UNIVERSIDADE FEDERAL DE OURO PRETO
DEPARTAMENTO DE DIREITO

Luiza Moreira de Carvalho

A RESPONSABILIDADE CIVIL NA LEI GERAL DE PROTEÇÃO DE DADOS:
natureza da obrigação e requisitos para o pedido de indenização individual

Ouro Preto
2021

Luiza Moreira de Carvalho

A RESPONSABILIDADE CIVIL NA LEI GERAL DE PROTEÇÃO DE DADOS:

natureza da obrigação e requisitos para o pedido de indenização individual

Monografia apresentada ao Curso de Direito da Universidade Federal de Ouro Preto como requisito parcial para a obtenção do título de Bacharel em Direito.

Orientadora: Profª. Dr.ª Juliana Evangelista de Almeida.

Ouro Preto

2021

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE OURO PRETO
REITORIA
ESCOLA DE DIREITO, TURISMO E MUSEOLOGIA
DEPARTAMENTO DE DIREITO

FOLHA DE APROVAÇÃO

Luiza Moreira de Carvalho

A RESPONSABILIDADE CIVIL NA LEI GERAL DE PROTEÇÃO DE DADOS:
natureza da obrigação e requisitos para o pedido de indenização individual

Monografia apresentada ao Curso de Direito da Universidade Federal
de Ouro Preto como requisito parcial para obtenção do título de Bacharel em Direito

Aprovada em 29 de abril de 2021

Membros da banca

Doutora - Juliana Evangelista de Almeida - Orientador(a) UFOP
Doutor - Roberto Henrique Pôrto Nogueira - UFOP
Graduada - Ana Laura Marques Gervásio - UFOP

[Juliana Evangelista de Almeida], orientador do trabalho, aprovou a versão final e autorizou seu depósito na Biblioteca Digital de Trabalhos de Conclusão de Curso da UFOP em 29/04/2021

Documento assinado eletronicamente por **Juliana Evangelista de Almeida**, **PROFESSOR DE MAGISTERIO SUPERIOR**, em 30/04/2021, às 17:46, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0166079** e o código CRC **611BC050**.

Referência: Caso responda este documento, indicar expressamente o Processo nº 23109.004062/2021-11 SEI nº 0166079

R. Diogo de Vasconcelos, 122, - Bairro Pilar Ouro Preto/MG, CEP 35400-000
Telefone: 3135591545 - www.ufop.br

RESUMO

O direito à proteção de dados pessoais é cadente na sociedade da informação. Apesar de ter influência direta na intimidade e a vida privada, esse direito funciona sob uma lógica diferente que deve ser analisada para seu melhor enquadramento enquanto direito da personalidade, pois está presente em todas as áreas da sociedade e impacta em diversos aspectos que regem a vida de milhões de indivíduos. Os meios de coleta e tratamento de dados atrai o interesse de diversas empresas e entidades, que buscam o máximo aproveitamento para alcance de seus objetivos. O desenvolvimento tecnológico é fonte de preocupação pela imprevisibilidade das consequências do seu uso indiscriminado desses dados, sendo principal motivador de mudanças quanto ao tema na esfera jurídica. Este trabalho tem como objetivo analisar a natureza jurídica e limites da responsabilidade civil dos agentes de proteção de dados no Brasil, a partir da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que traz conceitos importantes para a compreensão do tema e estabelece contornos da atuação dos agentes de tratamento de dados para que seja possível enfrentar os problemas causados pela exploração das novas tecnologias. Nesse intuito, a partir da exploração da legislação vigente, de pesquisa bibliográfica e documental, o trabalho trata, em primeiros capítulos, da evolução do papel dos dados na Sociedade da Informação e do enquadramento da proteção de dados como direito da personalidade autônomo, para, então, abordar os aspectos importantes da LGPD, tais como conceitos e princípio, que serão importantes para, ao final, entender qual a natureza jurídica da responsabilidade civil subjetiva dos agentes de tratamento de dados, bem como possibilidade de propor ação individual de indenização por danos causados em virtude do tratamento de dados pessoais.

Palavras-chave: Lei Geral de Proteção de Dados. Lei nº 13.709/2018. Responsabilidade Civil.

ABSTRACT

The right to the protection of personal data is prevalent in the information society. Despite having a direct influence on intimacy and private life, this right works under a different logic that must be analyzed for its best fit as a personality right, as it is present in all areas of society and impacts on several aspects that govern life millions of individuals. The means of data collection and treatment attracts the interest of several companies and entities, which seek the maximum use to achieve their objectives. Technological development is a source of concern due to the unpredictability of the consequences of its indiscriminate use of these data, being the main motivator of changes on the subject in the legal sphere. This work aims to analyze the legal nature and limits of civil liability of data protection agents in Brazil, based on the Data Protection Law (No. 13.709 / 2018), which brings important concepts for understanding the theme and it establishes outlines of the performance of data processing agents so that it is possible to face the problems caused by the exploitation of new technologies. In this sense, from the exploration of the current legislation, bibliographic and documentary research, the work deals, in first chapters, with the evolution of the role of data in the Information Society and the framing of data protection as a right of the autonomous personality, for, then, address the important aspects of the data protection law, such as concepts and principle, which will be important to, in the end, understand the legal nature of the subjective civil liability of the data processing agents, as well as the possibility of proposing individual action for damages. caused by the processing of personal data.

Keywords: Data Protection Law. Law No. 13,709 / 2018. Civil liability.

SUMÁRIO

1. INTRODUÇÃO

Inspirada na *General Data Protection Regulation* (GDPR), da União Europeia, a Lei Geral de Proteção de Dados (lei 13.709/18 – LGPD), que entra em vigor no corrente ano, traz uma série de inovações em relação à proteção do direito à privacidade e de dados pessoais como direitos individuais, além de garantir maior segurança jurídica para as empresas, atualizando conceitos antes esparsos em diversas normas setoriais.

Entre a lei brasileira e o diploma europeu, entretanto, há divergências muito relevantes. Uma delas é sobre o regime da responsabilidade civil dos agentes de proteção de dados. A LGPD, em seus artigos 42 a 45, estabelece as regras referentes à responsabilidade civil dos agentes de tratamento de dados pessoais, trazendo à tona o debate a respeito da natureza da obrigação de indenizar, se subjetiva - baseada na falta a um dever de conduta imposto ao agente de tratamento - ou objetiva - fundamentada no risco da atividade desenvolvida.

Outro ponto de discussão que tem sido pauta de debate candente entre os profissionais de proteção de dados, é a questão da (im)possibilidade de pedido de indenização individual em razão de eventual divulgação ou coleta indevida de dados pessoais.

Este trabalho se propõe justamente a contribuir com o debate para as questões alhures, todavia, não podemos chegar ao objeto do trabalho sem entender o contexto e processo de criação da LGPD.

A LGPD é considerada - sobretudo pelos profissionais do Direito Digital - um marco importantíssimo para a defesa da privacidade no Brasil, impactando os mais diversos setores e organizações. Dada sua relevância e por se tratar de uma lei relativamente nova, é importante que alguns aspectos sejam estudados com maior profundidade.

Ademais, para responder a problemática, objeto do presente trabalho monográfico, foi feita pesquisa bibliográfica em artigos, doutrina jurídica, legislações específicas e outras produções acadêmicas sobre o tema. Pelo que iniciamos este juízo a partir de uma abordagem sobre a relevância dos dados para a Sociedade da Informação.

Assim, na primeira parte deste estudo, trataremos de como os dados se tornaram um ativo para a sociedade e como a proteção de dados se tornou um direito da personalidade autônomo. Então, traçaremos as linhas gerais da Lei Geral de Proteção de Dados, abordando principais conceitos e definições trazidas pela lei, bem como seus princípios. Em seguida, abordaremos as proximidades sistemáticas da nova lei com outros diplomas protetivos, principalmente no que tange à questão da responsabilidade. Por fim, analisamos mais de perto os elementos normativos que são base para a conclusão de que a responsabilização na LGPD é de

natureza subjetiva e que a arquitetura jurídica da normativa reforça um sistema integrado destinado à tutela dos interesses coletivos, difusos e individuais homogêneos.

2. OS DADOS PESSOAIS ENQUANTO MERCADORIA NA SOCIEDADE DA INFORMAÇÃO: A RELAÇÃO ENTRE *BIG DATA* E O VAREJO

Não é novidade que a sociedade passa constantemente por transformações que alteram consideravelmente a forma de vida das pessoas. Dentro desse contexto fenomênico - e ainda que a atual organização social não se resuma ao ambiente virtual -as inovações tecnológicas assumem papel importante no estágio de organização da sociedade e da produção de riqueza, a medida em que possibilitam que grandes quantidades de informações advindas de qualquer lugar do mundo possam ser processadas e transmitidas em tempo quase real.

Nesse cenário, a informação se tornou o centro gravitacional da nova forma de organização social e econômica, denominada como *Sociedade da Informação*, pois não só altera as relações sociais, redefinindo as noções de tempo e espaço, mas tem valor comercial. Barreto Júnior (2015), ao abordar o tema, esclarece que:

> O advento do Informacionalismo é, indubitavelmente, a principal marca econômica da sociedade em rede. Reorganiza a produção de riqueza no sistema econômico, no qual há uma gradativa valoração da informação como mercadoria e fator de geração de valor econômico, o que torna a National Association of Securities Dealers Automated Quotations (Nasdaq), bolsa de valores das empresas tecnológicas, tão estratégica, em termos de organização econômica, quanto a tradicional New York Stock Exchange, denominada bolsa de Wall Street. As megacorporações informativas (Google, Facebook e Yahoo, entre outras) acumulam vestígios de informações sobre os usuários da Internet, tais como seus padrões de navegação, compras realizadas on-line, preferências culturais, religiosas e ideológicas, websites de interesse, verbetes e expressões pesquisadas nos websites de busca, entre outras, "impressões digitais eletrônicas" que servem para estabelecer uma categorização minuciosa de cada usuário na rede. [...] Circunscreve-se no fato de que há inúmeros usos para esses perfis eletrônicos, tal como direcionamento de publicidade on-line, oferta de mercadorias relacionadas ao perfil do consumidor, além de montar cadastros de valor incomensurável sobre os cidadãos da sociedade em rede. (BARRETO JUNIOR, 2015, p. 410).

Bioni (2020, p. 11) ressalta, no entanto, que não basta considerar apenas a informação em si para torná-la produtiva para a estratégia empresarial: é preciso convertê-la em conhecimento aplicado acerca do comportamento humano, mais precisamente sobre hábitos de consumo das pessoas. Assim, a nova ordem econômica utiliza dessas informações, que são dados sobre experiências humanas, como matéria prima para fins comerciais, segmentando campanhas para perfis específicos de consumidores e criando produtos cada vez mais personificados, que acabam guiando as escolhas dos usuários (BIONI, 2020).

Nesse sentir, a informação dita uma nova lógica de acumulação de capital, conhecida como *Capitalismo de Vigilância*,[1] que prospera graças a uma proposta denominada *Big Data*,[1] cujo principal propósito é extrair dados pessoais a fim de combiná-los para prever o comportamento dos consumidores. Nas palavras de Godoy,[2] "essa nova forma de mercado parte do princípio de que atender às necessidades reais dos indivíduos é menos lucrativo do que vender previsões de seu comportamento que foram coletados através de meios eletrônicos".

Para Zuboff, no entanto, a lógica do *Big Data* vai além de meras previsões de comportamento. A autora explica que para que os lucros cresçam, os prognósticos devem ser cada vez mais certos. Para tanto, será necessário que cada vez mais dados sejam minerados não só para prever, mas para modificar o comportamento humano como meio de produzir receitas e controle de mercado (ZUBOFF, 2019, p. 18).

Bioni explica que *Big Data* não é um sistema inteligente que prevê o futuro: "não se trata de ensinar o computador a pensar como um humano, trata-se apenas de uma nova metodologia para que tal ferramenta processe e organize dados para inferir a (re)ocorrência de acontecimentos" (BIONI, 2020, p. 36). Assim, *Big Data* é um método utilizado para inferir a probabilidade de eventos se repetirem no futuro através da correlação estabelecida entre fatos que configuram um determinado padrão:

> *Big Data* não se preocupa com a causalidade de um determinado evento, mas tão somente, com a probabilidade de sua ocorrência. Em vez de questionar por que algo acontece, procura diagnosticar o que está acontecendo. Não se está preocupado com a análise das razões que geram uma cadeia de eventos, mas, tão somente, com seu desencadeamento. (BIONI, 2020, p. 36).

Em sentido análogo, Boyd e Crawford, definem *Big Data* como:

> um fenômeno cultural, tecnológico e acadêmico baseado na interação de três fatores: (1) Tecnologia: maximização da precisão dos algoritmos e do poder de computação para reunir, analisar, relacionar e comparar grandes conjuntos de dados; (2) Análise: processamento de grandes conjuntos de dados para identificar padrões para atender às necessidades de ordem econômica, social, técnica e legal; e (3) Mitologia: a ampla crença de que grandes conjuntos de dados possibilitam uma forma mais avançada de inteligência e conhecimento que podem gerar *insights* até então impossíveis de se alcançar, de forma objetiva e confiável. (BOYD; CRAWFORD, 2012, p. 2, tradução nossa).

---

[1] Estas expressões são utilizadas por ZUBOFF (2019).

[2] GODOY, Karla. Experiências humanas e o capitalismo de vigilância riqueza em forma de dados. Disponível em: <http://redectidc.com.br/assets/files/Experiencias%20humanas%20e%20o%20capitalismo%20de%20vigilancia%20-%20riqueza%20em%20forma%20de%20dados.%20.pdf> Acesso em: 20 mar. 2021.

O que move as empresas e os governos para *Big Data* é justamente a possibilidade de encontrar relação entre conjuntos de dados que advêm de situações reais de sem, contudo, precisar entender suas causas, podendo fazer previsões para o futuro. *Big Data* é um sistema complexo, isso porque são praticamente impossíveis de serem interpretados pela mente humana, razão pela qual o processamento de dados massivos, como aqueles gerados a respeito da população das grandes cidades, por exemplo, têm demandado investimento em novas tecnologias - análise de dados a partir de algoritmos e uso de inteligência artificial - que permitam seu aproveitamento para a melhoria de serviços públicos, tais como a erradicação de epidemias, mapeamento de ações criminosas e organização do trânsito, entre outros benefícios.

Cediço que, com o processo de informatização dos sistemas de gestão e expansão da Internet, a população se torna cada vez mais dependente das tecnologias digitais para ter acesso a serviços e para possibilitar suas ações de trabalho e entretenimento. Hoje, existem mais de 4,5 bilhões de celulares inteligentes em uso no mundo, e mais de 20 bilhões de outros dispositivos conectadas à Internet, segundo indica o estudo "*Visual Networking Index – Global Mobile Data Traffic Forecast*". Entretanto, os números certamente aumentam gradativamente em razão da pandemia, isto porque a atual realidade exige uma sociedade conectada e multifacetária, sendo necessário a utilização de dispositivos que nos permitam infinitas conexões.

Na Internet, os usuários subvertem-se em consumidores, interagindo e compartilhando opiniões sobre suas experiências com determinados produtos ou serviço, passando a ter participação ativa no clico de consumo, o que condiciona confecção do próprio produto ou serviço: são cocriadores (*prosumer*).

A Internet oportuniza, assim, a organização dos dados pessoais de forma mais escalável, transformando-se em elemento estratégico e transformador do *marketing* em geral a medida em que possibilita experiencias cada vez mais personalizadas, propiciando o encontro entre os interesses dos consumidores e o bem de consumo de forma cirúrgica. Nesse sentir, os dados pessoais dos consumidores são ativos na economia da informação, eis que potencializam o êxito na indução ao consumo com a publicidade direcionada. Isso ocorre porque os dados pessoais são os registros de nossas atividades sociais e de nossa personalidade.

Nesse cenário, a capacidade de captação de dados foi elevada a instâncias surpreendentes, chegando aos conjuntos de informações de consumidores que são coletados através de cadastro de consumo ou banco de dados.

Oportuno mencionar, a respeito desse tema, que a legislação não faz distinção entre banco de dados e cadastro de consumo: os termos são tratados indistintamente pelo art. 43 do

CDC como atividade de coleta e arquivamento de informações de consumidores, ou arquivo de consumo. Todavia a doutrina, especialmente Herman Benjamin, adotou a expressão arquivos de consumo como gênero do qual as expressões bancos de dados e cadastros de consumidores são espécies, denominação dobrada utilizada pela Seção VI, do Capítulo V ('Das Práticas Comerciais') (GRINOVER; WATANABE; JUNIOR, 2011).

Nas lições de Herman Benjamin (GRINOVER; WATANABE; JUNIOR, 2011), as distinções entre banco de dados e cadastro de consumidores são classificadas em razão da origem da informação e seu destino no seguinte sentido: (i.) os bancos de dados têm caráter aleatório e os cadastros de consumo pressupõem uma relação jurídica dos fornecedores com os consumidores; (ii.) os bancos de dados organizam os dados para uma utilização futura (mediata) e os cadastros de consumidores se utilizam dos dados imediatamente; (iii.) nos bancos de dados a guarda dos dados prescinde de autorização dos consumidores e os cadastros de consumidores dependem de autorização prévia do consumidor; (iv.) os bancos de dados têm por objetivo a transmissão de informação a terceiro e os cadastros de consumidores utilizam os dados de forma pontual.

Em outras palavras, tanto o banco de dados como o cadastro são um conjunto de informações acerca de um consumidor. Entretanto, se distinguem à medida que, no banco de dados, as informações são coletadas no mercado, já o cadastro é composto pelas informações fornecidas pelo próprio consumidor.

Assim, milhares de base de dados são criadas para identificar padrões de comportamento na Internet (*profiling*) e existem vários exemplos que podem ilustrar quão manipulador e lucrativo pode ser este mercado. Por esta razão, de acordo com o portal Economatica[3] o valor de mercado da empresa Google Inc. é de US$531,4 bilhões, enquanto o da empresa *Facebook* é de US$326,2 bilhões. Irrefutável a vinculação da informação com o aspecto financeiro. Crespo (2011, p. 38) destaca que "a informática se transformou em importantíssimo instrumento de informação e esta, por seu turno, tornou-se valioso bem econômico" (CRESPO, 2011).

Importante destacar que, para fins deste estudo, não abordaremos as questões éticas envolvendo o tema. Entretanto, apenas à título de informação, há a ideia de que a lógica *Big Data* acaba por inserir o consumidor em uma bolha social, isso porque a utilização do *profiling* tende tornar a experiência de cada usuário na Internet tão personalizada que podem, inclusive, permitir ou restringir o acesso somente à informação cujo conteúdo é considerado relevante

[3] Disponível em: <https://economatica.com/estudos/2016/zero160203.pdf>. Acesso em: 16 mar. 2020.

para um determinado objetivo, ou seja, somente aqueles que não contradigam com convicções e interesses do fim que se pretende. Tal ideia que é bem ilustrada por Freitas e Pamplona (2017):

> Assim, a informação fragmentada é resultado da aplicação de sistemas de informação dispersos e heterogêneos, que estão sendo projetados de forma independente por diferentes empresas, a fim de aperfeiçoar individualmente a informação desejada por cada um dos usuários a partir de implementação de processos específicos com base no conjunto de dados de cada usuário. (FREITAS; PAMPLONA, 2017, p. 122).

Para melhoria das previsões, no entanto, é necessário que as bases de dados sejam alimentadas com as mais variadas informações possíveis. Para se obter esse tipo de variedade é preciso acessar informações que vão além de nomes e IPs, mas também sobre hábitos matinais, trajetos, caminhadas, dentre outros. O que se vive hoje, em verdade, é a observação permanente do comportamento dos indivíduos, cujas informações e dados pessoais são matéria-prima a ser explorada para geração de riqueza (BIONI, 2020, p.6). Em outras palavras, a economia movida a dados e o capitalismo de vigilância estão imbricados de forma substancial, porque a extensão do mercado baseado nessa lógica de acumulação exige a expansão da vigilância.

A operacionalização desse modelo de negócio, que condiciona o acesso a diversas oportunidades ao fornecimento de dados pessoais, coloca o titular dos dados em posição de desvantagem. Isso porque, para ter acesso a determinado produto ou serviço, como aplicativos por exemplo, o usuário é obrigado a consentir com a coleta de suas informações.

No entanto, o consumidor não sabe, ao certo, os custos efetivos desse trânsito informacional ou o que deles se pode extrair; do modo como é feito atualmente, o consentimento assume mais propriamente as vestes de um ato unilateral, cujo efeito é o de supostamente autorizar um determinado tratamento para os dados pessoais. Nesse sentir, evidencia Frazão:

> [...] o mercado de dados em geral cresce a partir da difusão de visões como a de que o modelo de negócios é justo, já que os usuários receberiam contrapartidas adequadas pelos seus dados, ou mesmo necessário, dado que haveria um verdadeiro trade-off entre inovação e privacidade, de maneira que a violação desta última seria o preço a pagar ou o mal necessário para o progresso tecnológico e os novos serviços que daí decorrem. Até a forma como a questão é apresentada já reflete a perspectiva utilitarista que permeia a análise, pois se parte da premissa de que, em nome da inovação, é justificável o sacrifício de direitos fundamentais elementares. (FRAZÃO, 2019, p. 31).

Assim, as políticas de privacidade atuam como um contrato de adesão, que partem da premissa que o usuário está predisposto a anuir com qualquer que seja o conteúdo descrito, a partir do momento em que decide utilizar os serviços ofertados. Por meio dessa técnica

contratual, pretende-se garantir a aprovação do usuário para legitimar toda e qualquer operação de tratamento de seus dados.

O que se experimenta, na prática, é que o usuário clica em um botão de “aceito”, mas dificilmente lê os longos e complexos termos e políticas de privacidade, além de que, muitas vezes, ele não possui conhecimento técnico suficiente para desvendar as peculiaridades da linguagem comumente utilizada nesses textos.

Dessa forma, e por inúmeras razões, tal mecanismo tem se mostrado falho, seja porque ele reforça a assimetria do mercado informacional, seja porque se trata de uma ferramenta que não capacita o consumidor para exercer controle sobre as suas informações pessoais.

Essa relação assimétrica de poder se expande ainda mais, conforme explica Bioni, em razão das limitações cognitivas do ser humano, que o impedem de calibrar efetivamente as “gratificações e as perdas mediatas e imediatas necessárias para racionalizar um processo de tomada de decisão genuíno a respeito do fluxo de seus dados pessoais” (BIONI, 2020, pág 138).

A respeito do tema, Zuboff defende a ideia de que usuários da nova ordem econômica não passam de carcaças abandonadas, como elefantes após a extração do marfim (ZUBOFF, 2019). Nesse contexto, o titular dos dados não tem controle do que pode acontecer com suas informações e está submerso em diversas incertezas a medida em que pode sofrer danos pela má utilização de seus dados pessoais. Danos estes que sequer podem ser antevistos, o que o coloca em condição de vulnerabilidade não só técnica, mas informacional e econômica: há uma sobreposição de fraquezas que são característicos de uma nova vulnerabilidade (BIONI, 2020, p.38).

Há que se considerar, ainda, que para além da captação de dados para fins comerciais, há também um prolongamento da pessoa por meio de seus dados, uma biografia digital que é resultado do fenômeno da datificação. Isso porque há uma segmentação e classificação de perfis ou padrões que é feita com base nas informações coletadas: criam-se estereótipos e esse é um fator importante para tomada de decisões.

Com a tecnologia e desenvolvimento dos algoritmos, diversas decisões começam a ser tomadas por uma inteligência artificial. São as decisões automatizadas, cuja base são os estereótipos criados com os dados coletados a respeito dos indivíduos. Essa já é uma realidade e exemplos não faltam. Não são mais os gerentes de banco que aprovam um crédito, é um algoritmo que vai coletar informações acerca de um indivíduo e gerar um valor, qual seja, se esse indivíduo é bom ou mal pagador. Com base nesse resultado serão calculados os valores dos créditos e as alíquotas de juros. Foi também um algoritmo que em março do ano passado

impossibilitou que uma pessoa sacasse o auxílio emergencial pelo caixa eletrônico, pois foi considerado morto com base nos dados que haviam sido coletados a seu respeito.[4]

Portanto, ter controle dos dados não é apenas uma questão segurança ou de saber para que fins eles serão utilizados, mas também uma forma de garantir que esses dados sejam coletados com qualidade para que as decisões tomadas a respeito de seu titular sejam justas. Isso porque a nossa capacidade de autodeterminação é cada vez mais calibrada com o uso que é feito dos nossos dados. Uma sociedade na qual os cidadãos não detêm controle sobre as suas próprias informações coloca em risco o seu próprio sistema democrático.

A Constituição protege uma série de aspectos específicos relacionados à privacidade do titular de dados. No ordenamento jurídico brasileiro há também legislações esparsas, seja no direito civil ou de natureza processual e outras normais setoriais nas quais algum aspecto da proteção da privacidade assume relevo (DONEDA, 2019, p.13).

Entretanto, para promover o empoderamento do titular dos dados surgiu a necessidade de regulação específica sobre o tema, não só porque o tratamento inadequado aos dados pessoais pode violar a privacidade, intimidade e outros direitos fundamentais do indivíduo, mas para conferir ao usuário algum poder de barganha capaz de equalizar as assimetrias. É nesse contexto que a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) cria corpo, tendo o "importante papel de reforçar a autonomia dos titulares dos dados e o necessário e devido controle que estes precisam exercer sobre os seus dados" (FRAZÃO, 2019, p. 31).

Feitas essas considerações, passemos agora à análise da categoria jurídica dos dados pessoais enquanto direito da personalidade.

[4] Notícia disponível em <https://g1.globo.com/rj/rio-de-janeiro/noticia/2020/05/19/considerado-morto-pela-caixa-trabalhador-do-rj-nao-consegue-sacar-o-auxilio-emergencial.ghtml>. Acesso em: 16 mar. 2021.

3. A PROTEÇÃO DE DADOS PESSOAIS COMO UM DIREITO DA PERSONALIDADE

Para partir ao estudo jurídico do direito à proteção de dados pessoais como um direito da personalidade é necessário estabelecer um diálogo entre o direito à privacidade enquanto garantia fundamental para o livre desenvolvimento da personalidade e o direito à proteção dos dados.

3.1 Direito à Privacidade e à Proteção de Dados Pessoais

Inicialmente, com relação ao tema proposto neste tópico, ressalta-se que a legislação brasileira não adotou o termo "privacidade",[5] mas "vida privada" e "intimidade", sem conceituá-los de forma específica. A despeito disso, a discussão termológica mostra-se infrutífera para os fins do estudo proposto neste trabalho, sendo viável o uso da palavra "privacidade" para tratar das questões levantadas acerca da tutela do direito à privacidade. Desse modo, como fez Cancelier (2017, p. 84), iremos optar pelo protagonismo da palavra "privacidade" para a referência à íntima (CANCELIER, 2017).

O conceito de privacidade está ligado às transformações ocorridas ao longo da história e da relação entre o ser humano e o espaço onde vive consigo. É possível observar, dessa forma, que o exercício desse direito está conectado a uma estrutura que o viabilize, pois se relaciona, mesmo que indiretamente, com o espaço onde se habita e se constrói a existência. Nas palavras de Bioni:

> O direito à privacidade tem sido historicamente articulado com base na dicotomia entre as esferas públicas e privada. Sempre esteve em perspectiva a demarcação de atividades que deveriam ser desempenhadas privativamente ou em público *vis-à-vis*. A habitação privada (casa) estabeleceria os contornos dessa dicotomia, sendo por excelência, o espaço para que as pessoas se refugiassem do escrutínio público. Isso é simbolizado a partir da metáfora de que o indivíduo tem a faculdade de se afastar da multidão (espaço público) para se recolher ao seu castelo (espaço privado). (BIONI, 2020, p.91).

Assim, muito embora o direito à privacidade não seja tema novo no debate jurídico, ele é um direito moderno, pois depende de uma tecnologia que o abrace para ser exercitado.

---

[5] Além desses termos, Cancelier (2017, p. 82) assevera que na Constituição de 1988 fala-se no sigilo da correspondência, das comunicações telegráficas, de dados e das comunicações telefônicas e da inviolabilidade da casa, porém para a discussão do direito à privacidade nos atentamos os demais termos.

Também segundo Doneda (2019, p. 130-131), a privacidade é historicamente compreendida a partir da dicotomia entre quais atividades deveriam ser exercidas na esfera pública e quais deveriam estar restritas ao espaço privado dos indivíduos, sendo limitado por uma compreensão de que a habitação dos indivíduos seria o local de refúgio do escrutínio público. Para Arendt (2010, p.77-85) o direito à privacidade é um pressuposto democrático, visto que a partir da fuga da "pressão social", os indivíduos podem vivenciar e experimentar suas subjetividades no espaço privado (ARENDT, 2010).

Assim, a definição do que é exposto sobre alguém, do que se quer tornar público ou não, a quem se deseja revelar algo ou o gral de interação com seus conhecidos e todos os demais, mais do que meramente uma preferência, é o que define propriamente um indivíduo, sendo basilar para a democracia, pois essencial para o livre desenvolvimento da personalidade. Tanto que o legislador a salvaguarda ao cidadão no início do artigo 21 do Código Civil de 2002 – "A vida privada da pessoa natural é inviolável […]".

É nesse contexto que a privacidade pode ser compreendida como uma garantia de não violação ou invasão de seus aspectos privativos, assim como o próprio artigo 5º, X da Constituição Federal e o artigo 21 do CC2002 preceituam ao determinarem a vida privada como inviolável (BIONI, 2020, p. 92-93).

Em outras palavras, a privacidade pode ser encarada como uma liberdade negativa de seu titular (direito de ser deixado só), que estabelecerá quais aspectos de sua vida estarão contidos em sua esfera privada e que, consequentemente, são tutelados por esse direito (RODOTÀ, 2012, p. 320). A pessoa tem direito de retrair aspectos de sua vida do domínio público e estar a salvo de interferências alheias (BIONI, 2020, p. 92). Esse é o entendimento clássico sobre o conceito de direito à privacidade, conceito este que se mostra limitado para o cenário atual, pois a própria definição acerca da privacidade é incerta, levando a privacidade a um status de termo "guarda-chuva", de conceituação abstrata ou considerada uma "palavra-camaleão" (BIONI, 2020, p.93). Assim, Stefano Rodotà destaca a necessidade de ampliação desse conceito para melhor adequar-se à atual realidade, considerando que vivemos em uma sociedade altamente digitalizada:

> Se este é o quadro global a ser observado, não é mais possível considerar os problemas da privacidade somente por meio de um pêndulo entre "recolhimento" e "divulgação"; entre o homem prisioneiro de seus segredos e o homem que nada tem a esconder; entre a "casa-fortaleza", que glorifica a privacidade e favorece o egocentrismo, e a "casa-vitrine", que privilegia as trocas sociais; e assim por diante. Essas tendem a ser alternativas cada vez mais abstratas, visto que nelas se reflete uma forma de encarar a privacidade que negligencia justamente a necessidade de dilatar esse conceito para

> além de sua dimensão estritamente individualista, no âmbito da qual sempre esteve confinada pelas circunstâncias de sua origem. (RODOTÀ, 2012, p. 25).

Logo, para Rodotà, há uma transformação do conceito de direito à privacidade, que passa a abarcar não só o poder de exclusão, de impedimento de interferências alheias, mas também a centralidade do controle do indivíduo sobre suas informações pessoais, ou seja, sua autodeterminação informativa.

Para Bioni, no entanto, ainda que a definição de privacidade seja difícil de ser estabelecida, ela deve permear a dicotomia entre o público e o privado e encarada como liberdade negativa, a medida em que é um direito estático, ou seja, que depende de que seu titular delimite quais fatos de sua vida devam ser excluídos do domínio público. Já a evolução do direito à privacidade para englobar o direito à proteção de dados deve consistir em proteção dinâmica e uma liberdade positiva do controle sobre as informações pessoais do titular desse direito. Além disso:

> [...] observa-se que cada vez mais a atividade de tratamento de dados impacta a vida das pessoas, em particular quando elas são submetidas a processos de decisões automatizadas que irão definir seu próprio futuro. Nesse contexto, o direito à proteção de dados pessoais tutela a própria dimensão relacional da pessoa humana em especial para que tais decisões não ocasionem práticas discriminatórias, o que extrapola e muito o âmbito da tutela do direito à privacidade. (BIONI, 2020, p.96).

Assim, para o autor, o direito à proteção de dados diferencia-se essencialmente do direito à privacidade, sendo um equívoco dogmático indicar a proteção de dados pessoais como uma mera evolução do direito à privacidade, não devendo ser reduzido a mera evolução do direito à privacidade (BIONI, 2020, p. 96-97).

Em conclusão a este título, considerando que em uma sociedade digital o tratamento de dados tem se tornado cada vez mais expansivo e impacta consideravelmente as mais diversas realidades sociais, a proteção de dados pessoais ergue-se como a tutela da “própria dimensão relacional da pessoa humana”, isso porque existe um leque de liberdades individuais relacionadas com a proteção de dados pessoais que extrapolam os limites de tutela do direito à privacidade. Enquanto este é atrelado a uma divisão das esferas pública e privada de seus titulares - uma liberdade negativa - aquele diz respeito a uma liberdade positiva, porque a capacidade de controle que titular exerce sobre seus dados independe do fato dessa informação ser pública ou privada (BIONI, 2020, p. 99).

Com isso, o direito à proteção de dados pessoais angaria autonomia própria: é um novo direito da personalidade. E não poderia ser de outra forma, tendo em vista que esse direito não pode estar atrelado a uma categoria específica, pois não se satisfaz com a técnica normativa do eixo da privacidade.

3.2 A proteção de dados como categoria autônoma a direito da personalidade

Inicialmente, cumpre esclarecer que a personalidade tratada neste estudo é aquela cuja proteção é canalizada para o desenvolvimento da pessoa humana, não se trata, portanto, de (in)aptidão de um sujeito ser titular de direitos e deveres.

Ao reconhecer o princípio da dignidade humana em seu artigo 1º, III, a Constituição Federal de 1988 se tornou um verdadeiro marco normativo da tutela dos direitos da personalidade, e trouxe também outras garantias, tais como a liberdade de expressão (art. 5º, IX) e o direito à informação (art. 5º, XV).

Para Tepedino (2004, p. 47), os direitos da personalidade não precisam estar concentrados como um único direito subjetivo representados a partir de múltiplas classificações para promover ampla proteção da pessoa em todos os seus aspectos (TEPEDINO, 2004). A dignidade humana seria, em verdade, uma cláusula geral de proteção das pessoas, isso porque atua conjuntamente no centro do discurso jurídico constitucional com os direitos fundamentais, sendo, portanto, dispositivos indissociáveis e essenciais para qualquer ordem jurídica verdadeiramente democrática (PASQUALINI, 1999, p. 80-81).

No Código Civil, também podemos observar que a dignidade humana se tornou centro da tutela jurídica, especialmente no bojo do capítulo referente aos direitos da personalidade. O sujeito, antes lido como neutro, passou a ser compreendido enquanto pessoa, aí está o foco de tutela de todo o ordenamento jurídico.

Foge aos limites deste trabalho adentrar na discussão sobre a tutela dos direitos da personalidade. Pragmaticamente, o que importa é que os direitos da personalidade são aqueles direitos inerentes a elementos corpóreos e incorpóreos que caracterizam e diferenciam uma pessoa. Dentre os exemplos mais comuns encontrados nos artigos 11 ao 21 do Código Civil, temos o direito à honra, à privacidade, à integridade física e psíquica. Desse modo o Direito nos protege de violações contra a individualidade (TEPEDINO, 2004, p. 29).

Entretanto, os direitos da personalidade não se limitam às situações previstas nas hipóteses do CC2002 supramencionadas e não podem ser vistos como taxativos, mas sim de maneira aberta (*numerus apertus*), o que abre caminho para o reconhecimento do direito à proteção de dados como novo direito da personalidade (BIONI, 2020, p. 50).

Na era da sociedade da informação, o fenômeno da datificação constitui um cenário de novos desafios para a tutela da personalidade humana, principalmente considerando que a sociedade e economia se orientam a partir das atividades de controle e armazenamento de dados

pessoais efetivadas pela economia de dados para mapeamento e categorização do perfil dos indivíduos, titulares das informações. Sobre o tema, Bioni:

> Os direitos da personalidade são uma noção inacabada que deve ser cultivada, especialmente frente ao abordado manancial de dados produzidos pelas pessoas na sociedade da informação. Por meio dessa premissa, será possível identificar uma nova variante dessa categoria jurídica para nela enquadrar a proteção dos dados pessoais. (BIONI, 2020, p.54).

Para Frazão, no cenário da sociedade de vigilância, o *Big Data* vigia todos os nossos passos, sendo capaz de capturar todas os rastros digitais deixados ao utilizarmos a Internet. É pouco provável uma compreensão acerca da dimensão do poder dos dados na sociedade contemporânea, mas essa alta capacidade de vigilância confere às plataformas digitais o poder sobre as escolhas dos indivíduos, influenciando-os e limitando-os em suas atividades e experiências (FRAZÃO, 2019, p. 25 e p. 38).

Assim, entende-se a justificativa dogmática para a "inserção dos dados pessoais na categoria de direitos da personalidade", isso porque tais "dossiês digitais" configuram um novo tipo de identidade, uma forma de prolongamento da pessoa. Assim, os dados pessoais não estão relacionados apenas às noções de privacidade, mas "transitam dentre mais de uma das espécies de direitos da personalidade" (BIONI, 2020, p.57).

Portanto, os dados pessoais configuram-se como uma extensão da personalidade, e são elementos substanciais da singularidade de cada indivíduo, capazes de o identificar em suas particularidades enquanto seres sociais. Disso decorre a importância de elevar a proteção de dados pessoais a um status de direito da personalidade, que inclusive está em vias de ser incluído na gama de direitos fundamentais pela PEC 17/20199 em pauta no plenário, de autoria do Senador Eduardo Gomes, que, logo imediatamente teve um pedido de coautoria de vários outros Senadores, fato que demonstra como o parlamento brasileiro está sensibilizado pela pauta. A PEC propõe destacar a proteção de dados do direito à privacidade num inciso à parte, notadamente porque esses direitos funcionam segundo lógicas distintas, portanto a prosta é dar maior roupagem a essa autonomia do direito à proteção de dados. Em todas as normativas estrangeiras esse mesmo debate vem florescendo, sobretudo na Carta Europeia de Direitos Fundamentais, que inscreveu a proteção de dados com direito fundamental cuja proteção deve se dar por aplicação e interpretação de uma autoridade independente.[6]

---

[6] *Artigo 8.º* Proteção de dados pessoais 1. Todas as pessoas têm direito à proteção dos dados de caráter 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

Há desdobramentos práticos muito significativos caso a PEC seja aprovada, sobretudo no que diz respeitos à transferência internacional de dados e criações de zonas de livre fluxo de informação. Muitos países, ao pensarem em acordos internacionais nesse sentido, procuram analisar não só se determinado país tem uma lei de proteção de dados e se há uma autoridade nacional relacionada ao tema, mas, principalmente, estudam como poder judiciário daquele país lida com a matéria.[7] Portanto, inscrever proteção de dados na Constituição como direito fundamental é, na nossa opinião, um ponto positivo, sobretudo porque tornará o supremo tribunal um fórum para discussão da pauta.

Cita-se que o próprio Superior Tribunal de Justiça já reconheceu a importância do tema e definiu, em decisão que é considerada um marco histórico, pela elevação da proteção de dados e do direito à autodeterminação informativa a direito fundamental autônomo, seguindo a linha da decisão do Tribunal Constitucional da então Alemanha Ocidental, de 1983, na qual foi declarada a inconstitucionalidade de dispositivos de uma lei que, à semelhança do caso brasileiro, criava um censo estatal e determinava a coleta de dados pessoais dos cidadãos para a otimização de políticas públicas.

A decisão da Corte proferida no dia 8 de maio de 2020, em votação quase unânime (10 votos a 1), referendou a medida cautelar deferida pela ministra Rosa Weber no âmbito de cinco ações diretas de inconstitucionalidade - propostas pelo Conselho Federal da Ordem dos Advogados do Brasil e por quatro partidos políticos (PSB, PSDB, PSOL e PCdoB), suspendeu a eficácia da Medida Provisória nº 954, de 17 de abril de 2020, que dispõe o seguinte:

> O compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência pública de importância internacional decorrente do coronavírus (covid19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. (BRASIL, 2020).

Vislumbrando ameaça à própria democracia constitucional, a decisão ratificada pelo Plenário do STF, da lavra da ministra Rosa Weber, enfatiza que não existem mais dados neutros ou insignificantes, uma vez que qualquer dado que leve à identificação de uma pessoa pode ser utilizado para a formação de perfis informacionais que serão usados por empresas e pelo Estado,

---

direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:12012P/TXT>. Acesso em: 16 mar. 2021.

[7] A análise foi elemento-chave para decisão da União Europeia em acordo com o Japão. O acordo criou o maior espaço de circulação segura de dados a nível mundial. Disponível em: <https://ec.europa.eu/commission/presscorner/detail/pt/IP_18_4501>. Acesso em: 16 mar. 2021.

razão pela qual qualquer dado que possibilite a identificação de uma pessoa merece proteção constitucional.

A importância da regulamentação da temática precisa abarcar da forma mais extensa possível a tutela da personalidade, considerando que a exploração dos dados pessoais ultrapassa um simples sentido de violação à privacidade, principalmente se levarmos em conta a conceituação clássica de privacidade assentada no direito de ser deixado só. As violações que podem ocorrer em um contexto de controle irregular e ilegal de dados pessoais alcançam muitas outras esferas do cidadão, colocando em risco até mesmo sua autonomia e individualidade (FRAZÃO, 2019, p. 100).

Em conclusão, a proteção de dados pessoais insere-se como categoria autônoma de direito da personalidade, sendo imprescindível para a Lei Geral de Proteção de Dados que todos os controladores e operadores de dados sejam vigiados, para que os titulares dos dados tenhamos clareza sobre a forma como seus dados serão tratados. A LGPD, ao normatizar essas questões, veio para estabelecer uma relação de confiança entre os diversos sujeitos envolvidos no tratamento de dados e características e nuances serão abordadas no capítulo a seguir.

4. CONSIDERAÇÕES SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS - LEI Nº 13.709/2018

Feita a breve análise acerca do desenvolvimento da tutela da privacidade, passaremos ao estudo da Lei nº 13.709/2018, intitulada Lei Geral de Proteção de Dados (LGPD), que surgiu como resposta jurídica aos fenômenos ocorridos na Sociedade da Informação. Isto posto, com o fim de melhor compreender ao tema deste estudo, neste capítulo serão abordados o histórico e o âmbito de aplicação da LGPD, bem como o conceito e classificação dos dados pessoais e os requisitos para o seu tratamento.

Inicialmente, cumpre apontar que a LGPD entrou em vigor em setembro de 2020 para todos os direitos, deveres e obrigações lá previstos, com exceção da fiscalização pela Autoridade Nacional de Proteção de Dados, que terá início apenas em 1º de agosto de 2021. Entretanto, aguarda designação a PL5762/2019 que propõe a prorrogação da data de entrada em vigor para 15 de agosto de 2022.

Oportuno destacar, aqui, que a LGPD entra em vigor junto uma intensa migração digital que foi acelerada pelo cenário da pandemia COVID-19, isso nos força a enfrentar com mais qualidade e celeridade os novos desafios trazidos com sua implementação. Desafios esses que não devem ser subestimados, isso porque a proteção de dados se tornou um diferencial determinante no mercado. Um exemplo disso é o caso emblemático da fuga em massa de usuários do aplicativo *WhatsApp*. Duas semanas após atualização de sua política de privacidade, cerca de 500 milhões[8] de usuários migraram para aplicativo concorrente denominado Telegram. Isso deixa claro que grande parte da população tem valorizado a questão da proteção de seus dados, e tende a passar a escolher com quem contrata ou faz negócio com base nessa garantia.

Dessa forma, e dado todo o desdobramento do que fora exposto até o momento neste trabalho, não é surpresa a inclinação dos ordenamentos jurídicos na criação de normas autônomas para a proteção de dados. Assim, a LGPD surgiu para regulamentar o uso, a proteção e a transferência de dados pessoais em território nacional, seja em âmbito público ou privado. O seu objetivo é garantir um efetivo controle por parte dos titulares sobre suas informações pessoais.

---

[8] Noticiado em: <https://www.terra.com.br/noticias/tecnologia/telegram-chega-a-500-milhoes-de-usuarios-com-fuga-do-whatsapp,b8d3aa7604cde108835d17c4316053e8zkz8vmv7.html>. Acesso em: 16 mar. 2021.

4.1 As gerações de leis de proteção de dados

Em seus apontamentos, Doneda (2019, p. 175-179), explica que as leis sobre proteção de dados pessoais podem ser divididas em quatro gerações. O autor demonstra que, inicialmente, as leis se propunham a regular a criação dos bancos de dados, que ganhavam grandes proporções nos anos 70, e a limitação de seu controle pelos órgãos públicos. Na época, havia pouca experiência sobre novas tecnologias, assim, a preocupação dos legisladores era mais voltada à sua expansão do que com processamento dos dados e privacidade do cidadão propriamente ditos (DONEDA, 2019).

Diante da multiplicação de centros de processamentos de dados, as leis de primeira geração não demoraram a se tornarem obsoletas. As normas, que estabeleciam minuciosamente o regramento sobre funcionamento de banco de dados, não conseguiram acompanhar a velocidade com que novos bancos de dados eram criados.

Em seguida, a segunda geração de leis de proteção de dados, surgida a partir da segunda metade dos anos 70, avançou no sentido de preocupar-se com a privacidade do indivíduo e no acesso de terceiros as suas informações, entretanto eram tidas como liberdades negativas a serem exercidas pelo próprio cidadão, oferecendo formas de controle para que o próprio titular tivesse maneiras de tutelar seus direitos individuais:

> Tal evolução refletia a insatisfação de cidadãos que sofriam com a utilização por terceiros de seus dados pessoais e careciam de instrumentos para defender diretamente seus interesses; além disso, o controle nos moldes das leis anteriores tornou-se inviável, dada a fragmentação dos polos de tratamento dos dados pessoais. Assim, criou-se um sistema que fornece instrumentos para o cidadão identificar o uso indevido de suas informações pessoais e propor a sua tutela. (DONEDA, 2019, p. 177).

Essas leis também se tornaram ultrapassadas e geraram uma importante mudança de paradigma: a terceira geração de normas de proteção dos dados pessoais foram pensadas para absorver o princípio de liberdade, isso porque o fornecimento de dados já havia se tornado requisito indispensável para a efetiva participação social. Assim, as novas leis, surgidas nos anos 80, garantiram ao titular a autodeterminação informativa referente à maneira a qual seus dados seriam coletados, tratados e para que pudesse, inclusive, questionar e interromper o fluxo de suas informações pessoais, que eram amplamente utilizadas pela Estado e entes privativos.

As leis de quarta geração sobre a proteção de dados pessoais, por sua vez, são aquelas que temos contado na atualidade e caracterizam-se por buscar suprir as desvantagens do enfoque individual. Nelas, há a aplicação de técnicas para efetivamente conter a disparidade

entre o titular dos dados pessoais e as entidades que os coletam e processam. Como se vê, neste momento há um aumento de proteção a direitos fundamentais do cidadão, assegurando o nível de proteção e cautela a ser tomada de acordo com o grau de sensibilidade do respectivo dado pessoal.

No cenário atual, prevalece o entendimento de que, para encarar a proteção de dados devemos superar a ótica ultrapassada da dicotomia entre tecnologia e privacidade, e partir da ideia de uma concepção do desenvolvimento tecnológico harmonizado com a preservação dos direitos fundamentais dos cidadãos. Em outras palavras, as inovações tecnológicas devem ser importantes aliadas para o resguardo da proteção de dados pessoais.

4.2 Cenário Internacional e processo de criação da LGPD

"Não existem mais dados insignificantes", essa foi a constatação precoce e acertada do Tribunal Constitucional Alemão em 1983, em julgamento que representa um verdadeiro marco histórico para a proteção de dados e estabeleceu um novo paradigma na tutela jurídica dos dados em todo o mundo. Nesse mesmo sentido, 37 anos mais tarde, o entendimento da ministra Carmen Lúcia na sessão do dia 7 de maio, quando o STF suspendeu por 10 votos a 1 a eficácia da Medida Provisória (MP) 954/2020, que previa o compartilhamento de dados de usuários de telecomunicações com o Instituto Brasileiro de Geografia e Estatística (IBGE).

Na decisão, o Tribunal Alemão asseverou, repita-se, em 1983, o seguinte:

> [...] hoje, com ajuda do processamento eletrônico de dados, informações detalhadas [...] de uma pessoa determinada [...] podem ser, do ponto de vista técnico, ilimitadamente armazenados e consultados a qualquer momento, a qualquer distância e em segundos. Além disso, podem ser combinados, sobretudo na estruturação de sistemas de informação integrados, com outros bancos de dados, formando um quadro da personalidade relativamente completo ou quase, sem que a pessoa atingida possa controlar suficientemente sua exatidão e seu uso. Com isso, ampliaram-se, de maneira até então desconhecida, as possibilidades de consulta e influência que podem atuar sobre o comportamento do indivíduo em função da pressão psíquica causada pela participação pública em suas informações privadas. (BVerfGe 65, 1, Volkszahlung).

Como se vê, no cenário europeu, a experiência com a proteção de dados é mais desenvolvida, sendo que diversos países do grupo produziram normas sobre a matéria nos anos 70 e 80, já com a principal atenção no princípio da dignidade humana. Temos também a consolidação europeia de outros princípios que serviram de inspiração para elaboração da Lei Geral de Proteção de Dados brasileira, tais como pertinência, proporcionalidade, finalidade e necessidade.

Apesar do pioneirismo, o Regulamento Geral sobre a Proteção de Dados Europeia (RGPD) nº 679, somente foi aprovado em 27 de abril de 2016, resultado da articulação do partido The Greens, visando a proteção da privacidade e dignidade humana, atingindo 28 Estados-membros. Mas a aprovação do regulamento criou uma forte influência internacional para que outros países também passassem a normatizar o tema de proteção de dados. Somando-se a isso, e provavelmente o fator mais determinante para a regulamentação por outros países, foram o surgimento de barreiras comerciais impostas àqueles sem previsão legal específica para o tema.

Importa destacar que o Brasil, antes mesmo da criação da LGPD, já era signatário de alguns acordos internacionais que possuem considerações sobre a proteção de dados pessoais, como a Convenção de Berna de 1886 e o Acordo sobre Aspectos dos Direitos de Propriedade Intelectual relacionados ao Comércio (TRIPS). De igual maneira, temos leis internas que também têm breves passagens sobre o tema da proteção de dados, a citar o Código de Defesa do Consumidor,[9] o Marco Civil da Internet,[10] Decreto Regulamentador do Marco Civil da Internet,[11] Lei do Cadastro Positivo,[12] Lei de Acesso à Informação,[13] Decreto Regulamentador da Lei de Acesso à Informação,[14] Lei do Sigilo das Instituições Financeiras, Decreto sobre Comércio Eletrônico,[15] BACEN, Estatuto da Criança e do Adolescente e o Código Brasileiro de Autorregulamentação Publicitária, dentre outras. Como se vê, o cenário anterior à da entrada em vigor da LGPD não era de vazio regulatório, mas sim de um verdadeiro quebra-cabeças, com diversas normas esparsas sobre o tema.

Essas normas, decretos e portarias dispersas precisavam ter a mesma sintonia, e ainda faltavam alguns conceitos básicos para a efetiva estruturação de um sistema de proteção de dados pessoais no Brasil. Por exemplo, o CDC trata do princípio da transparência em seu art. 4, caput, entretanto não explica o conceito de dado pessoal. Já o Decreto MCI, em seu art. 14, I, há o conceito de dado pessoal, mas lhe falta dispositivo sobre o princípio da transparência, e

---

[9] Art. 4, caput (princípio da transparência), art. 43, §1º (princípio da qualidade), art. 43, §2º (informação).
[10] Art. 7º, VII e IX (consentimento), art. 7º, VIII, caput (informação), art. 7º, VIII, "a" (princípio da minimização), art. 7º, VIII, "c" (princípio da finalidade).
[11] Art. 14, I (conceito de dado pessoal), art. 14, II (tratamento de dados), art. 13, §2º, I (princípio da finalidade), art. 13, §2º (princípio da minimização).
[12] Art. 2º, I (conceito de banco de dados), art. 5º, VII (princípio da finalidade), art. 3º, §3, I (princípio da minimização), art. 3º, §2, III (princípio da qualidade), art. 4º, IV, "b" (consentimento), art. 5º, II (direito de acesso), art.5º, III (direitos de retificação e cancelamento).
[13] Art. 4º, IV (conceito de dado pessoal), art. 4º, V (tratamento de dados), art. 5º, I (princípio da transparência), art. 4º, VIII (princípio da qualidade), art. 31, §2º, I (consentimento)
[14] Art. 3º, V (conceito de dado pessoal), art. 55°, I (sigilo), art. 55, II (consentimento), art. 57 (exceções ao consentimento), art. 58 (restrições ao sigilo), art. 61, caput, §1° e §2° (uso de informação pessoal por terceiro).
[15] Art. 4°, VII (princípio da segurança).

assim por diante. Ou seja, apesar de haver várias leis setoriais sobre o tema da proteção de dados pessoais, o que dificultava a própria aplicação desses dispositivos.

Além disso, o Brasil ansiava pela entrada na Organização para a Cooperação e Desenvolvimento Econômico (OCDE), cujo interesse já foi manifestado em 2017, no intuito de ser incluído no grupo de 36 países que desenvolvem uma cooperação internacional para incrementar os investimentos e demais práticas de colaboração cosmopolita[16]. Um dos fatores que levaram à promulgação da LGPD certamente é a motivação política, uma vez que possuir uma lei específica de proteção de dados pessoais é um dos requisitos para os membros da OCDE. Um dos requisitos para os membros da OCDE é possuir uma lei específica de proteção de dados, então esse é outro fator que levou à promulgação da LGPD brasileira.

De acordo com Bioni (2020, p.109), é importante saber, embora sua recente entrada em vigor, a LGPD não é uma legislação nova e já vinha sendo discutida desde 2010, ano em que foi feita uma das várias consultas públicas, referente a um anteprojeto de lei, que, a propósito, era bastante distinto da versão que viria a ser aprovada oito anos depois.

Durante o processo de criação da lei, alguns acontecimentos foram marcantes. Em 2013, por exemplo, o americano Snowden revelou um grande esquema de espionagem praticados por alguns países, o que ocasionou em um escândalo de dimensão mundial. Snowden revelou que determinados governos eram capazes de espionar e vigiar toda e qualquer pessoa no planeta através de comunicação eletrônica, especialmente quando estas usavam plataformas na Internet. Algumas declarações revelavam que até mesmo presidentes e chanceleres foram espionados. O Brasil, então, que havia revelado publicamente sua indignação, trabalhou para construir alianças com outras nações para poder reverter a situação ocorrida. O resultado disso foi a aceleração do Projeto de Lei referente ao Marco Civil da Internet, que culminou com sua aprovação.

Para a criação da LGPD houve milhares de contribuições ao longo de 10 anos, tanto do governo quanto da iniciativa privada, que, juntos, chegaram a uma conclusão sobre as melhores ideias para este projeto. Já no início de 2016, tal anteprojeto foi enviado para o Congresso Nacional, sendo então um dos últimos atos da então presidente Dilma Roussef. Sobre isso, segundo Bioni:

> O resultado foi um texto já bastante maduro que depois viria a ser a base do PLC 53/2018. Nas vésperas do seu afastamento, a presidenta Dilma Rousseff encaminhava o texto do anteprojeto à Câmara dos Deputados que se transformaria no PL 5276/2016, desde logo, tal iniciativa legislativa contou com o apoio de mais de 40 (quarenta)

[16] Definição disponível em: <http://www.oecd.org/latin-america/countries/brazil/brasil.htm>. Acesso em: 20 mar. 2021.

> entidades nacionais e internacionais que já afirmavam ser: "uma redação equilibrada a salvaguardar a inovação e a proteção da privacidade dos cidadãos. (BIONI, 2020, p. 1).

Outro acontecimento de grande relevância internacional foi o tumulto envolvendo a empresa britânica *Cambridge Analytica*, no que foi exposto que a organização coletou, por meio das famosas plataformas de redes sociais, dados pessoais de cerca de 50 milhões de usuários e utilizou-os para armazenamento e a análise dos gostos e preferências dos usuários. Esses dados foram utilizados para envio de publicidade direcionada na Grã-Bretanha, onde suspeita-se que isso tenha ajudado a influenciar na votação da saída do Reino Unido da União Europeia. Nos Estados Unidos, também há suspeita de que o uso desses dados coletados - destaca-se, à revelia do consentimento de seus titulares - para finalidades políticas, que teriam culminado na vitória do, agora ex-presidente, Donald Trump (GOGANI, 2018).

Inclusive, há indícios de que a referida empresa estaria preparada para prestar seus serviços no Brasil, durante o último pleito eleitoral para a Presidência da República, tendo tal informação vindo à tona.[17] A partir daí, houve pressão de vários parlamentares das casas legislativas sobre a necessidade de haver uma lei que protegesse a privacidade dos cidadãos brasileiros (MILHORANCE, 2018).

Outro fator que contribuiu para a promulgação da LGPD, segundo Katarivas (2019), repousa sobre a Lei Complementar n° 166, de 8 de abril de 2019, que dispõe sobre os cadastros positivos de crédito. Quando essa lei foi aprovada, determinava que era necessário haver o consentimento expresso do titular dos dados para que estes pudessem ser alocados em uma determinada base de dados referentes à histórico de (in)adimplência (KATARIVAS, 2019).

Muitas empresas gestoras tinham interesse no acesso a essas informações, porém, pretendiam a exclusão do consentimento prévio do titular, e que a adesão fosse automática ao cadastro positivo como direito de oposição.

A Câmara dos Deputados, em debate que envolveu membros da Sociedade Civil, concluiu que antes de colocar informações de mais de 100 milhões de cidadãos automaticamente acessíveis em uma base de dados, incluindo todo o histórico de créditos que revelariam muito sobre a vida de cada um desses indivíduos, necessário seria discutir regras e direitos adequados para os titulares da informação. Surge daí, um verdadeiro apoio na aprovação de LGPD, para que, após, pudessem ser votadas as alterações na Lei do Cadastro Positivo, que resultaram na Lei Complementar nº 166/2019 (KATARIVAS, 2019).

---

[17] Informação publicada em El País, disponível em <https://brasil.elpais.com/noticias/caso-cambridge-analytica/> Acesso em: 20 mar. 2021.

4.3 A LGPD como consolidadora do Marco Civil da Internet

Sir Tim Berners-Lee - apontado como criador da Internet na forma que conhecemos hoje – em pronunciamento divulgado no dia 24 de março de 2014 no site *World Wide Web Foundation*, demonstrou grande entusiasmo em relação a Lei n. 12.965, de 23 de abril de 2014 (Marco Civil da Internet), conforme segue a publicação:

> Se o Marco Civil for aprovado, sem maiores adiamentos ou modificações, este seria possivelmente o melhor presente de aniversário para os usuários de internet do Brasil e do mundo. Eu espero que, aprovando esta lei, o Brasil fixe sua orgulhosa reputação como um líder mundial em democracia e progresso social e ajude a inaugurar uma nova era, uma onde os direitos dos cidadãos em todos os países do mundo são protegidos por leis de direito digitais. (BERNERS-LEE, 2014, p.1, tradução nossa).

Isto posto, não se pode deixar de citar, neste estudo, a Lei nº 12.965/2014, denominada de Marco Civil da Internet/MCI, sendo esta, primariamente, uma normativa intrínseca quando se trata das relações realizadas através da Internet.

Conforme ensinamentos de Bioni (2020, p. 124), o MCI foi uma ação da sociedade civil brasileira tentando evitar que o Poder Legislativo regulamentasse a internet usando leis penais. Nesse contexto, o MCI procurou em abordar diversos direitos, garantias e deveres relativos à rede mundial de computadores, além de trazer inovações com relação ao direito fundamental à privacidade online. Nesse sentido, é o que informa Teixeira (2016):

> Preocupado com a possibilidade de eventualmente haver alguma limitação à liberdade de expressão ou alguma violação da privacidade dos usuários da internet, o Marco Civil expressa que a garantia a esses dois direitos constitucionais é condição para o pleno exercício do direito à acesso à rede mundial de computador. Ou seja, a violação a esses direitos implica em quebra da própria finalidade do advento do Marco Civil enquanto uma lei federal que objetiva tutelar os usuários da internet. (TEIXEIRA, 2016, p. 84).

Logo em seu artigo 3º, incisos II e III, o MCI estabelece, dentre outros princípios do uso da Internet no Brasil, o da proteção da privacidade e a proteção dos dados pessoais, na forma da lei (BRASIL, 2014), sendo que a proteção dos dados pessoais, conforme Teixeira (2016), que não foi tratada de forma tão específica nesta norma, deve ser disciplinada por uma lei posterior (no caso, a LGPD).

Com efeito, para o Direito Digital no Brasil, o MCI inaugurou a regulamentação das relações na Internet que eram, até então, tratadas por legislações não específicas. Aplicavam-se as leis do direito penal, do direito autoral e da personalidade, por exemplo.

Não obstante ao fato de que o MCI é considerado um marco para o Direito Digital, para Bastos (2018), ainda que houvesse adequação de certos institutos às mudanças que a sociedade contemporânea trouxe no mundo online, existiam algumas incongruências e lacunas que o MCI não fora capaz de preencher, vejamos:

> Necessitava-se, portanto, de maior regulamentação no âmbito do direito digital. Assim, o Marco Civil da Internet se destacou por prever princípios, garantias, direitos e deveres para o uso da Internet no Brasil. No entanto, ele próprio deixava uma importante lacuna: a questão dos dados pessoais no direito digital. Reconheceu as relações jurídico-virtuais e os efeitos delas no ordenamento. Dispôs, por exemplo, acerca dos crimes cibernéticos. Mas deixou de abordar como os dados fornecidos pelos usuários poderiam ser utilizados pelas empresas. (BASTOS, 2018, p. 1).

Ainda conforme a autora, o MCI deixou uma considerável omissão, em relação aos dados pessoais, eis que não abordou a forma como as empresas utilizariam os dados gerados pelos usuários (BASTOS, 2018, p. 1). Isso, por si, justificaria a importância da LGPD. Nesse sentindo, Carvalho e Pedrini afirmam:

> Evidencia-se que, no viés de proteção do usuário perante o ambiente virtual, deve-se considerar os preceitos principiológicos e diretrizes do Marco Civil da Internet, uma vez que são verdadeiras conquistas dos internautas frente ao mundo tecnológico. Entretanto, há, ainda, outro comando legislativo que deve ser igualmente observado, trata-se, pois, da LGPD, que trata detalhadamente e especificamente da proteção dos usuários, quando suas informações estão dispostas em banco de dados públicos ou privados. (CARVALHO; PEDRINI, 2019, p. 374-375).

Tanto o MCI quanto a LGPD são lei ordinária. Disso, surge o seguinte questionamento: Teria a LGPD o MCI, no todo (*ab-rogação*) ou ao em parte (*derrogação*)? Para responder a essa pergunta, devemos considerar ao menos três hipóteses.

A primeira hipótese diz respeito aos critérios hierárquico e temporal de hermenêutica. Sabendo que ambas as leis são de mesma hierarquia e sendo a LGPD posterior ao MCI, não seria absurdo pensar que aquela pudesse revogar todas as partes desta, principalmente nos dispositivos que se referem ao tratamento de dados pessoais. Em contrapartida, como o MCI tem caráter geral,[18] pois regula o funcionamento da Internet como um todo, permaneceriam em vigor seus dispositivos versando sobre os demais assuntos.

---

[18] GRAU, Eros Roberto; FORGIONI, Paula A. CADE vs BACEN: Conflitos de competência entre autarquias e a função da Advocacia-Geral da União. **Revista de Direito Mercantil, Industrial, Econômico e Financeiro**. São Paulo: Malheiros, ano XLIII, n.º 135, p. 7-25, jul./set. 2004. p. 13. "Os atributos da especialidade e da generalidade, que apartam as normas gerais das especiais, derivam de um juízo de comparação entre duas normas. Norma geral e norma especial não são geral e especial em si e por si, mas sempre relativamente a outras normas. Assim, uma norma que é geral em relação à outra, pode ser tida como especial em face de uma terceira."

Por outro lado, temos que o art. 60 da LGPD promoveu alterações expressas em dois artigos do MCI, se mantendo silente sobre a revogação de quaisquer outros. A conclusão que se chega, considerando uma interpretação a *contrario sensu (*TARELLO, 1980), que a intensão do legislador foi manter intactos todos os demais dispositivos do MCI, inclusive aqueles relacionados ao tratamento de dados pessoais. Esta é a segunda hipótese a ser considerada.

Há, ainda, uma terceira hipótese: o cotejo mais atento dos referidos diplomas legais revela algumas antinomias (BOBBIO, 1999, p. 86).[19] A citar, no que tange ao consentimento do titular para o tratamento de seus dados pessoais, o MCI, em seu art. 7º, inciso VII, dispõe que o consentimento deve ser expresso, ao passo que o art. 7º, inciso I da LGPD se contenta com o consentimento inequívoco. Ou seja, em tese, a LGPD admite outras formas de consentimento, tais como o verbal ou o implícito. No que tange a esse dispositivo em específico, a melhor interpretação aponta no sentido de que a LGPD revogou o MCI. Entretanto, existem outras repercussões da LGPD sobre o MCI, que vão além daquelas previstas no mencionado art. 60. Dessa forma, necessário analisar um por um os dispositivos do MCI que se referem ao tratamento de dados pessoais, para chegar a uma conclusão sobre quais foram eventualmente afetados pela LGPD.

Uma outra antinomia seria em relação à multa simples: enquanto a LGPD estipulou o valor até 2% (dois porcento) do faturamento do grupo econômico nacional ao qual pertence a pessoa jurídica infratora, limitado ao montante de R$ 50 milhões por infração, o MCI permite até 10% (dez porcento) do faturamento, sem, contudo, fixar valor máximo. Neste caso, é provável que a jurisprudência não admita a gradação da multa com base no dispositivo do MCI, isso porque as disposições especiais da LGPD são mais benéficas.

Conclui-se, portanto, que a relação entre a LGPD e o MCI é mais complexa do que aparenta, cabe questionar se estamos de fato diante de uma antinomia ou se os diplomas apenas se complementam. As situações concretas certamente desafiarão a jurisprudência. Enfim, o presente trabalho não tem pretensão de aprofundar o tema ou de fornecer respostas abrangentes, mas apenas abordar alguns aspectos sobre a complexidade do assunto e os desafios que estão por vir. Sendo assim, adiante faremos uma análise de pontos essenciais e conceitos da Lei Geral de Proteção de Dados propriamente dita.

---

[19] "Definimos a antinomia como aquela situação na qual são colocadas em existências duas normas, das quais uma obriga e a outra proíbe, ou uma obriga e a outra permite, ou uma proíbe e a outra permite o mesmo comportamento."

4.4 Aspectos relevantes sobre a Lei Geral de Proteção de Dados

A LGPD é a legislação brasileira determina a forma como os dados dos cidadãos podem ser tratados, e ainda prevê punições para transgressões a essas determinações. No dia 14 de agosto de 2018, foi sancionado no Congresso Nacional o PLC 53/2018, que dispõe sobre a proteção de dados pessoas e altera o Marco Civil da Internet, consolidando-se assim como a Lei Geral de Proteção de Dados brasileira.

Vimos, posteriormente neste trabalho, que o país já dispunha de mais de 40 normas que, direta ou indiretamente, tratavam da proteção à privacidade e aos dados pessoais. Todavia, a LGPD vem substituir e/ou complementar esse arcabouço regulatório setorial, que por vezes era conflituoso, o que trazia insegurança jurídica e tornava o país menos competitivo no contexto de uma sociedade cada vez mais movida a dados.

Tal como a GDPR, a LGPD motiva uma verdadeira mudança de paradigma na gestão dos dados, evidenciando a necessidade de construção de uma cultura de proteção de dados no país. A lei cria, portanto, um novo regramento para o uso de dados pessoais no Brasil, tanto no âmbito online quanto offline, nos setores privados e públicos, além de colocar o país no rol de mais de 100 países considerados adequados para proteger a privacidade e o uso de dados.

No que tange à sua estrutura, a LGPD é composta pelas seguintes seções: (i) disposições preliminares (objeto da lei e definições), (ii) tratamento de dados (quando ocorre, objeto e término), (iii) direitos do titular (sujeito passivo do tratamento), (iv) tratamento de dados pelo poder público (requisitos específicos em razão da publicidade e responsabilidade), (v) transferência internacional de dados (quando pode ocorrer), (vi) agentes de tratamento de dados (sujeito ativo do tratamento de dados – definição e responsabilidade), (vii) segurança e boas-práticas (deveres do sujeito ativo), (viii) fiscalização (poderes do regulador), (ix) Autoridade Nacional de Proteção de Dados (regime do regulador), (x) disposições finais. Inclusive, a regulação europeia apresenta uma estrutura análoga.[20]

Em suas disposições preliminares, a LGPD estabelece seus limites de aplicação, territorialidade, conceitos e princípios. Já nas disposições gerais, é apresentado ao intérprete o

[20] A GDPR assim é subdivida: (i) disposições gerais, (ii) princípios, (iii) direitos do titular dos dados, (iv) responsável pelo tratamento e subcontratante, (v) transferências de dados pessoais para países terceiros ou organizações internacionais, (vi) autoridades de controlo independentes, (vii) cooperação e coerência, (viii) vias de recurso, responsabilidade sanções, (ix) disposições relativas a situações específicas de tratamento, (x) atos delegados e ato de execução, (xi) disposições finais. Utilizamos esta versão como base: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1554-1-1>. Acesso em: 16 mar. 2021.

que se persegue com este diploma. Os fundamentos da lei tratam da materialização legal de alguns direitos e garantias fundamentais da nossa constituição: o art. 2º, no inciso I, estabelece como primeiro fundamento o respeito à privacidade. Este fundamento em específico está em total harmonia com o inciso X do art. 5º da Constituição Federal, que decreta a regra geral da inviolabilidade da intimidade e vida privada, que será replicada no inciso IV do mesmo artigo da LGPD. Podemos perceber então que está também relacionado a uma das bases do Estado Democrático de Direito, que é o respeito ao indivíduo. Pode parecer um tanto quanto óbvio hoje, mas essa concepção de indivíduo não era considerada em outras formas de organização do Estado. Cuida-se de uma das características do Estado Moderno.

4.4.1 Definições de dados pessoais

Conforme fora exposto no item 4.2 deste trabalho, a LGPD foi fruto de um longo processo legislativo que durou cerca de dez anos, no qual estavam em trâmite três principais projetos de lei: o PL n° 330/2013, criado no Senado Federal, e os PLs n° 4.060/2012 e n° 5.276/2016, criados pela Câmara dos Deputados. Como elucida Mangeth e Nunes (2018), o PL n° 4.060/2012 apresentou o texto normativo que expunha os usuários à diversos riscos, tratando da temática fora dos padrões mínimos impostos pela GRPD, motivo pelo qual foi alterada de forma significativa com o apensamento do PL n° 330/2013, ao seu texto. Já o PL n° 5.276/2016, possuía o texto idêntico ao regulamento europeu, e, por esse motivo, representou um grande avanço e foi considerado o projeto base para a construção da Lei Geral de Proteção de Dados brasileira (MANGETH; NUNES, 2018). Mas tendo em vista o objetivo do estudo aqui proposto, nos atentaremos aos pontos importantes dos anteprojetos em tópico específico, mantendo, por ora, foco em definições que são relevantes para a proposta deste capítulo. Assim, passamos a eles.

Logo no inciso I do art. 5º, temos a definição de dado pessoal como qualquer "informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018). Note que o referido dispositivo veio para complementar o art. 7º do MCI, em seu inciso primeiro, que já aludia ser direito do usuário a "I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação".[21]

[21] Marco Civil da Internet. Lei 12.965/2014. Art. 7º: "O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação. (BRASIL, 2014).

Cite-se que há duas classificações de dados pessoais, a reducionista e a expansionista. Segundo a teoria reducionista, dado pessoal consiste em uma informação que deve estar associada a algo específico, ou seja, deve possuir um vínculo direto e inequívoco com seu titular, por exemplo, um determinado número de CPF está vinculado diretamente a um titular, apenas. Em contramão, segundo a visão expansionista, que inclusive é adotada de forma majoritária, o dado pessoal segue um conceito amplo quanto a sua classificação, na qual a necessidade de associação direta entre dado e titular, apenas, é desconsiderada. De acordo com essa teoria, dado pessoal pode ser qualquer tipo de informação que permita a potencial identificação do seu titular, mesmo que não haja um vínculo direto com a informação (BIONI, 2020, p. 16). Assim, conforme sintetiza Bioni (2020):

> Ainda que divergentes, tais teorizações detêm o mesmo centro gravitacional. Ambas demandam uma análise contextual donde está inserido um dado, aferindo-se o seu grau de "identificabilidade" para, então, desencadear a compreensão se uma determinada informação está relacionada a uma pessoa identificada ou identificável. (SCHWARTZ; SOLOVE, 2011, apud BIONI, 2020, p. 17).

O mesmo artigo 5º define, ainda, o que é dado pessoal sensível, dado pessoal anonimizado, banco de dados e anonimização de dados, conforme se observa a seguir, *in literis*:

> II - dado pessoal sensível: 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; III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico; (...) XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. (BRASIL, 2018).

Há, portanto, três tipos de dados pessoais: (i) os dados pessoais *lato sensu*, são informações relativas a uma pessoa física identificada, bem como ao conjunto de informações distintas que podem levar à identificação dessa pessoa. São exemplos o nome, apelido, data de nascimento, um endereço de Internet Protocol (IP), imagens relativas às pessoas recolhidas através dos sistemas de videovigilância e gravação de chamadas telefônicas. Além disso, conforme § 2º do art. 12 da LGPD, poderão ser igualmente considerados como dados pessoais aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada. Por outro lado, não são dados pessoais, por exemplo, o Número de Identificação do Registro de Empresas (NIRE).

Seguindo essa linha de raciocínio, os (ii) dados pessoais sensíveis são aqueles ligados a questões mais subjetivas e comportamentais, e, por terem maior potencial lesivo, o seu tratamento deve observar regras mais severas, isto por se tratarem de direitos personalíssimos, tais como raça, opinião pública, vida sexual, conforme exposto alhures[22]. Assim, necessária a cumulação do consentimento do titular, de forma específica e destacada. Apenas será possível tratar os dados sensíveis sem tal requisito quando for demonstrado "a) cumprimento de obrigação legal ou regulatória pelo controlador".[23] Além disso, o artigo 11º refere-se a "sempre que possível" o dado sensível, quando tratado, será anonimizado.

Em outras palavras, em nome da utilidade pública e interesse coletivo, parece-nos ser possível, quando autorizado pelo titular, ser tratado o dado de forma anônima, e, como dito acima, gerar dados estatísticos, sem a possibilidade vincular o titular, região demográfica ou qualquer outra informação que possibilite a discriminação de um indivíduo ou coletividade.

Já (iii) os dados anonimizados, que são dados pessoais que tenham sido descaracterizados, codificados ou pseudonimizados. Nos termos do art. 12 da LGPD, os dados anonimizados estão, a princípio, excluídos do escopo de aplicação da lei, notadamente porque esses dados não têm o condão de identificar, de forma direta ou indireta o seu titular, portanto, não têm potencial de lhe causar danos e, por conseguinte, não requerem a proteção da lei. Porém, os dados anonimizados podem ser utilizados para reidentificar uma pessoa. Quando isso ocorre, eles se transformam em dados pessoais, portanto abrangidos pelo âmbito de aplicação do LGPD. A anonimização é, inclusive, um dos procedimentos previstos na LGPD para assegurar proteção aos dados pessoais, e deve ser utilizada sempre que possível.

Conforme mencionado anteriormente, a lei brasileiro sofreu significativa influência da GRPD, reconhecendo, logo em seu artigo 2º, a tutela dos dados pessoais como meio de resguardar os direitos da privacidade, liberdade de expressão, imagem, honra, livre iniciativa, livre concorrência e a defesa ao consumidor, além de utilizar termos importantes como a defesa da autodeterminação informativa (art. 2º, II) e a proteção dos direitos humanos (art. 2º, VII) como fundamentos da tutela de proteção de dados no Brasil.

---

[23] Art. 11: "O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador." (BRASIL, 2018).

4.4.2 Agentes de tratamento de dados

O texto também cria as figuras dos agentes de tratamento de dados pessoais, que são o Controlador[24] e o Operador,[25] sendo o último encarregado pelo tratamento dos dados pessoais de acordo com as disposições legais da matéria, nos termos do art. 37 e o primeiro responsável em manter devidamente o registro das operações de tratamento de dados pessoais, de acordo com o art. 39.

O mesmo artigo elucida que o controlador é pessoa, seja natural ou jurídica, de direito público ou privado, que é o responsável direto, ou seja, é que indica quais dados serão coletados e tratados, razão pela qual possui maior responsabilidade e autonomia, devendo cumprir todas as obrigações legais e os deveres anexos. O operador, por sua vez, é aquele que realiza a operação propriamente dita. Também pode ser pessoa física ou jurídica, de direito privado ou público, sendo sua responsabilidade, via de regra, mais branda que a do controlador. O Encarregado é o sujeito que se inter-relaciona com o titular, controlador e a finada autoridade nacional, sendo facilitado sua identidade e contato. O artigo 41 da lei atribui, em rol exemplificativo, diversas atividades ao encarregado, vejamos:

> § 2º As atividades do encarregado consistem em: I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da autoridade nacional e adotar providências; III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. (BRASIL, 2018).

Por banco de dados, entende-se como o [...] conjunto estruturado de dados pessoais, também conhecido como "*big data*". Entretanto, não são considerados agentes de tratamento o titular, o banco de dados e o encarregado, sendo citados neste tópico para fins de esclarecimento.

Os agentes de tratamento são subordinados à Autoridade Nacional de Proteção de Dados (ANPD), que é um órgão da administração pública direta federal que faz parte criada pela LGPD, cujas atribuições estão relacionadas a proteção de dados pessoais e da privacidade e

---

[24] Art. 5º Para os fins desta Lei, considera-se: [...] VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. (BRASIL, 2018).
[25] Art. 5º Para os fins desta Lei, considera-se: [...] VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. (BRASIL, 2018).

que, sobretudo, deve fiscalizar o cumprimento da lei, podendo sancionar, conforme art. 52, aqueles que cometam infrações com multas de 2% do faturamento da pessoa jurídica infratora, sendo este valor limitado ao montante de R$ 50.000.000,00 (cinquenta milhões de reais).[26] O art. 38 prevê ainda que a ANPD tem o poder de exigir a confecção do Relatório de Impacto à Proteção de Dados das atividades das empresas, resguardados segredos industriais, sendo esse um importante instrumento para a melhor compreensão dos riscos vinculados a coleta de dados em diferentes atividades econômicas. Esta é, inclusive, mais uma das diversas influências diretas do Regulamento Europeu no normativo brasileiro. Não obstante, a responsabilidade civil desses sujeitos será oportunamente analisada, esclarecendo o quanto exposto no código civil, bem como na LGPD.

Importa mencionar que o titular de um dado pessoal, conforme disposição do inciso V do art. 5º da LGPD, é a "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento" (BRASIL, 2018).

4.4.3 Princípios

A Lei Geral de Proteção de Dados, dentre diversas disposições, voltou-se, cuidadosamente, a estabelecer os princípios que deverão ser respeitados por ocasião do tratamento de dados. Com relação a estes princípios, estão todos previstos no art. 6º. Importa lembrar que, quando uma norma é denominada de princípio, significa que ela tem uma forma específica de ser interpretada. Nesse sentido, define Alexy, *in verbis*:

> O ponto decisivo na distinção entre regras e princípios é que princípios são normas que ordenam que algo seja realizado na maior medida possível dentro das possibilidades jurídicas e fáticas existentes. Princípios são, por conseguinte, mandamentos de otimização, que são caracterizados por poderem ser satisfeitos em graus variados e pelo fato de que a medida devida de sua satisfação não depende somente das possibilidades fáticas, mas também das possibilidades jurídicas. O âmbito das possibilidades jurídicas é determinado pelos princípios e regras colidentes. (ALEXY, 2006, p. 90).

[26] Rol completo das multas previstas pela Lei 13.709/18: "Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II; IV - publicitação da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração". (BRASIL, 2018).

Isto posto, os princípios elencados no mencionado art. 6º da LGPD têm importância significativa na compreensão e aplicação da normativa. Já no caput deste artigo se vê que, além dos princípios, deve-se observar a boa-fé, que, nesse caso, é objetiva por se tratarem de relações jurídicas em que interessam as repercussões de determinadas condutas, principalmente em em relação àquelas de caráter obrigacional (LÔBO, 2017). Portanto, passamos a analisar, brevemente, cada princípio individualmente.

4.4.3.1 Princípio da Finalidade

O primeiro princípio, previsto no art. 6°, inciso I, é o da finalidade, definido pelo normativo como a realização do tratamento para propósitos específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. Conforme salienta Doneda (2006):

> Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que é possível a estipulação de um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade (fora da qual haveria abusividade). (DONEDA, 2006, p. 216).

Segundo Pestana,[27] por legítimo, entende-se o propósito vinculado a uma finalidade movida pela boa-fé, legalidade e bom senso, distanciando-se, portanto, da iniciativa ilícita e de má fé. Já o propósito específico é aquele cujo objetivo é determinado e relevante, sendo vedada a finalidade genérica e indeterminada. Já propósitos explícitos dizem respeito à clareza de objetivos que deverão ser previamente determinados, não permitindo ambiguidades, que podem gerar dúvidas quanto ao seu conteúdo.

Por fim, esses objetivos devem ser informados ao titular e submetidos ao seu consentimento, sendo vedada a alteração subsequentemente, salvo, se nova, específica e expressa concordância for obtida desse mesmo titular.

4.4.3.2 Princípio da Adequação

No intuito de garantir a tutela dos direitos do titular de dados pessoais, o legislador apontou, no art. 6°, inciso II, o princípio da adequação. Este princípio estabelece que os dados

[27] Disponível em: <https://www.conjur.com.br/dl/artigo-marcio-pestana-lgpd.pdf>. Acesso em: 16 mar. 2021.

pessoais tratados devem ser compatíveis com a finalidade informada pelo agente e de acordo com o contexto do tratamento.

A adequação refere-se, portanto, ao nexo de pertinência lógica de conformidade que se estabelece entre o tratamento, a finalidade objetivada e a comunicação transmitida ao titular.

4.4.3.3 Princípio da Necessidade

Previsto no inciso III do referido dispositivo, o princípio da necessidade consubstancia-se na limitação do tratamento de dados pessoais ao mínimo necessário para realização da finalidade objetivada, com abrangência dos dados pertinentes e proporcionais.

Isso quer dizer que os agentes devem utilizar apenas os dados estritamente necessários para alcançar a uma finalidade - previamente delimitada e aprovada pelo titular dos dados correspondentes - e nos limites do que se mostrarem imprescindíveis para que essa finalidade seja alcançada. Nem poderia ser diferente, pois seria impróprio tratar dados impertinentes ou excessivos.

4.4.3.4 Princípio da Transparência

Previsto no art. 6º, VI da LGPD, o princípio da transparência visa garantir que aos titulares dos dados sejam prestadas informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e sobre os respectivos agentes de tratamento, resguardados os segredos industriais e comerciais.

Isso significa que todas as informações passadas pela organização, em todos os seus meios de comunicação, devem ser claras, precisas e verdadeiras.

O emprego de conteúdo excessivamente técnico não se compagina com o objetivo do princípio da transparência, já que o que se procura garantir é que qualquer pessoa, seja qual for o grau cultural que detenham, possam facilmente compreender o que ocorrerá com os seus dados.

4.4.3.5 Princípio da Segurança

O princípio da segurança – art. 6, VII, – compreende as medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. A ideia central

desse princípio, que atua junto ao princípio da prevenção, é de preservar o ambiente seguro, utilizando e aprimorando técnicas de segurança para mitigar e prevenir eventuais incidentes.

Para Pestana,[28] em caso de incidentes, segundo esse princípio, é irrelevante se a perda, acesso, alteração ou difusão resulte de uma conduta voluntária, ou seja, resultado de negligência, imprudência ou imperícia: a proteção dos dados é uma obrigação e o tratador deve prever todos os cenários de possíveis riscos e se precaver contra todos eles. Já para Oliveira (2019), a culpa não será presumida, mas oriunda de verificação técnica de determinada violação (OLIVEIRA, 2019, p. 22).

4.4.3.6 Princípio do Livre Acesso

Previsto no inciso IV, este princípio possibilita a clareza para o titular dos dados sobre a forma e duração do tratamento de suas informações. Deve haver um canal para que o titular tenha acesso aos dados que estão sob a tutela do agente de tratamento. Note que esse princípio gera uma obrigação, isto porque o agente fica incumbido na tarefa de abrir o seu arquivo para que o titular possa avaliá-lo, mas somente em relação aos dados que lhe dizem respeito. Essa consulta deve ser gratuita.

4.4.3.7 Princípio da Qualidade dos Dados

Como mencionado em tópicos introdutórios, a qualidade dos dados é importante a medida em que, com base nas informações coletadas, uma série de decisões serão tomadas a respeito do titular dos dados.

Para isso, o controlador deve tomar medidas para garantir que o dado reflita da melhor maneira possível a realidade:

> Qualquer imprecisão, seja um dado pessoal equivocado, seja desatualizado, pode ser catastrófico ao titular, como ocasionar um erro de tratamento médico, recusa de crédito, vedação de participação em concursos públicos, eliminação em processo seletivo, ou, até mesmo, uma prisão injusta. (MALDONADO; BLUM, 2019, p. 149).

Portanto, tal princípio consubstancia-se na garantia de exatidão, clareza, relevância e atualização desses dados. Ora, não poderia ser de outra maneira, se o titular libera acesso aos seus dados, o mínimo que pode esperar é que não contenham imprecisões.

---

[28] Disponível em: <https://www.conjur.com.br/dl/artigo-marcio-pestana-lgpd.pdf>. Acesso em: 16 mar. 2021.

4.4.3.8 Princípio da Segurança

Para que haja efetiva proteção de dados é imprescindível a observância da segurança. Isso significa que os agentes de tratamento devem aplicar todos os meios possíveis, sejam eles de amparo técnicos ou de conscientização, para manter a segurança das informações tratadas. Isso para evitar acessos não autorizados e vazamentos de dados.

Este princípio é importante para este trabalho, porque implica na responsabilidade por eventuais danos causados por incidentes. Cumpre salientar que os riscos do empreendimento devem ser mitigados pela aplicação de procedimentos, meios e tecnologias capazes de impedir as tentativas e falhas no processo de tratamento de dados.

Importante considerar aqui, que, para Pestana,[29] para o princípio da segurança, é irrelevante "se a perda, acesso, alteração ou difusão resulte de uma conduta voluntária e, portanto, ilícita, ou se decorra de um mero acidente, seja ou não resultado de negligência, imprudência ou imperícia". Isto porque, para o autor, o agente de tratamento é obrigado a prever todos as possibilidades que possam ocorrer envolvendo o acesso e manuseio indevido as informações.

4.4.3.9 Princípio da Prevenção

Ainda que pareça redundante, mas a prevenção deve ser a tônica da segurança. Por isso, o legislador resolveu prestigiar este princípio de forma expressa para que, no processo de tratamento, sejam adotadas as medidas necessárias para prevenir a ocorrência de danos, estabelecendo que tais medidas devem ser tomadas desde a concepção do projeto, se possível.

Para tanto, destaca-se a importância do encarregado, que, como mencionado alhures, é o responsável por atuar na comunicação entre o controlador, titulares dos dados e a Agência Nacional de Proteção de Dados.

4.4.3.10 Princípio da Não Discriminação

Segundo princípio da não discriminação, previsto no art. 6, inciso IX, é vedada a utilização de dados pessoais com fins discriminatórios considerados ilícitos ou abusivos, sendo

[29] Disponível em: <https://www.conjur.com.br/dl/artigo-marcio-pestana-lgpd.pdf>. Acesso em: 16 mar. 2021.

que esses dois aspectos são limitadores para caracterizar certas atividades como discriminatórias. De acordo com Mulholland (2018), é possível o tratamento diferenciado de dados, mas desde que respeitado o princípio da boa-fé objetiva. Nesse sentido:

> Isto é, aparentemente, seria legítimo ao operador de dados realizar tratamentos de segregação, no sentido de diferenciação, sem que, com isso leve a consequências excludentes que poderiam ser consideradas ilícitas. Assim, por exemplo, seria legítimo a um operador de dados que esteja realizando a precificação de um serviço de seguros de automóveis, tratar de maneira diferenciada os dados de mulheres entre 35 e 45 anos e mães, com a finalidade de oferecimento de um valor que reflita os riscos de danos usualmente ocasionados ou sofridos por esse grupo determinado de pessoas. (MULHOLLAND, 2018, p. 163-164).

Assim, não se pode excluir de titulares de dados pessoais, no momento de seu tratamento, informações determinadas por características, sejam elas de origem racial ou étnica, opinião política, religião ou convicções, geolocalização, filiação sindical, estado genético ou de saúde ou orientação sexual, em desrespeito à boa-fé.

4.4.3.11 Princípio da Prestação de Contas

O princípio da responsabilização e prestação de contas tem importância central na disciplina do tratamento de dados. Segundo esse princípio, os sujeitos do tratamento de dados têm o ônus de responderem por seus atos, na medida de suas ações ou omissões. Isso os obriga, além de cumprir com todos os requisitos legais, que comprovem a efetividade das medidas adotadas e, em caso de descumprimento e dano ao titular, haverá responsabilização. Nesse sentido:

> Prever a responsabilização e a prestação de contas como princípio demonstra a intenção da Lei em alertar os controladores e os operadores de que são eles os responsáveis pelo fiel cumprimento de todas as exigências legais para garantir todos os objetivos, fundamentos e demais princípios nela estabelecidos. E não basta somente pretender cumprir a Lei, é necessário que as medidas adotadas para tal finalidade sejam comprovadamente eficazes. Ou seja, os agentes deverão, durante todo ciclo de vida de tratamento de dados sob sua responsabilidade, analisar a conformidade legal e implementar os procedimentos de proteção dos dados pessoais de acordo com a sua própria ponderação de riscos. (MALDONADO; BLUM, 2019, p. 166-167).

Vale citar, aqui, que nas lições de Rosenvald (2017), a responsabilidade civil vai além da função apenas restaurativa, pois se presta também a uma função preventiva, cumprindo um papel civilizatório. Por isso, o princípio da prestação de contas assume relevante papel para este trabalho, conforme se verificará em tópico específico (ROSENVALD, 2017).

4.4.4 Atribuições da Autoridade Nacional de Proteção de Dados

Como citado anteriormente, a Autoridade Nacional de Proteção de Dados foi criada para implementar e fiscalizar a LGPD. Porém, essa não será a única função do órgão, de acordo com o art. 55 de legislação de proteção de dados, compete e são responsabilidades da ANPD: (i) zelar pela proteção dos dados pessoais nos termos da legislação, incluindo a Lei Geral de Proteção de Dados; (ii) zelar pela observância dos segredos comerciais e industriais, ao mesmo tempo que preserva a proteção de dados pessoais e o sigilo de informações protegidas por lei; (iii) elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; (iv) fiscalizar e aplicar sanções em casos de descumprimento à legislação no que diz respeito ao tratamento de dados, assegurando o contraditório, a ampla defesa e o direito de recurso; (v) gerenciar petições do indivíduo titular dos dados pessoais contra o controlador, após comprovação do cidadão de que o controlador não solucionou sua reclamação no prazo determinado pela LGPD; (vi) promover entre a população o conhecimento e a conscientização sobre as normas e as políticas públicas sobre proteção e privacidade de dados pessoais, assim como estudos sobre o tema; (vii) estimular as instituições a adotar padrões para seus serviços e produtos que tornem mais fácil para os indivíduos controlarem seus dados pessoais, levando em consideração as particularidades da atividade e do porte das organizações; (viii) atuar de forma cooperativa com as autoridades de proteção de dados pessoais de outros países; (ix) divulgar as melhores práticas para a publicidade das operações de tratamento de dados pessoais, preservando os segredos comerciais e industriais; (x) a qualquer momento, solicitar que as entidades do poder público prestem informações sobre o âmbito, a natureza dos dados e quaisquer outros detalhes do tratamento de dados realizado por elas; (xi) editar relatórios de impacto à proteção de dados pessoais nos casos em que o tratamento dessas informações represente alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos por lei; (xii) elaborar e divulgar relatórios anuais discorrendo sobre a gestão de suas atividades, que devem incluir o detalhamento das receitas e despesas do órgão; (xiii) ouvir os agentes de tratamento e a sociedade em matéria de interesse relevante e prestar contas sobre suas atividades e planejamento; (xiv) realizar auditorias ou providenciar a realização de auditorias sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluindo do poder público; (xv) resignar agentes de tratamento para eliminar irregularidades, incertezas e situações de risco relacionados ao tratamento e à privacidade de dados pessoais; (xvi) editar normas, orientações e procedimentos diferenciados, inclusive quanto aos prazos, para auxiliar microempresas, empresas de pequeno porte, empresas de inovação e startups a se adequarem às regras de

proteção e privacidade de dados; (xvii) garantir a simplicidade, a clareza, a acessibilidade e a devida adequação do tratamento dos dados pessoais de idosos; (xviii) comunicar as infrações penais relacionadas à lei às autoridades competentes e, quando o descumprimento for por parte de órgãos e entidades da administração pública federal, também aos órgãos de controle interno; (xix) implementar mecanismos simplificados, inclusive pela internet, para o registro de reclamações e denúncias sobre o tratamento de dados pessoais em desconformidade com a lei.

Na medida em que a LGPD tem um desenho bastante peculiar, é importante entender que a responsabilidade é compartilhada entre todos os sujeitos que compõe o ecossistema da proteção de dados no Brasil para entendermos o modelo de regulamentação cristalizado na legislação protetiva.

5. RESPONSABILIDADE CIVIL NO ORDENAMENTO JURÍDICO BRASILEIRO

Relativo ao ramo do direito obrigacional, a responsabilidade civil é um instituto que decorre do reconhecimento dos direitos pessoais, ou seja, são normas que visam manter o bom convívio em sociedade, garantindo que, uma vez prejudicado determinado direito, haverá a reparação do dano que infligido. A violação, portanto, é ato ilícito que gera a obrigação de reparar e cria um vínculo jurídico que outorga a uma parte o direito de exigir da outra que cumpra determinada prestação (GONÇALVES, 2016, p. 45).

Não é proveitoso, para este trabalho, tratar da evolução histórica da responsabilidade civil no ordenamento brasileiro, basta que citemos que, para Rosenvald, o instituto é hodiernamente organizado de uma forma a abarcar a responsabilidade em que não é necessário provar a culpa (ROSENVALD, 2017).

Nessa responsabilidade civil objetiva, entende-se que, provados o dano e o nexo causal, há o dever de reparar. Conforme art. 393 do Código Civil, o causador do dano apenas se desincumbe se demonstrar a ocorrência de exclusão do nexo causal, como na ocorrência de caso fortuito ou força maior. A doutrina não é unânime ao tratar de caso fortuito e força maior. Adotaremos, neste trabalho, a lição de Tartuce, que considera *"*caso fortuito como o evento totalmente imprevisível decorrente de ato humano ou de evento natural. Já a força maior constitui um evento previsível, mas inevitável ou irresistível, decorrente de uma ou outra causa*"* (TARTUCE, 2016, p. 436).

Outro marco intransponível no que tange a responsabilidade civil é o Código de Defesa do Consumidor, Lei nº 8.078 de 1990. A Constituição, ao determinar que o Estado promovesse a defesa do consumidor,[30] reconheceu a vulnerabilidade deste e, consequentemente, no Código de Defesa do Consumidor, a responsabilidade pelos danos causados em decorrência da relação de consumo independe de prova de culpa, salvo a responsabilidade dos profissionais liberais.

É fato que ambos os sistemas de responsabilidade (objetivo e subjetivo) foram contemplados pelo legislador na codificação de 2002. Apesar da inovação, a responsabilidade subjetiva, que ganhou relevo com o Código Napoleônico de 1804 inspirando o Código Civil de 1916, permaneceu viva no art. 186 do diploma atual, que assim dispõe: "Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito". Portanto, o atual Código Civil compatibilizou ambos os sistemas de responsabilização existentes.

---

[30] art. 5º, inciso XXXII e art. 170, inciso V da CF.

Fato é que, segundo Schwab (2018) estamos vivendo a Quarta Revolução Industrial, notadamente em razão da evolução tecnológica. Essa evolução, não é novidade, resulta na alteração na forma de tratamento dos fatos jurídicos e institutos de direito para abarcar as novas peculiaridades (SCHWAB, 2018). Nesse contexto, novas perspectivas da responsabilidade civil se estabelecem, com crescente ampliação das hipóteses de responsabilidade objetiva, a jurisprudência tem amalgamado na ampliação das hipóteses de indenização pelo dano presumido (SCHREIBER, 2015).

Para Godoy (2019), as novas tecnologias trazem à tona novos riscos. O autor propõe que estes devem ser analisados à luz da releitura dos institutos tradicionais da responsabilidade civil, cabendo às novas leis estabelecer regras de conduta no espaço virtual, deveres imputados aos agentes dessa nova relação jurídica, prevendo critérios de escolha daquele que ressarcirá por eventual dano provocado (GODOY, 2019).

No que tange às disposições da LGPD, vimos que, uma vez em posse (legítima e consentida) dos dados pessoais ou sensíveis, os agentes de tratamento poderão tratá-los livremente desde que observados os princípios e limites estabelecidos pela legislação e regulação oriunda da Autoridade Nacional de Proteção de Dados, sob pena de incorrer em responsabilidade civil, tema que discutiremos nos próximos tópicos deste capítulo

5.1. A Responsabilidade Civil na Lei Geral de Proteção de Dados:

O tema da responsabilidade e ressarcimento de danos imputados aos agentes de tratamento foi inserido na Seção III do Capítulo VI, intitulado “Dos agentes de tratamento de dados pessoais”. O *caput* do art. 42 “caput” prevê o dever de reparação civil por dano patrimonial, moral, individual ou coletivo, imposto aos controladores e operadores, em ocasião das operações de tratamento de dados em que haja violação à LGPD.

Como visto no tópico 4.1.2, a legislação de proteção de dados estabelece um conjunto de princípios e regras que procuram criar um ambiente de responsabilidade proativa, ou seja, de cunho preventivo, considerando o risco potencial de ocorrência de lesão na coleta e tratamento de informações, especialmente ante os riscos inerentes à uma sociedade de classificação (FRAZÃO, 2019, p. 35), e propõe um sistema de responsabilização capaz a propiciar a efetiva tutela da vítima e a reparação integral do dano distribuídos entre os arts. 42 a 45 da lei.

O art. 42 da LGPD[31] contém uma cláusula geral de responsabilidade, imputando a obrigação de indenizar ao controlador ou operador que, descumprindo a lei, causar dano patrimonial ou extrapatrimonial aos titulares dos dados pessoais violados. A LGPD estabeleceu, de forma similar ao Código de Defesa do Consumidor - CDC (Lei 8.078/90), a solidariedade dos agentes de tratamento que causarem lesão (art. 42, § 1º, I e II) e permitiu a inversão do ônus da prova por critério judicial (art. 42, § 2º) para mitigar a assimetria na relação entre controladores, operadores e titulares de dados pessoais.

Para Tasso (2020), o referido dispositivo, não exclui nem prevê o elemento culpa, e conclui "que são utilizados apenas dois critérios objetivos para fundamentar a responsabilidade, quais sejam, o exercício da atividade de tratamento de dados e a violação da legislação de proteção de dados" (TASSO, 2020).

No art. 43, a LGPD traz as hipóteses de exceção da responsabilidade dos agentes de tratamento, quando ocorre quando demonstrarem que i) não realizaram o tratamento dos dados pessoais, ii) se o realizaram, não violaram as normas de proteção de dados pessoais ou iii) que o dano foi causado por terceiro ou pelo próprio titular (art. 43, I a III).[32] O conceito de tratamento irregular de dados está previsto no dispositivo seguinte,[33] que ocorrerá quando contrariar a disciplina legal (art. 44, caput) ou quando não fornecer a segurança legitimamente esperada pelo respectivo titular (art. 44, I a III). Note que o § único do estabelece o dever de

---

[31] Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. § 1º A fim de assegurar a efetiva indenização ao titular dos dados: I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei; II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.§ 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa. § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente. § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso. (BRASIL, 2018).

[32] Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem: I - que não realizaram o tratamento de dados pessoais que lhes é atribuído; II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro. (BRASIL, 2018).

[33] Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado. Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano. (BRASIL, 2018).

indenizar derivado da violação de normas técnicas oriundas da Autoridade Nacional de Proteção de Dados (ANPD).

Já o art. 45, último da Seção III, ressalva que as situações de lesão a direito de consumidor ou pessoa a ele equiparada continuam sujeitas à disciplina do microssistema de relações de consumo instituído pelo CDC (Lei 8.078/90).

O tratamento da responsabilidade civil no âmbito da LGPD tem sido tema cadente nos debates e na doutrina moderna, isso porque a sua aplicabilidade concreta ainda não foi exprimida em julgados ou decisões administrativas de cunho normativo a balizar o debate sobre a responsabilidade civil dos agentes de tratamento, já que as sanções serão aplicadas somente a partir de agosto de 2021.

O fato é que, como elucida Tasso, há imprecisão normativa quanto ao sistema de responsabilidade civil adotado pela LGPD, pois o enunciado do art. 42 não teria sido suficientemente claro quanto ao regime de responsabilidade civil adotado pela norma (CAPANEMA, 2020, p. 165-167). Nesse contexto, há duas linhas que se formaram a respeito do tema cujo embate é travado entre posições que afirmam ter a lei estabelecido um sistema baseado na responsabilidade objetiva ou subjetiva, sendo respeitáveis ambos os posicionamentos (TASSO, 2020, p. 104). Debates dessa natureza tem se intensificado nas relações entre direito e Internet, conforme observado por Tepedino e Silva:

> Tais linhas teóricas compartilham o esforço de definição das soluções mais adequadas aos novos problemas. Identificam-se, nesse sentido, variadas formulações que enunciam princípios éticos próprios para a regulação dos robôs e demais sistemas autônomos. As célebres Leis de Asimov servem como boa representação do quanto exposto: o temor (ou encanto) das novidades tecnológicas parece instigar a formulação de novas regras e novas soluções. Empreende-se, assim, grande esforço para a concepção de respostas que se possam reputar adequadas aos novos desafios suscitados pela inteligência artificial. (TEPEDINO; SILVA, 2019, p. 70).

Para os autores Mendes e Doneda, que se filiaram à linha de responsabilidade civil objetiva, o principal argumento é que a atividade de tratamento de dados representa um risco intrínseco, na medida em que há uma potencialidade danosa significativa em caso de violação dos direitos dos titulares, que se caracterizam, como visto no capítulo 3, por sua natureza de direito personalíssimo e de direito fundamental. Em outras palavras, o tratamento de dados pessoais se encaixaria como atividade de risco (MENDES; DONEDA, 2018).

Nesse diapasão, considerando o CC a fonte última irradiadora de princípios e regras de direito privado, a interpretação do art. 42 da LGPD não poderia ser realizada de forma incoerente com o disposto no art. 927, que estabelece a forma excepcional de responsabilização

objetiva: “Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.”

A conclusão de que a atividade de tratamento de dados é de risco, para essa corrente, vem do próprio art. 42 da LGDP, anteriormente abordado, que reconhece o risco de forma implícita na expressão “em razão do exercício de atividade de tratamento de dados pessoais”, bem como explicitamente admitidos em outros dispositivos da norma (art. 5º, XVII; art. 38, § único; art. 44, II; art. 48, caput c/c § 1º, IV; art. 50, caput c/c § 1º; art. 55, XIII).

Devlin assevera que, por mais zeloso que seja o agente, nenhuma atividade humana é livre de riscos (DEVLIN, 2015, p. 99), devendo o direito fixar regras que permitam alocá-los adequadamente. Em sentido análogo, Stajn, esclarece que “se os riscos são probabilidades de ganhos ou perdas, quanto a estas, é preciso modelar instrumentos que permitam transferir ou mitigá-las (STAJN, 2011, p. 8).

Também as considerações a respeito da finalidade da lei e dos princípios por ela adotados (necessidade, prestação de contas, entre outros), levam os referidos autores a concluir que o legislador optou por um regime de responsabilidade objetiva, vinculando o exercício da atividade de tratamento de dados pessoais a um risco inerente, potencialmente causador de danos a seus titulares.

Outro argumento, defendido por Novakosk e Naspolini, é que a LGPD não pode desconsiderar a coerência interna do sistema de responsabilidade civil no direito brasileiro e todo a trajetória do instituto ao longo da história, que, para os autores, prestigia a responsabilidade civil objetiva, fundada nos princípios de equilíbrio na distribuição dos riscos, na equidade no tratamento dos agentes e das vítimas, e no ideal de solidariedade social, concentra suas preocupações na reparação do dano injusto causado à vítima, o que se mostraria essencial na sociedade da informação e do risco (NOVAKOSKI; NASPOLINI, 2020). Nesse sentido:

> [...] a história já demonstrou que a adoção dos modelos de culpa presumida ou de responsabilidade objetiva, que flexibilizaram a dificuldade da prova da culpa, não limitaram o desenvolvimento de novas tecnologias. Ao contrário: assegurou-se o pleno desenvolvimento tecnológico e industrial e os custos dos modelos de responsabilização objetivos, em especial nas relações de consumo, foram incorporados pelo mercado sem prejuízo do ressarcimento das vítimas de danos injustos, implementando-se o modelo solidarista de responsabilidade fundado na atenção e no cuidado para com o lesado. Ademais, já pontuava Rodotà, o argumento de eventual aumento dos custos de proteção dos dados pessoais para as empresas não é decisivo, vez que não se pode considerar que interesses ligados à proteção de dados pessoais dos titulares sejam de status inferior aos interesses empresariais. (MORAES, 2019, p. 4).

Para os autores, não faria sentido a LGPD ter criado um sistema de proteção de dados pessoais se, na concretização deste sistema, ele fosse débil ao propiciar uma situação de perpetuação do estado de lesão a um direito de personalidade.

Um outro argumento utilizado é de que a responsabilidade não poderia ser subjetiva, eis que o tratamento também pode ser feito por ente público que responde objetivamente, conforme asseveram, Novakoski e Naspolini (2020):

> Seria contraditório, ainda, que a LGPD permitisse que a responsabilidade civil decorrente de um mesmo fato objetivamente considerado —violação de normas de proteção de dados pessoais— pudesse ter tratamento diferenciado conforme a natureza do agente envolvido, isto é, subjetiva para agentes de direito privado e objetiva para entes de direito público, dado que, não tendo regulado explicitamente a responsabilidade civil destes últimos, a respectiva responsabilidade civil forçosamente observará a teoria do risco administrativo (art. 37, § 6º, CF/88), logo, será objetiva para os atos comissivos e subjetiva para os omissivos. (NOVAKOSKI; NASPOLINI, 2020, p. 170).

A respeito do tema, Tasso faz assevera que a responsabilidade civil do ente público se dá com fundamento na teoria do risco administrativo, e que pode ser tanto subjetiva quanto objetiva:

> Dessa forma, segundo o entendimento do Supremo Tribunal Federal, a responsabilidade estatal no espectro das atividades de tratamento de dados pessoais é analisada segundo os critérios da responsabilidade objetiva para os atos comissivos, aqui exemplificados como o tratamento e o compartilhamento irregular de dados e, por outro lado, segundo os pressupostos da responsabilidade subjetiva em se tratando de ato omissivo, como, por exemplo, a não observância das normas de prevenção e de segurança da informação a oportunizar o vazamento de dados pessoais dos cidadãos. (TASSO, 2020, p. 105).

Para autores como Tasso (2020) e Guedes e Meireles (2019), a LGPD adotou a teoria subjetiva da responsabilidade civil, sendo imprescindível a prova da conduta culposa do agente de tratamento na ocasião do dano, por sua vez fundamentada (i) na omissão na adoção de medidas de segurança para o tratamento adequado dos dados e (ii) no descumprimento das obrigações impostas na lei (TASSO, 2020; GUEDES; MEIRELES, 2019).

As autoras Sampaio e Meireles explicam que o Capítulo VI da LGPD que trata das condutas a serem seguidos pelos agentes de tratamento de dados em relação a segurança, sigilo, boas práticas e governança de dados, seria o fundamento para o reconhecimento da responsabilidade subjetiva (GUEDES; MEIRELES, 2019).

Na análise das excludentes de responsabilidade do artigo 43, o inciso II parece indicar a adoção de uma excludente tipicamente relacionada às hipóteses de responsabilidade civil subjetiva ao estabelecer que só não serão responsabilizados se, ainda que exista o dano, não

houver violação da legislação de proteção de dados. A violação da lei seria o elemento subjetivo da obrigação de indenizar e indicaria a conduta culposa do agente de tratamento de dados.

Em outras palavras, o legislador teria deixado indícios de que a LGPD adota a teoria subjetiva da responsabilidade civil, calcadas (i) no artigo 42, quando menciona as medidas de segurança; (ii) no art. 43, II, quando estabelece excludente de ilicitude referente ao cumprimento das normas da LGPD.

Para Tasso, a LGPD não ignorou a coerência interna do sistema de responsabilidade civil no direito brasileiro, mas criou um sistema de responsabilidade civil compatível com o CC e o CDC para regular as relações jurídicas de direito privado baseadas no tratamento de dados pessoais:

> A despeito dos embates doutrinários, verifica-se que a Lei Geral de Proteção de Dados elegeu o sistema de responsabilidade civil subjetiva em perfeito alinhamento com o Código Civil, inserindo-se de forma harmoniosa no mosaico legislativo, o mesmo ocorrendo em relação ao Código de Defesa do Consumidor que, dado o tratamento Constitucional da defesa do consumidor, atrai para seu sistema de responsabilidade objetiva os fatos jurídicos dessa natureza. (TASSO, 2020, p. 113).

Para Gualda e da Matta,[34] não é possível encarar toda atividade de tratamento de dados como sendo de risco em virtude da ampla variabilidade das atividades envolvendo o tratamento, sendo que alguma delas tem baixo potencial danoso, "como a troca de cartões de visita em atividades comerciais", e a concluem que adotar o modelo de responsabilização objetiva é contraditório com o próprio espírito da lei, a medida em que seria um desincentivo, aos agentes de tratamento, observarem as boas práticas de tratamento de dados pessoais e isso seria um prejuízo ao próprio titular dos dados:

> [...] a responsabilização objetiva dos agentes de tratamento os tornaria responsáveis pelos danos causados a titulares, independentemente de qualquer conduta contrária à legislação. Ou seja, eles poderiam ser responsabilizados por ocorrências de dano aos titulares que não decorressem de qualquer previsão legal ou regulatória sobre os parâmetros necessários ao tratamento de dados. Nesse cenário, ficaria a dúvida: se a conduta do agente não importa para a aplicação da responsabilidade, qual a razão para a adoção de boas práticas ou o investimento em medidas de adequação custosas? Parece-nos que a interpretação mais apropriada da responsabilidade estabelecida na LGPD é a de que ela seria baseada na culpa (ainda que se possa argumentar pela responsabilidade civil com a culpa presumida). Essa interpretação também se manifesta como apontando para o melhor interesse do próprio titular de dados, isso porque o incentivo às boas práticas – resultante do foco na conduta culposa do agente – resulta em maior proteção para o titular. (GUALDA; DA MATTA, 2020, p. 1).

---

[34] Disponível em: <https://www.machadomeyer.com.br/pt/inteligencia-juridica/publicacoes-ij/tecnologia/responsabilidade-subjetiva-na-lgpd>. Acesso em: 16 mar. 2021.

Sendo assim, a responsabilidade civil seria baseada na culpa e as empresas poderão demonstrar em juízo as medidas efetivamente tomadas para manter a conformidade com a legislação e com a regulação de proteção de dados para resguardar-se contra hipóteses de responsabilização. Adotar o modelo de responsabilidade subjetiva seria uma forma de garantir, inclusive, o melhor interesse do titular de dados, isso porque o incentivo às boas práticas resulta em maior proteção para o titular.

Bioni e Dias[35] fazem um estudo bastante interessante sobre o tema da responsabilidade civil na LGPD. Para os autores, há um abandono deliberado do regime de responsabilidade civil objetiva e a adoção de técnica legislativa mais prescritiva quanto às excludentes de reponsabilidade civil. Para compreender os argumentos dos autores, necessário fazer um primeiro corte ao tema ora analisado.

Conforme visto no capítulo 4.2, foram quase dez anos de debate para que se chegasse à redação atual da Lei Geral de Proteção de Dados. Entender alguns aspectos de seu processo de criação é importante para compreendermos o papel da culpa no regime de responsabilidade civil no âmbito da LGPD. Processo esse que foi permeado por ricos debates públicos que deixaram pistas hermenêuticas para a definição do modelo de regime de reponsabilidade adotado.

A primeira versão do anteprojeto dispunha, em seu art. 6°:

> Art. 6°: O tratamento de dados pessoais é atividade de risco e todo aquele que, por meio do tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, é obrigado a ressarci-lo, nos termos da lei.

Também a segunda versão dispunha que a segunda que os agentes da cadeia responderiam, "independentemente da existência de culpa", pela reparação dos danos, *in literis*: "Art. 31. O cedente e o cessionário têm responsabilidade solidária pelo tratamento de dados realizado no exterior ou no território nacional, em qualquer hipótese, independente de culpa".

Como se vê, tanto a primeira versão do anteprojeto de lei a proposta legislativa do Senado Federal, expressamente adotavam um regime de reponsabilidade civil objetiva. Já a versão final da lei, consolidada no art. 42, eliminou os termos antes apresentados – "independentemente de culpa" ou "atividade de risco" – que eliminariam expressamente a culpa como um dos pressupostos da responsabilidade civil. Para os autores, é possível

[35] Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/662/506>. Acesso em: 16 mar. 2021.

depreender, assim, que houve abandono deliberado do regime de responsabilidade civil objetiva.

Além disso, princípio da responsabilidade e prestação de contas prescreve que os agentes devem desmontar da adoção de medidas eficazes capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, poderia levar a crer, se analisado isoladamente, que se trata de uma obrigação de resultado, o que implicaria em presunção de culpa. No entanto, a obrigação seria de meio, isso porque tanto o art. 46, que conceito de *privacy by design* ao definir que "agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito", quanto o art. 50, que dispõe que que a aptidão das medidas a serem adotadas deve ser ajustada de acordo as características da atividade de tratamento de dados em questão, levando em consideração "a gravidade dos riscos" que dela derivam para o titular; prescrevem uma norma de conduta e encerram uma obrigação de meio.

Os autores concluem que a LGPD adotou o modelo de responsabilidade civil subjetiva com alto grau de objetividade, isso porque facilitou a configuração do dever de indenizar, isso porque exige um "alto nível de diligência quanto ao estado da arte e da técnica como já o vem fazendo parte da doutrina consumerista, então se tornará extremamente difícil o agente de tratamento de dados afastar a sua culpa" (BIONI; DIAS, 2020).

Os autores propõem, no entanto, que mais importante do que a análise dualista de responsabilidade é analisar mais de perto os elementos normativos que restringiriam ou alargariam a discussão de culpabilidade para fins de responsabilização:

> Deve-se, assim, avançar para além da análise binária do regime jurídico de responsabilidade civil da LGPD, julgando-o de natureza objetiva ou subjetiva. Isto porque não deve haver dúvidas de que a política legislativa adotada exige a investigação em torno de um juízo de culpa dos agentes de tratamento de dados, mas, ao mesmo tempo, prescreve uma série de elementos com alto potencial de erosão dos filtros para que os agentes de tratamentos de dados sejam responsabilizados. Resultado parece ir no sentido deum regime jurídico de responsabilidade civil subjetiva com alto grau de objetividade. (BIONI; DIAS, 2020, p.22).

Por fim, diante de todo o debate acerca da natureza jurídica da responsabilidade na LGPD, não parece que o legislador simplesmente "esqueceu" de tratar de alguns temas. Em verdade, é nítido que o Brasil segue uma tendência legislativa que não mais aposta na lógica de comando e controle (lógica responsiva punitiva). O próprio desenho da lei de proteção de dados segue uma lógica na qual o legislador, de antemão, verifica que esse é um campo de regulação

onde há assimetria de informação, ou seja, não há como prever a dimensão do mercado a ser regulado porque é quase impossível enxergar todas as particularidades desse nicho diante do grande impacto regulatório que a lei traz, por isso a lei surge para estabelecer metas.

Nesse sentido, Bioni desenvolve o conceito de *accountability*, para demonstrar que a preocupação da legislação atual se refere não apenas ao poder do titular sobre os seus dados, mas à garantia de que os agentes econômicos, bem como o órgão regulador, estão sendo responsáveis para que prejuízos não sejam criados. Não é à toa que, como vimos no tópico 4.4.4, a lei estabelece obrigações e responsabilidades também para a Autoridade Nacional de Proteção de Dados e não apenas para os agentes de tratamento (BIONI, 2020).

Em conclusão, a despeito das respeitáveis opiniões que sustentam que o legislador estabeleceu a responsabilidade civil objetiva e considerando que o risco da atividade de tratamento de dados vai variar de acordo com cada setor, os argumentos dos autores Bioni e Dias nos parece pertinente para dizer que o legislador, intencionalmente, removeu do texto da lei a responsabilidade objetiva. Ora, se a lei não contém palavras inúteis - máxima basilar da hermenêutica jurídica - tampouco são excluídas palavras por mero capricho.

Soma-se a isto, o fato de que o legislador optou por eximir responsabilização dos agentes de tratamento caso comprovem "que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados" (art. 43, II). De igual modo, a LGPD dispõe sobre a responsabilidade civil pela violação à segurança dos dados, sendo que tal responsabilização surge somente caso as "medidas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação" não tenham sido adotadas. Esses elementos contidos no texto da lei afastam a aplicação do sistema de responsabilidade civil objetiva porque evidenciam o importante papel da culpa nesse sistema de responsabilização.

Um outro elemento que reforça, ainda que indiretamente, o regime de responsabilidade civil de natureza subjetiva é o fato de que a LGPD dedica uma seção específica sobre "Boas Práticas e da Governança" e "Segurança e Boas Práticas". A LGPD, portanto, deixa claro que será feito um juízo de valor em torno da conduta do agente de tratamento para sua responsabilização, que poderão demonstrar em juízo, as medidas efetivamente tomadas para manter a conformidade com a legislação para resguardar-se contra hipóteses de responsabilização.

Sem prejuízo, seria o caso de avaliar então se o tratamento de dados seria uma atividade de risco em si. Há uma ampla variabilidade das atividades de tratamento de dados pessoais, que podem se referir a condutas com baixo potencial danoso. Acerca do tema, ao tratar do Relatório

de Impacto à Proteção de Dados Pessoais, ao prescreve tal instrumento para casos em que as atividades de tratamento de dados fossem de “alto risco”, o legislador parece deixar pista de que não há nivelamento de risco para toda e qualquer atividade de tratamento de dados. Assim, considerando que a jurisprudência classificou a atividade de risco somente aquelas que objetivamente apresentem grave potencial ofensivo a direitos de terceiros, considerando que nem toda atividade de tratamento de dados são de alto risco, temos, mais uma vez, afastada a responsabilidade de natureza objetiva.

Ao elaborar um texto “em aberto” a LGPD atribuiu bastante discricionariedade para os agentes de tratamento de dados pessoais: é ele quem avalia, por exemplo, a melhor base legal para o tratamento que realiza, dentre outras questões. Não obstante, a lei exige que o agente preste contas sobre todas as atividades que englobam esse tratamento, que deve estar escorado no texto legal. A prestação de contas, como visto, não é apenas do agente de tratamento de dados pessoais, mas também do órgão regulador, que deve coordenar e orientar os agentes de tratamento a realizar o tratamento de forma correta. Portanto, o que a lei se propõe é criar um ecossistema de proteção de dados formado por diversos sujeitos que colaboram entre si.

Assim, verifica-se que a Lei Geral de Proteção de Dados elegeu o sistema de responsabilidade civil subjetiva. Se fosse diferente, haveria o esvaziamento do que propõe a lei, que é incentivar o fortalecimento de uma cultura de proteção de dados no Brasil. Não obstante, é possível a responsabilização objetiva do agente de tratamento quando restar demonstrada a relação de consumo, isto porque o Art. 45 da LGPD prescreve que as hipóteses de violação no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas no CDC.

6. A TUTELA COLETIVA NA PROTEÇÃO DE DADOS PESSOAIS

A LGPD assegura ao titular, em seu art. 21 e dentre outros direitos, que "Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo" e traz, ainda, importante questão processual na defesa das garantias nela previstas, enfatizando "A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva". Dessa forma, não resta dúvida de que além da tutela individual da proteção de dados a LGPD também trouxe expressamente a tutela coletiva dos direitos e garantias nela contidos.

Ao debruçar-se sobre o tema, Roque (2019, p. 8) relembra a classificação trazida pelo CDC, que divide os direitos coletivos em nas seguintes categorias, sendo que há regimes jurídicos distintos para cada uma delas: (i) direitos difusos; (ii) direitos coletivos em sentido estrito e (iii) direitos individuais homogêneos. As hipóteses (i) e (ii) tratam da tutela de direitos coletivos, enquanto na última, dos direitos individuais homogêneos, trata-se de tutela coletiva de direitos acidentalmente coletivos, que são individuais homogêneos (ROQUE, 2019).

O autor assevera que é um equívoco atribuir, a princípio, a categoria de direitos coletivos a matéria em abstrato, tal como a tutela dos dados pessoais, eis que algumas nuances do caso concreto podem fazer incidir uma espécie ou outra de direito coletivo. Nesse sentido, a tutela coletiva dos dados pessoais pode envolver:

> [...] direitos difusos (por exemplo, no caso em que se pretende corrigir algum tratamento inadequado de dados pessoais realizado por autoridades públicas, relativamente a todos os que vivem em certa localidade – tutela indivisível e sem que exista uma relação jurídica base prévia que delimite o grupo), coletivos em sentido estrito (ilustrativamente, na hipótese em que se pede a adequação do tratamento de dados pessoais realizado por uma empresa, relativamente a seus consumidores – tutela também indivisível, mas referente a uma relação jurídica de consumo base) e individuais homogêneos (por exemplo, pleito de danos morais e materiais veiculado contra certa empresa decorrente do vazamento de dados de um grupo de pessoas – tutela que poderia ser postulada em ações individuais, existindo uma origem comum para os danos alegados). (ROQUE, 2019, p.10).

Nesse sentido, o autor conclui que "a categorização de um direito coletivo, portanto, dependerá invariavelmente da análise da causa de pedir e do pedido de tutela jurisdicional concretamente formulado", e propõe que, para identificar qual categoria de direito coletivo incide em cada caso, devem ser respondidas duas perguntas: se (i) a tutela é divisível, isto é, "passível de cisão em processos individuais, sem repercutir necessariamente na esfera jurídica

de outros titulares". Caso a resposta seja positiva, estaremos diante de direitos individuais homogêneos; caso contrário, uma segunda pergunta deve ser feita, qual seja, (ii) "sendo a tutela indivisível, existe alguma relação jurídica base responsável pela conformação do grupo"? Se, por sua vez, a resposta for positiva, resta configurada a presença do direito coletivo em sentido estrito, caso a resposta seja negativa e, portanto, a formação do grupo estiver baseada em meras circunstâncias fáticas, estaremos diante de direito difuso.

Concluindo a análise da tutela coletiva da proteção dos dados pessoais, questiona-se quem seriam, então, os legitimados para a propositura das respectivas ações. A LGPD não fez menção sobre essa questão, portanto, deve-se utilizar as principais fontes do processo coletivo, quais sejam, a Lei da Ação Civil Pública (Lei 7.347/1985), especificamente em seu art. 5º; e o art. 82 do código consumerista.

Assim, conforme se depreende da leitura dos artigos supramencionados, são legitimados à propositura da ação por reparação em ocasião do vazamento de dados: o Ministério Público, a Defensoria Pública, quando houver hipossuficientes, a Administração Pública, incluindo a ANPD, e as associações civis, nos termos da legislação de regência.

Quanto ao indivíduo, de acordo com o que destaca Roque, só será legitimado para Ação Popular, muito embora, em razão das peculiaridades que revestem esta ação, seja difícil, para o autor, imaginar hipótese na qual ela seria cabível. De todo modo, Roque não descarta a possibilidade de legitimidade do indivíduo para deflagração de ações coletivas, quando por exemplo, no município em que residir, não existirem outros legitimados e a violação for perpetrada pela Administração Pública (ROQUE, 2019, p.12 e 13).

Em síntese, a partir da leitura conjunta dos arts. 22 e 42 da LGPD, bem como dos dispositivos da Lei da Ação Civil Pública e do Código de Defesa do Consumidor, conclui-se que a legislação brasileira permitirá uma atuação repressiva, em nível administrativo, para a tutela da proteção de dados pessoais, valendo-se do microssistema de proteção de direitos difusos, além de fomentar a atuação de entidades civis especializadas e do próprio Ministério Público e ANPD por meio do poder judiciário.

Cabe citar, aqui, o julgamento do Recurso Extraordinário (RE) 1101937, que discute a constitucionalidade do artigo 16 da Lei da Ação Civil Pública, que limita a eficácia dessas sentenças à competência territorial do órgão que a proferir. Até o momento, votaram seis ministros, todos pela inconstitucionalidade da norma.

O fator preocupante envolvendo essa questão é que os dados de brasileiros são espalhados por toda Internet e mecanismos para sua proteção são necessários, sob pena de haver graves prejuízos a toda sociedade. A questão é alarmante, principalmente considerando os

escândalos de vazamentos de dados, a citar, os ocorridos no último ano: o vazamento de dados do Ministério da Saúde, que expos dados sensíveis da população, o vazamento de dados da Enel, concessionária de energia elétrica de São Paulo, e, por fim, o vazamento noticiado em 11 de janeiro de 2020, no qual dados detalhados de 223 milhões de brasileiros foram vazados.

Se considerarmos hipótese em que 10% dos brasileiros judicializem, de forma individual, as pretensões para reparar os danos advindos dos mencionados vazamentos, teremos cerca de 20 milhões de novas ações no Poder Judiciário, que conta, ao menos até dezembro de 2019, com 77,1 milhões de processos que abarrotarão ainda mais referido órgão[36].

Logo, limitar a sentença coletiva ao seu órgão prolator, conforme propõe o art. 16 da LACP, não só trará grave insegurança jurídica, mas contribuirá com o abarrotamento das varas judiciais que, inclusive, contam com recursos finitos e não podem ficar à mercê de demandas individuais propostas uma em cada Estado brasileiro.

Isto posto, sendo a proteção de dados um desafio a ser enfrentado pelo Poder Judiciário, considerando tudo que fora exposto até o momento, o STF tem oportunidade garantir a abrangência nacional das decisões proferidas no âmbito de uma ação civil pública e, consequentemente, evitar um possível colapso no sistema, pelo que se espera que o art. 16 seja julgado inconstitucional.

Aliás, o risco de abarrotamento pode se tornar ainda maior caso se adote a responsabilidade civil objetiva e a teoria do dano *in re ipsa*, isto porque o prejudicado sequer precisaria comprovar ter sofrido um dano real para que se configure a violação e passe a ter direito à reparação por danos morais.

O caminho para que se evite a judicialização em massa é a transparência e conscientização contumaz dos titulares de dados no sentido de demonstrar, de forma assertiva, que a porta de entrada para resolver qualquer celeuma é inicialmente com o seu respectivo controlador e não com o Judiciário.

---

[36] Dados retirados da publicação Justiça em Números 2020 (ano base 2019) do CNJ. Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2020/08/WEB_V2_SUMARIO_EXECUTIVO_CNJ_JN2020.pdf.>. Acesso em: 16 mar. 2021.

7. CONSIDERAÇÕES FINAIS

Vivemos em uma sociedade na qual a informação se tornou o centro gravitacional da nova forma de organização social e econômica. A circulação de dados não só altera as relações sociais, redefinindo as noções de tempo e espaço, mas tem valor comercial.

A atual ordem econômica utiliza informações, que são dados sobre experiências humanas, como matéria prima para fins comerciais, segmentando campanhas para perfis específicos de consumidores e criando produtos cada vez mais personificados, que acabam guiando as escolhas dos usuários. Para que essa lógica de acumulação funcione, é preciso que cada vez mais dados sejam coletados.

Neste cenário, o titular dos dados assume posição de vulnerabilidade, pois sua capacidade de autodeterminação é cada vez mais calibrada pelas informações que são coletadas a seu respeito, tais como acesso a determinado programa de linha de crédito e diversas outras oportunidades sociais que são filtradas pelo processamento de dados dos cidadãos.

Para promover o empoderamento do titular dos dados surgiu a necessidade de regulação específica sobre o tema, não só porque o tratamento inadequado aos dados pessoais pode violar a privacidade, intimidade e outros direitos fundamentais do indivíduo, mas para conferir ao usuário algum poder de barganha capaz de equalizar as assimetrias.

Recentemente, o STF confirmou a existência de "um verdadeiro direito fundamental à proteção de dados pessoais", como um "direito à autodeterminação informacional como um contraponto a qualquer contexto concreto de coleta, processamento ou transmissão de dados passível de configurar situação de perigo", conforme voto do ministro Gilmar Mendes no julgamento ADI 6.387/DF. Assim, a proteção de dados pessoais insere-se como categoria autônoma de direito da personalidade.

Assim, a Lei Geral de Proteção de Dados - Lei nº 13.709/2018, representa um marco para o desenvolvimento de uma cultura de proteção de dados no país, trazendo uma série de conceitos, princípios, direitos e deveres para as instituições privadas e públicas e para a Autoridade Nacional de Proteção de Dados, vocacionados a regular o tratamento de dados pessoais.

É de se notar que, além de representar um empoderamento ao titular dos dados, com a LGPD, o país entra para o grupo de países que contam com um nível adequado em termos de proteção de dados pessoais, como é o caso dos Estados da União Europeia.

Diante do impacto que a lei representa aos indivíduos e organizações, é importante delimitar as obrigações dos agentes de tratamento de dados e, via de consequência, fixar regime

jurídico para sua responsabilização, bem como analisar a possibilidade de ações individuais em decorrência de danos causados em violação ao disposto na lei.

Apesar de a Lei Geral de Proteção de Dados Pessoais ser, intencionalmente, econômica com relação ao modelo de responsabilidade adotado e à tutela dos individuais e coletivos, nos parece a natureza jurídica da responsabilidade é subjetiva e que sua arquitetura jurídica reforça um sistema integrado destinado à tutela dos interesses coletivos, difusos e individuais homogêneos. Enfim, o trabalho mostrou que um exercício de leitura e interpretação da LGPD que seja isolado, deixando de compreender aspectos relevantes sobre sua criação, será empobrecedor e limitante.

REFERÊNCIAS

ALEXY, Robert. **Teoria dos Direitos Fundamentais**. São Paulo: Malheiros Editores, 2006.

ARENDT, Hannah. **A condição humana**. Tradução de Roberto Raposo. Rio de Janeiro: Forense Universitária, 2010.

BARRETO JUNIOR, Irineu Francisco. Proteção da Privacidade e de Dados Pessoais na Internet: O Marco Civil da rede examinado com fundamento nas teorias de Zygmunt Bauman e Manuel Castells. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; DE LIMA; Cintia Rosa Pereira. (orgs.). **Direito & Internet III**. São Paulo: Quartier Latin, 2015. p. 100-127.

BASTOS, Athena. **Direito digital: guia da lei geral de proteção de dados pessoais: LGPD**. 2018. Disponível em: https://blog.sajadv.com.br/direito-digital-lei-de-protecaode-dados/. Acesso em: 20 mar. 2021.

BERNERS-LEE, Tim. **Marco Civil: Statement of Support from Sir Tim Berners-Lee**. World Wide Web Foundation. 24 de março de 2014. Disponível em: <https://webfoundation.org/2014/03/marco-civil-statement-of-support-from-sir-tim-berners-lee/>. Acesso em: 20 mar. 2021.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2020.

BIONI, Bruno Ricardo; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. **Civilistica.com**, Rio de Janeiro, ano 9, n. 3, p.1-23, 2020.

BOBBIO, Norberto. **Teoria do Ordenamento Jurídico**. 10. ed. Brasília: Universidade de Brasília, 1999.

BOYD, Danah; CRAWFORD, Kate. Critical questions for Big Data. **Information, Communication & Society**, v. 15, n. 5, p. 662-679, 2012.

BRASIL, Assembleia Legislativa. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 20 mar. 2021

BRASIL. Lei no 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 11 set. 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em: 20 mar. 2021.

BRASIL. Lei n. 10.406, 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União**, Brasília, DF, 11 jan. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/2002/L10406compilada.htm>. Acesso em: 20 mar. 2021

BRASIL. Marco Civil da Internet. Lei 12.965 de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**. <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 20 mar. 2021.

BRASIL, Assembleia Legislativa. **Lei 13.709/2018**. Regulamenta a proteção de dados. Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm> Acesso em: 20 mar. 2021.

BRASIL. Senado Federal. **Proposta de Emenda à Constituição n° 17, de 2019**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Câmara dos Deputados, 2019. Disponível em: < https://www25.senado.leg.br/web/atividade/materias/-/materia/135594>. Acesso em 20 mar. 2021

BRASIL. Medida provisória n. 954, de 17 de abril de 2020. Complementa a Lei nº 13.979, de 6 de fevereiro de 2020, para dispor sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel

Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística. **Diário Oficial da União**: edição: 74-C, Brasília, DF, p. 1, 17 abr. 2020.

CANCELIER, Mikhail Vieira de Lorenzi. **Infinito Particular: Privacidade no Século XXI e a Manutenção do Direito de estar só**. Rio de Janeiro: Lumen Juris, 2017.

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. **Cadernos Jurídicos: Direito Digital e proteção de dados pessoais**, São Paulo, ano 21, n. 53, p. 163-170, jan./mar. 2020.

CARVALHO, Gisele Primo; PEDRINI, Tainá Fernanda. Direito à privacidade na lei geral de proteção de dados pessoais. **Revista da ESMESC**, Florianópolis, v. 26, n. 32, p. 363-382, ago. 2019.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.

DEVLIN, Alan. **Principles of law and economics**. Nova York: Routledge, 2015.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados**. 2.ed. São Paulo: Thomson Reuters Brasil, 2019.

EUROPEAN UNION. **General data protection regulation EU** (2016/679). Disponível em: <https://gdpr-info.eu/>. Acesso em: 20 mar. 2021.

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. (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. p. 23-52.

FREITAS, Cinthia Obladen de Almendra; PAMPLONA, Danielle Anne. Cooperação entre estados totalitários e corporações: o uso da segmentação de dados e profiling para violação de

direitos humanos. *In*: RUARO, Regina Linden; MAÑAS, José Luis Piñar; MOLINARO, Carlos Alberto (orgs.). **Privacidade e proteção de dados pessoais na sociedade digital**. Porto Alegre: Editora Fi, 2017. p. 130.

GODOY, Cláudio Luiz Bueno. A responsabilidade civil na era digital. *In*: **Congresso internacional de responsabilidade civil do IBERC**, São Paulo [S. l.]: 2019.

GOGANI, Ronaldo. **O maior roubo de dados da história do Facebook que ajudou a eleger Donald Trump**. Meio Bit, 2018. Disponível em: <https://meiobit.com/381701/facebookcambridge-analytica-roubo-dados-ajudou-campanha-donald-trump-e-brexit/>. Acesso em: 20 mar. 2021.

GONÇALVES, Carlos Roberto. **Responsabilidade Civil**. 17. ed. São Paulo: Saraiva, 2016.

GRINOVER, Ada Pelligrini; WATANABE, Kasuo; JUNIOR, Nelson Neri. **Defesa do Consumidor: comentado pelos autores do anteprojeto**. 10. ed. Rio de Janeiro: Forense Universitária, 2011.

GUALDA, Diego; DA MATTA, Laura Aliende. **Responsabilidade subjetiva na LGPD**. Inteligência Jurídica Machado Meyer. 04 de dezembro de 2020. Disponível em: <https://www.machadomeyer.com.br/pt/inteligencia-juridica/publicacoes-j/tecnologia/responsabilidade-subjetiva-na-lgpd>. Acesso em: 20 mar. 2021.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau, "Término do tratamento de dados", *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais**. São Paulo: Editora RT, 2019, p. 231.

KATARIVAS, Nicole. **A lei do cadastro positivo e a lei geral de proteção de dados: conflito ou sinergia?** Migalhas. 25 de março de 2019. Disponível em: <https://www.migalhas.com.br/depeso/298656/a-lei-do-cadastro-positivo-e-a-lei-geralde-protecao-de-dados-conflito-ou-sinergia>. Acesso em: 20 mar. 2021.

LÔBO, Paulo. **Direito Civil: parte geral**. 6. ed. São Paulo: Saraiva, 2017.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de Dados comentada**. São Paulo: Revista dos Tribunais, 2019.

MANGETH, Ana Lara; NUNES, Beatriz Marinho. **A proteção de seus dados pessoais está em jogo no Senado**. Its Feed. 6 de junho de 2018. Disponível em: <https://feed.itsrio.org/senado-vs-c%C3%A2mara-seus-dados-pessoais-em-jogo-97d7b0cefc54>. Acesso em: 20 mar. 2021.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova lei geral de proteção de dados. **Revista de direito do consumidor**, Brasília, v. 120, p. 469-483, nov./dez. 2018.

MILHORANCE, Flávia. **O que se sabe sobre a atuação da Cambridge Analytica no Brasil.** 2018. Disponível em: <https://projetocolabora.com.br/ods8/o-que-se-sabesobre-a-atuacao-da-cambridge-analytica-no-brasil/>. Acesso em: 20 mar. 2021.

MORAES, Maria Celina Bodin de. LGPD: um novo regime de responsabilização civil dito proativo. **Civilistica - Revista Eletrônica de Direito Civil**, Rio de Janeiro, ano 8, n. 3, 2019. Disponível em: <http://civilistica.com/lgpd-um-novo-regime/>. Acesso em: 20 mar. 2021.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018.

NOVAKOSKI, André Luis Mota; NASPOLINI, Samyra Haydêe Dal Farra. Responsabilidade civil na LGPD: problemas e soluções. **Conpedi Law Review**, Florianópolis, v. 6, n. 1, p. 158-174, 2020.

OLIVEIRA, José Eduardo da Silva. **Responsabilidade civil dos agentes de proteção de dados no Brasil**. 2019. Monografia (Curso de Direito do Centro de Ciências Jurídicas) - Universidade Federal da Paraíba, João Pessoa, 2019.

PASQUALINI, Alexandre. **Hermenêutica e sistema jurídico**. Porto Alegre: Livraria do Advogado, 1999.

RODOTÀ, Stefano. **Il diritto di avere**. Roma-Bari: Laterza, 2012.

ROQUE, André. A Tutela Coletiva dos Dados Pessoais na Lei Geral de Proteção de Dados (LGPD). **Revista Eletrônica de Direito Processual**, Rio de Janeiro, v. 20, n. 2, p. 1-19, mai./ago. 2019.

ROSENVALD, Nelson. **As funções da responsabilidade civil: a reparação e a pena civil**. 3. ed. São Paulo: Saraiva, 2017.

SCHREIBER, Anderson. **Novos paradigmas da responsabilidade civil. A erosão dos filtros da reparação à diluição dos danos**. 6. ed. São Paulo: Atlas, 2015.

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

SCHWARTZ, Paul; M. SOLOVE, Daniel J. **The PII Problem: Privacy and a New Concept of Personally Identifiable Information**. Review law 86N.Y.U.L.Q. Rev. 1814, 2011. Disponível em: <https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2638&context=facpu bs>. Acesso em: 20 mar. 2021.

STAJN, Rachel. **Sistema financeiro**. Rio de Janeiro: Elsevier, 2011.

TARELLO, Giovanni. **Trattato di Diritto Civile e Commerciale: L'interpretazione della legge**. Milano: Giuffrè, v. I, t. 2, 1980.

TARTUCE, Flávio. **Direito Civil. Direito das obrigações e responsabilidade civil**. 11. ed. Rio de Janeiro: Forense, 2016.

TASSO, Fernando Antonio. A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor. **Cadernos Jurídicos**, São Paulo, ano 21, n. 53, p. 97-115, jan./mar. 2020.

TEIXEIRA, Tarcísio. **Marco Civil da Internet Comentado**. São Paulo: Almedina Brasil, 2016.

TEPEDINO, Gustavo. **Temas em Direito Civil**. 3. ed. Rio de Janeiro: Renovar, 2004.

TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. Desafios da inteligência artificial em matéria de responsabilidade civil. **Revista Brasileira de Direito Civil**, Belo Horizonte, v. 21, p. 61-86, jul./set. 2019.

ZUBOFF, Shoshana. Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação. *In*: BRUNO, Fernanda; CARDOSO, Bruno; KANASHIRO, Marta *et al*., (orgs). **Tecnopolíticas da vigilância: perspectivas da margem**. São Paulo: Boi Tempo, 2019. p. 17-68.