágio anterior a informação (DONEDA, 2021, p. 140), pois é a partir do processo da sua análise e tratamento que se torna informação relevante da qual é possível construir um ativo lucrativo, num processo denominado mineração de dados (*data mining*).

A despeito da diferença terminológica entre dado e informação pessoal, importante evidenciar o cuidado do legislador em não relevar essa distinção, pois foi adotada a acepção ampla dados pessoais, portanto, sob a ótica jurídica, ambas terminologias servem para projetar um fato relacionado a personalidade do titular.

Os dados são a matéria-prima que será extraída e lapidada de maneira que gere conhecimento sobre algo, ou melhor, sobre alguém.[34] Nesse cenário, que já se demonstrou muito lucrativo[35], as organizações buscam se adaptar ao momento

[33] Metainformação, conforme Danilo Doneda (DONEDA, 2021, p. 155).
[34] Shoshana descreve que "Dados são a matéria-prima necessária para os novos processos de manufatura do capitalismo de vigilância." (ZUBOFF, 2020, p. 82).
[35] Reportagem do Valor Econômico disponível em: https://valorinveste.globo.com/mercados/renda-variavel/empresas/noticia/2022/06/15/veja-o-ranking-das-empresas-mais-valiosas-do-mundo-e-saiba-quem-e-a-unica-latino-americana.ghtml. Acesso em 29 jan. 2023.

mercadológico, no qual coletar e tratar a maior quantidade possível de dados pessoais e transformá-los em ativo.

Nesse contexto, na medida em que as informações acerca das pessoas são transformadas em mercadoria, a concepção sobre os dados pessoais deve ser ressignificada de modo a serem encarados como uma extensão ou projeção da própria personalidade, e, como tal, protegida sob o manto da dignidade humana, base fundamental de um Estado democrático.

No seu conceito, o direito de proteção aos dados pessoais tem como premissa a concepção ampla do que venha a ser dados pessoais. Isto é, tudo aquilo que se relaciona à pessoa[36] e que possa retratar características da sua personalidade. Por isso, refere-se ao corpo eletrônico.

Nesse contexto, vale ressaltar que não há dados pessoas irrelevantes frente ao fluxo de dados (SARLET, 2021, p. 22), pois tamanha é a capacidade de processamento que, mesmo um dado simples, como sexo, tem potencial para violação à direitos fundamentais.

Assim, o direito de proteção de dados pessoais muda a perspectiva do direito de uma liberdade negativa, vinculada a privacidade, para um direito autônomo que exprime uma liberdade positiva, vinculada a uma projeção da personalidade que necessita de uma efetiva tutela, e não apenas a inviolabilidade.

Esse é o ponto-chave para melhor compreender a relação entre esses dois institutos. A TIC e a sociedade de vigilância baseada na utilização de dados pessoais como matéria-prima para a obtenção de vantagens indevidas, levaram à necessidade de criar um direito autônomo, mais abrangente que a privacidade, para contemplar o direito do titular de controlar seus dados e com isso, ampliar a proteção da liberdade.

A proteção dos dados pessoais assume papel marcante em meio ao desenvolvimento da tutela da pessoa natural na medida em que aspectos relacionados às informações pessoais correspondem a toda e qualquer projeção da personalidade, seja relacionada a esfera privada, seja relacionada a esfera pública.

36 Nesse sentido, a LGPD define no artigo 5º, I, dado pessoal como a informação relacionada a pessoa natural identificada ou identificável.

Vista sob esse ângulo, a proteção de dados assume características próprias e considera imprescindível que, para que o dado seja merecedor da tutela, deve estar ligado, necessariamente, a uma projeção da personalidade do seu titular.

Segundo Danilo Doneda, a proteção de dados "[...] manteve o nexo de continuidade com a disciplina da privacidade, da qual é uma espécie de herdeira, atualizando-a e impondo características próprias." (DONEDA, 2021, p. 177).

Assim, enquanto o direito à privacidade preserva a vida privada, intimidade, sigilo, honra da pessoa natural e o controle ao acesso ou interferência à essa esfera privada; a proteção de dados se concentra em tutelar as informações pessoais submetidas a tratamento, independentemente de serem consideradas as esferas privada ou pública.

Vale ressaltar que Bruno Bioni chama atenção quando à falha construção dogmática que coloca a proteção de dados como uma extensão da privacidade. Neste sentido, a privacidade é uma liberdade negativa e estática, no sentido de não interferência de terceiros na esfera privada, por conseguinte, a mera abstenção de violação da privacidade não abarca suficientemente a proteção dos dados pessoais. Isto porque, a proteção de dados tem um espectro mais amplo que a privacidade, pois "rompe com a dicotomia público-privado" e assume dupla função de direito negativo e direito positivo (BIONI, 2021, p. 90-95).

Para o referido autor, o cerne da normatização do conteúdo da privacidade está relacionado ao que é considerado público e privado, sendo a sua lógica centrada na liberdade negativa de o indivíduo não sofrer interferência alheia. Já a proteção de dados é uma liberdade positiva, merecendo ampla proteção desde que o dado seja relacionado à pessoa natural.

Feita essa diferenciação para constatar a já superada diferença entre tutela da privacidade e proteção de dados, este estudo avança para a visão sobre proteção de dados no ordenamento jurídico brasileiro.

3.3 Proteção de dados no Brasil

Até a promulgação de uma lei específica para tratar do tema, a proteção de dados no Brasil já era prevista de maneira tangenciada na Constituição Federal, estritamente quanto aos aspectos relacionados à privacidade como visto na seção

anterior. Além disso, também pode-se depreender a proteção de dados na disposição sobre *habeas data* e em disposições infraconstitucionais.

A Constituição Federal ao prever o *habeas data* no artigo 5º, LXXII, estabelece uma salvaguarda parcial acerca da proteção dos dados pessoais, pois nesta disposição, a garantia constitucional da pessoa sobre o conhecimento (acesso) e retificação de informações limita-se àqueles constantes em banco de dados públicos (SARLET, 2021, p. 17).

Além disso, a proteção de dados também foi prevista de maneira esparsa em legislações infraconstitucionais como no artigo 43 do Código de Defesa do Consumidor (CDC)[37], ao dispor sobre banco de dados e cadastros de consumidores estabelece o direito destes o acesso às informações, inclusive dados pessoais.

Como forma de suprir a assimetria naturalmente decorrente da relação de consumo, o CDC estabeleceu o princípio da transparência como sendo um dos fundamentos para a Política Nacional de Relações de Consumo que, conjugado ao direito à informação previsto como um direito do consumidor no artigo 6º, III, atuam no sentido de proteger a vulnerabilidade do consumidor nesta relação.

Assim, o CDC estabeleceu uma visão embrionária de alguns princípios indispensáveis ao tratamento de dados pessoais como a transparência, a qualidade e a limitação temporal para o armazenamento das informações, conferindo ao consumidor uma principiante autodeterminação informativa.

A Lei do Cadastro Positivo, Lei nº12.414/2011 inaugurou a disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. À semelhança do CDC, essa lei criou bases para a formação e controle dos bancos de dados, conferindo ao titular a autodeterminação informativa a partir das noções de *opt-in/opt-out* de base de dados.

Também há o Marco Civil da Internet, Lei nº 12.965/2014, que estabelece a proteção dos dados pessoais como um dos princípios do uso da internet no Brasil[38].

Válido de notar que enquanto se discutia o projeto de lei do Marco Civil da Internet, revelações de Edward Swnoden incluíam fatos relacionados à espionagem

[37] Artigo 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

[38] No artigo 3º, III do Marco Civil da Internet tem como princípio a proteção de dados pessoais, na forma da lei, remetendo para a necessidade de uma legislação específica sobre o tema.

realizada pelos EUA em comunicações da ex-presidente Dilma Rousseff e mostraram ao mundo as implicações e potencialidades das tecnologias de informação e comunicação, refletindo tempos depois também na necessidade de maior proteção aos dados pessoais.

A pulverização de leis esparsas sobre o tema, causava insegurança jurídica e não protegia suficientemente todos os aspectos necessários para uma efetiva proteção de dados diante da complexidade da sociedade sob vigilância. Assim, uma das funções da LGPD também está em unificar a aplicação e o entendimento acerca da proteção dos dados pessoais.[39]

Em maio de 2020, enquanto perdurava a *vacatio legis* da LGPD, o STF proferiu notável decisão em sede de Ação Direta de Inconstitucionalidade[40] acerca do direito à proteção de dados pessoais reconhecendo o seu caráter autônomo e fundamental.

O julgamento analisava a inconstitucionalidade da Medida Provisória nº 954 editada durante a pandemia de COVID-19, que determinava que as empresas de telecomunicação disponibilizassem ao Instituto Brasileiro de Geografia e Estatística (IBGE), em meio eletrônico, dados pessoais dos seus consumidores com a finalidade de construir uma produção estatística oficial (MENDES; RODRIGUES JÚNIOR; FONSECA, 2021).

Em seu voto, a Ministra Relatora Rosa Weber reconhece o direito à proteção de dados a partir da ampliação dos direitos à privacidade, à liberdade e ao livre desenvolvimento da personalidade:

> A Constituição da República confere especial proteção a intimidade, à vida privada, à honra e à imagem das pessoas ao qualificá-las como invioláveis, enquanto direitos fundamentais da personalidade, assegurando indenização pelo dano material ou moral decorrente da sua violação (art. 5º, X). O assim chamado direito à privacidade (*right to privacy*) e os seus consectários direitos à

[39] Com relação a isso, Danilo Doneda e Laura Schertel em reflexões iniciais sobre a LGPD, identificaram como um dos desafios a serem enfrentados pela nova lei, a interpretação sistemática com as diversas leis que tratam do tema da proteção de dados, considerando o aparente conflito. De modo geral, em aparente conflito de lei no tempo, a solução tradicional é pela especialidade. Assim, notadamente quanto ao CDC e Marco Civil da Internet, esses autores entendem que a justaposição de disposições deverá encontrar solução simultânea, coerente e coordenada a partir do diálogo das fontes, conforme anteriormente referenciado por Claudia Lima Marques. (MENDES e DONEDA, 2018, p. 479). De igual modo, Bruno Bioni discorre acerca do papel da LPGD em coordenação com o restante do ordenamento jurídico brasileiros, propondo um diálogo da fontes visando uma intersecção e complementação das normas. (BIONI, 2021, p. 269).

[40] STF, ADI 6387, Relatora Ministra Rosa Weber. Data de publicação DJe. 12/11/2020.

> intimidade, à honra e à imagem emanam do reconhecimento de que a personalidade individual merece ser protegida em todas as suas manifestações.
> [..]
> Tais informações, relacionadas à identificação – efetiva ou potencial – de pessoa natural, configuram dados pessoas 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 XI). Sua manipulação e tratamento, desse modo, hão de observar, sob pena de lesão a esses direitos, os limites delineados pela proteção constitucional.

Nesse momento, confirmou o entendimento de que as informações vinculadas à pessoa merecem a tutela jurídica pois possuem um espectro mais amplo do que somente aquelas revestidas de sigilo, relacionadas a esfera privada, bastando que o dado fosse relativo à pessoa, que já mereceria a salvaguarda constitucional.

A despeito do consenso originado no Brasil acerca do direto fundamental implícito à proteção de dados pessoais, o tema tomou forma principalmente a partir da promulgação da Emenda Constitucional 115/2022 (EC 115/2022).[41] A proteção de dados pessoais que, até então, era implicitamente positivado através da tutela da privacidade e outros direitos constitucionais, passou a ser um direito fundamental previsto expressamente na Constituição Federal brasileira.

Com isso, o Brasil estabelece que privacidade e proteção de dados são direitos constitucionais distintos e autônomos, possuindo centros gravitacionais diferentes, o primeiro para proteger a esfera privada da pessoa a partir do controle de acesso e interferências e, a segunda, abrange a tutela jurídica dado pessoal como projeção da personalidade do seu titular.

O impacto da EC 115/2022, originada da PEC 17/2019, está em reconhecer como direito fundamental, a proteção dos dados numa sociedade digital demandando o comando constitucional à proteção do livre desenvolvimento da personalidade, da cidadania e às liberdades dos brasileiros; bem como dando a competência constitucional para tratar sobre o tema, demonstrando com isso, a diretriz única, centralizada em nível federal, ideal na proteção do tratamento de dados pessoais, assim como nos demais direitos fundamentais.

[41] Promulgada em 10 de fevereiro de 2022, a Emenda Constitucional 115 incluiu o inciso LXXIX ao artigo 5º dos direitos fundamentais "é assegurado, os termos da lei, o direito a proteção dos dados pessoais, inclusive nos meios digitais"; incluiu o inciso XXVI ao artigo 21 para estabelecer a competência da União organizar e fiscalizar, nos termos da lei, a proteção e o tratamento de dados pessoais; e incluiu no artigo 22 o inciso XXX como competência privativa da União a proteção e o tratamento dos dados pessoais.

Atribuir ao tema status constitucional, confere-se a importância atinente ao pilar ético-jurídico de maior relevância no nosso ordenamento jurídico, conforme asseveram Gilmar Mendes e Paulo Gonet Branco (2021, p. 140):

> [...] os direitos fundamentais assumem posição de definitivo realce na sociedade quando se inverte a tradicional relação entre Estado e indivíduo e se reconhece que o indivíduo tem, primeiro, direitos, e, depois, deveres perante o Estado, e que os direitos que o Estado tem em relação ao indivíduo se ordenam ao objetivo de melhor cuidar das necessidades dos cidadãos.

Por fim, cumpre transcrever a análise realizada pela Associação Data Privacy Brasil de Pesquisa ao descrever os impactos da inclusão da proteção de dados no rol dos direitos fundamentais:

> Portanto, a promulgação da mencionada emenda é um marco de grande importância para os mais diversos setores e principalmente para o processo gradual e constante da consolidação da cultura de proteção de dados pessoais no Brasil, que agora adquire status de direito fundamental autônomo e, consequentemente, de cláusula pétrea, possibilitando o exercício da cidadania dentro de uma sociedade datificada.
> O reconhecimento explícito da proteção de dados pessoais na Constituição Cidadã ajudará a diferenciar esse direito do direito à privacidade, ampliará a compreensão de sua relação umbilical com a cidadania e permitirá uma ampliação da gramática de direitos fundamentais em políticas públicas intensivas em dados e nas relações privadas. Trata-se de mudança profunda em dimensão política que pode redefinir a discussão sobre cidadania no século XXI.[42]

Diante disso, a Emenda Constitucional, além de reforçar a proteção de dados prevista em leis infraconstitucionais esparsas já referenciadas, deu maior ênfase à Lei Geral de Proteção de Dados Pessoais de 2018, ao conferir status constitucional com aplicabilidade imediata[43] e vinculante à proteção de dados pessoais.

3.4 LGPD como o marco regulatório

No Brasil, a criação de uma lei para a proteção dos dados pessoais acompanhou o ritmo mundial, em especial seguindo a linha adotada na Europa, e

[42] Disponível em: https://www.observatorioprivacidade.com.br/2022/02/10/a-constitucionalizacao-da-protecao-de-dados-pessoais-no-brasil-e-a-trajetoria-ate-a-promulgacao-da-pec-17-2019/. Acesso em 31 jan. 2023.
[43] Constituição Federal artigo 5º § 1º As normas definidoras dos direitos e garantias fundamentais têm aplicação imediata.

veio dar segurança ao titular dos dados pessoais, criando uma cultura de proteção e valorização da pessoa natural.

A LGPD entrou em vigor no dia 18 de setembro de 2018[44] dispondo no artigo 1º, o objetivo de proteger os direitos fundamentais de liberdades, de privacidade e o livre desenvolvimento da personalidade da pessoa natural mediante o estabelecimento de regras bem definidas para o tratamento dos dados pessoais, a fim de limitá-lo para mitigar os riscos inerentes dessa atividade.

A LGDP possui o aspecto de aplicação geral[45] e foi promulgada para complementar e traçar diretrizes transversais até então inexistentes, unificando a aplicação das demais legislações infraconstitucionais que já tratavam da proteção de dados pessoais, criando um sistema regulatório unitário sobre a matéria (BIONI, 2022, p. 62).

Durante o seu processo de elaboração que perdurou cerca de dez anos, a LGPD apresentou soluções para proteção ao corpo eletrônico e amparou o desenvolvimento tecnológico no contexto da sociedade de vigilância.

A Associação Data Privacy Brasil de Pesquisa em 'Memória da LGPD'[46] apresenta interessante cronologia sobre os debates sociais relativos à proteção de dados do Brasil, fazendo referência desde 1970 até a promulgação da LGPD.

O Projeto de Lei da Câmara nº 4.060/2012[47] de iniciativa de Milton Monti (PL/SP) que recebeu o número de 53/2018 ao ser recebido pelo Senado, teve diversos desdobramentos até chegar ao texto legal em vigor.[48]

Foi um Projeto de Lei que teve o envolvimento e diversos representantes e interesses, sendo uma das características o multissetorialismo das partes envolvidas (BIONI; RIELLI, 2022, p. 16). Em linhas gerais, a forma multissetorial de

[44] Relativamente às sanções administrativas aplicadas pela Autoridade Nacional de Proteção de dados entrou em vigor em 1º de agosto de 2021 com a Lei nº 13.853/2019.

[45] A aplicação geral consiste na abrangência e transversalidade da lei, aplicada aos setores público e privado, sem distinguir a operação pelo qual o tratamento é realizado, bem como, o ambiente (se digital ou físico), conforme artigo 3º da LGPD.

[46] Associação Data Privacy Brasil de Pesquisa. Observatório da Privacidade – Memória LGPD. Disponível em: https://www.observatorioprivacidade.com.br/memorias/. Acesso em 31 jan. 2023.

[47] Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066. Acesso em 16 mar. 2023.

[48] Outros projetos de lei recebidos no Congresso para a proteção de dados pessoais o PL 330/2013 (Senador Antonio Carlos Valadares PSB/SE) e o PL5.276/2016 de iniciativa do Ministério da Justiça (BIONI; RIELLI, 2022, p. 20-21).

construção da LGPD demonstra a necessidade de imposição de uma lei geral estabelecendo uma nova dogmática com estratégia ampla para compatibilizar diversos interesses, com uma única e principal finalidade: a efetiva proteção dos dados pessoais do fluxo de dados.

Por isso, é uma lei que se utiliza da técnica legislativa da cláusula geral que está associada à utilização de palavras ou expressões com conteúdo jurídico indeterminado que estabelecem um mínimo tangível para permitir que sejam aplicados concretamente pelo juiz, de acordo com os valores constitucionais estabelecidos no ordenamento jurídico.[49]

O uso das cláusulas gerais oferece ao intérprete da lei uma fórmula abstrata, porém direcionada pelos valores fundamentais, de um conteúdo fixo garantido de proteção e oferecendo flexibilidade na adequação do princípio ao caso concreto.[50]

Uma marcante característica da LGPD no ordenamento jurídico brasileiro foi a instituição de um modelo *ex ante* de proteção de dados. Em termos gerais, a lei brasileira seguiu a tendência traçada pelo GDPR[51], fruto de uma evolução histórica legislativa europeia, da qual se extrai uma regulação preventiva guiada pelo cumprimento dos deveres pelos agentes para que se ajustem ao caso concreto, promovendo o estabelecimento de regras mais eficientes e alinhadas com os objetivos da lei.

Sendo assim, a LGPD, cria um ambiente saudável e de confiança para a proteção de dados, pois viabiliza a adequação dos agentes às regras nitidamente voltadas para a segurança e prevenção dos titulares, sem dispensar a importância da regulação e fiscalização pela ANPD.

[49] "Ao lado da técnica de legislar com normas regulamentares (ou seja, através de previsões específicas e circunstâncias), coloca-se a técnica das cláusulas gerais. Legislar por cláusulas gerais significa deixar ao juiz, ao intérprete, uma maior possibilidade de adaptar a norma às situações de fato." (PERLINGIERI, 2002, p. 27).

[50] Gustavo Tepedino no seu paradigmático artigo assim descreve sobre as cláusulas gerais "As constituições contemporâneas e o legislador especial utilizam-se de cláusulas gerais convencidos que estão da sua própria incapacidade, em face da velocidade com que evolui o mundo tecnológico, para regular todas as inúmeras e multifacetadas situações nas quais o sujeito de direito se insere. Cláusulas gerais equivalem a normas jurídicas aplicáveis direta e imediatamente nos casos concretos, não sendo apenas cláusulas de intenção [...]" (TEPEDINO, 2004, p. 19).

[51] Ao analisar as racionalidades regulatórias convergente entre GDPR e LGPD, Bruno Bioni e Laura Schertel concluíram que: "Na análise comparativa ora realizada, sobressai a convergência entre três aspectos importantes, quais sejam, nos princípios enunciados por ambas as regulamentações, no modelo *ex ante* de proteção, bem como no papel central da *accountability* em ambos os modelos regulatórios. No que diz respeito ao *enforcement*, foi positivado pela Medida Provisória 869, posteriormente convertida na Lei 13.853/2019" (BIONI; MENDES, 2020, p. 799).

Se por um lado, o desenvolvimento tecnológico trouxe inúmeras inovações e benefícios para a sociedade moderna, por outro, criou riscos cada vez mais graves, que precisam ser gerenciados para que, de forma preventiva, sejam adotadas medidas que evitem a ocorrência de danos aos titulares de dados pessoais

Portanto, em um contexto no qual abusividades recorrentes já foram experimentadas pela sociedade, tornou-se imprescindível no debate regulatório sobre proteção de dados, levar em consideração o estabelecimento de regras que assegurassem o controle preventivo e mitigador dos riscos inerentes ao tratamento de dados, tendo em vista o claro objetivo da lei em proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade (FRAZÃO, 2020, p. 111).

Na medida que o agente exerce atividades de tratamento de dados, deve atuar de acordo com os riscos que decorrem dessa prática, se adaptando aos critérios e autorizações estabelecidos pela lei. Portanto, o agente deve observar que toda a regulação se baseia em dois fatores, o primeiro que o conceito ampliado de dado pessoal, que considera qualquer dado vinculado ou atribuível ao titular, uma extensão da própria pessoa; e o segundo, para a realização do tratamento de dado pessoal, o agente deve, necessariamente, se fundamentar uma das bases legais autorizativas para tanto, conforme artigo 7º e artigo 11, que trata das bases legais para tratamento de dados sensíveis.

Observa-se que a lei dispõe conceitos e limites para que o agente identifique o enquadramento na base legal autorizativa, levando em consideração a natureza do dado (pessoal, sensível, anonimizado ou pseudoanonimizado), devendo, assim, estabelecer as medidas de segurança preventivas para que o objetivo maior, a proteção dos dados pessoais, seja atingido.

De acordo com Danilo Doneda e Laura Schertel (2018), a lei possui 5 eixos principais nos quais se articula: i) unidade e generalidade da aplicação; ii) legitimação para o tratamento de dados (hipóteses autorizativas), conforme artigo 7º e 11º; iii) princípios e direitos do titular, especialmente no artigo 6º e os dispositivos do Capítulo III; iv) obrigações dos agentes de tratamento, dentre outras, aquelas previstas nos artigos 27 a 41 e artigo 46; e por último v) a responsabilização dos agentes, artigos 42 a 45 (MENDES; DONEDA, 2018, p. 471-477).

Essa reflexão leva a uma aplicação da LGPD em níveis[52], que orienta o agente na delimitação da atividade às hipóteses autorizativas para o tratamento. Assim, para se adequar à lei, o agente deve primeiro analisar suas próprias condições de tratamento, tomando como referência quais dados pessoais irá tratar de acordo com a necessidade e finalidade do seu modelo de negócio.

Feito isso, o agente deve se certificar quanto à observância dos limites impostos pelos princípios e garantir o atendimento aos direitos do titular. Passadas todas essas etapas, o agente, por fim, consolida uma estrutura de conformidade consistente, que irá manter esse sistema de análise em níveis permanente, atualizado especialmente de acordo com as orientações da ANPD e devidamente registrado.

Dessa forma, a lei permite que o agente opte entre os níveis de risco da sua atividade, mediante a análise das condições do tratamento de dados que realiza no seu modelo de negócio e, com base nisso, ajuste seus processos internos para atender às obrigações legais, levando em consideração quais medidas serão adotadas proteger os dados sob tratamento.

A vantagem desse modelo é fazer uma calibragem entre a necessária segurança jurídica do titular e, ao mesmo tempo, viabilizar a circulação de dados pessoais, adotando regras fluídas que irão se adaptar aos negócios de acordo com a necessidade e riscos do caso concreto (CABRAL, 2019, p. 44).

Diante do exposto, a lei dá um voto de confiança ao agente, na medida que limita as hipóteses autorizativas para o tratamento dos dados pessoais, ficando a cargo do agente demonstrar o cumprimento de tais medidas, como será visto na próxima seção deste estudo.

3.5 Fundamentos e princípios

A LGPD foi elaborada a fim de criar um ambiente regulado para proteção aos dados pessoais, estabelecendo princípios, direitos e deveres para o seu tratamento, aplicáveis a pessoas físicas ou jurídicas que realizam qualquer tipo de operacionalização desses dados, ou seja, que colete, produza, recepcione,

[52] Com a mesma lógica dos eixos, Ana Frazão propõe a aplicação da lei em 5 níveis: i) identificação da espécie de dado; ii) existência de base legal, iii) observância de princípios; iv) direitos do titular; v) programas e procedimentos de conformidade (FRAZÃO; CARVALHO; MILANEZ, 2022, p. 119-120).

classifique, utilize, acesse, reproduza, transmita, distribua, processe, arquive, armazene, elimine, avalie ou controle a informação, modifique, comunique, transfira, difunda ou extraia dados pessoais.[53]

Os princípios estabelecidos pela LGPD encontram seus fundamentos[54] no artigo 2º, e são regidos pelos valores constitucionais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Consoante dispõe o artigo 2º, inciso I, a privacidade é, propositalmente[55], o primeiro fundamento. Não há dúvidas que a privacidade está intrinsecamente relacionada à proteção de dados pessoais tendo em vista que, por meio dos dados pessoais, são extraídas informações que espelham a necessidade de proteção da inviolabilidade da esfera privada.

No contexto digital, toda e qualquer informação necessita de proteção, especialmente, aquelas relativas à vida privada e intimidade, como saúde, religião ou orientação sexual, de modo geral classificadas como dados sensíveis[56] pois, usualmente, tais informações no âmbito do tratamento de dados podem ocasionar graves infrações à igualdade.

Como visto anteriormente, a privacidade consiste no direito de controlar as informações sobre a própria vida, imagem e intimidade, e do mesmo modo, garantir o livre desenvolvimento da personalidade.

O segundo fundamento da LGPD é a autodeterminação informativa, que está associado ao direito de controlar o uso dos dados pessoais pelo próprio indivíduo, e por isso, está intimamente ligado a tutela da personalidade como direito fundamental de liberdade.

---

[53] O art. 5º, X da LGPD conceitua o tratamento de dados pessoais como sendo toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

[54] Danilo Doneda e Laura Schertel denominam os fundamentos de 'princípios fundamentais' para aqueles que estabelecem as principais balizas e que guiam os princípios contidos no artigo 6, que contém uma carga substancial mais forte (MENDES; DONEDA, 2018, p. 474).

[55] "Em que pese a inexatidão jurídica do termo 'respeito', o estudo da privacidade é essencial para a proteção de dados pessoais, uma vez que estão intimamente relacionados." (SOUZA; MAGRANI; CARNEIRO, 2020, p. 47).

[56] A LGPD no art. 5º, II conceitua dados sensíveis como sendo dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Acerca do desenvolvimento do conceito da autodeterminação informativa, tem-se a decisão paradigmática recorrentemente referenciada do Tribunal Constitucional alemão[57] que serviu como inspiração para a legislação europeia e brasileira. Laura Schertel Mendes realizou estudo aprofundado deste julgamento no qual analisou o caminho percorrido até o reconhecimento desse direto, partindo da evolução jurisprudencial que sedimentou a amplitude do direito de livre desenvolvimento da personalidade baseado no tripé: i) proteção abrangente, portanto, um direito geral; ii) autodeterminação, que corresponde ao "direito da pessoa em decidir por ela mesma como deseja se apresentar em público" e, iii) a abstração, como uma forma adequada de responder aos riscos ainda desconhecidos decorrente de uma sociedade moderna em constante mutação (MENDES, 2020, p. 1-18).

A partir desse tripé fundador, consolidou-se na Alemanha importante decisão do Tribunal Constitucional proferida em 1983, que serviu como parâmetro para diversas legislações no que diz respeito da autodeterminação informativa, inclusive para a brasileira. Nesse julgamento, o Tribunal reconheceu o direito a autodeterminação informativa diante da análise da constitucionalidade da lei sobre recenseamento. A decisão baseou-se fundamentalmente no direito à proteção dos dados, considerando que a proteção à privacidade já tinha sido ultrapassada em jurisprudências anteriores. Assim, reconheceu que autodeterminação informativa do titular dos dados pessoais seria uma parte do direito de livremente desenvolver a personalidade (BIONI, 2021, p. 99).

De tal modo, o direito a autodeterminação informativa é o critério para "[...] decidir quais informações individuais ele (o titular) fornece *a quem* e sob *quais* circunstâncias [...]" (MENDES, 2020, p. 10).

Outro fator marcante desse julgamento alemão foi a construção de que o direito à autodeterminação informativa impõe ao agente, a obrigação de realizar o tratamento de dados pessoais de forma transparente e vinculada a propósitos específicos (BIONI, 2021, p. 101).

[57] A sentença proferida em 1983 pelo Tribunal Constitucional Federal Alemão consolidou o termo autodeterminação informativa como sendo o direito de uma pessoa de decidir por si mesmo acerca da divulgação e uso dos seus dados (BVerfGE 65, 1). Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html. Acesso em 26 jan. 2023.

Esse pensamento influenciou significativamente a legislação brasileira no que diz respeito a autodeterminação informativa como um direito autônomo. A LGPD estabelece a autodeterminação informativa como o direito de controlar sobre suas próprias informações (DONEDA, 2021, p. 173), e com isso decidir sobre as informações pessoais que podem ser utilizadas e quais devem ser omitidas ou desconsideradas no tratamento dos dados pessoais.

Importante ressaltar que esse direito, garante a proteção de dados pessoais para além do mero consentimento no momento da coleta, pois também considera o controle sobre os dados durante o seu tratamento.

Quanto a isso, Bruno Bioni chama atenção sobre a interpretação de que a autodeterminação informativa estaria vinculada apenas ao momento do consentimento seria um equívoco, pois, do contrário, estaria servindo às avessas e desprotegendo o titular uma vez consentido o uso dos dados, objeto de exploração ilimitada (DONEDA, 2021, p. 101-102).

A autodeterminação informativa funciona como fator de equilíbrio entre as forças de poder entre titulares e agentes, possuindo dupla função de i) garantir que o fornecimento dos dados pessoais seja consentido e livre de pressões decorrentes da falta de paridade entre o titular e o agente de tratamento e, ii) funciona como limitador ao agente para que este somente trate os dados estritamente necessários para as finalidades específicas.

De tal modo, relaciona-se o direito a autodeterminação informativa com o princípio da autonomia do titular sobre seus dados, no sentido subjetivo de decisão individual deste acerca da coleta, uso, compartilhamento e descarte dos seus dados; mas por outro lado, vincula-se à noção de livre desenvolvimento da personalidade, conferindo-se um caráter "[...] metaindividual ou coletivo como uma pré-condição para uma ordem comunicacional livre e democrática [...]" (SARLET, 2021, p. 24).

Sobre a nova definição de poderes, Stefano Rodotà chama atenção acerca da possiblidade de o controle exercido pelo cidadão sobre seus dados está além do viés de assegurar a sua exatidão, podendo se tornar uma forma de equilibrar os novos poderes que vem se delineando na era digital (RODOTÀ, 2008, p. 37).

Um fator influente para o entendimento da autodeterminação informativa é a compreensão do conceito de dados pessoais que deve ser considerado na sua acepção ampla, superando a noção das esferas público e privado. Isso porque, não

é suficiente para proteger direitos da personalidade, a análise dos dados pessoais restritos à esfera íntima ou privada, pois há aspectos que não estão contemplados nessa limitante classificação. Por isso, mais adequado observar que a autodeterminação informativa tem por objeto proteger todos os dados pessoais e informações vinculados à pessoa, independentemente de *quais* sejam e *qual* âmbito estão inseridos (privado ou público).

Da mesma forma, pouco vale a natureza ou a relevância dos dados, pois em um ambiente tecnológico, a análise de qualquer dado é relevante e tem potencial para traçar perfis indesejados pelo titular, em razão do poder de perfilamento e dos riscos dele decorrentes, qualquer dado importa, por mais simplório que seja.

A partir do controle das próprias informações e da forma como são tratados os dados pessoais, as pessoas são livres para exercer suas escolhas e, efetivamente, autogovernar-se, como forma de extensão da própria autonomia privada.

Em 2015 o STF ao julgar um *habeas data* de um cidadão que desejava ter acesso às informações constantes nos sistemas automatizados de controles de pagamentos de tributos da Secretaria da Receita Federal, deu provimento ao recurso reconhecendo o direito subjetivo do contribuinte com base na autodeterminação informativa. Assim, em seu voto, o Ministro Gilmar Mendes discorreu:

> Então, a mim, parece-me, digna de nota, desde logo, é exatamente a ideia de que, no plano processual, nós temos o *habeas data* com o propósito, o intento de tutelar aquilo que entendemos ser uma proteção da autonomia privada nesse âmbito da autodeterminação sobre os dados, que ganha cada vez mais importância, na medida em que temos toda essa ampla evolução tecnológica. (BRASIL, 2015, p. 1) [58]

Para dar efetividade a esse fundamento, a LGPD dispõe, nos artigos 18 e 20, sobre os direitos do titular dentre eles, o acesso às informações acerca do tratamento dos dados para corrigir, atualizar, eliminar, realizar sua portabilidade, solicitar revisão de decisões automatizadas, dentre outros. Assim, para torná-los efetivos, os agentes têm obrigações legais de manter mecanismos eficazes para garantir a autodeterminação informativa do titular, adotando estruturas organizacionais organizadas para prevenir riscos aos direitos do titular decorrentes das atividades de tratamento.

Segundo Ana Frazão, é fundamental entender que a LGPD

[58] STF RE 673.707, Relator Ministro Luiz FUX, Tribunal Pleno, julgado em 17/06/2015.

> [...] evidencia o seu importante papel de reforçar a autonomia informativa dos titulares dos dados e o necessário e devido controle que estes precisam exercer sobre seus dados, a fim de se colocar um freio nas vicissitudes que possibilitaram a consolidação do estágio atual da economia movida a dados [...]. (FRAZÃO; CARVALHO; MILANEZ, 2022, p. 13).

O terceiro fundamento da lei é a liberdade de expressão, de informação de comunicação e de opinião. No contexto da sociedade de vigilância, a liberdade de expressão tomou novos contornos porque a tecnologia permite uma escalada quantitativa e qualitativa marcada pela onipresença da digitalização de informações. A velocidade e a abrangência com a qual a informação hoje chega às pessoas é imensa e personalizada.

A liberdade de expressão está prevista na Constituição Federal no artigo 5º, IV e XIV, para assegurar a livre manifestação de pensamento e o direito ao acesso à informação. Também está contemplada no artigo 220 quando dispõe sobre a vedação à restrição da manifestação de pensamento, da criação, da expressão e da informação.

A liberdade de expressão é um dos corolários do Estado democrático de direito, pois é um pilar para proteção da pessoa natural na sua liberdade de se comunicar e de receber informações.

Conforme anota Gilmar Mendes e Paulo Branco (2021, p. 272).

> A plenitude da formação da personalidade depende de que se disponha de meios para conhecer a realidade e as suas interpretações, e isso como pressuposto mesmo para que se possa participar e debates e para que se tomem decisões relevantes. O argumento humanista, acentua a liberdade de expressão como corolário da dignidade humana [...].

O resultado do conhecimento obtido por meio da Tecnologia da Informação e Comunicação permite a manipulação em massa de informação e conteúdo que chegam aos destinatários de maneira personalizada e com isso contribui para uma nova forma de controle social. Nos primórdios, este controle permaneceu exclusivo dos Estados até que o seu uso se popularizasse entre particulares, transformando a dinâmica de poderes.

Transcreve-se, abaixo, a reflexão de Danilo Doneda sobre esse fenômeno:

> [...] o controle sobre a informação foi sempre um elemento essencial na definição de poderes dentro de uma sociedade, a tecnologia operou a intensificação dos fluxos de informação e, consequentemente, de suas fontes e seus destinatários.

> Essa mudança, a princípio quantitativa, acaba por influir qualitativamente, mudando a natureza e o eixo de equilíbrio na equação entre poder – informação-pessoa-controle. Isso implica a necessidade de conhecer a nova estrutura de poder vinculada a essa nova arquitetura informacional. (DONEDA, 2021, p. 35).

O vigilantismo digital é capaz de modular comportamentos, e com isso, torna-se ameaça à liberdade de expressão, de informação de comunicação e de opinião porque, com o perfilamento dos indivíduos, é possível, por meio de algoritmos, selecionar os conteúdos de cada usuário, ou grupos de usuários, mais tendencioso ou sensível a determinado tipo de conteúdo.

A gravidade disso está no fato de que o fluxo de informação não circula livremente na rede, visto que é direcionado pelas preferências dos usuários, criando, com isso, verdadeiras bolhas de informação que limitam a comunicação livre e o acesso à informação no ambiente digital (SARLET; SIQUEIRA, 2022, p. 45).

O quarto fundamento da LGPD é a inviolabilidade da intimidade, da honra e da imagem, pelo qual a lei reforça o direito negativo de não violação, repetindo valores já invocados na Constituição Federal no artigo 5º, X. Assim, reforça o dever de cuidado dos agentes de tratamento de dados e promove, propositivamente, a proteção e segurança de dados que espelhem situações abrangidas por esses direitos.

Enfatiza, com isso, a necessidade do ser humano de ser deixado em paz no seu aspecto mais íntimo, seu castelo, e ter, a partir do respeito à sua esfera privada, garantido a tranquilidade de livremente desenvolver sua personalidade e realizar suas escolhas, sem a observação ou julgamento alheios.

Shoshana Zuboff (2020, p. 538) denomina esse espaço reservado e exclusivo do indivíduo de “direito ao santuário”, reconhecendo-o como necessário “antidoto ao poder”.

O quinto fundamento da lei é o desenvolvimento econômico e tecnológico e a inovação. Está associado ao interesse da sociedade que, na proteção de dados pessoais, seja estabelecida uma convergência entre interesses aparentemente opostos, quais sejam, o desenvolvimento tecnológico e os direitos fundamentais dos titulares.

Assim, reconhecendo a importância da livre circulação de dados, a LGPD estabelece que o desenvolvimento tecnológico deve ter como base o objetivo de proteger os dados pessoais de modo que sociedade obtenha os benefícios da

inovação e da tecnologia, sem que deles decorram violações à direitos fundamentais.

A criação de novos modelos de negócio propiciada pela economia movida a dados precisa ser incentivada. Contudo, o que se pretende com este fundamento é a proteção para as pessoas a fim de evitar ilegalidades por parte dos agentes de tratamento. A regulação realça o papel na promoção do desenvolvimento tecnológico e a inovação com a criação de ambiente seguro, confiável e sustentável.

Nesse aspecto, o objetivo maior da LGPD relativo à proteção de dados pessoais, deve ser alcançado por meio dos seus fundamentos, ou seja, a regulação deve garantir a proteção desde que seja proporcional e não impeça a inovação, colocando em igual patamar a privacidade, a autodeterminação informativa e o desenvolvimento tecnológico (CABRAL, 2019, p. 56).

A promoção do desenvolvimento econômico possui estreita relação com a autodeterminação dos dados porque é por meio do controle dos próprios dados (autodeterminação informativa, que abrange o momento do consentimento e durante todo o período enquanto perdurar o tratamento dos dados) que é estabelecido o uso correto e justo do fluxo informacional, bem como o atendimento às legítimas expectativas do titular. Uma vez observados esses dois requisitos, fica garantido ao agente de tratamento, a livre circulação de dados. Ou seja, o tratamento de dados é autorizado desde que seja realizado de forma legítima e respeite os direitos do titular.

Por isso, é falacioso dizer que primar pela proteção de dados e privacidade seria impeditivo do desenvolvimento tecnológico. O que se espera é que a noção de progresso tecnológico esteja condicionada à observância de valores fundamentais para a sociedade, sendo uma questão de congruência e não de interesses contrapostos.[59]

O sexto fundamento da lei é a livre iniciativa, a livre concorrência e a defesa do consumidor, que estabelece sob a ótica concorrencial proteção aos empreendedores do meio digital, conforme disposto no artigo 170 da Constituição Federal.

[59] "A tecnologia, potente e onipresente, propõe questões e exige resposta 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 reafirmação de seu valor fundamental – a pessoa humana – ao mesmo tempo que fornece seguranças devidas para a viabilidade das estruturas econômicas dentro da tábua axiológica constitucional." (DONEDA, 2021, p. 65).

A livre iniciativa e livre concorrência são fundamentos do sistema econômico capitalista pois asseguram a liberdade de empreender em um mercado competitivo. Ao reconhecê-los como fundamento, a LGPD assegura que tais direitos também são garantidos diante da nova realidade, dada a relevância que os dados assumiram como um significativo insumo da sociedade contemporânea.

De igual modo, é preciso proteger também a sobrevivência do mercado diante de práticas predatórias concorrenciais exercidas por grandes agentes econômicos que impactam negativamente o mercado e, consequentemente, o direito dos consumidores.

Essa proteção limita, por exemplo, a manipulação de mercado exercido por grandes plataformas digitais (como *Google* e *Facebook*) cujo papel é concentrar a complexidade de relações entre provedores de conteúdo, vendedores de produtos e serviços e consumidores (FRAZÃO, 2021, p. 540).

Nesse sentido, Shoshana Zuboff salienta que as atividades no meio digital tendem a ser monopolistas, como exemplo, a experiência do Google como ferramenta de busca, cujo resultado direciona a lista de interesse da empresa.[60]

O poder de controlar o mercado destinado a poucos agentes desequilibra a liberdade de empresa e afronta direitos dos consumidores quando limita o acesso destes a um ambiente livremente concorrencial.

Adicionalmente, esse aspecto relacionasse-se à dinâmica de poder e controle exercida pelos *gatekeepers* que se utilizam de mecanismos de manipulação e direcionamento das escolhas dos usuários na rede. Esse controle é feito a partir da restrição e direcionamento do conteúdo que chega aos consumidores, a partir da

[60] "A incessante exigência por superávit em escala prediz um comportamento corporativo que favorece a exclusividade. Como a busca é o alicerce das operações de oferta do Google, a companhia tem todo o incentivo para seduzir usuários para sua plataforma, seu conteúdo e serviços adicionais da busca e então usar seus "métodos, aparatos e estruturas de dados" de bastidores para uma extração eficiente. A tendência à exclusividade produz uma gama de práticas consideradas "monopolistas" na perspectiva dos sistemas reguladores do século XX. Essas representações, ainda que válidas, omitem os elementos mais evidentes da nova ordem. O imperativo de extração exige que tudo seja possuído. Nesse novo contexto, bens e serviços são meras rotas de suprimento vinculadas à vigilância. Não é o carro; são os dados comportamentais extraídos do ato de conduzi-lo. Não é o mapa; são os dados comportamentais gerados a partir da interação com ele. O objetivo aqui está de modo contínuo expandindo fronteiras que acabam por descrever o mundo e tudo dentro dele, o tempo todo.
Tradicionalmente, monopólios sobre bens e serviços desfiguram mercados ao eliminar de forma injusta a concorrência a fim de aumentar os preços de acordo com a própria vontade. Sob o capitalismo de vigilância, contudo, muitas das práticas definidas como monopolistas na realidade agem como meios de açambarcar suprimentos de matéria-prima derivados dos usuários." (ZUBOFF, 2020, p. 158-159).

análise de tendências e propensões destes por algoritmos que se utilizam neurociência, psicologia e sociologia para aferir comportamentos-padrão de massa e, assim, delinear suas escolhas.

Como resultado da predeterminação de escolhas dos consumidores, os *gatekeepers* podem moldar o mercado, especialmente o de consumo e, com isso, restringir a livre iniciativa, a livre concorrência e ferir direitos dos consumidores.

Assim, a lei que regula a proteção de dados deve igualmente promover o desenvolvimento de novos modelos de negócio no ambiente digital para que os agentes econômicos disputem de modo equilibrado no mercado, limitando a concentração de poder e assegurando aos consumidores o acesso a produtos e serviços diversificados.

Logo, com relação aos fundamentos previstos nos incisos V e VI do artigo 2º da LGPD, importante notar a preocupação do legislador de proteger o titular dos dados e, ao mesmo tempo, proteger os agentes econômicos quando observa aspectos de promoção ao desenvolvimento tecnológico, à inovação e livre iniciativa e livre concorrência, tudo isso como uma forma de garantia do estado democrático de direito.

O sétimo e último fundamento da LGPD está relacionado aos direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Ao conceituar direitos humanos, Gilmar Mendes e Paulo Gonet traçam a distinção entre estes e direitos fundamentais, consistindo o primeiro em postulados universais de bases jusnaturalistas e filosóficas, enquanto os direitos fundamentais são estabelecidos positivamente no ordenamentos jurídicos (MENDES; BRANCO, 2021, p. 151).

Nesse sentido, a Declaração Universal de Direitos Humanos proclamada pela Assembleia Geral das Nações Unidas em 1948, dispõe acerca dos direitos humanos de caráter universal, servindo como base para o estabelecimento de direitos fundamentais em diversos países, inclusive no Brasil.

A Constituição Federal brasileira no seu artigo 1º, III estabelece a dignidade da pessoa humana como sendo o fundamento principal do ordenamento jurídico, colocando a pessoa na centralidade das relações e promovendo o desenvolvimento da sua personalidade.

Acerca da personalidade, Perlingieri (2002, p. 155-156) a descreve como sendo um "valor fundamental do ordenamento" básico de inúmeras situações existenciais. Este autor explica ainda acerca da dimensão coletiva da tutela da personalidade que não está restrita aos direitos individuais pertencentes aos sujeitos, tendo em vista que estes vivem em sociedade e, com ela, estabelecem relações em comunidade. Assim, a tutela da personalidade deve abranger também direitos individuais e coletivos, estabelecendo o indivíduo como centro das relações sociais (PERLINGIERI, 2002, p. 38-39).

Nessa perspectiva coletiva, a proteção de dados tem papel basilar na tutela de valores universais como o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Em mesmo sentido, Rodotà (2008, p. 19) aponta para a proteção de dados como uma expressão de liberdade e dignidade pessoais, não podendo ser tolerada a utilização dos dados pessoais de maneira a colocar a pessoa em posição objetificada e sob permanente vigilância.

Isso porque, na sociedade de vigilância a malversação dos dados pessoais pode subjugar os indivíduos, propiciar a concentração de poder e o autoritarismo, e assim, violar valores humanos fundamentais para a sociedade.

Diante da análise acerca dos fundamentos da LGPD, verifica-se que a proteção de dados vai além da tutela da privacidade e da autodeterminação dos dados na medida em que se baseia em valores constitucionais de alto relevo para a sociedade como a liberdade, igualdade, cidadania e democracia.[61]

Além dos fundamentos supracitados, a LGPD elenca expressamente nos incisos do artigo 6º os princípios essenciais aplicáveis ao tratamento de dados pessoais. Nesse sentido, vale antes ressaltar que a principiologia da LGPD está baseada no reconhecimento de que os dados pessoais pertencem a seus titulares, por

[61]Para Ana Frazão, os fundamentos da proteção de dados pessoais pode ser sistematizada da seguinte maneira: "i) proteção de dados pessoais como forma de endereçar os efeitos nefastos do capitalismo de vigilância e contornar os efeitos adversos da violação da privacidade como um negócio; ii) proteção de dados pessoais como forma de endereçar os riscos que os algoritmos representam às liberdades individuais e à própria democracia; iii) proteção de dados como forma de endereçar o problema da opacidade e da ausência de *accountability* da economia movida a dados; iv) proteção de dados pessoais como forma de endereçar os riscos do poder crescente de grandes agentes, como as plataformas digitais, sobre os cidadãos." (FRAZÃO; CARVALHO; MILANEZ, 2022, p. 15).

isso, impôs diversos limites e uma série de cuidados para o tratamento de dados (FRAZÃO, 2020, p. 102).

O caput do artigo 6º trata da boa-fé objetiva[62] a ser aplicada para toda e qualquer atividade de tratamento de dados pessoais. Assim, a lei refere-se aos deveres de conduta do agente de tratamento relativos à lealdade e probidade quanto à legítima expectativa do titular (FRAZÃO; CARVALHO; MILANEZ, 2022, p. 73).

Em outras palavras, é dever do agente de tratamento a realização de condutas objetivas que demonstrem concretamente o uso dos dados pessoais relacionado com a finalidade esperada pelo titular.

Assim, a noção de lealdade oferece ao titular a confiança de que seus dados pessoais serão adequadamente tratados e protegidos pelos agentes, sempre em conformidade com a lei (FRAZÃO; CARVALHO; MILANEZ, 2022, p. 74).

Desta forma, o princípio da boa-fé se relaciona com o princípio da finalidade, pois confere a legitimidade do tratamento desde que estabelecidos os propósitos específicos, explícitos e informados para a sua realização.

Nesse cenário, Helen Nissenbaum propõe a análise da 'privacidade contextual' que consiste no direito do titular ao apropriado fluxo de informações pessoais. A legítima expectativa, segundo essa autora, pode ser aferida a partir da análise casuística de adequação da estrutura do fluxo de dados composta por: i) contexto: ambiente social predominante em que ocorre o fluxo de informação e os potenciais impactos nocivos; ii) atores: emissores, destinatários e os titulares envolvidos; iii) atributos: o conteúdo da informação pessoal; e iv) princípios da transmissão: análise de restrição e confidencialidade da informação (NISSENBAUM, 2011, p. 127-182).

Bruno Bioni, ao analisar a teoria de Helen Nissenbaum, faz uma alusão da privacidade contextual como um 'óleo' que lubrificaria as engrenagens do mercado na sociedade de vigilância, visto que a privacidade contextual reside na confiança depositada pelo titular com base na sua legítima expectativa de que o tratamento de dados será realizado de acordo com o contexto de uma relação previamente estabelecida (BIONI, 2021, p. 235).

[62] Sobre o tema ver MARTINS-COSTA, Judith. **A boa-fé no direito privado**: critérios para sua aplicação. São Paulo: Saraiva, 2018.

Assim sendo, a legítima expectativa do titular funciona como um termômetro para identificar possíveis desvios de conduta no tratamento dos dados quanto a finalidade informada.

Previsto no artigo 6º, I da LGPD, o princípio da finalidade serve como um limitador dos propósitos declarados pelo agente de tratamento porque garante, ao titular, a razoável expectativa que seus dados serão utilizados para os fins específicos e informados.

A LGPD, ao prever que toda e qualquer atividade de tratamento de dados pessoais deve respeitar o princípio da finalidade, restringe a utilização tão-somente daqueles dados indispensáveis para alcançar os propósitos do tratamento pelo agente.

O dispositivo legal tem o objetivo de, a partir da expressa e específica finalidade, permitir ao titular o exercício do autogoverno sobre seus dados pessoais, possibilitando a averiguação da correlação entre a base legal[63] utilizada para justificar o tratamento e o efetivo tratamento.

Este princípio está intrinsicamente ligado às bases legais que fundamentam o tratamento dos dados pessoais pelos agentes, pois o motivo que justifica a coleta contidos das bases legais previstas nos artigos 7º e 11 da LGPD, deve ser compatível com o objetivo perseguido durante todo o tratamento dos dados (FRAZÃO; CARVALHO; MILANEZ, 2022, p. 79).

Por isso que, mesmo nos casos em que o consentimento é dispensado ou quando os dados são públicos (artigo 7º, §3º e 4º), os agentes de tratamento

[63] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
I - mediante o fornecimento de consentimento pelo titular;
II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
VII - para a proteção da vida ou da incolumidade física do titular ou de terceiros;
VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

permanecem com o dever de observar os direitos do titular conforme os princípios estabelecido na LGPD, devendo analisar o contexto e circunstâncias nos quais o dado pessoal é tratado, a fim de realizar a verificação da compatibilidade e pertinência (TEFFÉ; VIOLA, 2020, p. 11).

Considerando o pressuposto que os dados pessoais são uma projeção da personalidade do seu titular, o agente de tratamento não pode usá-los diversamente da finalidade declarada, restringindo-se a utilizá-los de forma compatível e no mínimo necessário para a realização dos objetivos perseguidos. Não se admite, por conseguinte, tratamento de dados com finalidades genéricas (DONEDA, 2021, p. 319).

Igualmente não são admitidos usos secundários ou extensões para além do que foi informado ao titular. Desta maneira, fundamenta-se a restrição ao fluxo de dados a terceiros, um dos principais pilares que sustenta o capitalismo de vigilância.

Vale lembrar que a lei exige a renovação do consentimento quando a finalidade do uso dos dados se tornar diferente daquela declarada no ato da sua coleta. Caso o agente altere a finalidade do uso dos dados em mesma base legal ou base legal distinta da original, deverá obter novo consentimento, caso contrário incorrerá em ilegalidade pelo descumprimento do princípio da finalidade. Além disso, a nova finalidade deverá ter relação com aquela originalmente declarada.[64]

A racionalidade do princípio da finalidade é oferecer ao titular a salvaguarda do uso dos dados de acordo com os objetivos especificados no momento da coleta, servindo como fator para ponderar a razoabilidade da utilização e em situações ulteriores.

Assim, remete-se novamente à proposta da estrutura da integridade contextual quanto a análise da legítima expectativa conforme a teoria de Helen Nissenbaum, supracitada. Tal análise deve ser feita no caso concreto, uma vez que a incompatibilidade não é automática e nem pode ser avaliada em abstrato, mas deve

[64] "Não basta, entretanto, que a nova finalidade seja tão somente específica e legítima, ela deve ser também compatível com a finalidade original. Ou seja, ainda que seja confirmada a especificidade e a legitimidade da nova finalidade escolhida par ao tratamento posterior, ele só poderá ser realizado caso essa nova finalidade seja também compatível com aquela que justificou a coleta do dado pessoal em momento anterior." (FRAZÃO; CARVALHO; MILANEZ, 2022, p. 81).

ser verificada a sua pertinência e compatibilidade da nova finalidade com a autorização inicial do titular dos dados pessoais[65].

Passando para o exame do próximo princípio disciplinado no artigo 6º da LGPD, o princípio da adequação previsto no inciso II determina a compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o seu contexto.

O princípio da adequação demanda a verificação se a finalidade informada está proporcionalmente adequada ao contexto do tratamento dos dados pessoais. Desta forma, o princípio tem a função de também limitar o uso dos dados àquilo que foi originalmente informado, a partir da forma com a qual o agente irá realizar o tratamento.

Pode-se perceber que os princípios da finalidade, adequação e necessidade estão intrinsecamente ligados, formando uma tríade quase inseparável na perspectiva da proteção de dados pessoais. Essa zona de congruência e justaposição entre esses três princípios pode ser observada no voto da Ministra Rosa Weber no já citado julgamento da acerca da inconstitucionalidade da Medida Provisória nº 954:

> Nessa linha, ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP n. 954/2020 não oferece condições para avaliação da sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades. Desatende, assim, a garantia do devido processo legal (art. 5º, LIV, da Lei Maior), em sua dimensão substantiva. (BRASIL, 2020, p. 1).[66]

No trecho acima transcrito, observa-se que a determinação do meio pelo qual será realizado o tratamento irá garantir a pertinência da adequação e da necessidade para a finalidade proposta para evitar que o tratamento dos dados seja realizado de maneira descontextualizada e no limite do mínimo necessário.

Previsto no artigo 6º, III da LGPD, o princípio da necessidade restringe o agente, em termos quantitativo e qualitativo, quanto ao uso dos dados ao mínimo necessário para a realização do tratamento declarado.

[65] Nesse aspecto Frazão, Carvalho e Milanez (2022, p. 82-83) apresentam os critérios para aferir a licitude do tratamento baseada no parecer 3/2013 da GDPR quais sejam: i) a relação entre a finalidade do tratamento originalmente concedido e o posterior; ii) o contexto da coleta e as legítimas expectativas do titular, iii) a natureza do dado e o impacto da finalidade do tratamento posterior, e iv) as garantias aplicadas pelo agente relativos à segurança e prevenção de impactos indevidos.
[66] STF, ADI 6387, Relatora Ministra Rosa Weber. Data de publicação DJe. 12/11/2020.

O princípio da necessidade estabelece a vedação sob dois aspectos: quantitativo, ou seja, a vedação de tratamento de dados excessivos e o qualitativo, dados desproporcionais e descontextualizado com a finalidade (FRAZÃO; CARVALHO; MILANEZ, 2022, p. 86).

Assim, fica assegurado ao titular que o tratamento será tão-somente sobre os dados estritamente necessários e adequados para os devidos fins, servindo de baliza e limitação para o agente para tratamento, evitando com isso, que informações desnecessárias e dados não pertinentes sejam coletados e tratados.

Um exemplo claro de aplicação prática do princípio da necessidade está contido no artigo 10§1º da LGPD, ao dispor que o tratamento baseado no legítimo interesse do controlador poderá ocorrer somente aos dados pessoais estritamente necessários para alcançar o objetivo informado.

Conforme observado por Carlos Affonso Pereira de Souza, Eduardo Magrani e Giovana Carneiro (2020, p. 55) acerca dos modelos de negócios, este princípio têm como pressuposto evitar a excessiva acumulação de dados pessoais sob justificativas genéricas como melhoria dos serviços, ressaltando que esse modo de operação está nitidamente em descompasso com as leis de proteção de dados.

Estabelecido no artigo 6º, IV da LGPD, o princípio do livre acesso garante ao titular a realização de consulta facilitada e gratuita sobre a forma e a duração do tratamento dos seus dados, assim como a sua integralidade. Para que o titular possa exercer o adequado controle sobre suas informações, deverá a ele ser assegurado, a qualquer momento, o conhecimento sobre os próprios dados.

Vale ressaltar que a integralidade do acesso mencionada no dispositivo legal deve corresponder a toda e qualquer informação do titular, contemplando com isso os dados pessoais e as informações obtidas por análises algorítmicas, desde que relacionadas ao titular.

A aplicação prática deste princípio está disciplinada em disposições, como artigo 9º (direito de acesso) e de maneira implícita nos artigos 18 e 19 (requisição de acesso), de igual modo prevista no artigo 20 (revisão das decisões) da LGPD (FRAZÃO; CARVALHO; MILANEZ, 2022, p. 87).

Desta forma, o agente deve disponibilizar ao titular protocolos de atendimento que permitam a requisição, simples e imediata dos dados para oportunizar a verificação de *quais* dados estão sendo tratados e *como*.

Assim, a partir do livre acesso aos seus dados sob tratamento, o titular poderá exercer seu direito à autodeterminação informativa como também poderá controlar possíveis alterações relacionadas à finalidade e adequação na sua utilização.

Seguindo a ordem topológica da legislação, o princípio da qualidade dos dados, previsto no artigo 6º, V da LGPD, estabelece a garantia dos agentes de tratamento a exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

A racionalidade deste princípio está na veracidade e atualidade dos dados. O cidadão tem o direito de conhecer os seus dados pessoais que estão sob tratamento e exigir a sua correção, caso estejam inexatos ou desatualizados, demandando dos agentes de tratamento dos dados que atendam ao mínimo de veracidade condizente com a realidade do titular.

Remete-se à noção de corpo eletrônico, como um novo tipo de identidade da pessoa natural, pelo qual todos os dados armazenados e tratados (dossiês digitais) devem corresponder informações corretas e atualizadas, pois somente assim, será autenticamente projetada a identidade do titular (BIONI, 2021, p. 57).

O princípio determina ao agente de tratamento a obrigação de criar mecanismos para permitir a verificação, atualização e correção dos dados pessoais pelo titular, para que não reflitam informações diversas da realidade do titular. Em outras palavras, deve conceder ao titular o acesso e a transparência do tratamento dos seus dados para garantir-lhe a possibilidade de exigir a correção.

Na sociedade de vigilância, é fundamental que a representação eletrônica da pessoa, seu corpo eletrônico, corresponda de maneira fidedigna aos aspectos da sua personalidade, pois é, muitas vezes, a única forma com a qual o sujeito estabelece suas relações no ambiente digital. Por isso, uma eventual representação falha, pode impactar a forma com a qual a pessoa é tratada em determinado contexto, podendo, inclusive, gerar fatores discriminatórios, ou gerar perdas de chances ou oportunidades (DONEDA *et al.*, 2019, p. 98).

Pelo princípio da transparência, disposto no artigo 6º VI, os titulares têm a garantia de conhecimento claro, preciso e acessível sobre os aspectos relacionados ao tratamento dos seus dados pessoais, limitado aos segredos comerciais e industriais do agente de tratamento.

A transparência, sob o ponto de vista da proteção de dados pessoais, tem o objetivo de oferecer ao titular dos dados todas as informações, de maneira clara e compreensível acerca de *quais* dados e *qual* o tratamento foram submetidos, *quem* são os agentes estão envolvidos, *como* os critérios são utilizados e os resultados obtidos (conforme artigo 20º§1º), tudo isso para permitir ao titular o exercício efetivo da autodeterminação informativa.

É um dos princípios de grande valor quando relacionado ao tratamento de dados pessoais, pois mitiga a opacidade geralmente presente nos algoritmos da qual, muitas vezes, decorrem abusos e discriminações.

A opacidade algorítmica, resumidamente, consiste no desconhecimento acerca de como funcionam os algoritmos, seja pela técnica de processamento de dados, seja pela complexidade das bases de dados, o fato é que muitas vezes não é possível, ou viável, conhecer como um algoritmo toma uma decisão, o que pode levar a injustiças ou discriminações.[67]

Assim, ao regular sobre proteção de dados, é imprescindível que a transparência e a responsabilidade dos agentes sejam aspectos relevantes para o tratamento seguro dos dados pessoais.

Entretanto, muitas vezes a transparência esbarra no segredo do negócio, dificultando o controle do processo de tratamento de dados pelo titular. O legislador, nesse tema, ponderou entre dois relevantes valores: a transparência e a proteção aos segredos no negócio, estabelecendo o segundo como limitador à aplicação do primeiro, privilegiando o direito de propriedade intelectual sob o fundamento de que a total transparência de determinados modos de operação, possa vir a causar danos ao negócio (FRAZÃO; CARVALHO; MILANEZ, 2022, p. 92).

Como todo direito, os direitos fundamentais também não são absolutos. Tais limites estão na imposição de outros direitos também consagrados na Constituição, e, na ponderação entre direitos, deve ser levado em consideração a proteção dada aos bens jurídicos relevantes em conflito, buscando a razoabilidade e proporcionalidade no contexto constitucional.

[67] Muitos modelos são programados a partir da realidade e a sociedade contém muitos preconceitos decorrentes de vieses humanos, isso aplicados em softwares, pode ser bastante nocivo. Cathy O'Neil chamou esses softwares de "armas de destruição em massa", por serem carregados de vieses humanos, acabam por replicar tendências sociais de discriminação e opressão enquanto alargam a assimetria de poder (O'NEIL, 2020).

Quando se trata de sistemas computacionais, geralmente o segredo do negócio está contido no código fonte do sistema, logo, protegido do dever de transparência do agente. Mesmo assim, a proteção do código fonte não exime o agente de fornecer, minimamente, ao titular os critérios básicos do tratamento a fim de propiciar o controle razoavelmente inteligível dos seus dados (FRAZÃO; CARVALHO; MILANEZ, 2022, p. 93).

Disposto no artigo 6º, VII da LGPD, o princípio da segurança estabelece como dever do agente a utilização de medidas técnicas e administrativas hábeis a proteger os dados pessoais dos riscos inerentes a atividade de tratamento de dados, quais sejam: acessos não autorizados, situações acidentais, ilícitas de destruição, perda, alteração ou comunicação.

O cenário já experimentado no ambiente digital é inseguro, tendo noticiado inúmeros vazamentos de dados e incidentes de segurança, cuja recorrência é um desafio para os agentes que tem a obrigação de adotar medidas aptas a proteger os dados pessoais.

Tal comando objetiva a proteção dos dados de acessos indevidos e a qualidade dos dados, por considerar a alteração indevida como uma das hipóteses de tratamento ilícito de dados. Em vista disso, o artigo 44 da LGPD define como irregular quando o tratamento dos dados não fornecer a segurança que o titular pode esperar. Com isso, observa-se a íntima relação deste princípio com os princípios da boa-fé e da prevenção.

Com efeito, o artigo 46 §1º da LGPD já indica alguns critérios a serem levados em consideração na compatibilidade entre segurança e riscos, como a natureza do dado e as características do tratamento que, apesar de haver indicativo para que a ANPD estabeleça as diretrizes e os padrões mínimos de segurança[68], em tais casos, o agente deve adotá-los como critérios relevantes no gerenciamento do risco na medida e compatibilidade com seu modelo de negócio como interpretação sistemática derivada dos demais princípios do artigo 6º.

Assim, acerca das medidas administrativas, nota-se que o princípio tem aplicação prática da abordagem de gerenciamento de risco. Por isso, a lei no artigo 50 §2º faz referência a outros critérios que podem ser considerados na avaliação

[68] Válido de nota que a ANPD já se pronunciou acerca da segurança da informação para agentes de tratamento de pequeno porte. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf. Acesso em 21 mar. 2023.

dos riscos, além das características do tratamento e natureza dos dados, quais sejam; estrutura, escala, volumetria das operações, a probabilidade de ocorrência dos eventos de risco e a gravidade dos danos aos titulares. A partir do reconhecimento destes cenários, o agente de tratamento deve identificar possíveis riscos e estabelecer os respectivos controles para evitar que se tangibilizem ou para mitigar seus os impactos.

Já com relação às medidas técnicas dispostas no artigo 46, a lei refere-se à prevenção de incidentes, por meio de tecnologias hábeis para garantir a segurança da informação. Nesse sentido, orienta a adoção de soluções tecnológica, implantadas no desenvolvimento dos sistemas da organização, desde a sua concepção e enquanto durar o tratamento dos dados.

Como será visto mais a diante neste estudo, são exemplos dessas medidas o *privacy by design* que consiste na colocação desde a concepção e no desenvolvimento do sistema, de medidas preventivas de riscos à privacidade e a proteção e dados, e o *privacy by default* que se refere a colocação de medidas de segurança automaticamente inseridas por padrão no sistema, não sendo necessária nenhuma conduta do titular para ativar qualquer dispositivo de segurança (SOUZA, 2020, p. 424).

O princípio da prevenção previsto no artigo 6º VIII da LGPD, obriga o agente realizar ações preventivas para evitar a ocorrência de danos no âmbito do tratamento de dados pessoais. Com isso, o agente de tratamento tem a obrigação de, a partir dos riscos identificados na sua atividade de tratamento, implantar controles para previr a ocorrência incidentes e criar ações e respostas para reduzir seus impactos.

Assim, ao estabelecer expressamente o princípio da prevenção, o legislador deu enfoque na gravidade dos danos que podem advir da malversação de dados pessoais, que podem atingir indivíduos e coletividade e cujos impactos são irreversíveis ou de difícil reparação. Daí o direcionando da lei para a importância do gerenciamento de risco (prevenção) relacionados à segurança da informação, em prejuízo da responsabilização dos agentes (FRAZÃO; CARVALHO; MILANEZ, 2022, p. 98).

O princípio da prevenção possui dois aspectos que devem ser observados: o primeiro o dever de evitar a ocorrência de danos aos titulares dos dados pessoais e o segundo de mitigar seus efeitos, caso se concretizem.

De acordo com a natureza do dado e o processo de tratamento, o nível do risco de exposição do titular pode variar, exigindo do agente a adoção das medidas de segurança e prevenção ajustadas ao risco que efetivamente está exposto. Isso evita, por exemplo, custos para adoção de medidas superiores à verdadeira necessidade do agente e, por outro lado, evita que medidas insuficientes sejam adotadas para altos riscos.

A abordagem de gerenciamento de risco adotada pela legislação brasileira também oferece maior flexibilidade para que a proteção de dados pessoais seja aplicada nas situações que realmente importa, ajustada às caraterísticas dos dados, do tratamento e da tecnologia utilizada. Portanto, a diversificação de agentes, em razão do porte ou das características dos negócios, os riscos aos quais estão submetidos também muda o nível de proporção necessário (FRAZÃO, 2021, p. 45).

Nesse sentido, é importante que os agentes de tratamento conheçam muito bem seus processos internos e os reflexos do seu negócio sobre os titulares e coletividade, pois, somente assim, será possível identificar, minimamente, os impactos de um incidente de segurança.

Como será visto no próximo capítulo deste estudo, para o pleno entendimento ao princípio da prevenção, é primordial que o agente estabeleça voluntariamente boas práticas de governança de dados de modo que adote ações como, treinamento e conscientização corporativas além da implantação de processos internos de gestão de riscos para o monitoramento e mitigação dos eventos de risco (artigo 50). A esses padrões regulatórios, o agente deverá ainda agregar, quando necessário, outros padrões de segurança ajustados ao negócio e adequados ao mercado em que atua, para evitar ou mitigar a ocorrência de danos decorrentes de um incidente de segurança de dados.

Conforme artigo 6º, IX da LGP, o princípio da não discriminação consubstancia a vedação ao tratamento dos dados pessoais de maneira discriminatória ou abusiva.

A proibição de uso ilegal e discriminatório deve contemplar todos os dados pessoais relativos ao titular, contudo, é notória e, infelizmente comum, a incidência de discriminações algorítmicas quando envolvem o perfilamento e o uso de dados sensíveis (como raça, sexo, orientação sexual etc., conforme artigo 5º, II da LGPD).

Isso ocorre porque informações sensíveis possuem natureza existencialista (DONEDA *et al.*, 2019, p. 99) de alta capacidade discriminatória (MULHOLLAND, 2020, p. 123), pois denotam aspectos que podem identificar, por exemplo, se o titular pertence a algum grupo social marginalizado, suas condições socioeconômicas, aspectos da sua saúde, informações comportamentais íntimas, dentre outros aspectos.

Assim, a potencialidade lesiva do uso indevido de dados pessoais, especialmente os sensíveis, pode ocasionar graves danos à liberdade e igualdade substancial, pelo que é proibido que o tratamento dos dados resulte em algum desfavorecimento de alguém ou de um grupo de pessoas.

Vale lembrar que os algoritmos são baseados em cálculos matemáticos e estatísticos complexos e incompreensíveis aos humanos. Quando se trata de inteligência artificial com aprendizado de máquina (*machine learnig*) a complexidade aumenta, pois, muitas vezes, nem os programadores conseguem identificar todo o processo realizado pelo algoritmo até chegar à determinada decisão.

A discriminação estatística, ou viés algorítmico, está relacionada a opacidade dos algoritmos e aos processos de classificação de pessoas ou grupos, utilizando a generalização de pessoas com a finalidade de obter maior probabilidade ter determinados comportamentos ou apresentar determinadas qualidades (DONEDA, MENDES, *et al.*, 2019, p. 100). A generalização para a tomada de decisão algoritimica pode gerar tratamentos odiosos, preconceituosos e injustos, perpetuando disparidades sociais.

Com o reconhecimento desses padrões, os algoritmos são capazes de julgar o indivíduo a partir das características do grupo ao qual pertence. Aliás, conforme chama atenção Ana Frazão, discriminação e preconceitos arraigados na sociedade, tendem a ser interpretados de maneira automática pelos algoritmos como um padrão, replicando-os nos seus processos e decisões (FRAZÃO; CARVALHO; MILANEZ, 2022, p. 103).

Por isso, para Caitlin Mulholland (2020, p. 273) é essencial para evitar processos de tomada de decisão algorítmica discriminatórias apurar se o agente adota ativamente medidas de promoção à proteção de dados e não discriminação.

Isso porque, o viés discriminatório pode surgir a partir da base de dados utilizada pelo sistema ou pela programação que o constitui. Por isso, na construção de um sistema, especialmente se utilizar algoritmos de inteligência artificial, seus desenvolvedores devem fazer com que o código da programação contenha mecanismos ativos de neutralização dos possíveis vieses discriminatórios.

Visando coibir algoritmos discriminatórios, além dos princípios, a LGPD estabelece no artigo 20, o direito do titular de revisão das decisões tomadas por sistemas automatizados, a partir do dever do controlador dos dados de prestar informações, mediante solicitação, acerca dos critérios e procedimentos utilizados para a decisão automatizada. Assim, o controlador deve estar preparado para atender a tal solicitação e fornecer ao titular, informações acerca da metodologia empregada, respeitado o segredo do negócio.

E, se no exercício desse direito, a transparência for negada pelo agente sob o argumento do segredo do negócio, para não desamparar o titular, a lei apresenta como solução a possibilidade de realização de auditoria pela Autoridade Nacional de Proteção de Dados (ANPD), conforme artigo 20, §2º. Contudo, sobre isso, importante destacar que é uma possibilidade, não uma obrigação, o que leva à crítica de que o controlador pode vir a negar o acesso com base nessa disposição com a expectativa que a ANPD não fará auditoria.

Sobre essa disposição ainda recaem outras críticas no sentido da asseguração da qualidade das informações prestadas pelo agente, que podem não ser compreendidas pelo titular, ou seja, apesar de o comando expressamente dispor que a explicação seja clara, pode ser que, ainda assim, não alcance a compreensão do destinatário, o titular.

O último princípio previsto no artigo 6º está disposto no inciso X da LGPD refere-se à responsabilização e prestação de contas**.** Significa dizer que é obrigação dos agentes demonstrar a efetiva adoção de processos corporativos que adotem, de maneira eficaz, o cumprimento da regulação de proteção de dados (*accountability).*

Essa obrigação de transparência e prestação de contas, está caracterizada na prática, como a obrigação dos agentes de manter registro das informações relativas ao tratamento pessoais, que poderão ser requisitadas pelo titular, assim como pela ANPD.

No tocante ao princípio da responsabilização, um fator preponderante é a constatação de que os danos decorrentes de violações à privacidade e a proteção de dados foram potencializados quando o tratamento passou a ser realizado no meio digital. Por isso, por ser uma atividade essencialmente de risco, os agentes têm o dever de diligência e transparência em demonstrar que todas as medidas foram adotadas de maneira eficaz para que eventual dano não ocorra.

Dessa forma, no âmbito do tratamento de dados, o princípio da responsabilização tem vinculação direta com o princípio da prestação de contas, pois deste decorre a necessária transparência quanto aos processos internos do agente de modo que haja uma efetiva prevenção quanto aos danos decorrentes das atividades de tratamento.

Após a abordagem acerca de cada princípio da LGPD, é possível depreender que, na medida em que são estabelecidos os limites e as obrigações dos agentes de tratamento, a lei tem o objetivo principal de proteção dos dados pessoais do titular baseada na gestão de riscos (*risk-based approach*), inclusive quanto aos aspectos técnicos para a segurança da informação (CUEVA, 2021, p. 66).

No capítulo a seguir, será analisado como o *compliance* de dados pode ser um valioso aliado dos agentes no apoio a adoção de boas práticas de governança para o atendimento aos princípios do artigo 6º, em especial a boa-fé, adequação, da transparência, da segurança, da prevenção e da responsabilização e prestação de contas, bem como a regulação já existente da ANPD; a partir dos quais os agentes constroem uma estrutura organizada para melhor gerir os riscos decorrentes das suas atividades.

4 *COMPLIANCE* DE DADOS

4.1 Modelo de corregulação

Da forma que tem sido usada na sociedade contemporânea, a TIC causa impactos sem precedentes na humanidade, razão pela qual, deu origem às principais mudanças regulatórias no âmbito da tutela da privacidade e proteção de dados.

A regulação jurídica tradicional, realizada exclusivamente pelo Estado e fundamentada na definição de comando-controle (*enforcement)*, foi adotada nas primeiras leis que abordaram o tema da privacidade e na, ainda incipiente, proteção de dados.

Contudo, a história já mostrou que, diante de uma sociedade cada vez mais complexa e da expansão do avanço tecnológico, esse modelo rígido, baseado no temor à sanção, tem-se mostrado insuficiente, especialmente no que tange à resposta jurídica (responsabilização penal, civil ou administrativa).

Como já foi mencionado, a proteção de dados é um direito fundamental que se relaciona com outros como liberdade, privacidade e livre desenvolvimento da personalidade. Assim, a regulação baseada exclusivamente na responsabilização, se torna ineficiente, dadas as circunstâncias de gravidade e irreparabilidade de tais ofensas.

Na análise das fragilidades da regulação estatal baseada, exclusivamente, no comando-controle[69] aplicada ao tema da proteção de dados, Ana Frazão destaca que estudos da economia comportamental, da economia neo-industrial e da sociologia econômica, demonstram que a existência de sanção não é fator preponderante para fazer com que as pessoas cumpram uma lei. Em verdade, há diversos fatores sociais e culturais são considerados para que uma lei possa ser cumprida com efetividade (FRAZÃO, 2020, p. 39-41).

De modo oposto, a total falta de regulação estatal (livre mercado), deixando a cargo dos agentes autorregulação a partir das relações privadas, não é uma opção viável, considerando que a proteção de dados é um direito fundamental altamente

[69] Danilo Doneda explica os modelos pelos termos *desregulation* e *regulation*. O primeiro consiste, de maneira geral, na eliminação ou diminuição das regras e vínculos de conduta estabelecidos pela autoridade reguladora. Já a *regulation* está associada a um conjunto normativo e de controles para assegurá-los (DONEDA, 2021, p. 326-327).

impactado pelo mercado da tecnologia que tem potencial danoso. Portanto, deixar a cargo exclusivo da regulação pelo mercado, poderia trazer graves prejuízos para o titular, tendo em vista a inerente assimetria informacional existente na relação entre agente de tratamento e titular de dados.

Adicionalmente, a regulação sem intervenção estatal poderia colocar o próprio mercado digital em risco, considerando a tendência natural de monopólio das grandes plataformas digitais. Visto isso, a regulação pelo Estado não pode ser afastada quando se trata de proteção de dados, necessitando da sua intervenção para corrigir as graves assimetrias inerentes do mercado.

Diante das carências existentes entre o cumprimento da lei relacionadas a cada uma dessas abordagens, e da necessidade de levar em consideração, na estrutura jurídica sobre a proteção de dados as diversas variáreis e incertezas que decorrem da inovação tecnológica, bem como seus efeitos sobre a sociedade; concebeu-se, para a LGPD o modelo da corregulação (FRAZÃO, 2021, p. 50-52).

Em resumo, o modelo de corregulação na proteção de dados comporta a criação de uma lei, de caráter geral e transversal, que, a partir da definição principiológica consistente e de padrões de conduta que se autorregulam criando, ao lado da legislação, uma maior participação proativa dos agentes na proteção de dados. [70]

Neste modelo[71], fica claro o reconhecimento da importância das regras sociais surgidas no mercado, sobre as quais o Estado estabelece as diretrizes, limites e o monitoramento (ZANATTA, 2015, p. 450).

[70] "Hoje, visto que a experiência do passado demonstra a rápida obsolescência das disciplinas muito rígidas e chama a atenção para as intervenções institucionais dotadas de flexibilidade, pode-se propor que o ambiente jurídico favorável a uma disciplina adequada da circulação das informações seja caracterizado pelos seguintes elementos:
i) Uma disciplina de base, constituída essencialmente por cláusula gerais e normas processuais;
ii) Normas para casos específicos, possivelmente presentes em leis autônomas, relacionadas com as atividade de determinados sujeitos ou com a disciplina de categorias específicas de informações;
iii) Uma autoridade administrativa independente, eventualmente dotada de poderes para a adaptar a situações particulares os princípios contidos nas cláusulas gerais;
iv) Uma disciplina de recurso à autoridade judiciária, não somente nos sistemas nos quais isso é exigido pela norma constitucional, mas de modo geral, para enraizar também essa matéria princípios análogos aos de um *Bill of Rights* ou do *Due Process*, segundo uma linha que tende a aproximar a matéria aqui considerada aos direitos civis;
v) A previsão de um controle difuso, confiado à iniciativa de indivíduos e grupos" (RODOTÀ, 2008, p. 87-88).

[71] De acordo com Miriam Wimmer, "[...] os autores distinguem a autorregulação pura; a corregulação (compreendida como a autorregulação com algum nível de supervisão ou ratificação governamental); e o *enforcement self-regulation* ou autorregulação regulada, em que existe a

Além da previsão do *enforcement*, aplicação de sanções e responsabilização pela ANPD caso o agente descumpra as obrigações legais, a LGPD tem em vista a proatividade (individual) e a cooperação (por associações) entre os agentes para a criação de instituições fortes e comprometidas com a proteção de dados e privacidade.

Pretende-se, com isso, o protagonismo por parte dos agentes em encontrar soluções compatíveis com o seu modelo de negócio, considerando que "[...] seria desastroso pretender uma aplicação linear e absolutamente uniforme da LGPD [...]" (FRAZÃO, 2021, p. 35).

A corregulação se concretiza na LGPD em dois principais vetores principiológicos, o primeiro com o princípio da responsabilização e prestação de contas que obriga o agente de tratamento ao cumprimento e à comprovação de condutas diligentes e assecuratórias da proteção de dados orientadas e monitorados pela ANPD; o segundo com o princípio da boa-fé e da adoção das boas práticas e governança dos dados previsto no artigo 50 da lei.

Neste diapasão, o *compliance* assume papel complementar à lei sob a forma de atuação da iniciativa privada (FRAZÃO; OLIVA; ABILIO, 2020, p. 677). Assim, se apresenta como uma importante ferramenta de autorregulação para dar efetividade à LGPD, com três funções primordiais: i) realizar a aderência dos processos organizacionais à lei, ii) estabelecer o gerenciamento de risco decorrentes do tratamento de dados e iii) estabelecer boas práticas de governança.

Na sequência, será feita uma abordagem acerca do *compliance* no âmbito do tratamento de dados como um suporte da governança corporativa, para a tutela dos dados pessoais por meio da adoção de boas práticas de conformidade, com o objetivo de dar efetividade aos princípios e direitos consagrados na LGPD.

4.2 Conceito e atribuições

O *compliance* é instrumento que auxilia a governança corporativa[72] para a criação e manutenção de um ambiente hígido, em todas as suas relações, aumentando a confiança na organização (CRESPO, 2020, p. 159).

possibilidade de imposição, pelo Estado, de medidas de *enforcement* privado, assim como o *enforcement* público e regras privadas." (WIMMER; PIERANTI, 2021, p. 217).

[72] De acordo com o IBGC, governança corporativa é "o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios,

De maneira geral, o *compliance* é responsável por garantir que as empresas cumpram regulações, construindo políticas internas e práticas adequadas para o seu atendimento. Para tanto, estabelece regras com base no gerenciamento dos riscos organizacionais, avaliando as potenciais ameaças do negócio e, a partir delas, instituídas as medidas de prevenção, mitigação e aculturamento, de maneira que demonstrem que a organização está em busca da conformidade (SAAVEDRA; CRESPO, 2020).

Ana Frazão define *compliance* como sendo o

> [...] conjunto de ações a erem adotadas no ambiente corporativo para que se reforce anuência da empresa à legislação vigente, de modo a prevenir a ocorrência de infração ou, já tendo ocorrido o ilícito, propiciar o imediato retorno ao contexto de normalidade e legalidade [...]. (FRAZÃO; OLIVA; ABILIO, 2020, p. 675) .

Em vista disso, de acordo com Bruno Dantas e Leonardo Silva, as atividades a serem executada pelo *compliance* possuem três momentos bem marcantes: i) conhecimento das regras de mercado no qual a organização está inserida; ii) adequação a tais regras; e iii) adoção de medidas mitigadoras, caso essas regras sejam violadas (DANTAS; SILVA, 2021, p. 303).

Desta forma, é possível notar que o *compliance* atua basicamente na detecção, prevenção e remediação de riscos organizacionais, criando mecanismos de atuação e respostas a partir de procedimentos internos como políticas e processos corporativos estabelecidos para tal finalidade.

A rigor, levando em consideração a estrutura, o *compliance* de dados não se distingue muito do modelo tradicional. Contudo, considerando que a LGPD, dedicou um capítulo para tratar da segurança da informação e boas práticas de governança, tem-se um forte indicativo que a proteção dos dados pessoais deve ser promovida para além da mera conformidade à lei.

conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas. As boas práticas de governança corporativa convertem princípios básicos em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor econômico de longo prazo da organização, facilitando seu acesso a recursos e contribuindo para a qualidade da gestão da organização, sua longevidade e o bem comum." Disponível em: https://www.ibgc.org.br/conhecimento/governanca-corporativa#:~:text=Governan%C3%A7a%20corporativa%20%C3%A9%20o%20sistema,controle%20e%20demais%20partes%20interessadas. Acesso em 12 mar. 2023.

Por serem os dados pessoais o principal recurso que move a sociedade de vigilância, a sua operacionalização se tornou indispensável para as organizações especialmente aquelas que tratam dados de alto risco[73].

Por isso, além de assegurar a devida proteção aos dados, a lei também procura proporcionar segurança jurídica aos agentes de tratamento, garantindo-lhes, em determinadas circunstâncias e respeitados os parâmetros legais, fica autorizado o uso dos dados pessoais no desempenho dos negócios.

Para equilibrar ambos os interesses (de proteção e de tratamento dos dados), a LGPD é

> [...] uma lei fundamentalmente principiológica, baseada em princípios, cláusulas gerais, *standards* de comportamento e conceitos abertos que precisam ser consolidados e adaptados à situação particular de cada agente de tratamento e dos riscos dos respectivos tratamentos [...]. (FRAZÃO, 2021, p. 45).

Portanto, a lei assume qualidades próprias, em razão do seu caráter preventivo, baseadas em princípios e conceitos abertos que devem ser ajustados na medida do modelo de negócio do agente. O cumprimento da lei pode variar de acordo com as características do agente de tratamento.

Diante da necessidade de estabelecer estruturas corporativas consolidadas para o atendimento das obrigações do agente, é possível dizer que o *compliance* tradicional adquire mais uma função, ou seja, servir de aliado para dar cumprimento efetivo à LGPD.

Assim, o *compliance* de dados visa auxiliar os agentes de tratamento na aplicação das regras estabelecidas na LGPD e no cumprimento da regulação emitida

[73] A ANPD já se pronunciou acerca das características do alto risco no tratamento dos dados pessoais na Resolução nº 2 CP/ANPD, de janeiro de 2022:
Art. 4º Para fins deste regulamento, e sem prejuízo do disposto no art. 16, será considerado de alto risco o tratamento de dados pessoais que atender cumulativamente a pelo menos um critério geral e um critério específico, dentre os a seguir indicados:
I - critérios gerais:
a) tratamento de dados pessoais em larga escala; ou
b) tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares;
II - critérios específicos:
a) uso de tecnologias emergentes ou inovadoras;
b) vigilância ou controle de zonas acessíveis ao público;
c) decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, inclusive aquelas destinadas a definir o perfil pessoal, profissional, de saúde, de consumo e de crédito ou os aspectos da personalidade do titular; ou
d) utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos.

pela ANPD, por meio de uma estrutura corporativa consolidada e coordenada, estipulando as ações necessárias para que as atividades relacionadas ao tratamento de dados estejam em conformidade com a lei e normas regulamentares, nivelando as medidas de segurança e controles internos de acordo com as atividades desempenhadas e os riscos existentes.

Noções de autovigilância, autorregulação e autorresponsabilidade são fundamentais para um programa de *compliance* sobre as quais se delineiam o alcance e compromisso da organização com o cumprimento da lei (OLIVA; ABÍLIO; COSTA, 2021).

Por isso, tal como o modelo tradicional, o *compliance* de dados utiliza uma verificação voltada para três elementos: pessoas, processos e tecnologia, que irão orientar a estrutura de governança em dados a partir de cinco passos: i) identificar; ii) avaliar; iii) priorizar e decidir; iv) tratar e controlar; e por último, v) monitorar e reportar.

O papel do gerenciamento da conformidade no âmbito do tratamento de dados pessoais visa garantir que as atividades executadas pelos agentes sejam conduzidas de acordo com a lei e regulação. A LGPD, por sua vez, estabelece uma série de obrigações decorrentes dos princípios que devem ser cumpridas pelos agentes de tratamento, dentre elas: i) o mapeamento e registro de todas as operações e tratamento de dados pessoais[74]; ii) a identificação dos dados pessoais e a correspondente base legal associada[75]; iii) disponibilização de mecanismos para permitir o exercício de direitos dos titulares[76]; iv) a adoção de medidas técnicas e

[74]Art. 6º, X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

[75] Art. 6º, I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

[76] Art. 6º, V - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

administrativas de segurança e prevenção adequadas a cada risco verificado[77]; v) estabelecimento de canal de comunicação entre os titulares e agentes, sendo esse o papel do encarregado (artigo 5º, VIII) indicado pelo controlador para intermediar o trato entre titulares e agente, bem como entre este e a ANPD (artigo 41)[78].

Adicionalmente a essas obrigações há duas outras cuja adoção depende de condições diferenciadas, são elas: i) elaboração do relatório de impacto à proteção de dados pessoais, conforme artigo 38, que poderá ser solicitado pela ANPD[79] e a elaboração de avaliação do tratamento baseado no legítimo interesse, conforme artigo10 §3º da LGPD.

Vale fazer uma reflexão sobre os programas de *compliance* que não têm, na prática, a estrutura necessária para exercer a devida proteção. Os programas de *compliance* 'de gaveta', não configuram mecanismos controle e de boa governança, pois não apresentam requisitos mínimos que assegurem a sua efetividade.

Nesse sentido, Ana Frazão, Milena Donato e Vivianne Abílio descrevem dez situações que podem configurar um efetivo programa de *compliance*:

i) Avaliação contínua de riscos e atualização do programa;
ii) Elaboração de Códigos de ética e conduta;
iii) Organização compatível com o risco da atividade;
iv) Comprometimento da alta administração;
v) Autonomia e independência do setor de *compliance*;
vi) Treinamentos periódicos;
vii) Monitoramento constante dos controles e processos inclusive para atualização do programa;
viii) Canais seguros e abertos de comunicação de infrações e mecanismos de proteção dos informantes;

[77] Art. 6º, VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

[78] Art. 6º, V - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

[79] Art. 6º, VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.
VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

> ix) Detecção, apuração e punição das condutas contrárias ao programa de *compliance*. (FRAZÃO; OLIVA; ABILIO, 2020, p. 678).

Muito embora não seja obrigatório, o *compliance* de dados, confere aos agentes diversas vantagens, a primeira é a prevenção de infrações relacionadas à proteção de dados e ainda, a mitigação dos resultados danosos que advirem de descumprimentos.

Em segundo lugar, é inerente a um programa de *compliance* o monitoramento permanente da eficiência dos controles, conforme consta no artigo 50, §2º, I, f da LGPD, visando a pronta identificação de eventual descumprimento, antes que se tangibilize em dano propriamente dito.

Para tanto, a terceira vantagem é construir uma estrutura organizada e transversal na empresa que, baseada em valores e princípios instituídos através de políticas e códigos de condutas, alinhada a outras áreas da organização, em especial, as áreas que exercem atividades de gestão dos ativos de tecnologia, para a criação de uma cultura de observância e cuidados com dados pessoais.

Além desses aspectos corporativos voltados para atuação interna da organização, verifica-se outras vantagens. Em quarto lugar, o aumento da confiança e credibilidade da organização, representando como um diferencial competitivo com alto valor reputacional.

No tocante à quinta vantagem, o *compliance* será o meio de comprovação do tratamento adequado, contribuindo com o afastamento da responsabilidade do agente conforme o artigo 43, II da lei, assim como, demonstrando o cumprimento de deveres como o artigo 8º, §2º (prova do consentimento) e artigo 42§2º (ônus da prova em processo judicial) (OLIVA; ABÍLIO; COSTA, 2021, p. 147).[80]

A sexta vantagem da implantação de um programa de *compliance* de dados tem relação com o critério de redução da sanção aplicada pela ANPD que premia os agentes que comprovarem a adoção das medidas que assegurem segurança e proteção aos dados pessoais, consoante a disposição do artigo 52, §1º.

Para efetivamente obter tais vantagens, o programa de *compliance* de dados requer uma estrutura corporativa sólida e organizada para o atendimento de deveres

[80] Válida de nota a observação de Carlos Konder e Leonardo Fajngold ao refletirem sobre a possibilidade de o *compliance* de dados ser considerado para eventual excludente de responsabilidade em caso de danos decorrentes da malversação de dados, afastando a irregularidade do tratamento de dados pessoais mediante a comprovação de utilização de técnicas apropriadas e disponíveis (KONDER; FAJNGOLD, 2021, p. 352).

de diligência, transparência, informação e segurança dos dados pessoais, construído na medida e no nível dos riscos da atividade do agente pois, somente assim será capaz de demonstrar que as atividades são desempenhadas tomando as precauções necessárias em prol da proteção dos dados pessoais.

Assim, por mais que haja a aplicação de sanções por descumprimentos à lei (*enforcement*), esta é apenas uma parte de um projeto maior para a criação de uma verdadeira cultura de proteção de dados, por meio da utilização da cooperação entre os agentes e a ANPD assumindo papel mais amplo do que mero fiscalizador (FRAZÃO; CARVALHO; MILANEZ, 2022, p. 405).

4.3 Segurança e sigilo

A segurança é um dos pilares para a efetividade da proteção dos dados pessoais e, como já abordado, está previsto no princípio da segurança consoante artigo 6º, VII da LGPD.[81]

Por consequência, a lei destina um capítulo específico para tratar da segurança e boas práticas de governança, no qual estabelece as hipóteses que ameaçam a integridade dos dados especificando-as por acessos não autorizados e incidentes ou ilícitos de destruição, perda, alteração, comunicação ou difusão.

Até o momento a ANPD dispôs os padrões mínimos de segurança apenas para agentes de pequeno porte. Assim, enquanto não forem estabelecidos esses padrões mínimos para a segurança em tratamento de dados de alto risco, assim considerados aqueles tradados em larga escala ou que possam afetar direitos fundamentais e que utilizam tecnologias inovadoras, de vigilância ou ainda que utilizem dados sensíveis, de crianças, adolescentes e idosos; os agentes podem, minimamente, adotar os padrões já existentes, sem prejuízo de outros que advenham com novas orientações da Autoridade Nacional.

De acordo com o Guia orientativo para Agentes de Pequenos Porte emitido pela ANPD, segurança da informação pode ser compreendida pelo

[81] Há na legislação brasileira outras normas que se relacionam com o sigilo e segurança de dados pessoais, nesse sentido há Constituição com disposições de proteção à intimidade e vida privada, artigo 5º, X inviolabilidade do sigilo, artigo 5º, XII, *habeas data*, artigo 5º LXXII; além de previsão em leis infraconstitucionais como o Código de Defesa do Consumidor sobre banco de dados, artigo 43 e o Marco Civil da Internet sobre o tratamento de dados pessoais na rede, artigos 7º, 13 e 15.

> [...] conjunto de ações que visam à preservação da confidencialidade, integridade e disponibilidade da informação. Esse conjunto de ações impacta todo o ambiente institucional das empresas, com objetivo de prevenir, detectar e combater as ameaças digitais [...]. (BRASIL, 2021, p. 1).[82]

Conforme menciona Ana Frazão, a segurança da informação possui quatro vetores decorrentes do princípio da segurança: (i) confidencialidade dos dados: proteção contra a comunicação e difusão; (ii) subsistência dos dados: proteção contra destruição ou perda; (iii) integridade dos dados: proteção contra adulterações, e, de maneira indireta, (iv) disponibilidade dos dados: contra-ataques de *ransomware* ou sequestro de dados (FRAZÃO; PINTO, 2022).

Portanto, é dever do agente de tratamento encontrar soluções eficazes para garantir a segurança dos dados pessoais. Afinal, são considerados irregulares os tratamentos que deixarem de observar a legislação ou quando não atender a expectativa de segurança do titular, conforme previsto no artigo 44 LGPD.

Trata-se de obrigação de adoção de medidas operacionais a serem concebidas no âmbito da Tecnologia da Informação (TI), implementadas e observadas em todas as fases do tratamento de dados.

Nesse sentido, apesar de a LGPD[83] não prever expressamente sobre *privacy by design,* é possível extraí-lo a partir da ideia contida no artigo 46, §2º ao determinar que todas as medidas de segurança deverão ser observadas desde a fase de concepção até a execução do serviço ou produto.

A metodologia *privacy by design* surgiu do movimento *Privacy Enhancing Technologies* (PETs) que enxerga a tecnologia como um instrumento de proteção da privacidade e dos dados pessoais, uma oportunidade de usá-la a favor do titular dos dados. Assim, seriam consideradas toda e qualquer tecnologia que promova a privacidade e proteção de dados por meio de melhorias implantadas na construção dos modelos computacionais.

Há duas principais motivações que justificam a necessidade de segurança e prevenção na proteção de dados pessoais, a primeira relativa ao aumento de episódios de vazamento de dados envolvendo invasão de sistemas ou banco de

[82] Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-guia-de-seguranca-para-agentes-de-tratamento-de-pequeno-porte. Acesso em 17 mar. 2023.
[83] Diferentemente da LGPD, a GDPR estabelece expressamente os critérios de *privacy by design* e *privacy by default* no artigo 25, 2. (BIONI, 2021, p. 191).

dados por terceiros (*hackers*), onde a segurança é comprometida em razão da ação de terceiros; e a segunda relativa a condutas dolosas ou culposas do próprio agente de tratamento que não atenta para seus deveres legais.

Para a ANPD, incidente de segurança

> [...] é qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais. (BRASIL, 2022, p. 1)[84]

De acordo com o Relatório de custos da violação de dados de 2022, emitido pela IBM (2022)[85], 83% das empresas pesquisadas sofreram mais de uma violação de dados, sendo o custo total, em média, avaliado em US$4,35 milhões por violação. Das empresas entrevistadas, 59% não implementam estratégias *zero trust* (abordagem baseada no pressuposto de que as identidades dos usuários, ou a própria rede, já podem estar comprometidas em uma violação), e tiveram um custo médio a mais de US$ 1milhão devido às violações.

Outro dado interessante desse relatório é que, das empresas que afirmaram possuir um plano de resposta a incidentes, 63% obtiveram redução média dos custos associados correspondente a US$ 2,66 milhões nos custos de violação. Isso demonstra que ter um plano de resposta a incidentes, testado regularmente, levou a uma redução considerável nos custos de violação.

Adicionalmente, o Centro de Estudos, respostas e tratamentos de incidentes de segurança no Brasil (CERT.br) contabilizou em 2020, o total de 665.079 incidentes de segurança reportados. [86]

Ainda que esses números retratem incidentes de segurança de maneira global, ou seja, considera violações a dados pessoais e dados operacionais, a partir de tais resultados é possível aferir os altos números envolvidos e por isso, a proteção contra incidentes deve ser pauta prioritária das governanças corporativas.

Nesse sentido, o artigo 46 da LGPD, ao dispor sobre as medidas de segurança de sistemas computacionais que tratam dados pessoais, cria para os agentes a obrigação de adotar salvaguardas para evitar, ou mitigar, incidentes de segurança.

---

[84] Disponível em: https://www.gov.br/anpd/pt-br/assuntos/semana-da-protecao-de-dados-2022/incidentes-de-seguranca-com-dados-pessoais. Acesso em 23 mar. 2023.
[85] Disponível em: https://www.ibm.com/br-pt/reports/data-breach. Acesso em 23 mar. 2023.
[86] Disponível em: https://www.cert.br/stats/incidentes/. Acesso em 23 mar. 2023.

A lei, contudo, não discrimina quais medidas de segurança técnicas devem ser adotadas, deixando a cargo do agente a missão de gerir seus riscos de forma adequada e compatível com o seu modelo de negócio, deixando no mesmo artigo §1º que sejam estabelecidas pela ANPD[87] a definição das diretrizes mínimas dos padrões de segurança técnicas.

É nesse espaço que o *compliance* pode ser um forte aliado do agente no cumprimento da lei. As medidas, do ponto de vista tecnológico, a serem implantadas e monitoradas pelo *compliance* devem estabelecer um ambiente organizacional que permita o processamento e cruzamento de dados de maneira segura a ataques cibernéticos ou adulterações, assim como, a realização de auditorias e consequentemente a identificação dos possíveis responsáveis por danos causados por vazamentos acidentais ou utilização indevida.

Para tanto, um bom programa de *compliance* deve ser responsável por garantir o cumprimento da lei e da regulação, estabelecendo diretrizes organizacionais para a adoção das práticas devidas para seu atendimento[88]. Tais diretrizes são constituídas de acordo com o gerenciamento dos riscos que consiste no processo de identificar, quantificar e administrar as medidas preventivas e mitigadoras, com o intuito de alcançar o equilíbrio entre o tratamento e a minimização de exposição do titular às vulnerabilidades decorrentes dele.

Assim, considerando que de acordo com a responsabilização e prestação de contas, dispostos no artigo 6º X, o agente deve demonstrar diligência na adoção de medidas eficazes e capazes de comprovar o cumprimento dos princípios e regras atinentes à proteção de dados pessoais, tal demonstração pode ser feita por meio da comprovação de um programa de *compliance* de dados sólido e bem estruturado.

Por isso, o *compliance* não pode ser compreendido como mais um custo operacional, mas uma forma de oportunidade em agregar valor reputacional à organização, indo além da capacidade de prevenir sanções.

E ainda, o *compliance* auxilia a governança corporativa na definição da estratégica para que medidas de prevenção, mitigação e aculturamento sejam

[87] Válido de nota que a ANPD já se pronunciou acerca da segurança da informação para agentes de tratamento de pequeno porte. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf. Acesso em 21 mar. 2023.
[88] A ISO/IEC estabelece a norma 27000/2018 para estabelecer boas práticas de segurança da informação.

incorporadas no dia a dia das rotinas operacionais, de maneira que demonstrem que a organização está em busca da conformidade.

Vale destacar que incidentes de segurança também podem ocorrer por falhas humanas (por exemplo perda de um *pendrives*), assim, nem sempre medidas técnicas são suficientes para evitá-los. Por isso, a conscientização e o aculturamento por meio de campanhas de *endomarketing* são importantes para a promoção da segurança dos dados pessoais tratados nas organizações.

Ocorre que nem sempre empresas conseguem, por questões de porte ou financeiras, estruturar uma área de *compliance* para tratar de tais questões. Por isso, tendo em vista o objetivo maior de segurança dos dados pessoais, a ANPD publicou o Guia orientativo de Segurança da informação para agentes de tratamento de pequeno porte[89] no qual apresenta algumas recomendações de medidas a serem adotadas as quais são listadas nos parágrafos a seguir.

No que diz respeito às medidas técnicas que a LGPD faz referência, de acordo com o guia supracitado, podem ser: i) controle de acesso; ii) segurança dos dados pessoais armazenados; iii) segurança nas comunicações; e iv) manutenção de programa de gerenciamento de vulnerabilidades.

Quanto ao controle de acesso, deve estabelecer níveis de acesso de cada usuário para garantir que somente pessoas autorizadas tenham acesso aos dados pessoais. O controle de acesso deve observar fatores: identificação, obrigatoriedade autenticação por meio de login e senhas exclusivos, podendo adotar a autenticação multi-fatores[90] (MFA) e controle do registro de acessos, autorização para estabelecer a identificação como obrigatória e auditoria para ter o controle do histórico de navegação e uso do sistema.

No que diz respeito à segurança dos dados pessoais armazenados, deve-se levar em consideração inicialmente a quantidade e natureza dos dados armazenados. Significa dizer que o agente deve tão-somente reter dados que são necessários (artigo 6º III) para o desenvolvimento do negócio com finalidade específica (artigo 6º, I) e compatível com aquela informada ao titular.

---

[89] Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-guia-de-seguranca-para-agentes-de-tratamento-de-pequeno-porte. Acesso em 16 mar. 2023.

[90] A autenticação multi-fatores (MFA) utilizada para acessar sistemas ou base de dados que contenham dados pessoais, consiste em estabelecer uma camada adicional de segurança para o processo de login da conta, exigindo que o usuário forneça duas formas de autenticação.

Adicionalmente, o agente deve fazer a gestão e controle das atividades de transferências, preferencialmente por meio tecnológicos, para manter o controle da guarda, com isso deve-se evitar que dados pessoais de sistemas corporativos sejam transferidos para arquivos externos da organização, como *pendrives*.

Ainda no aspecto da segurança de dados armazenados, a organização deve estabelecer política de *backup* (cópias de segurança) que são submetidos aos mesmos cuidados dos arquivos em uso, inclusive no que diz respeito ao estabelecimento de prazo determinado para o armazenamento.

Cabe ressaltar que a retenção de dados sensíveis deve ser objeto de maior diligência por parte do agente adotando, além das medidas citadas, soluções que impeçam a identificação do titular, como a pseudoanonimização[91] bem como a criptografia.

Acerca da anonimização vale esclarecer que são procedimentos técnicos de informática que permitem a desvinculação dos dados pessoais à pessoa natural titular, retirando, com isso, a capacidade de identificação efetiva ou potencial da pessoa, conforme artigo 5º XI e 12 § 4º da LGPD.

Quanto a segurança das comunicações, pretende-se que o agente adote medidas de cuidem da transmissão, utilizando conexões cifradas (uso de TLS/HTTPS) ou aplicativos com criptografia ponta aponta. Além disso, no que diz respeito ao tráfego de rede, devem ser adotadas diligências como sistema firewall para monitorar, detectar e bloquear conexões a redes não confiáveis. Sugere-se para tanto, o uso de *firewall* de aplicação web (*Web Application Firewall* – WAF).

Em igual medida, utilização de antivírus integrados, ferramentas *anti-spam* e filtros devem ser usados nos serviços de e-mail da organização.

Nesse aspecto, novamente questões com sigilo e confidencialidade dos dados, especialmente no tocante a dados sensíveis, por isso, exige-se que a transmissão utilize canais restritos, observados os protocolos de acesso supracitado.

O último tópico relacionado às boas práticas aplicadas em medidas técnicas refere-se à manutenção de programa de gerenciamento de vulnerabilidades. Esse ponto refere-se ao monitoramento e implantação de versões atualizadas de sistemas e aplicativos, de maneira que sejam utilizadas as últimas versões disponibilizadas

[91] Pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro (art.13 §4 da LGPD).

pelos desenvolvedores. Demanda, portanto, a instalação de correção de segurança (*patches*). Além disso, a adoção e atualização dos softwares de antivírus ou *antimalwares*, que detectam, impedem e tomam medidas contra programas maliciosos, como vírus. Por fim, varreduras periódicas de antivírus em todos os dispositivos da organização.

Além das medidas supracitadas, há ainda, para as organizações que utilizam serviços em nuvem, como por exemplo servidores, bando de dados e sistemas com análise e inteligência pela internet, é imprescindível verificar se os fornecedores destes serviços adotam as medidas previstas em recomendações internacionais e as boas práticas de segurança da informação, utilizando-se para isso mecanismos de nível de serviço (*Service Level Agreemen*t – SLA).

No que diz respeito às medidas administrativas na forma do artigo 46 da LGPD, cuja finalidade é promover a segurança e demonstrar a boa-fé e diligência do agente, devem ser adotadas: i) política de segurança da informação; ii) conscientização e treinamento; e iii) gerenciamento de contratos.

A primeira, relativa ao estabelecimento da política de segurança da informação[92], que geralmente consiste em um documento formalizado pela organização, contendo as diretrizes estratégicas com o objetivo de estruturar e implementar as medidas sobre os riscos identificados. Importante ressaltar que a política deve ser periodicamente revisada para se ajustar às novas condições ou retificar experiências pretéritas.

A segunda medida é conscientização e treinamento que irão estabelecer a cultura da segurança da informação na organização, de modo que no dia a dia das atividades organizacionais os colaboradores tomem os cuidados necessários sobre suas obrigações e responsabilidades no tratamento dos dados. Nesse aspecto, importante ressaltar que os empregados podem ser vítimas de *phising* enquanto utilizam os e-mails corporativos. Por isso, a empresa deve divulgar, constantemente, o cuidados que os empregados devem ter para evitar de serem vítimas de incidentes de segurança como esse.

Com relação ao gerenciamento de contratos como terceira medida de segurança administrativa, e i) contempla a relação de trabalho com os empregados

[92] "Trata-se de documento que apresenta as diretrizes para garantir a segurança das informações, prescrevendo ações, proibições, boas práticas e até mesmo sanções." (SOUZA, 2020, p. 430).

consiste na assinatura de um *Non Disclosure Agreement* (NDA) pelos empregados para que se comprometam e se responsabilizem por dados confidenciais no desempenho das suas atividades laborais; ii) relações comerciais com prestadores de serviços ou fornecedores para definição de papeis e responsabilidades quanto à observância à legislação. Nesse ponto, os contratos com empresas de TI devem ter especial atenção no que se refere à inclusão de cláusulas que assegurem a segurança da informação, regras de compartilhamento, relação entre controlador e operador e cláusula para dispor sobre a vedação quanto a tratamentos incompatíveis com aqueles definidos em contrato.

Após observar as medidas administrativas básicas que, no entendimento da ANPD são aplicáveis aos agentes de tratamento de pequeno porte, vale ressaltar que, para empresas de médio e grande porte, ainda que não exista uma orientação própria emitida pela autoridade, espera-se que além daquelas previstas no guia, esses agentes se utilizem de outras normas e práticas de marcado que sejam adequadas ao seu porte e risco.

4.4 Boas práticas e Governança

Consoante dispõe o artigo 50, a lei faculta aos agentes, individualmente ou por associações, a adoção voluntária de boas práticas e de governança que estabeleçam condições de organização, regime de funcionamento, procedimentos para atendimentos aos direitos dos titulares ou às obrigações específicas, bem como, ações educativas, mecanismos de supervisão e mitigação de riscos entre outros aspectos relacionados ao tratamento de dados pessoais.

Desse modo, para estabelecerem boas práticas os agentes de tratamento devem estipular uma estrutura corporativa que observe as condições de organização, regime de funcionamento, procedimentos, normas de segurança, atendimento aos padrões técnicos e as obrigações específicas, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos, na forma do artigo 50§1º da LGPD.

Adicionalmente, no §2º do mesmo artigo, critérios como natureza dos dados, escopo, finalidade, probabilidade e gravidade dos riscos envolvidos, são indicados como parâmetros para o gerenciamento dos riscos.

Assim, a adequação do agente à LGPD perpassa pelo estabelecimento do objeto, ou seja, quais dados serão coletados, a finalidade explícita, a amplitude de utilização e a necessidade da coleta a fim de demonstrar a sua efetiva utilização.

De maneira complementar, a lei indica o emprego de arquiteturas de segurança de dados nos sistemas utilizados (artigo 49), ações de treinamento e conscientização corporativas e implantação de processos internos de gestão de riscos para o monitoramento e mitigação dos eventos de risco (artigo 50). A esses padrões de segurança, o agente deverá ainda agregar, quando necessário, outros de acordo com o negócio e adequados ao mercado em que atua.

Guiado pelos princípios da segurança e da prevenção previstos, o agente precisa observar os requisitos mínimos para adoção das medidas de segurança técnica e administrativas que deverão ser implementadas de modo a proteger seus bancos de dados e comunicações contra vazamentos e acessos não autorizados, sob pena de aplicação das sanções administrativas aplicáveis pela Autoridade Nacional e eventual responsabilização civil, conforme artigo 44 (SOUZA, 2020, p. 420-421).

Entretanto, para os agentes se adequarem às obrigações estabelecidas na LGPD, é preciso investimentos não apenas financeiros mas, principalmente dedicação de toda a organização para instituir o uso ético dos dados pessoais, e, essencialmente, o comprometimento da alta direção, sem a qual dificilmente o tema ocupará uma pauta na governança estratégica do agente.

4.5 Autoridade Nacional de Proteção de dados pessoais

Como foi visto até o momento, a LGPD privilegia uma abordagem facilitadora e viabilizadora para o tratamento dos dados pessoais deixando a cargo dos agentes, dentro dos limites legais, a definição da estratégia mais eficiente para o seu cumprimento, sem relegar o viés sancionatório das atividades desalinhadas com a Lei.

Essa abordagem é fruto da construção regulatória híbrida, baseada no incentivo para a adoção de boas práticas de governança de dados pelos agentes ao mesmo tempo que estabelece os comandos e sanções em caso de descumprimento legal.

De igual modo, a abordagem baseada em riscos obriga o agente a prevenir, detectar e combater as ameaças de violação aos direitos fundamentais protegidos pela Lei. Esse modelo permite o ajuste adequado de cada agente aos riscos relacionados ao tratamento de dados pessoais, e permite maior eficácia das medidas a serem adotadas pelos agentes.

O papel da Autoridade Nacional de Proteção de Dados nesse contexto é fundamental para a efetiva proteção de dados pessoais pois, considerando que a LGPD é uma lei com forte carga principiológica, a atuação regulatória tem o objetivo de dar maior segurança jurídica por meio de instrução e detalhamento do arcabouço normativo.

Desde a elaboração da LGPD (enquanto projeto de lei) e mesmo após sua promulgação, houve muitos debates sobre a natureza jurídica, constituição e competências da Autoridade Nacional. Para que a instituição cumpra os objetivos delineados na Lei deve ser independente técnica e financeiramente, por isso, a criação da ANPD no Brasil foi envolta de muitas indefinições.

Dentre as disposições que foram objeto de veto presidencial[93], os artigos 55 a 59 que criavam e estabeleciam a competência da ANPD, foram retirados em razão da inconstitucionalidade por vício de iniciativa.

No mesmo ano, a Medida Provisória 869/2018, posteriormente convertida na Lei 13.853/2019, criou a ANPD, situando-a como sendo um órgão vinculado à Presidência da República.

Vale a dizer que no modelo legal adotado no Brasil inspirado no padrão europeu[94], a autonomia da instituição e sua especialização técnica são primordiais para seu funcionamento eficaz, considerando que, nitidamente, a proteção de dados pessoais envolve setores públicos e privados na figura dos agentes de tratamento.

O principal receio quanto à Lei 13.853/2019 era assegurar a necessária independência do órgão mesmo estando vinculado ao Poder Executivo, ainda que

[93] Mensagem de veto nº 451, DE 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Msg/VEP/VEP-451.htm. Acesso em 05 jun 2023.

[94] Leonardo Parentoni discorre sobre o modelo proposto na União Europeia onde a autoridade de proteção de dados pessoais são estruturadas geralmente para tratar especificamente o tema, considerando independente a autoridade baseada em requisitos constantes na GDPR como i) não estar sujeitas a influências externas; ii) recursos humanos, financeiros, técnicos e infraestrutura necessários para o desempenho das funções; iii) selecionar e dispor sobre recurso humano e iv) independência financeira. (PARENTONI, 2021. p. 169-170).

houvesse a disposição do artigo 55-B que assegurava a autonomia técnica e decisória da ANPD.

À guisa das críticas existentes na época quanto a vinculação da autoridade, vale transcrever a ponderação de Leonardo Parentoni: “o fato de estar (a ANPD) formalmente inserida na estrutura da Presidência da República, por si só, não é certeza de que faltará isenção dos seus diretores, para atuar de forma alheia a pressões” (PARENTONI, 2021. p. 170).

De todo modo, a mesma Lei 13.853/2019 já previa no seu artigo 55-A §1º e §2º que a natureza jurídica da ANPD era transitória, podendo ser transformada pelo Poder Executivo em entidade da administração pública federal indireta submetida ao regime autárquico e vinculada à Presidência da República, avaliação que ocorreria 2 anos após a estruturação regimental da instituição.

Foi por meio do Decreto nº 14.460/22 que a ANPD foi transformada em autarquia de natureza especial, mantidas a estrutura organizacional e a competências, bem como dotada de autonomia técnica e financeira, contudo, ainda vinculada à Presidência da República.

Com isso, preencheu-se os alguns requisitos necessários para a atuação da instituição, salvo a desvinculação do Poder Executivo. A última e mais recente alteração ocorreu com o Decreto 11.348/23 que vinculou a ANPD ao Ministério da Justiça.

A matéria da proteção de dados pessoais possui uma posição transversal na sociedade movida a dados, visto que não se limita a um setor econômico específico, mas a todos aqueles que realizam algum tipo de tratamento conforme previsto na LGPD.

Diante da complexidade decorrente da multiplicidade de atores, a ANPD deve ser capaz de dar respostas rápidas e eficazes aos diversos tipos e níveis de agentes de tratamento, bem como, apresentar regulação dinâmica o suficiência para que corresponda às mudanças tecnológicas.

Sob esse aspecto, torna-se necessária a adoção de uma regulação responsiva, com a participação da sociedade civil, academia e impressa na construção do

arcabouço regulatório[95]. A disposição contida no artigo 55-J, inciso XIV[96] da LGPD segue essa lógica responsiva diante de tanta diversidade e dinamicidade, permitindo que a Autoridade Nacional tome decisões transversais e estratégicas aplicadas em todos os níveis e com maior grau de credibilidade e efetividade.

Ao analisar as atribuições da ANPD em conjunto com o Planejamento Estratégico da instituição, é clara a missão de zelar pela proteção dos dados pessoais[97]. Para tanto, as atribuições previstas na LGPD no artigo 55-J permitem que a ANPD execute, basicamente, três funções: orientação, regulação e fiscalização.

No que diz respeito à função orientativa, podem ser destacadas as seguintes atribuições: a promoção na população de conhecimento sobre as normas e as políticas públicas em matéria de proteção de dados pessoais e das medidas de segurança (inciso VI) e o estímulo para a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis (inciso VIII).

Quanto à função reguladora, possuem destaque: elaboração de diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade (inciso III) e edição de regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei (inciso XIII).

E por fim, relativas à função de fiscalização, destacam-se as atribuições: de fiscalização e aplicação de sanções em caso de tratamento de dados realizado em descumprimento à legislação (inciso IV) e realização de auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização sobre o tratamento de dados

[95] No site da ANPD ficam disponíveis todas as formas de incentivo à participação popular ocorridas até o momento. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/audiencias-e-consultas-publicas/participacao-social. Acesso em 04 jun. 2023.

[96] Art. 55-J Compete à ANPD: XIV – ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento;

[97] Observa-se no Planejamento Estratégico da ANPD para 2021-2023 os objetivos estratégicos delineados nos três pilares de atuação da autoridade, são eles: 1) Promover o fortalecimento da cultura e Proteção de Dados Pessoais; 2) Estabelecer ambiente normativo eficaz para a Proteção de Dados Pessoais; e 3) Aprimorar as condições para o cumprimento das competências legais. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/planejamento-estrategico-anpd-versao-2-0-06072022.pdf. Acesso em 18 mai. 2023.

pessoais efetuado pelos agentes de tratamento, incluído o poder público (inciso XVI).

A insegurança jurídica ocasionada pelos altos e baixos no processo de criação e implantação da ANPD, repercutiu diretamente na atuação da instituição. Desde a constituição até o momento atual, é possível notar o esforço na priorização de temas mais prementes de regulação, conforme se afere das Agendas Regulatórias 2021-2022[98] e 2023-2024[99].

A ANPD publicou regras para viabilizar a sua atuação, criou seu Regimento Interno[100], instituiu o Comitê de Governança[101], estabeleceu o processo de regulação[102] e o processo de fiscalização e sancionatório[103].

Igualmente, foram elaborados guias orientativos, notas técnicas e estudos técnicos. Quanto aos guias orientativos (assim como os fascículos) já publicados pela ANPD, tem por objetivo determinar instruções relevantes e, por vezes, definir conceitos que não estão claros na LGPD. E documentos aproximam os interessados ao efetivo cumprimento da Lei.

Vale ressaltar que na cultura brasileira, a população ainda possui pouco conhecimento acerca da importância da proteção de dados pessoais, ainda há muito a ser feito em termos de conscientização tanto os titulares, como dos agentes de tratamento. A ANPD, nesse contexto, possui papel relevante no que diz respeito ao estímulo para a mudança de cultura na sociedade.

De acordo com a pesquisa Grupo Daryus[104] o fato de 80% das empresas brasileiras ainda não estão adequadas à Lei, demonstra que a ANPD precisa ampliar a conscientização sobre a relevância da proteção de dados pessoais, evitando com isso, o viés sancionatório que lhe compete.

---

98 Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313 Acesso em 19 mai. 2023.

99 Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-anpd-n-35-de-4-de-novembro-de-2022-442057885 Acesso em 19 mai. 2023.

100 Portaria nº 1, de 8 de março de 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-1-de-8-de-marco-de-2021-307463618 Acesso em 18 mai. 2023.

101 Portaria nº 15, de 2 de julho de 2021. Disponível em: https://www.in.gov.br/web/dou/-/portaria-n-15-de-2-de-julho-de-2021-329780585. Acesso em 18 de mai. 2023.

102 Portaria nº 16, de 8 de julho de 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-16-de-8-de-julho-de-2021-330970241. Acesso em 18 de mai. 2023.

103 Resolução CD/ANPD nº 1, de 28 de outubro de 2021, posteriormente retificado pela Resolução CD/ANPD nº 4, de 24 de fev. 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/regulamentacoes-da-anpd/resolucao-cd-anpd-no1-2021. Acesso em 18 de mai. 2023.

104 Disponível em: https://materiais.idesp.com.br/pesquisa-protecao-e-privacidade-de-dados. Acesso em 07 jun.2023.

A progressiva exposição dos titulares no ambiente *on line* associado ao aumento dos incidentes de segurança, obrigam os agentes de tratamento à adequação à Lei.

Em que pese a grande importância da publicação de orientações por parte da ANPD, vale destacar que aqueles que buscam aplicar tais instruções na prática, de certo modo, são titulares ou agentes que já reconhecem a importância da proteção de dados pessoais. Por outro lado, ainda há muitos agentes de tratamento que sequer iniciaram o processo de adequação, e é com esses que a ANPD deve tomar medidas de monitoramento mais ágeis e repressivas.

Assim, em outubro de 2021 a ANPD promulgou a Resolução nº 1 CP/ANPD para estabelecer o processo de fiscalização e o processo administrativo sancionador prevendo os ritos e critérios a serem adotados nas fiscalizações, em consonância com a competência prevista no artigo 52 da LGPD. Contudo, a resolução que trata da dosimetria das sanções foi publicada em fevereiro de 2023, pela Resolução CD/ANPD nº 4/2023.

Muito embora a competência sancionatória supracitada, o processo fiscalizatório da ANPD tem, dentre as premissas previstas[105], o estímulo à promoção da cultura da proteção de dados pessoais e a adoção de medidas proporcionais ao risco identificado e à postura dos agentes regulados.

Ainda que a LGPD faculte a adoção de governança dos dados por parte dos agentes, ela está nitidamente ligada abordagem preventiva de riscos.

[105] Resolução CD/ANPD nº 1/2021 Art. 17. O processo de fiscalização da ANPD observará as seguintes premissas:

I - alinhamento com o planejamento estratégico, com os instrumentos de monitoramento das atividades de tratamento de dados e com a Política Nacional de Proteção de Dados Pessoais e da Privacidade;

II - priorização da atuação baseada em evidências e riscos regulatórios, com foco e orientação para o resultado;

III - atuação integrada e coordenada com órgãos e entidades da administração pública;

IV - atuação de forma responsiva, com a adoção de medidas proporcionais ao risco identificado e à postura dos agentes regulados;

V - estímulo à promoção da cultura de proteção de dados pessoais;

VI - previsão de mecanismos de transparência, de retroalimentação e de autorregulação;

VII - incentivo à responsabilização e prestação de contas pelos agentes de tratamento;

VIII - estímulo à conciliação direta entre as partes e priorização da resolução do problema e da reparação de danos pelo controlador, observados os princípios e os direitos do titular previstos na LGPD;

IX - exigência de mínima intervenção na imposição de condicionantes administrativas ao tratamento de dados pessoais; e

X - exercício das atividades fiscalizatórias que melhor se adequem às competências da ANPD.

Neste diapasão, os artigos 50 e 51 da LGPD, elencam medidas de boas práticas de governança, facultando e, acima de tudo, incentivando, os agentes de tratamento a adoção de medidas que garantam e evidenciem a proteção dos dados.

Na Agenda Regulatória 2023-2024 verifica-se a previsão de iniciativa para a edição de orientações de boas práticas na qual a ANPD deve estabelecer em breve as diretrizes, dentro dos limites estabelecidos pela LGPD, de maneira que os agentes de tratamento de dados possam ter clareza sobre as instruções para adequar seus processos corporativos.

Nesse cenário, instituir um programa de *compliance* de dados implica na adoção de uma estrutura que requer a identificação do cenário corporativo perante o tratamento de dados para que seja possível a adequação às normas já existentes, ainda que haja carência de instruções de como executá-las na prática. Essa carência ocorre especialmente para os agentes de tratamento de dados com alto risco.

Até o momento, a ANPD orienta apenas quanto aos agentes de pequeno porte, para os demais, o que deve ser feito por ora, é a análise dos estudos, notas técnicas já emitidas para dali extrair a melhor atuação para esses agentes.

De todo modo, o primeiro passo, é a instauração do programa de *compliance*, para a criação de um ambiente corporativo com a finalidade de cumprimento da lei e da regulação existente, sem prejuízo de realizar a atualização do programa na medida em que novas orientações forem publicadas pela Autoridade.

Naturalmente, a existência do princípio da responsabilização e prestação de contas estabelece um dever para os agentes pela atividade de tratamento de dados demonstrar que está tomando as medidas efetivas para o cumprimento da lei e da regulação. A forma com a qual o agente de tratamento evidenciará à ANPD a efetividade no cumprimento é a partir das evidências contidas no programa de *compliance* de dados bem estruturado e cercado de medidas capazes de comprovar a prevenção dos riscos que está sujeito. Isso porque a ANPD deve considerar os riscos em função do comportamento dos agentes e de como ele aloca recursos para a adoção de ações compatíveis com os riscos.

Os dispositivos da LGPD nos quais há a referência a riscos são relatório de impacto (Artigo 5º XVII e artigo 38), incidentes de segurança (artigo 48), nos programas de governança em privacidade (artigo 50).

Vale dizer que a LGPD não apresenta uma definição precisa do que é considerado risco, compete à ANPD regular sobre os critérios que serão considerados para que o agente demonstre a regularidade da sua atividade de tratamento.

Recentemente, a ANPD publicou no seu site uma lista de esclarecimentos acerca da Relatório de impactos à Proteção de Dados, onde aborda a questão do risco, fazendo referência ao Guia Orientativo para tratamento de dados de empresas de pequeno porte de onde pode-se extrair a interpretação acerca de alto risco. Enquanto não se tem uma regulação efetiva sobre o tema, a página pode ajudar a esclarecer algumas dúvidas e servem de orientação aos agentes.

Nesse sentido, a ANPD recomenda a elaboração do RIPD, usando exemplos como: se o tratamento de dados pessoais for em larga escala; envolver dados sensíveis; ou ainda se o tratamento for por ferramenta automatizada, da qual possa resultar a negativa para o exercício de um direito ou para a utilização de um serviço.

Como informa na ANPD tais critérios não são exaustivos, ficando a cargo do agente, a verificação da circunstâncias que contemplam impactos à direitos fundamentais dos titulares e a probabilidade de ocorrência no caso concreto para que adote as medidas de prevenção e segurança adequadas.

Mesmo com esses esclarecimentos, permanece a preocupação quando a necessidade de avaliação dos riscos e as formas efetivas para a mitigação. Nesse sentido, espera-se que a ANPD elabore recomendações mais assertivas que contribuam efetivamente para a construção dos padrões de conduta esperados para os programas de *compliance* de dados.

5 CONCLUSÃO

Os avanços tecnológicos ocorridos nas últimas décadas transformaram de maneira sem precedentes o modo de viver em sociedade, impactando sobremaneira aspectos sociais, econômicos e políticos.

Este fenômeno foi uma consequência da massificação do uso da internet, dispositivos inteligentes, inteligência artificial, dentre outras Tecnologia da Informação e Comunicação disruptivas, que causaram a fusão entre os ambientes físico e digital e, ao mesmo tempo, possibilitaram uma escalada quantitativa e qualitativa de acumulação e processamento de dados pessoais.

Assim, na economia movida a dados, organizações coletam, processam e analisam dados pessoais para obtenção de resultados de predição comportamental e tendências dos titulares com a finalidade de usá-los para os propósitos do negócio.

Ao analisar os impactos do fenômeno causado pelas mudanças promovidas pelo desenvolvimento tecnológico, Shoshana Zuboff cunhou o termo Capitalismo de vigilância que consiste em "[...] uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais dissimuladas de extração, previsão e vendas." (ZUBOFF, 2020, p. 8).

O capitalismo de vigilância originou-se com o uso de algoritmos para aferição dos comportamentos *online* dos usuários para obter melhorias nos próprios serviços, em ciclos de *feedback*. Contudo, logo se percebeu que as vantagens da análise comportamental e a sua capacidade de predição poderiam servir para publicidade direcionada.

Contudo, algoritmos projetados para coletar, selecionar e processar informações das mais variadas possíveis, direta e indiretamente, por meio da aferição de comportamentos *on-line* com a finalidade de traçar perfis das pessoas, se usados indiscriminadamente, podem ameaçar direitos fundamentais de privacidade, liberdade e livre desenvolvimento da personalidade.

Isto porque, modelos são programados a partir da realidade, e com isso transpõem para o ambiente digital condições existentes na sociedade. Assim vieses humanos podem ser replicados automaticamente nos algoritmos gerando situações de injustiças e discriminações. Cathy O'Neil chamou esses softwares de "armas de

destruição em massa", pois são carregados tendências sociais muitas vezes repletos de opressão e discriminação, enquanto reforçam o poder.

Assim, a Tecnologia da Informação e Comunicação contribuiu para uma nova forma de controle social, muito sutil, na qual os indivíduos têm seus dados extraídos no uso de sistemas ou dispositivos conectados à internet que além dos usos inerentes ao bem ou serviço, servem de matéria prima para atividades outras, diferentes daquelas para as quais está sendo usado.

No princípio, alguns discursos retóricos a favor do fim da privacidade foram usados para fundamentar a manutenção do uso dos dados pessoais de forma indiscriminada em um estado de total falta de regulação sobre o tema.

No entanto, para a proteção da dignidade da pessoa humana, foi necessário ampliar as proteções disponíveis antes conferidas apenas às pessoas físicas, para a sua projeção eletrônica, já que relações estavam sendo estabelecidas no ambiente digital.

Todo esse movimento protetivo de resgate da pessoa humana face a despossessão dos seus dados, decorrente da economia movida a dados, se deu ao longo de décadas e derivou a evolução regulatória para dar respostas jurídicas consistentes à proteção de dados pessoais.

Neste percurso, enquanto a proteção de dados era vista como um direito implícito derivado de direitos da privacidade, da liberdade e do livre desenvolvimento da personalidade, surgiu a noção de autodeterminação informativa, que consiste no direito do titular em controlar o fluxo dos seus dados e quem deles pode fazer uso.

Paralelamente, uma vez identificada a existência de uma grande assimetria de poder entre agentes e titulares dos dados pessoais, verificou-se que, mesmo com a autodeterminação informativa, há casos em que o mero o consentimento é incapaz de dar a devida proteção à pessoa natural.

Assim, o reconhecimento do direito autônomo da proteção de dados mostrou-se fundamental para frear a tendência de normalização da exploração dos dados pessoais para todo e qualquer fim.

Diversas discussões acerca da adoção de uma regulação com abordagem ampla, harmônica e cogente que contemplasse a proteção de dados como um direito autônomo, ocorreram em todo o mundo, mas foi em 2016, com a publicação do

Regulamento Geral de Proteção de dados (GDPR), que a regulação sobre a proteção de dados foi contundente, repercutindo em diversos países.

Desta forma, seguindo a tendência da linha adotada na Europa e considerando a tecnologia atual e a que está por vir, o ordenamento jurídico brasileiro, promulgou a Lei Geral de Proteção de Dados Pessoais em 2018, com o claro objetivo de proteção dos dados pessoais para impor limites a sua coleta e operacionalização com vistas à salvaguarda do titular.

A lei brasileira de caráter geral, se prestou a unificar o entendimento sobre a proteção de dados pessoas já existentes em legislações infraconstitucionais esparsas, utilizando para isso, técnica legislativa das cláusulas gerais, por meio de conteúdo jurídico indeterminado e princípios de maneira a estabelecer o mínimo tangível de conteúdo normativo para que seja adaptado às situações concretas.

Acerca da principiologia da LGPD, além dos fundamentos previstos no artigo 2º, a lei elenca no artigo 6º os princípios essenciais aplicáveis ao tratamento de dados pessoais, reconhecendo que eles pertencem a seus titulares, mas que, ao mesmo tempo, são essenciais para movimentar a sociedade.

Por isso, a lei brasileira, ao reconhecer a necessidade de equilibrar a proteção dos dados pessoais e autorizar o fluxo de dados, adota a abordagem baseada em riscos. Significa que a lei estabelece os limites e critérios autorizativos para o uso dos dados pessoais, obrigando os agentes a adequar suas atividades para garantir segurança no tratamento de dados. Essa abordagem baseada em riscos, demonstra a intenção de construir uma regulação eficaz, abrangente e adaptável aos modelos de negócio dos agentes.

Desta maneira, a lei dispõe os requisitos que autorizam o agente realizar o tratamento dos dados desde que devidamente justificado em, ao menos uma, base legal, levando em consideração a natureza dos dados (pessoal, sensível, anonimizado), obrigando-o à adoção de medidas de segurança para alcançar o objetivo maior de proteção dos dados pessoais.

Assim, a regulação impõe obrigações aos agentes de acordo com os níveis de risco de exposição do titular conforme o tipo de tratamento realizado, dispondo, para tanto, de ferramentas de *enforcement* e de *accountability* que permitem à Autoridade Nacional de Proteção de Dados avaliar a estratégia mais adequada ao contexto.

A previsão de sanção em caso de descumprimento das obrigações legais é insuficiente para a efetiva proteção de dados, porque o objetivo é assegurar valores fundamentais que são naturalmente irreparáveis. O projeto maior perseguido pela lei brasileira é a disseminação de uma cultura baseada na proteção de dados pessoais.

Para isso, utilizou-se do modelo de corregulação, apostando, para o cumprimento da lei, em uma perspectiva de legitimidade, ou seja, a lei estimula a adesão voluntária dos agentes às boas práticas de governança de dados, conforme previsão do artigo 50.

Nesse sentido, incentiva a proatividade dos agentes em estabelecer estruturas organizadas que demonstrem o seu comprometimento com a proteção dos dados.

Desse modo, o agente ao instituir uma estrutura organizada de governança de dados, garante o cumprimento da regulação por meio da adoção de políticas e processos corporativos adequados aos modelos de negócio para salvaguarda dos impactos decorrentes dos riscos no tratamento de dados, conferindo a transparência necessária para estabelecer uma relação de confiança e segurança aos direitos dos titulares.

Assim, o *compliance* de dados pode ser valioso aliado dos agentes no apoio a adoção de boas práticas e governança no atendimento aos princípios do artigo 6º, em especial da boa-fé, adequação, da transparência, da segurança, da prevenção e da responsabilização e prestação de contas, bem como a regulação da ANPD.

Em que pese a instalação de um bom programa de *compliance* pelas organizações, possa impactar seus custos de operação, é necessário não apenas em razão do risco de sanções ou responsabilizações, mas porque tem se tornado um fator reputacional cada vez mais relevante perante os titulares e o mercado como um todo.

As preocupações com o futuro da humanidade diante dos avanços tecnológicos têm sido pauta de diversas discussões jurídicas, e o direito tem o papel fundamental nesse contexto de definição da tutela dos bens jurídicos relevantes e quais as expectativas se têm sobre eles, diante de tantas incertezas.

A rigor, não é possível saber quais serão as próximas inovações e como elas irão impactar os seres humanos, contudo a legislação de proteção de dados tem o

papel de definir quais os limites que não podem ser ultrapassados, sob pena afrontarem direitos fundamentais do ser humano.

Vale ressaltar, que a ANPD nesse contexto é uma importante instituição para dar efetividade à lei, por meio das suas atribuições e papel estratégico na promoção da proteção de dados no Brasil. Mas para tanto, espera-se que após sua estabilização como autarquia de natureza especial, a ANDP prossiga na sua missão com total independência técnica e financeira.

A adoção do *compliance* de dados como um mecanismo de aculturamento organizacional para o cumprimento da lei e da regulação, apresenta-se paralelamente como um instrumento de propagação da cultura da proteção dos dados pois, além do fator reputacional no mercado, pode funcionar para disseminar a relevância da segurança dos dados e do caráter preventivo da sua proteção na sociedade.

Desse modo, citando Stéfano Rodotà (2008, p. 20-21) "[...] a proteção de dados constitui não apenas um direito fundamental entre outros: é o mais expressivo da condição humana contemporânea [...]", eis que merece que esta consciência se refletia em um novo ativismo da comunidade empresarial.

6 Referências bibliográficas

ALBERGOTTI, Reed. Facebook Experiments Had Few Limits. **The Wall Street Journal**, p. 1-4, jul. 2014. Disponível em: https://www.wsj.com/articler/facebook-experiments-had-few-limits-1404344378. Acesso em 15 jan. 2023.

BIONI, Bruno Ricardo; RIELLI, Mariana M. A construção multissetorial da LGPD: história e aprendizados. *In*: BIONI, Bruno Ricardo. **Proteção de dados**: contexto, narrativas e elementos fundantes. Curitiba: Appris, 2022. p. 15-47.

BIONI, Bruno Ricardo; ZANATTA, Rafael A. F. A infraestrutura jurídica da economia de dados: dos princípios de justiça às leis de dados pessoais. *In*: BIONI, Bruno R. **Proteção de dados:** contexto, narrativas e elementos fundantes. Curitiba: Appris, 2022. p. 67-103.

BIONI, Bruno Ricardo. Inovar pela lei. *In*: BIONI, Bruno Ricardo. **Proteção de dados:** contexto, narrativas e elementos fundantes. Curitiba: Appris, 2022. p. 61-65.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 3. ed. São Paulo: Editora Forense, 2021.

BIONI, Bruno Ricardo. Regulação de dados é uma janela de oportunidade. *In*: BIONI, Bruno R. **Proteção de dados**: contexto, narrativas e elementos fundantes. Curitiba: Appris, 2022. p. 57-59.

BIONI, Bruno; MENDES, Laura S. Regulamento europeu de proteção de dados pessoais e a Lei Geral brasileira de proteção de dados: mapeando convergências na direção de um nível de equivalência. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena D. **Lei Geral de proteção de dados pessoais e suas repercussões no Direito brasileiro**. 2. ed. São Paulo: Thomson Reuters, 2020. p. 792-814.

BRANCO, Sérgio. As hipóteses de aplicação da LGPD e as definições legais. *In*: MULHOLLAND, Caitlin. **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago, 2020. p. 15-42.

BRASIL. **ANPD publica Guia de Segurança da Informação para Agentes de Tratamento de Pequeno Porte.** Brasília, DF: ANPD, 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-guia-de-seguranca-para-agentes-de-tratamento-de-pequeno-porte. Acesso em 24 mar. 2023.

BRASIL. Supremo Tribunal Federal. **STF RE 673.707, Relator Ministro Luiz FUX, Tribunal Pleno, julgado em 17/06/2015**. Brasília, DF: STF, 2015.

BRASIL. Supremo Tribunal Federal. **STF, ADI 6387, Relatora Ministra Rosa Weber. Data de publicação DJe. 12/11/2020**. Brasília, DF: STF, 2020.

CABRAL, Filipe F. **Proteção de dados pessoais na atividade empresarial**. Rio de Janeiro: Lumen Juris, 2019. 204 p.

CARVALHO, Angelo P. D. O papel da estratégia de segurança da informação nos mecanismos de compliance de dados: em busca de uma abordagem integrada. *In*: FRAZÃO, Ana; CUEVA, Ricardo V. B. **Compliance e políticas de proteção de dados**. São Paulo: Thomson Reuters, 2021. p. 225-300.

CRESPO, Marcelo X. D. F. Risk assessment e relatórios de impacto: ferramentas para avaliação de riscos em programas de compliance digital e de proteção de dados. *In*: CRESPO, Marcelo X. D. F. **Compliance no direito digital**. São Paulo: Thomson Reuters, 2020. (Coleção compliance; 3).

CUEVA, Ricardo Villas Bôas. Impactos do programa de compliance de dados sobre outros programas e compliance. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas. **Compliance e políticas de proteção de dados**. São Paulo: Thomson Reuters, 2021. p. 65-76.

DANTAS, Bruno; SILVA, Leonardo R. D. Á. Risco, compliance e proteção de dados. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas. **Compliance e políticas de proteção de dados**. São Paulo: Thomson Reuters, 2021. p. 301-317.

DONEDA, Danilo *et al*. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. *In*: TEPEDINO, Gustavo; MENEZES, Joyceane B. D. **Autonomia privada, liberdade existencial e direitos fundamentais**. Belo Horizonte: Forum, 2019. p. 95-114.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, v. 12, n. 2, p. 91-108, jul./dez. 2011.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 3. ed. Rio de Janeiro: Editora Revista dos Tribunais, 2021. 368 p.

FERREIRA, Lucia M. T. Direito fundamental à proteção de dados. *In*: SCHREIBER, Anderson; MARTINS, Guilherme M.; CARPENA, Heloisa **Direitos fundamentais e sociedade tecnológica**. Indaiatuba: Foco, 2022. p. 241-256.

FOER, Frankiln. **O Mundo que não pensa**: a humanidade diante do perigo real da extinção do homo sapiens. Tradução de Debora Fleck. Lisboa: Leya, 2019. 240 p.

FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. **Curso de Proteção de dados pessoais**: fundamentos da LGPD. São Paulo: Grupo GEN, 2022. 496 p.

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. Compliance de dados. *In*: TEPEDINO, Gustavo; FRAZÂO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. 2. ed. São Paulo: Thomson Reuters, 2020. p. 669-706.

FRAZÃO, Ana; PINTO, Mariana. Compliance de dados e incidentes de segurança. *In*: PINEIRO, Caroline D. R. **Compliance entre a teoria e a prática**: reflexões contemporâneas e análise dos programas de integridade das companhias listadas no novo mercado. Indaiatuba: Foco, 2022. p. 35-56.

FRAZÃO, Ana. Big data e aspectos concorrenciais do tratamento de dados pessoais. *In*: MENDES, Laura S. *et al*. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 535-552.

FRAZÃO, Ana. Fundamentos da proteção de dados pessoais - Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena D. **Lei Geral de Proteção de dados pessoais e suas repercussões no Direito Brasileiro**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. p. 23-53.

FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de dados. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato Lei Geral de **Proteção de dados pessoais e suas repercussões no Direito Brasileiro.** 2. ed. São Paulo: Thomson Reuters, 2020. p. 97-126.

FRAZÃO, Ana. Propósitos, desafios e parâmetros gerais dos programas de compliance e das políticas de proteção de dados. *In*: FRAZÃO, Ana; CUEVA, Ricardo V. B. **Compliance e políticas de proteção de dados**. São Paulo: Thomson Reuters, 2021. p. 33-63.

GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. *In:* PALHARES, Felipe. **Temas atuais de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2020. p. 245-271.

HAN, Byung-Chul. **Sociedade da transparência**. Petrópolis, RJ: Editora Vozes, 2016.

IBM. **Custo de uma violação de dados em 2022**. [*S.l.*: IBM], 2022. Disponível em: https://www.ibm.com/br-pt/reports/data-breach. Acesso em 23 mar. 2023.

KONDER, Carlos N.; FAJNGOLD, Leonardo. O papel dos mecanismos de compliance e das políticas de proteção de dados para a proteção de dados sensíveis. *In*: FRAZÃO, Ana; CUEVA, Ricardo V. B. **Compliance e políticas de proteção de dados.** São Paulo: Thomson Reuters, 2021. p. 341-367.

LOUZADA, Luiza. Princípio da LGPD e os bancos de perfis genéticos: instrumentalizando a garantia de direitos no processo penal. **Revista do Advogado**, p. 90-98, nov. 2019.

MACHADO, Rony Max; FUJITA, Jorge S. Os impactos da sociedade da informação no direito à privacidade da pessoa natural e da pessoa jurídica. **Revista THESIS JURIS**, São Paulo, p. 258-278, jul./dez. 2018.

MAIA, Roberta M. M. A titularidade de dados pessoais prevista no art. 17 da LGPD: direito real ou pessoal? *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de dados pessoais e suas repercussões no Direito brasileiro**. São Paulo: Thomson Reuters, 2020. p. 127-152.

MAIA, Roberta M. M. O legítimo interesse do controlador e o término do tratamento de dados pessoais. *In*: MULHOLLAND, Caitlin. **A LGPD e o novo marco normativo no Brasil.** Porto Alegre: Arquipélago, 2020. p. 99-120.

MALDONADO, Viviane N.; OPICE BLUM, Renato. **LGPD**: Lei Geral de Proteção de Dados Pessoais Comentada. 4. ed. Rio de Janeiro: Revista dos Tribunais, 2022. 474 p.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 16. ed. São Paulo: Saraiva Jur, 2021.

MENDES, Laura S. Autodeterminação informativa: a história de um conceito. **Pensar - Revista de Ciências Jurídicas**, v. 25, n. 4, p. 1-18, out./dez. 2020.

MENDES, Laura S.; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de dados. **Revista de Direito do Consumidor**, São Paulo, v. 120, p. 469-483, nov./dez. 2018.

MENDES, Laura S.; RODRIGUES JÚNIOR, Otavio Luiz; FONSECA, Gabriel C. S. D. O Supremo Tribunal Federal e a proteção constitucional dos dados pessoais: rumo a um direito fundamental autônomo. *In*: MENDES, Laura S. *et al*. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 61-71.

MONTEIRO FILHO, Carlos E. D. R. Breve ensaio em tema dos fundamentos do Direito Civil-constitucional e a concepção do direito fundamentos à proteção de dados. *In*: MENEZES, Joyceane Bezerra de; CICCO, Maria Cristina de; RODRIGUES, Francisco Luciano Lima. **Direito Civil na legalidade constitucional algumas aplicações**. Indaiatuba: Foco, 2021. p. 51-59.

MULHOLLAND, Caitlin; FRAJHOF, Isabella Z. Inteligência Artificial e a Lei de Proteção de Dados Pessoais: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de machine learning. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin. **Inteligência Artificial e Direito**. 2. ed. São Paulo: Thomson Reuters, 2020. p. 267-292.

MULHOLLAND, Caitlin; LATERÇA, Priscila Silva. A proteção de dados pessoais e a tutela de direitos fundamentais à luz da Lei Geral de Proteção de dados. *In*: VIANA, Manuela Trindade; BADIN, Luciana. **A vida política das tecnologias digitais**. Rio de Janeiro: PUC-Rio, 2022. p. 133-149.

MULHOLLAND, Caitlin. Inteligência Artificial e discriminação de gênero. *In*: SCHREIBER, Anderson; MARTINS, Guilherme M.; CARPENA, Heloisa. **Direitos Fundamentais e sociedade tecnológica**. Indaiatuba: Foco, 2022. p. 169-181.

MULHOLLAND, Caitlin. Mercado, pessoa humana e tecnologias: a Internet das coisas e a proteção do direito à privacidade. *In*: EHRHARDT JÚNIOR, Marcos; CORTIANO JÚNIOR, Eroulths. **Transformações no direito privado nos 30 anos da Constituição**: estudos em homenagem a Luiz Edson Fachin. Belo Horizonte: Fórum, 2019. Disponível em: https://www.jur.ouc-rio.br/wp-content/uploads/2021/08/CAITLIN-SAMPAIO-Mercado-Pessoa-Humana-e-Tecnologias.pdf. Acesso em 20 jan. 2023.

MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. *In*: MULHOLLAND, Caitlin. **A LGPD e o novo marco normativo do Brasil**. Porto Alegre: Arquipélago, 2020. p. 121-156.

NISSENBAUM, Helen. A Contextual approach to privacy online. Daedalus: **Journal of the American Academy of Arts & Sciences**, n. 140, v. 4, fall 2011. Disponível em: https://www.amacad.org/publication/contextual-approach-privacy-online. Acesso em 20 jan. 2023.

NISSENBAUM, Helen. **Privacy in context:** tecnology, policy, and the integrity of social life. New York: Stanford Law Books, 2009. 288 p.

O'NEIL, Cathy. **Algoritmos de destruição em massa**: como o big data aumenta a desigualdade e a ameaça à democracia. Tradução de Rafaela Abraham. [*S.l.*]: Editora Rua do Sabão, 2021. 342 p.

OLIVA, Milena Donato; ABÍLIO, Vivianne da Silveira; COSTA, André Brandão Nery. Elementos essenciais para estruturação de efetivos programas de compliance de proteção de dados. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas. **Compliance e políticas de proteção de dados**. São Paulo: Thomson Reuters, 2021. p. 137-160.

OLIVEIRA, Caio César de. A Autoridade Nacional de Proteção de Dados (ANPD) e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. *In*: MULHOLLAND, Caitlin. **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago, 2020. p. 371-391.

PARENTONI, Leonardo N. Por que confiar na Autoridade Nacional de Proteção de Dados? **Revista da Faculdade de Direito UFMG**, Belo Horizonte, n. 79, p. 163-192, jul/dez 2021.

PEIXOTO, Erick L. C.; EHRHARDT JÚNIOR, Marcos. Os desafios da compreensão do direito à privacidade no sistema jurídico brasileiro em face das novas tecnologias. *In*: EHRHARDT, Marcos; LOBO, Fabíola A. **Privacidade e sua compreensão do direito brasileiro**. Belo Horizonte: Fórum, 2019. p. 33-53.

PEIXOTO, Erick Lucena Campos Peixoto, EHRHADT JÚNIOR, Marcos. Breves notas sobre a ressignificação da privacidade. **Revista Brasileira de Direito Civil – RBDCivil**, Belo Horizonte, v. 16, p. 35-56, abr./jun. 2018.

PEIXOTO, Erick Lucena Campos; ERHHARDT JÚNIOR, Marcos. Breves notas sobre a ressignificação da privacidade. **Revista Brasileira de Direito Civil - RBDCivil**, Belo Horizonte, v. 16, p. 35-56, 2018.

PERLINGIERI, Pietro. **O Direito Civil na Legalidade Constitucional**. Tradução de Maria Cristina De Cicco. Rio de Janeiro: Renovar, 2008.

PERLINGIERI, Pietro. **Perfis do Direito Civil**. Tradução de Maria Cristina De Cicco. 3. ed. Rio de Janeiro: Renovar, 2002.

RODOTÀ, Stefano. A antropologia do homo dignus. **Civilistica**, Rio de Janeiro, v. 6, n. 2, p. 1-17, jan./mar. 2017. Disponível em: http://civilistica.com/a-antropologia-do-homo-dignus/. Acesso em 21 jan. 2023.

RODOTÀ, Stefano. **A vida na sociedade de vigilância**. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. 382 p.

SAAVEDRA, Giovani Agostini; CRESPO, LIana I. A. Cunha. Compliance: origem e aspectos práticos. *In*: CRESPO, Marcelo X. D. F. **Compliance no Direto Digital**. São Paulo: Thomson Reuters, 2020. p. 30-43.

SARLET, Gabrielle B. S.; RODRIGUEZ, Daniel Piñeiro. A Autoridade Nacional de Proteção de Dados (ANPD) e os desafios tecnológicos: alternativas para uma estruturação responsiva na era da governança digital. **Revista Direitos Fundamentais & Democracia**, v.27, n.3, p. 217-253, set/dez 2022.
SARLET, Ingo W. O direito fundamental à proteção de dados pessoais na Constituição Federal Brasileira de 1988. **Privacy an data protection magazine**, p. 12-49, 2021.

SARLET, Ingo W.; SIQUEIRA, Andressa D. B. Algumas notas sobre liberdade de expressão e democracia: o caso das assim chamadas "fake news". *In*: SCHREIBER, Anderson; MARTINS, Guilherme M.; CARPENA, Heloisa. **Direitos fundamentais e sociedade tecnológica**. Indaitatuba: Foco, 2022. p. 39-59.

SCHWAB, Klaus. **Aplicando a Quarta Revolução Industrial**. São Paulo: Edipro, 2018.

SCHULMAN, Gabriel; KOSIAK, Ana Carolina C. A proteção de dados pessoais na legalidade constitucional: estudo de caso sobre o censo do IBGE. *In*: MENEZES, Joyceane Bezerra de; CICCO, Maria Cristina de; RODRIGUES, Francisco Luciano Lima. **Direito Civil na legalidade constitucional**: algumas aplicações. Indaiatuba: Foco, 2021. p. 179-204. Disponível em: https://www.wsj.com/articler/facebook-experiments-had-few-limits-1404344378. Acesso em 15 jan. 2023.

SNOWDEN, Edward. **Eterna vigilância**. Tradução de Sandra Martha Dolinsky. São Paulo: Planeta do Brasil, 2019. 288 p.

SOLOVE, Daniel J. I've got nothing to hide and other misunderstanding of privacy. **San Diego Law Review**, v. 44, p. 745, 2007. Disponível em: https://ssrn.com/abstract=998565. Acesso em 26 jan. 2023.

SOLOVE, Daniel J. **The digital person**: technology and privacy in the information age. New York: New York University Press. 2006. 283 p.

SOUZA, Carlos A. P. D. Segurança e Sigilo dos dados pessoais: primeiras impressões à luz da Lei 13.709/2018. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena D. **Lei Geral de proteção e dados pessoas e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters, 2020. p. 413-437.

SOUZA, Carlos Affonso *et al*. From privacy to data protection: the road ahead for the Inter-American Spystem of human rights. **The International Journal of Human Rights**, 2020.

SOUZA, Carlos Affonso; MAGRANI, Eduardo; CARNEIRO, Giovana. Lei Geral de Proteção de Dados Pessoais: uma transformação na tutela dos dados pessoais. *In*: MULHOLLAND, Caitlin. **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago, 2020. p. 43-64.

TEFFÉ, Chiara S. D.; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legas. **Civilistica**, a. 9, n. 1 2020. Disponível em: https://civilistica.com/tratamento-de-dados-pessoais-na-lgpd/. Acesso em 25 jan. 2023.

TEPEDINO, Gustavo. Premissas metodológicas para a constitucionalização do Direito Civil. *In*: TEPEDINO, Gustavo. **Temas de Direito Civil**. Rio de Janeiro: Renovar, 2004.

VASCONCELOS, Beto; DE PAULA, Felipe. A autoridade Nacional de Proteção de Dados: origem, avanços e pontos críticos à luz das mudanças recentes. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de dados pessoais e suas repercussões no Direito brasileiro**. São Paulo: Thomson Reuters, 2020. p. 707-733.

VÉLIZ, Carissa. **Privacidade é poder**. Tradução de Samuel Oliveira. São Paulo: Editora Contracorrente, 2021. 300 p.

WARREN, Samuel; BANDEIS, Louis. The right to privacy. **Civilistica**, v. 2, n. 3, jul./set. 2013 1890. Disponível em: http://civilistica.com/the-right-to-privacy/. Acesso em 28 jan. 2023.

WARREN; Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Law Review**, Harvard, v. 4, n. 5, p. 193-220, dec. 1890.

WIMMER, Miriam; PIERANTI, Octavio Pena. Programas de compliance e a LGPD: a interação entre autorregulação e a regulação estatal. *In*: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas. **Compliance e políticas de proteção de dados**. São Paulo: Thomson Reuters, 2021. p. 205-221.

WIMMER, Miriam. A LGPD e o balé dos princípios: tensões e convergências nas aplicação dos princípios de proteção de dados pessoais ao setor público. *In*: FRANCOSKI, Denise D. S. L.; TASSO, Fernando Antonio. **A Lei Geral de Proteção de Dados Pessoais**. São Paulo: Thomson Reuters, 2021. p. 163-186.

YOUYOU, Wu; KOSINSKI, Michal; STILLWELL, David. Computer-based personality judgments are more accurate than those made by humans. **PNAS**, v. 112, p. 1036-1040, jan. 2015. Disponível em: www.pnas.org/cgi/doi/10.1073/pnas.1418680112. Acesso em 16 mar. 2023.

ZANATTA, Rafael A. F. A proteção de dados pessoais entre leis, códigos e programação: os limites do Marco Civil da Internet. *In*: DE LUCCA, Newton; SIMÂO FILHO, Adalberto; PEREIRA LIMA, Cíntia Rosa. **Direito e Internet III**: Marco Civil da Internet. São Paulo: Quartier Latin, 2015. p. 447-470.

ZUBOFF, Shoshana. **A era do Capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2021.