UNIVERSIDADE DE BRASÍLIA – UNB
FACULDADE DE DIREITO – FD/UNB
CURSO DE BACHARELADO EM DIREITO

RODRIGO DA COSTA ALVES

REGIMES DE RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LEI Nº 13.709/18

BRASÍLIA
2020

RODRIGO DA COSTA ALVES

REGIMES DE RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LEI Nº 13.709/18

Monografia apresentada como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Direito da Universidade de Brasília.

Orientador: Prof. Gabriel Jamur Gomes.

BRASÍLIA
2020

RODRIGO DA COSTA ALVES

REGIMES DE RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LEI Nº 13.709/18

Monografia apresentada como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Direito da Universidade de Brasília.

Orientador: Prof. Gabriel Jamur Gomes.

BRASÍLIA, 18 DE DEZEMBRO DE 2020.

BANCA AVALIADORA

_____

Professor Orientador Gabriel Jamur Gomes

_____

Professora Tainá Aguiar Junquilho

_____

Professor Frank Ned Santa Cruz

AGRADECIMENTOS

Creio que nenhuma obra é fruto independente e solitário de seu autor. No meu caso, posso falar sem sombra de dúvida que não estaria aqui sem o apoio incondicional da minha mãe e do meu irmão. Não poderia deixar de reconhecer o amor, carinho, compreensão e fé que vocês sempre depositaram em mim.

Mesmo com todas as dificuldades da vida, minha mãe, Luzia, sempre me possibilitou a segurança necessária para que eu pudesse chegar a qualquer lugar, e com a certeza de que só o estudo iria me propiciar uma vida que ela nunca teve. Obrigado, mãe, por ser meu maior exemplo de perseverança.

Meu irmão, Bruno, do mesmo modo, me apoiou incondicionalmente, seja financeira ou afetivamente, nesse caminho. Sempre esteve ao meu lado para que eu pudesse estudar e alcançar todos os meus objetivos. E mais, acreditou em mim mesmo quando eu não tive essa mesma fé. Obrigado, irmão, pois sem a sua fé em mim eu não estaria aqui hoje. Enfim, devo tudo, pois sem vocês não seria nada!

Não poderia deixar de agradecer também ao meu amigo Rinaldo, uma pessoa que sempre acreditou na ascensão social por meio da educação. Obrigado por ter insistido, junto com meu irmão, para que eu fizesse o vestibular. Graças a vocês esse sonho está se realizando. Obrigado a todos os amigos e amigas que contribuíram para que esse trabalho tenha sido concluído com êxito.

Por fim, mas não menos importante, agradeço a minha companheira Mariana por estar ao meu lado esses anos e ser minha melhor amiga. Você tornou essa jornada mais bonita e prazerosa. Obrigado por ser uma parte tão especial da minha vida.

É necessário sempre acreditar que um sonho é possível
que o céu é o limite e você é imbatível;
que o tempo ruim vai passar, é só uma fase;
que o sofrimento alimenta mais a sua coragem;
que a sua família precisa de você,
lado a lado se ganhar, pra te apoiar se perder [...]
(Racionais MC's, *A Vida é Desafio*)

RESUMO

Trata-se de trabalho de conclusão de curso que se propõe a revelar os argumentos a respeito dos regimes de responsabilidade civil dos agentes de tratamento na Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018. O trabalho buscou demonstrar qual o regime predominante na legislação, com o objetivo de clarificar o modo pelo qual os infratores da lei (agentes de tratamento) serão responsabilizados. Para isso, utilizou-se da pesquisa bibliográfica, tendo como fontes primárias a legislação de regência (Lei nº 13.709/2018), principais obras referentes à teoria da responsabilidade civil, bem como obras da literatura jurídica especializada referente à proteção de dados pessoais. Como fontes secundárias, foi utilizada a legislação correlata ao tratamento de dados pessoais, como Marco Civil da Internet e General Data Protection Regulation (GDPR), além de julgados relevantes sobre o assunto. Como resultado, concluiu-se que o regime de responsabilidade civil objetivo é o que melhor atende aos anseios do legislador, que considera o risco como elemento intrínseco do tratamento de dados.

Palavras-chave: Agentes de tratamento. Responsabilidade Civil. Lei Geral de Proteção de Dados Pessoais. Responsabilidade Civil Subjetiva. Responsabilidade Civil Objetiva.

ABSTRACT

This course conclusing work aims to reveal the arguments regarding the controllers and processors' civil liability regimes in the General Data Protection Act (LGPD), Law 13709, August 14, 2018. This study focuses on providing a demonstration as to which regime predominant in the legislation, in order to clarify the way in which those who fail to comply (controllers and processors) are to be held responsible. Bibliographic research was used, basing itself primarily in the governing legislation (Law No 13709), the main works in the subject of the theory of civil liability, as well as works of specialized doctrine regarding the protection of personal data. As secondary sources, legislation related to the treatment of personal data, such as the Brazilian Civil Rights Framework for the Internet (Law No 12965) and The General Data Protection Regulation (GDPR), were analyzed, as well as relevant trials on the subject. It was thus concluded that the objective civil liability regime serves as a better possibility considering the wishes of the legislator, who considers risk as an intrinsic element of data processing.

Keywords: Controller and Processor. Civil Liability. General Data Protection Act. Subjective Civil Liability. Objective Civil Liability.

SUMÁRIO

1 INTRODUÇÃO

A Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais - LGPD, sistematizou a proteção de dados pessoais no Brasil, tratando o tema de maneira ampla e geral. Contudo, a lei silenciou a respeito do regime de responsabilização aplicável àqueles que descumprirem suas normas, se subjetivo, centrado na culpa, ou objetivo, centrado no risco da atividade, o que despertou o interesse para uma investigação doutrinária mais aprofundada.

Ao não estabelecer um regime claro de responsabilidade a ser aplicado aos agentes de tratamento (controlador e operador) em caso de violação as suas disposições, a LGPD deixou em aberto um dos pontos mais importantes para sua efetividade, qual seja, a definição do critério de responsabilização do violador de suas disposições. A importância do tema se revela na medida em que a escolha por um ou outro regime irá impactar diretamente no titular de dados, que terá maior ou menor ônus para comprovar a violação de seus direitos.

Isso porque, o regime de responsabilidade civil subjetivo, baseado no conceito de culpa, exige que o titular de dados demonstre a violação dos deveres impostos pela lei, bem como a vontade de agir e a previsibilidade do resultado (conceito clássico de culpa) ou a inadequação da conduta do agente de tratamento frente a uma situação concreta (conceito de culpa normativa). Já a responsabilidade civil objetiva está baseada sobretudo no risco criado pela atividade. Se o tratamento de dados for considerado como uma atividade de risco, basta ao titular de dados demonstrar o nexo causal entre a conduta e o dano, sem necessidade de prova quanto ao elemento subjetivo do agente.

Nesse contexto, o presente trabalho se propôs a analisar os argumentos da literatura jurídica a respeito de qual seria o regime de responsabilização civil dos agentes de tratamento de dados na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, 14 de agosto de 2018). Para o desenvolvimento do trabalho, foram elaboradas duas hipóteses principais de pesquisa, baseadas em leituras preliminares de parte da literatura jurídica referente ao assunto, quais sejam: a adoção da prevenção de danos como valor máximo a ser perseguido pelos agentes de tratamento, o que deveria refletir no regime de responsabilidade civil a ser adotado; e a segunda hipótese se baseou na afirmação segundo a qual o risco criado pelos agentes de tratamento enseja a escolha do regime objetivo de responsabilidade.

O trabalho se estrutura em dois eixos principais. O primeiro se dedica, resumidamente, à Lei Geral de Proteção de Dados, especialmente no que diz respeito aos conceitos essenciais,

aos direitos dos titulares de dados, ao tratamento de dados pessoais e aos agentes de tratamento. O segundo eixo se ocupa da análise das categorias da responsabilidade civil subjetiva e objetiva, fazendo um breve panorama para situar o leitor. Por fim, trata-se diretamente dos elementos caracterizadores da responsabilidade civil subjetiva e objetiva.

1.1 Justificativa de pesquisa

A LGPD constitui importante mudança no marco regulatório que sistematiza o tratamento de dados pessoais no Brasil e reforça os princípios da autodeterminação informativa, da inviolabilidade da intimidade e da vida privada. Isso porque, trata-se de lei que faz parte de um *continuum* regulatório. Trata-se de relevante passo no sistema de proteção de dados pessoais que vinha sendo construído ao longo dos anos, o qual, contudo, não possuía norma exclusiva sobre o tema[1].

Dentre os dispositivos que podem levantar certos questionamentos, aqueles relativos à responsabilidade e ao ressarcimento de danos (art. 42 a 45) em casos de descumprimento de suas disposições levantaram maior interesse para a realização de uma pesquisa mais aprofundada. Isso porque, sem a reparação pelos danos causados ante o descumprimento das normas relativas ao tratamento de dados pessoais, a nova legislação não terá a efetividade que dela se espera.

A literatura jurídica atual já levanta questionamentos a respeito do regime de responsabilidade previsto na lei, tendo em vista que a legislação não adota um regime de responsabilização muito claro. Alguns autores entendem que se trata de um regime de responsabilização objetiva por considerarem o tratamento de dados uma atividade de risco (MENDES; DONEDA, 2018; MULHOLLAND, 2020, MENDES; DONEDA, 2018). Para outros, o modelo adotado é o da responsabilidade civil subjetiva[2], calcado na demonstração de culpa do ofensor, ou até mesmo um regime diferenciado, calcado na prevenção (BODIN DE MORAES, 2019).

Cumpre destacar que o tema da responsabilidade civil dos agentes de tratamento de dados ainda não foi tratado amplamente pela da literatura jurídica especializada, de modo que

[1] Nesse sentido, conferir o artigo "Os princípios norteadores da proteção de dados pessoais no Brasil" (BELLIZE OLIVEIRA; PEREIRA LOPES, 2019), que bem explicam a evolução desse sistema e a concretização dos princípios da proteção de dados pessoais na nova legislação (Lei nº 13.709/18).

[2] Sustentam essa posição, na literatura jurídica brasileira, Gisela Sampaio Guedes e Rose Melo Vencelau, no artigo "Término do tratamento de dados" (GUEDES; VENCELAU, 2019).

a pesquisa se baseou nas principais obras já publicadas sobre a temática, acima referenciadas como exemplo.

Ante o exposto, a falta de clareza na legislação demanda estudos para averiguar como se dará o modelo de responsabilização dos infratores da lei, de maneira a dar maior efetividade a seus dispositivos. Nesse contexto, o presente trabalho terá por objetivo principal, sem pretensão de exaurimento da matéria, expor os argumentos a respeito de qual seria o regime de responsabilização civil dos agentes de tratamento na Lei Geral de Proteção de Dados Pessoais. Por fim, em que pese a importância da responsabilização administrativa e penal, as consequências que daí decorrem são de cunho sancionatório para o agente causador. A responsabilização civil, por outro lado, busca a reparação da vítima e o retorno ao status quo anterior, de modo que o presente trabalho se concentrará em uma das funções da responsabilidade civil, qual seja, a reparação.

1.2 Problema de pesquisa

O presente trabalho terá como problema principal a identificação do regime de responsabilização civil dos agentes de tratamento de dados na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, 14 de agosto de 2018).

1.3 Hipótese de pesquisa

Para o adequado desenvolvimento do trabalho, foram elaboradas as seguintes hipóteses de pesquisa:

- a LGPD adotou a prevenção de danos como valor máximo a ser perseguido pelos agentes de tratamento, de modo que o regime de responsabilidade a ser adotado deve refletir esse posicionamento;
- o risco criado pelos agentes de tratamento enseja a objetivação da responsabilidade civil, sendo este o regime mais adequado para se garantir a proteção dos direitos dos titulares de dados pessoais.

1.4 Metodologia

A metodologia utilizada será a pesquisa bibliográfica. Serão fontes primárias de pesquisa: a) a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), b) principais obras referentes à teoria da responsabilidade civil e c) obras da literatura jurídica especializada referente à proteção de dados pessoais. Serão fontes secundárias: a) legislação correlata ao tratamento de dados pessoais, como Marco Civil da Internet e *General Data Protection Regulation*, bem como b) julgados relevantes sobre o assunto.

2 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LGPD

2.1 Contextualização do tema

A proteção de dados pessoais é, sem dúvida, um dos assuntos mais relevantes e urgentes da atualidade. Isso porque, os dados pessoais são os insumos da nova economia digital, dos quais decorrem diversas implicações que não se restringem à esfera dos direitos individuais dos titulares de dados. Nesse sentido, Ana Frazão, ao tratar da relação existente entre dados e algoritmos, destaca que

> se os dados são os insumos e os *inputs* da economia digital, os algoritmos são os instrumentos por meio dos quais os dados são processados e podem ser revertidos em resultados *(outputs)* a serem utilizados para as mais diversas finalidades. Muito além de aperfeiçoar estratégias econômicas já existentes, como seriam os casos do marketing personalizado *(target marketing)* e das classificações ou perfilizações *(profiling)*, **tais aplicações podem levar à total modificação do cenário econômico, político e social**. (FRAZÃO, 2019a, p. 32, grifos meus).

Nesse cenário, a proteção de dados é a forma pela qual se buscará preservar a integridade dos direitos individuais, como liberdade e igualdade e, até mesmo, a democracia, de modo que este é um tema transversal, que impacta indivíduos e sociedades de maneiras diversas e significativas. Assim, uma legislação abrangente e efetiva sobre a temática, que seja capaz de criar mecanismos para a efetivação dos princípios da autodeterminação informativa, da inviolabilidade da intimidade e da vida privada – princípios com relevante *status* constitucional (art. 5º, X) –, é urgente no contexto atual.

Embora o tema da proteção de dados pessoais e, de maneira mais abrangente, da privacidade, não seja recente – nem no mundo, tampouco no Brasil[3] –, apenas com a aprovação de um marco regulatório seria possível aprimorar e consolidar a proteção de dados no Brasil. Isso se tornou possível com a Lei nº 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), que adere a padrões internacionais, especialmente a

[3] A preocupação com a privacidade foi expressa por Samuel Warren e Louis Brandeis no artigo The Right to Privacy, publicado em 1890. No Brasil, a privacidade é objeto da legislação ordinária (Lei do Habeas Data, a Lei de Arquivos Públicos, o Código Civil, o Código de Defesa do Consumidor, a Lei de Acesso à Informação, Lei do Cadastro Positivo e, mais recentemente, o Marco Civil da Internet) e constitucional (CF, art. 5º, X). Essa evolução legislativa evidencia a construção de um sistema de proteção de dados através da interpretação sistemática dessas normas, não estando o ordenamento jurídico brasileiro completamente desamparado de normas protetivas da privacidade dos cidadãos. Nesse sentido, Cf. BELLIZZE OLIVEIRA; PEREIRA LOPES, 2019).

General Data Protection Regulation (GDPR)[4] e normatiza a proteção de dados no país de maneira sistemática e abrangente.

A LGPD regulamenta no Brasil o tratamento de dados realizado por pessoa natural ou por pessoa jurídica de direito público ou privado, bem como estabelece os princípios e as bases legais para o tratamento de dados, as obrigações dos agentes de tratamento e os direitos dos titulares e a transferência internacional de dados (art. 3º, art. 6º, art. 7º e 17º, dentre outros). Junta-se a outras leis protetivas dos direitos dos titulares de dados, especialmente, o Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014), para aperfeiçoar o arcabouço normativo e permitir maior robustez aos direitos dos titulares de dados.

Esclareça-se que não é o foco do presente trabalho traçar um panorama histórico da evolução legislativa no que se refere à privacidade e à proteção de dados pessoais. Mais importante é ter em mente que a LGPD surgiu de uma tendência global de significativas mudanças nas legislações de diversos países no sentido de garantir maior privacidade e segurança aos dados pessoais dos indivíduos[5].

A essa tendência de preocupação com a temática, somem-se os recentes escândalos de vazamento de dados, como o ocorrido no Facebook, em que houve o compartilhamento de dados de milhares usuários com a empresa britânica Cambridge Analytica[6]. Nesse caso, dados pessoais de milhares de usuários foram usados para segmentação e envio de publicidade direcionada para eleitores americanos (CONFESSORE, 2018).

---

[4] Também conhecido como "Regulamento Geral de Proteção de Dados Pessoais da União Europeia", que entrou em vigor em 25 de maio de 2018, e trouxe um novo entendimento sobre a proteção de dados pessoais, para além território europeu.

[5] Como exemplo, a própria General Data Protection Regulation (GDPR), da União Europeia, e o Consumer Data Protection Act, lei de privacidade e proteção de dados da Califórnia, EUA.

6 A Cambridge Analytica era uma empresa britânica de consultoria política que oferecia serviços de comunicação estratégia baseada em mineração e análise de dados. Em março de 2018 foi revelado que o Facebook entregou, sem autorização de consentimento de nenhuma forma, dados pessoais de milhares de usuários para a empresa, que posteriormente foram usados para influenciar o processo eleitoral. A descoberta de que o Facebook entregou informação pessoal de milhares de usuários causou espanto e gerou debates sobre os impactos da tecnologia na privacidade e bem-estar dos cidadãos. Para mais informações a respeito do caso, cf: PERUZZI, Antonio et al. How News May Affect Markets' Complex Structure: The Case of Cambridge Analytica, disponível em: https://www.mdpi.com/1099-4300/20/10/765?type=check_update&version=2. Acesso em: 10 de nov. de 2020; HANNA, Mina J.; ISAAK, Jim. User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection, , disponível em: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8436400. Acesso em: 10 de nov. de 2020; KOZLOWSKA, Iga. Facebook and Data Privacy in the Age of Cambridge Analytica. Disponível em: https://jsis.washington.edu/news/facebook-data-privacy-age-cambridge-analytica/. Acesso em: 10 de nov. de 2020; CHEN, Adrian. Cambridge Analytica and our lives inside the surveillance machine. Disponível em: http://personal-computing.coryarcangel.com/Cambridge-Analytic.pdf. Acesso em: 10 de nov. de 2020; e MONOKHA, Ivan. Surveillance: The DNA of Platform Capital – The Case of Cambridge Analytica Put into Perspective. Disponível em: https://ora.ox.ac.uk/objects/uuid:15e74c10-225f-4bd7-b086-8e1fdb1b79e8/download_file?file_format=pdf&safe_filename=Manokha%252C%2BSurveillance%252C%2BAAM.pdf&type_of_work=Journal+article. Acesso em: 10 de nov. de 2020.

A preocupação com o tema fez surgir elevado número de países que possuem legislação protetiva de dados pessoais. Na América Latina, apenas o Suriname não conta com uma legislação geral ou setorial regulando a matéria (GONZÁLEZ, 2018)7.

Em observância à evolução mundial sobre o tratamento e proteção de dados pessoais, o parlamento brasileiro aprovou a Lei Geral de Proteção de Dados Pessoais, sancionada em 14 de agosto de 2018. O art. 1º da lei sintetiza seu escopo – tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado – e objetivos – proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da pessoa natural[8]. Ainda, classifica suas disposições como de interesse nacional e de observância pela União, Estados, Distrito Federal e Municípios. Trata-se, portanto, de uma lei nacional, de caráter obrigatório para todas as entidades da Administração Pública.

Da leitura do art. 2º, que estabelece seus fundamentos, pode-se concluir que suas pretensões vão muito além da proteção da privacidade, sendo um instrumento legislativo de defesa do desenvolvimento econômico e tecnológico, da livre iniciativa e da livre concorrência, bem como dos direitos humanos, do livre desenvolvimento da personalidade, da dignidade e do exercício da cidadania pelas pessoas naturais – art. 2º, III, V, VI e VII – (FRAZÃO, 2019b). A legislação também tutela os princípios da liberdade e igualdade, pois os agentes de tratamento devem, desde o início e até o final do tratamento de dados, prezar pela observância dos princípios estabelecidos na legislação, como a não discriminação (art. 6º, IX) e respeito às liberdades civis e direitos individuais (art. 6, X).

Uma pergunta que pode ser levantada é: por que dados pessoais são tão importantes para a economia moderna e porque protegê-los com leis eficientes? A importância dos dados pessoais para a economia moderna é deduzida a partir do fato de que os dados podem ser utilizados por inúmeras atividades econômicas, para inúmeras aplicações, desde identificação de um perfil consumidor específico e até mesmo para revelar o quadro de saúde de um indivíduo.

No atual estágio do capitalismo, os dados passam a ter uma importância estratégica para os modelos de negócio da economia digital, no que se convencionou chamar de *data-driven*

---

[7] GONZÁLEZ, Mariana. **Conheça o cenário das leis de proteção de dados ao redor do mundo**. IdBlog., 14 fev. de 2020. Disponível em <https://blog.idwall.co/protecao-de-dados-cenario-mundial-das-leis/#:~:text=Na%20Col%C3%B4mbia%2C%20a%20quest%C3%A3o%20da,de%20processamento%20de%20dados%20pessoais.>. Acesso em 10 de nov. 2020.

[8] Para uma visão mais abrangente dos objetivos da lei, cf. FRAZÃO, 2019c.

economy, ou seja, economia movida a dados. Contudo, a importância dos dados pessoais não se restringe à esfera econômica. Isso porque, a partir do processamento de dados pessoais por algoritmos, o acesso a uma série de direitos e oportunidades pode ser dificultado, o que revela uma dimensão que transcende a esfera econômica da utilização de dados.

Ao refletir sobre esse processo, Ana Frazão destaca o fato de os algoritmos poderem "decidir quem terá acesso à crédito e a que taxa de juros, quem será contratado para trabalhar em determinada empresa, qual a probabilidade de reincidência de determinado criminoso [...]" (FRAZÃO, 2019a, p. 33). Daí extrai-se que os dados possuem uma importância transversal para a sociedade, para as liberdades individuais e para a democracia, o que demanda ações para reforçar a autodeterminação informativa dos titulares de dados frente aos agentes do mercado.

Importante destacar que o direito à proteção dos dados pessoais nasce como um direito de defesa em face do Estado, mas hoje assume contornos muito diferentes, porquanto

> o tratamento desarrazoado de dados pessoais pode fomentar a criação de pequenos Leviatãs, cujo potencial ofensivo à vida privada e à dignidade humana pode se igualar ou até mesmo exceder aquele representado pelo Estado. (CUEVA, 2017, p. 64).

A criação de bancos de dados com enorme volume de informações levanta preocupações ante a crescente consolidação de uma sociedade de vigilância, controlada pelo governo e grandes *players* econômicos, possibilitando a criação do que o professor Frank Pasquale descreve como *one-way-mirror*, ou seja, tais agentes - Estado e Mercado - sabem tudo a respeito dos cidadãos, enquanto estes nada sabem sobre aqueles (FRAZÃO, 2019a).

Como se depreende desse contexto, a violação dos dados pessoais vai além da invasão de privacidade, podendo trazer riscos inclusive para a democracia e para o exercício da cidadania – como o caso Cambridge Analytica demonstrou recentemente. Pode-se concluir, portanto, que a LGPD transborda de preocupações sobre privacidade e irá atingir diversas áreas da vida, desde relações de consumo até preocupações concorrenciais[9], devido a uma economia que atribui cada vez mais relevância à sua utilização.

Por fim, tais dados representam verdadeiros "indicativos de aspectos da nossa personalidade" (DONEDA, 2019. p. 24) e "[...] certas formas de tratamento de nossos dados pessoais podem implicar na perda da nossa autonomia, da nossa individualidade e, ainda, da

[9] Nesse sentido, importante destacar os esforços do Conselho Administrativo de Defesa da Concorrência em promover estudos sobre concorrência e proteção de dados, filtros econômicos para a detecção de cartéis e concorrência em mercados digitais (Cf.: **CADE contrata consultores técnicos para elaboração de estudos**. Disponível em: http://www.cade.gov.br/acesso-a-informacao/concursos-e-selecoes/consultoria-vagas-concluidas/cade-contrata-consultores-tecnicos-para-elaboracao-de-estudos. Acesso em: 23 fev. 2020).

nossa liberdade" (DONEDA, 2019. p. 24). Exatamente em função da importância e relevância do tema para o país, para as empresas sujeitas a sua disciplina e para os titulares de dados, especialmente, a LGPD deve ser estudada pela comunidade acadêmica e debatida nos mais diversos canais de comunicação para que não reste dúvidas quanto a sua interpretação, aplicação e efetividade, notadamente no que diz respeito ao seu regime de responsabilização.

Ante o exposto, considerando a importância da natureza dos dados pessoais e das situações jurídicas que deles decorrem, a investigação a respeito do regime de responsabilidade a ser aplicado aos agentes de tratamento em casos de violação aos direitos dos titulares se faz tão necessária. Nos próximos capítulos, a importância da definição desse regime jurídico de responsabilidade será mais bem explorada.

2.3 Conceitos Essenciais da LGPD para a Compreensão do Tema

Antes de aprofundarmos o tema da responsabilidade civil propriamente dita dos agentes de tratamento de dados, faz-se necessária uma breve introdução das categorias descritas na lei, essenciais para a compreensão do tema, dispostas especialmente a partir do art. 5º. Como se verá posteriormente, os responsáveis pelo tratamento de dados são chamados pela legislação de "agentes de tratamento", designados pela lei como "controlador" e "operador" (art. 5º, IX).

O primeiro conceito a ser apresentado é o conceito de "titular de dados pessoais", definido pela lei como "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento" (art. 5º, V). Titular nada mais é do que o "dono" do dado pessoal a que se refere o tratamento.

O segundo conceito essencial é o "dado pessoal". É a categoria central da lei sobre a qual recai a atividade dos agentes de tratamento de dados. De acordo com a definição da lei, "dado pessoal é a informação relacionada a pessoa natural identificada ou identificável" (art. 5º, I). O dado pessoal se desdobra em outra categoria de maior relevância, que tem a proteção da essência do indivíduo como marca principal, que é a categoria do "dado pessoal sensível", definido pela lei como "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" (art. 5º, II).

Os dados sensíveis são uma categoria específica de dados pessoais (DONEDA, 2019) cuja utilização indevida poderia levar a patentes situações de discriminação, visto que tratam

de aspectos personalíssimos do titular de dados, como sua orientação sexual ou opinião política. São dados que, quando utilizados indevidamente, podem causar um "dano qualificado no que tange à pessoa humana" (KONDER, 2019, p. 446). Segundo Danilo Doneda,

> [...] estes **[dados sensíveis]** seriam determinados tipos de informação que, caso sejam conhecidas e submetidas a tratamento, podem se prestar a uma potencial utilização discriminatória ou lesiva e que apresentaria maiores riscos potenciais do que outros tipos de informação. (DONEDA, 2019, p. 142-143, grifos meus).

Nesse sentido, a tutela dos dados pessoais tidos como sensíveis se relacionam intrinsecamente com a tutela da dignidade da pessoa humana. Conforme leciona Carlos Nelson Konder,

> Nesse sentido, a dignidade da pessoa humana, para além de princípio, configura-se em cláusula geral, apta a abarcar uma infinidade de formas de proteção e promoção do sujeito. Consequentemente, deve ser vista com naturalidade e multiplicação de novas formas de manifestação da dignidade, se vierem com o objetivo de combater novos mecanismos de instrumentalização ou subjugação da pessoa humana e promover meios de seu livre desenvolvimento. (KONDER, 2019, p. 447).

Importante destacar que um dado pessoal pode adquirir a qualificação de "sensível" quando associado a um outro dado pessoal. Por exemplo, uma pessoa que se locomove de sua residência até um renomado instituto de tratamento de câncer e posteriormente usa o cartão de crédito para comprar medicamentos utilizados no tratamento dessa doença. Os dados de localização e do histórico de compra não representam risco, isoladamente considerados, mas quando combinados, fornecem um quadro referente à saúde do titular de dados. Esses dados podem estar agrupados em "bancos de dados" definidos pela lei como "conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico" (art. 5º, IV), o que facilita seu acesso e combinação, caso não haja a diligência devida para proteger esses dados de acessos não autorizados.

A crítica a esse entendimento destaca que os efeitos do tratamento de uma informação não podem ser conhecidos previamente de modo que, mesmo um dado não sensível pode revelar aspectos sensíveis "quando submetidos a um determinado tipo de tratamento" (DONEDA, 2019, p. 143), o que se leva a afirmar que "um dado, em si, não é perigoso ou discriminatório - mas o uso que se faz dele pode sê-lo" (DONEDA, 2019, p. 144). Ademais, seria impossível a

proibição da coleta e tratamento desse tipo de dados, uma vez que seu uso pode ser legítimo e necessário[10], como o caso do tratamento de dados inerentes ao contrato de seguro.

Nesse sentido,

> [...] Para a mensuração do risco a ser garantido, tem toda relevância a análise dos dados pessoais do segurado. Há íntima relação que se estabelece entre dados pessoais e risco coberto, na medida em que o conjunto de características subjetivas e comportamentais do segurado (e.g. sexo, idade, profissão, endereço, estado de saúde, consumo de cigarro) define fatores que influenciam na dimensão do risco, aumentando ou diminuindo a probabilidade de sinistro. Desse modo, a análise dos dados do segurado é determinante para a formação da base econômica do contrato, com o cálculo do prêmio, e, inclusive, para a seleção do risco, de modo que o segurador tenha as condições necessárias para decidir sobre a contratação e precisar seus contornos, delimitando o âmbito de riscos cobertos. Neste particular, observa-se que, para a conformação da base econômica do contrato, o segurador organiza todo um sistema contratual voltado à gestão científica e financeira do risco, cujos pilares são a mutualidade e a técnica atuarial. A mutualidade nada mais é do que uma técnica de divisão do risco entre os membros de determinado grupo. (MIRAGEM, 2020, pg. 4.).

Desse modo, percebe-se que, por sua importância, os dados pessoais sensíveis merecem uma especial proteção por parte dos agentes de tratamento. Prosseguindo com os conceitos essenciais, talvez uma categoria que possa minimizar os riscos do tratamento de dados sensíveis seja tornar o dado anonimizado, que seria um "dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento" (art. 5º, III).

Para fins da LGPD (art. 12, caput), dados anonimizados não são dados pessoais, uma vez que não podem mais ser associados, direta ou indiretamente, a um titular. Há certa controvérsia sobre a eficácia do processo de anonimização, pois há quem afirme que "sempre haverá a possibilidade de reversão do seu processo e a conseguinte identificação de um indivíduo" (BIONI, 2015, p. 4). De todo modo, caberá à Autoridade Nacional de Proteção de Dados, "órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional" (art. 5º, XIX), "dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais", na forma do §3, do art. 12 da LGPD.

[10] Nesse sentido, o art. 7º da lei, ao estabelecer os requisitos para o tratamento de dados, ou as "bases legais" para a realização do tratamento, dispõe que "o tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] IX - quando necessário para atender aos **interesses legítimos do controlador ou de terceiro**, exceto no caso de prevalecer em direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais".

A lei dispõe de outras categorias[11], as quais deixamos de citar, pois não se relacionam diretamente com o objeto do trabalho. O conceito e desdobramentos de tratamento de dados pessoais, previsto na referida Lei, em seu art. 5º, inciso X, serão melhor analisados no tópico a seguir.

2.4 Dos Direitos dos Titulares de Dados

Os direitos dos titulares de dados estão dispostos no Capítulo III, a partir do art. 17 da lei, porém, podem ser visualizados logo nos capítulos anteriores quando da disposição dos fundamentos e princípios orientadores da lei. Os artigos iniciais já demonstram uma enunciação de direitos que vão muito além da defesa da privacidade, especialmente ao dispor como objetivo da lei a proteção de direitos fundamentais de "liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (BRASIL, 2020d)[12] e como fundamentos mais importantes a autodeterminação informativa, o respeito à privacidade, o livre desenvolvimento da personalidade e o exercício da cidadania, conforme expresso no art. 2º.

Em uma primeira análise, percebe-se que a legislação confere ao titular de dados pessoais uma gama de direitos a serem exercidos frente aos agentes de tratamento, cuja atividade deve levá-los em consideração durante toda a existência do tratamento de dados pessoais do titular, conforme destacado no art. 9º. Importante destacar o protagonismo de uma concepção de privacidade associada à "construção de uma esfera pessoal na qual seja possível

[11] Art. 5. XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados; XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado; XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro; XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados; XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco; XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

[12] Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de **proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural**. No mesmo sentido, o artigo 17 da lei, ao dispor que "toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os **direitos fundamentais de liberdade**, de intimidade e de privacidade, nos termos desta Lei". (BRASIL, 2020d).

a liberdade de escolha e, consequentemente, o desenvolvimento da personalidade" (DONEDA, 2019, p. 130) ou como o "direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular" (RODOTÀ, 2008, p. 15), concepção visualizada logo nos primeiros artigos da lei, quando da definição de seu objetivos e fundamentos[13].

Como se percebe, os artigos iniciais já expressam direitos dos titulares de dados de maneira bastante significativa, como a autodeterminação informativa e a inviolabilidade da intimidade, da honra e da imagem, descritos nos incisos II e IV, do art. 2º. Ademais, os princípios estampados no art. 2º representam "o éthos da lei, ou seja, o que não se pode perder de vista ao interpretar a lei" (GARCIA *et al.*, 2020, p. 17).

Importante mencionar que os direitos dos titulares de dados também decorrem diretamente dos princípios estabelecidos pelo art. 6º da lei, conforme importante publicação do Comitê Central de Governança de Dados, intitulado *Guia de Boas Práticas – Lei Geral de Proteção de Dados*, elaborado para dar suporte à implementação no âmbito da Administração Pública Federal. A título de exemplo, o Guia destaca que o titular de dados tem direito a um "tratamento de dados vinculado aos propósitos legítimos, específicos, explícitos e informados, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades" (BRASIL, 2020a, p. 13), direito ao qual corresponde exatamente o conteúdo do princípio da finalidade, descrito no art. 6º, I[14].

Do mesmo modo que cada princípio pode se desdobrar em um direito para os titulares de dados, também encerram em seu conteúdo deveres aos agentes de tratamento de dados. Assim, os agentes de tratamento devem coletar o mínimo de dados pessoais e utilizá-los para a realização dos fins informados ao titular (art. 6º, I, II e III), informando aos titulares quais dados estão sendo tratados, qual a forma e duração do tratamento e quem são os responsáveis pelo tratamento (art. 6º, IV, V e VI), se medidas técnicas e administrativas de segurança, prevenção de danos e de tratamentos discriminatórios estão sendo adotadas (art; 6º, VII, VIII e IX) e, por fim, se tomaram todas as medidas eficazes e capazes de comprovar o cumprimento das normas de proteção dispostas ao longo da lei (art. 6º, X).

[13] Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, **com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.** Art. 2º A disciplina da proteção de dados pessoais tem como **fundamentos:** I - o respeito à privacidade; II - a **autodeterminação informativa** [...]. (BRASIL, 2020d).

[14] No mesmo sentido, Ana Frazão (2018b) também faz uma associação entre os direitos dos titulares de dados e os princípios dos quais aqueles decorreriam.

Observa-se a partir disso que antes mesmo de adentrar no capítulo específico dos direitos dos titulares (Capítulo III, arts. 17 a 22), a LGPD já traz um arcabouço protetivo em favor do titular, que se repetirá ao longo da lei[15]. Posteriormente, o art. 18 traz um rol de direitos do titular de dados oponíveis em face do controlador de dados.

À exceção da portabilidade de dados a outro fornecedor de serviço ou produto (art. 8º, V)[16], todos os outros direitos já haviam sido mencionados previamente, seja expressamente ou como decorrência de algum princípio do art. 6º. Sobre o rol de direitos do art. 18, a professora Ana Frazão (2018b) menciona interessante característica dos direitos previstos no artigo, qual seja, o direcionamento para os controladores de dados,

> o que pode ser considerado uma falha técnica, pois, como se verá adiante, ao se tratar dos deveres e responsabilidades dos agentes de tratamento, **vários deles também serão oponíveis aos operadores e encarregados**. Melhor teria sido se o legislador brasileiro, a exemplo do Regulamento Europeu, tivesse identificado como titular dos deveres os responsáveis pelo tratamento de dados, categoria mais ampla que abrange, mas não se restringe, ao controlador, nos termos das definições constantes do próprio art. 5º, da LGPD. A referida falha técnica é, de certa forma, reparada pelo § 3º, do art. 18, ao prever que "Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento." Em tal previsão, além de possibilitar o exercício dos direitos por meio de representantes legalmente constituídos, fica claro que o exercício de pretensão por parte dos titulares pode ser feito a agentes de tratamento, categoria que engloba controladores e operadores (LGPD, art. 5º, IX). (FRAZÃO, 2018b, grifo meu).

O art. 18, conforme a crítica acima, não traz direitos exercitáveis apenas em face dos controladores de dados, mas sim em face dos agentes de tratamento (art. 18, §3º). Ainda, alguns deles (art. 18, I e II) não representam grande novidade, principalmente porque já previstos como decorrência dos princípios do livre acesso[17], da qualidade dos dados[18] e da transferência[19], conforme destaca Ana Frazão (2018b).

---

[15] Nesse sentido, veja-se o art. 17, que assegura a toda pessoa natural a titularidade de seus dados pessoais e garante os direitos fundamentais de liberdade, de intimidade e de privacidade, já mencionados nos arts. 1º e 2º.

[16] Nesse sentido, a professora Ana Frazão (2018b), na parte IX da série de artigos publicados sobre o direito dos titulares, anota que "a portabilidade já havia sido mencionada no § 4º do art. 11 da LGPD, mas apenas para deixar claro que é vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nos casos de portabilidade de dados quando consentido pelo titular. Entretanto, a lei ainda não havia dado os devidos contornos ao referido direito". (FRAZÃO, 2018b).

[17] Art. 6º. IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais. (BRASIL, 2020d).

[18] Art. 6º V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. (BRASIL, 2020d).

[19] Art. 6º VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial. (BRASIL, 2020d).

Importante destacar ainda o direito do titular de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional (art. 18, §1º), inclusive para obter informação a respeito da confirmação de existência ou o acesso a dados pessoais, em formato simplificado, imediatamente ou no prazo de 15 (quinze) dias para declaração clara e completa (art. 19, I e II). O direito de petição também poderá ser exercido perante os organismos de defesa do consumidor (art. 18, §8º).

Por fim, importante ter em mente que para uma correta compreensão dos direitos dos titulares de dados é preciso que se tenha uma visão sistemática da LGPD, pois os direitos dos titulares de dados não foram expostos de maneira, o que demanda dos intérpretes uma análise de toda a lei para entender a exata dimensão dos direitos ali estabelecidos.

2.5 Tratamento de Dados Pessoais: Conceito, Princípios e Pressupostos

A lei destaca no inciso X, do art. 5º, um conceito ampliado de tratamento, que abarca diversas operações realizadas com dados pessoais, quais sejam

> Art. 5º [...] X - toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

O tratamento de dados está condicionado à observância de certos princípios específicos para garantir a regularidade do tratamento de dados levado a cabo pelos agentes de tratamento. O art. 6º da lei enuncia 10 princípios, entre os quais merecem destaque os princípios da "segurança", "prevenção" e da "responsabilização e prestação de contas". Ao exigir dos agentes de tratamento de dados que limitem o tratamento ao mínimo necessário para a realização de suas finalidades ou que adotem medidas técnicas e administrativas para proteger os dados pessoais de acessos não autorizados, percebe-se que a LGPD adotou a prevenção de danos como um valor a ser perseguido pelos agentes de tratamento.

Nesse sentido, o Capítulo VII, Seção II, "Das Boas Práticas e da Governança", atribui aos controladores e operadores, na aplicação dos princípios da "segurança" (art. 6º, VII) e "prevenção" (art. 6º, VIII), a possibilidade de

> Art. 50 [...] §2º, II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de

> boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.

A exigência da observância da prevenção de danos no contexto tecnológico decorre do aumento de problemas de cibersegurança ao redor do mundo nos últimos anos. De fato, as organizações passaram a ser alvos cada vez mais frequentes de ataques visando roubar dados, de modo que a resposta pela remediação tardia não se mostrava mais efetiva[20].

A prevenção também possui um papel de relevância no estudo da responsabilidade civil, sendo considerada "objetivo primordial da responsabilidade civil contemporânea" (ROSENVALD, 2017)[21]. Nesse sentido, Nelson Rosenvald (2017) destaca que o direito remediador deve ceder espaço ao direito proativo, privilegiando a proteção de bens jurídicos existenciais e patrimoniais e não apenas reagindo ao dano consumado.

Ainda segundo o autor,

> [...] toda pessoa ostenta o dever de evitar causar um dano injusto, agindo conforme a boa-fé e adotando comportamentos prudentes para impedir que o dano se produza ou que se reduza a sua magnitude. Ademais, caso o dano já tenha sido produzido, que se evite o seu agravamento (duty to mitigate the own loss). (ROSENVALD, 2017, p. 97).

A prevenção de danos na responsabilidade civil figura como uma medida de gerenciamento de riscos e eliminação prévia da possibilidade de realização do prejuízo. Esse gerenciamento pode ser melhor executado por meio da estipulação de deveres e comportamentos prévios, seja por meio de uma norma legal ou por uma norma regulamentar (SCHREIBER, 2015). Como um marco regulatório, a LGPD estipula deveres cujos objetivos são proteger direitos e mitigar a possibilidade de ocorrência de danos e, como demonstrado ao longo do trabalho, está articulada de uma maneira muito específica, qual seja, buscar a prevenção de danos como um valor máximo a ser seguido pelos agentes de tratamento.

A prevenção buscada pela LGPD tem por objetivo a proteção dos princípios constitucionais como a igualdade, liberdade e pleno exercício da cidadania e "abrange também uma tutela negativa preventiva ou inibitória, no sentido de evitar situações potencialmente

[20] No livro *Lei Geral de Proteção de Dados: Guia de Implementação*, os autores discorrem sobre esse processo: "A universalização do acesso à internet e o estabelecimento de redes globais de comunicação de dados trouxeram consigo o surgimento dos problemas de cibersegurança. Antes restritos aos antigos mainframes e às redes locais com atores internos às empresas, os acessos indesejados aos dados das empresas e ou sob sua guarda passaram a ser comuns, oriundos também de atores externos e desconhecidos. Um fator relevante é a ocorrência desses ataques de forma extemporânea, com frequência elevada e com um grau de dano às vezes extremamente relevante." (GARCIA *et al.*, 2020, p. 7).

[21] O autor traz como exemplo da relevância da função preventiva o Projeto de Código Civil e Comercial da Argentina de 2012, que dispõe no art. 1.708: "Funções da responsabilidade. As disposições deste Título são aplicáveis à prevenção de danos, a sua reparação e os casos em que seja admissível a sanção pecuniária dissuasiva".

lesivas a tais interesses, bem como uma tutela positiva, comprometida em promover a sua máxima realização" (SCHREIBER, 2015, p. 229). A prevenção também representa na responsabilidade civil "a passagem de um sistema repressivo para um proativo, preventivo, que se antecede à ocorrência de danos. Diante dos riscos da vida moderna, deve-se agir logo para se prevenir" (CAVALIERI FILHO, 2019, p. 11). Como se vê, o conteúdo da prevenção buscada na LGPD corresponde exatamente à prevenção na responsabilidade civil moderna.

Ademais, considerando a relevância e importância dos dados pessoais, conforme exposto nos tópicos anteriores, uma solução pela remediação não se mostra a resposta mais adequada. Quanto a isso, a LGPD previu mecanismos para mitigar o risco de dano pelo tratamento de dados pessoais, endereçando aos agentes de tratamento o dever de zelar pelos dados que estão sob sua responsabilidade.

O relatório de impacto à proteção de dados pessoais, previsto no art. 5º, inciso X, é talvez o instrumento mais importante por meio do qual os agentes de tratamento irão revelar as bases legais, a forma de obtenção do consentimento, dentre outras medidas e salvaguardas dos direitos dos titulares ao realizar o tratamento de dados. A legislação define o relatório de impacto como a "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco".

O relatório de impacto à proteção de dados pessoais é instrumento por meio do qual se poderá verificar se o agente de tratamento adotou medidas para prevenir a ocorrência de danos, de modo que a não demonstração pelo agente "da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais" (art. 6º, X) levará a responsabilização do agente de tratamento. A prevenção, portanto, tem uma dupla função: garantir a preservação dos direitos dos titulares e serve como parâmetro para se responsabilizar o agente de tratamento no caso de ocorrência de dano. Por outro lado, o princípio da prevenção e prestação de contas (art. 6º, X) tem por objetivo reparar o dano causado e reestabelecer a vítima ao status quo ante.

A demonstração, por parte dos agentes de tratamento, de que adotaram todas as medidas de proteção de dados pessoais que a lei prevê, funciona como cláusula de exclusão de responsabilidade, nos termos do art. 43, inciso II[22]. Também são hipóteses de "exoneração de

[22] Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:[...] II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, **não houve violação à legislação de proteção de dados** (BRASIL, 2020d).

responsabilidade" a comprovação de que não realizaram o tratamento de dados que lhes é atribuído (art. 43, I) e a culpa exclusiva do titular dos dados ou de terceiros.

Ao lado dessas hipóteses previstas na LGPD, a literatura jurídica atual identifica três categorias de exclusão do nexo causal: fato exclusivo da vítima, fato de terceiro e caso fortuito e força maior (CAVALIERI FILHO, 2019). A culpa exclusiva da vítima ou fato exclusivo da vítima e o fato de terceiro são categorias aceitas pela LGPD (art. 43, III) e pela literatura jurídica e jurisprudência nacional. Contudo, tais hipóteses têm admitido relativa flexibilização, pois são consideradas "como risco que o agente lesivo deveria ter levado em consideração e que, por este motivo, consiste em evento inapto a afastar a relação de causalidade" (SCHREIBER, 2015, p. 251).

No que se refere ao caso fortuito e força maior, há certa controvérsia sobre qual seria o conteúdo exato de cada uma dessas categorias. Entretanto, pode-se concluir como "elemento comum a ambos a inevitabilidade; só que no fortuito a inevitabilidade decorre da imprevisibilidade e na força maior da irresistibilidade" (CAVALIERI FILHO, 2019, p. 99). Na atividade de tratamento de dados, especialmente no uso de dados sensíveis, a previsibilidade do evento danoso deve ser sempre levada em consideração, adotando o agente todas as medidas de salvaguarda, na esteira do que foi previsto na LGPD, sendo a prevenção um valor máximo. Aqui, é importante a utilização da noção de "estado da técnica", de modo a saber se o agente adotou, realmente, todas as medidas possíveis.

Nesse sentido, Sérgio Cavalieri Filho destaca que

> A noção do estado da técnica é essencial na aferição da responsabilidade dos prestadores de serviços de alto risco em vista da sofisticação tecnológica de que dispõem para fornecê-los. Por isso, determinados eventos, outrora considerados inevitáveis, atualmente, sob o estado da técnica, permitem a tomada de providências técnicas preventivas, visando elidir o dano, que se torna objetivamente previsível (CAVALIERI FILHO, 2019, p. 100).

Por fim, importante destacar que a inevitabilidade deve ser apurada na situação concreta, vislumbrando as peculiaridades de cada caso, de modo que não se pode inferir que qualquer evento considerado inevitável irá afastar o nexo de causalidade. O cair de um raio em um data center, por exemplo, que fragilize as barreiras de acesso a determinada base de dados, não pode ser considerado como evento inevitável, pois tendo em vista a natureza da prestação do serviço (tratamento de dados pessoais e/ou dados pessoais sensíveis, por exemplo), deve o agente adotar o mais avançado estágio do estado da técnica e equipar suas instalações com os mais

modernos meios tecnológicos que possam mitigar a possibilidade de risco de dano aos titulares de dados (CAVALIERI FILHO, 2019). Sendo o caso de um fortuito interno[23], inerente à organização da empresa e relacionado aos riscos da atividade, não será o agente de tratamento exonerado da responsabilidade. Entretanto, sendo o caso de fortuito externo[24], cuja demonstração de autonomia em relação aos riscos da empresa e inevitabilidade sejam demonstrados, pode-se concluir que o agente de tratamento será exonerado da responsabilização civil[25].

Em que pesem os entendimentos diversos que possam ser levantados, apenas na hipótese de fortuito externo e na comprovação de não realização do tratamento de dados é que os agentes de tratamento não serão responsabilizados civilmente. Com isso, percebe-se que as excludentes de responsabilidade previstas na LGPD não são taxativas, de modo que os agentes de tratamento podem encontrar na literatura jurídica, na jurisprudência e no Código Civil hipóteses de exoneração da responsabilidade civil.

Além da obediência aos princípios e direitos dos titulares, a LGPD previu requisitos legais para sua realização, entendidos como hipóteses legais de tratamento de dados pessoais. Dentre essas hipóteses legais de tratamento, a exigência de consentimento prévio do titular (art. 7º, I) merece ser mais bem analisada, tendo em vista o tratamento que a lei confere a essa hipótese de tratamento de dados. O consentimento deve ser dado de maneira livre, inequívoca, baseado em informações claras, precisas e facilmente acessíveis sobre a realização do tratamento (art. 6º, VI) e restrito às finalidades específicas informadas ao titular de dados. Ou seja, o titular de dados concorda com o tratamento de seus dados para uma finalidade determinada, de modo que "autorizações genéricas para o tratamento de dados pessoais serão nulas", na forma do art. 8º, §4º.

[23] Segundo Sergio Cavalieri Filho, "o fortuito interno não exclui a responsabilidade do fornecedor do serviço, porque está ligado à organização da empresa. Embora sua ocorrência seja inevitável, as consequências são evitáveis, pelo menos em grande parte, pelo estado da técnica" (CAVALIERI FILHO, 2019, p. 101).

[24] Segundo Sergio Cavalieri Filho, "o fortuito externo é também fato imprevisível e inevitável, mas estranho à organização do negócio, não guarda relação de causalidade com a atividade do fornecedor, absolutamente estranho ao serviço, via de regra ocorrido em momento posterior ao seu fornecimento. Duas são as características do fortuito externo: autonomia em relação aos riscos da empresa e inevitabilidade, razão pela qual exclui a responsabilidade do fornecedor do serviço" (CAVALIERI FILHO, 2019, p. 101).

[25] Segundo entendimento exarado pelo Superior Tribunal de Justiça: A força maior e o caso fortuito vêm sendo entendidos, atualmente, como espécies do gênero fortuito externo, no qual se enquadra a culpa exclusiva de terceiros, sendo aquele fato, imprevisível e inevitável, estranho à organização da empresa; contrapondo-se ao fortuito interno, que, apesar de também ser imprevisível e inevitável, relaciona-se aos riscos da atividade, inserindo-se na estrutura do negócio (REsp 1450434/SP, Rel. Ministro LUIS FELIPE SALOMÃO, QUARTA TURMA, julgado em 18/09/2018, DJe 09/11/2018).

O fornecimento do consentimento deverá ser feito "por escrito ou por outro meio que demonstre a manifestação de vontade do titular" (art. 8º), em "cláusula destacada das demais cláusulas contratuais" (art. 8, §1º), cabendo ao controlador "o ônus da prova de que o consentimento foi obtido em conformidade com o disposto na Lei" (art. 8º., §2º), sendo vedado "o tratamento de dados pessoais mediante vício de consentimento" (art. 8, §3º). Como se vê, trata-se de uma hipótese legal extremamente qualificada, pois exige e concorrência de diversos requisitos para sua realização, cabendo ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com os requisitos da lei (art. 8º, §2º).

Observe-se que caso o controlador necessite compartilhar os dados pessoais com outros controladores, deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas na Lei (art. 7º, §5º) e, mesmo no caso de dispensa de consentimento, os agentes de tratamento ainda deverão observar princípios gerais e garantir os direitos dos titulares (art. 7º, §6).

O consentimento inicialmente concedido também pode ser revogado a qualquer momento, mediante manifestação expressa do titular (art. 8º, §5º). A revogabilidade do consentimento a qualquer tempo tem uma razão de ser: é certo que o tratamento de dados influi diretamente sobre a privacidade do indivíduo e que o conceito de privacidade caminhou de um "direito de ser deixado só" para um conceito de "determinação da própria esfera pessoal", com uma feição existencial muito proeminente, ligado à própria personalidade humana. Desse modo, "a possibilidade de revogação das manifestações de vontade é considera ínsita a todo tipo de exercício de autonomia existencial" (NUNES DE SOUZA; GUIA SILVA, 2019, p. 267).

Nesse sentido, Rose Melo Vencelau Meireles (2009 *apud* NUNES DE SOUZA, 2019, p. 267), a respeito da autonomia existencial destaca que

> a revogabilidade decorre do princípio do consentimento qualificado, sobretudo, quando da disposição resulte limitação ao exercício de direito da personalidade, pois somente a limitação voluntária é admissível. Permite-se que o disponente se arrependa da declaração de vontade que expressou e a revogue, até o momento anterior ao da execução material do ato".

De igual modo, Cristiano Chaves de Frias, Nelson Roselvald e Felipe Braga Neto entendem que

> nas situações jurídicas meramente patrimoniais, o consentimento dado é irrevogável; já nas situações existenciais, ele é eminentemente revogável. Quando se trata de direitos ligados à própria personalidade humana, há que se considerar que o particular, mesmo depois de ter consentido com a limitação, tem também o poder de revogar tal manifestação, já que não há como obrigar

> a pessoa a dispor do direito se não há mais voluntariedade no ato. (FARIAS, 2017, p. 892).

Assim, ainda que o direito de revogação do consentimento não fosse expressamente previsto na lei, a possibilidade decorreria da própria natureza do direito de privacidade, cuja transformação resultou na construção de uma esfera protetiva da liberdade de escolha do indivíduo e do desenvolvimento da personalidade (DONEDA, 2019). Não obstante a importância de todas as outras hipóteses legais de tratamento de dados pessoais, não há maior necessidade de aprofundamento em cada uma delas, pois o que se deve ter em mente é que os agentes de tratamento só poderão realizar o tratamento de dados quando ancorados em alguma hipótese legal, não podendo simplesmente armazenar dados pessoais com objetivo de utilização futura, nas hipóteses do art. 16[26].

Ademais, além das exigências acima destacadas, o art. 46 destaca a obrigatoriedade de os agentes de tratamento adotarem

> [...] 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.

No mesmo sentido, é o art. 6º, inciso VII, que conceitua "segurança" como "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão". Com base nesse inciso, extraem-se as seguintes medidas que podem ser adotadas pelos agentes de tratamento: manter lista de acesso a informações sensíveis, realizar o registro de acesso a informações sensíveis para leitura, alteração e remoção e revisar o registro de acesso às informações sensíveis (GARCIA, *et al.*, 2020).

Em complementação a esse dever de mitigação e prevenção de dados, a autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável a exigência e proteção de dados[27], que deverão ser observadas "desde a fase de concepção do produto ou do

[26] Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, **autorizada a conservação para as seguintes finalidades**: I - cumprimento de obrigação legal ou regulatória pelo controlador; II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados (BRASIL, 2020d).

[27] Art. 46. § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei. (BRASIL, 2020d).

serviço até a sua execução" (art. 46, §2º), além de "estimular a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais" (art. 51). Nesse sentido, "a International Standards Organization (ISO) já possui um conjunto de padrões técnicos reconhecidos internacionalmente como as melhores práticas atuais no âmbito da proteção de dados. Essa é, por exemplo, uma diretriz objetiva que pode ser usada no momento" (DAVID, 2019, pg. 74).

No contexto de responsabilização dos agentes de tratamento, a autoridade nacional de proteção de dados terá o importante papel de definir categorias abertas na lei, como legítimo interesse e risco, de modo que sua atuação, em um primeiro momento, deverá ser mais elucidativa do que punitiva.

Nesse sentido, importante destacar que

> Como próximos passos nesse debate, podemos afirmar, que na nossa perspectiva a ANPD não deve estabelecer um conceito fechado sobre o que é risco em uma orientação futura sobre o tema e, sim, demonstrar nessas orientações como o risco pode ser avaliado através de metodologias para avaliação de risco e elaboração de relatórios de impacto à proteção de dados pessoais. Para isso, será necessário a ANPD estabelecer critérios mínimos de análise, isso significa que a partir de estudos de caso é possível indicar quais tipos de operações de tratamento de dados pessoais podem apresentar alto risco. O Working Party fez isso no contexto europeu, contudo, é necessário dar um passo além. Apresentar operações de tratamento de dados pessoais, que fundamentadas em metodologias, possam ser classificadas como operações de alto risco na LGPD. (GOMES, 2020, p. 267).

Ante o exposto, entende-se que a ANPD terá um importante papel na definição de importantes conceitos na legislação, inclusive na análise de risco que irá influenciar a aplicação da responsabilidade civil objetiva.

2.6 Agentes de Tratamento: Controlador e Operador

A Lei Geral de Proteção de Dados Pessoais define os sujeitos responsáveis pelo manuseio de informações pessoais como "agentes de tratamento" (art. 5º, IX), gênero do qual são espécies o "controlador" e o "operador". A definição dessas figuras é encontrada na própria lei, que delineia o conceito de controlador como "pessoa natural ou jurídica, de direito público[28] ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (art. 5º, VI), e o operador, por sua vez, é definido como "pessoa natural ou jurídica, de direito público

[28] As regras concernentes ao tratamento de dados pessoais pelo poder público estão dispostas no artigo 23 da legislação e não serão objeto de uma análise mais aprofundada no presente trabalho.

ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (art. 5º, VII). Ambos são disciplinados em capítulo próprio (arts. 37 a 40), e serão explorados adiante.

Há, ainda, a figura do encarregado de dados (art. 41), que não será objeto do presente trabalho, pois a LGPD, em sua Seção III, ao tratar da responsabilidade e do ressarcimento de danos, indica apenas os agentes de tratamento (controlador e operador) como responsáveis pela indenização em caso de danos aos titulares.

Dessa primeira definição dada pela própria lei, é possível indagar se há uma premissa na legislação de que existe hierarquia entre os agentes de tratamento, sendo o controlador figura mais proeminente, acima do operador de dados, pois ao segundo compete executar aquilo que foi definido pelo primeiro. De todo modo, cada um será responsável pelo ressarcimento dos danos que causar em razão do exercício da atividade de tratamento de dados pessoais, mas poderão responder solidariamente em algumas situações (art. 42).

O operador, por exemplo, 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 se equipara ao controlador, salvo nos casos de exclusão previstos no art. 43 (art. 42, §1º, I). 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 (art. 42, §1º, I e II).

Essa identificação dos controladores e operadores envolvidos no fluxo de tratamento de dados é de extrema importância para o correto endereçamento da ação de responsabilização correspondente e evitar a propositura em face de agente que não realizou o tratamento dos dados pessoais. Nesse sentido, a própria lei define a identificação do controlador como um direito do titular para garantir o acesso facilitado às informações sobre o tratamento de seus dados[29].

A identificação dos agentes de tratamento também é relevante para a elaboração do Relatório de Impacto à Proteção dos Dados Pessoais (RIPD), definido no tópico anterior. Ainda, a lei dispõe em seu art. 38 que "a autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os

[29] Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: I - finalidade específica do tratamento; II - forma e duração do tratamento, observados os segredos comercial e industrial; **III - identificação do controlador;** (grifos meus) (BRASIL, 2020d).

segredos comercial e industrial". Importante frisar que a lei apenas disciplina o conteúdo mínimo desse instrumento, que

> deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados" (art. 38, § único)[30].

Outra exigência da legislação é que controlador e operador mantenham "registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse" (art. 37). Por fim, dispõe o art. 39 que "o operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria".

A despeito do Capítulo VI, seção III, tratar especificamente da responsabilização dos agentes de tratamento, a definição das atribuições de cada um não é tarefa fácil. Isso porque, as exigências a eles dirigidas estão disciplinadas em toda a lei de maneira difusa, como forma de deveres e padrões de conduta, devendo mitigar a possibilidade de ocorrência de danos aos titulares de dados e respeitando as exigências da lei para tornar apto o tratamento realizado.

3 RESPONSABILIDADE E RESSARCIMENTO DE DANOS

3.1 Responsabilidade Civil Subjetiva e Objetiva: Apontamentos necessários

O presente tópico não buscará realizar uma digressão histórica da responsabilidade civil subjetiva e objetiva. Será, antes, uma exposição suscinta, com o objetivo de situar o leitor a respeito dos elementos caracterizadores da responsabilização, se deverá se dar com base na demonstração de culpa (responsabilidade subjetiva) ou no risco da atividade (responsabilidade objetiva).

A responsabilidade civil pode ser definida como a "obrigação de reparar danos que infringimos por nossa culpa e, em certos casos determinados pela lei" (BRAGA NETTO; FARIAS; ROSENVALD, 2019, p. 37). Se é certo que o dano ocorreu, deve-se procurar saber qual será o fundamento da responsabilização daquele que deu causa: se deve analisar a sua

[30] O Relatório de Impacto à Proteção dos Dados Pessoais (RIPD) é mais um dos temas da legislação a ser regulamentado pela Autoridade Nacional de Proteção de Dados Pessoais (ANPD). Sobre esse e demais temas que merecem regulação na legislação. Conferir *ANPD: Pontos a Serem Regulados, do Instituto LGPD Acadêmico*. Disponível em: https://bit.ly/3efpd3O. Acesso em: 7 jul. 2020.

culpa no evento danoso ou se o risco da atividade que desempenha o causou. Para isso, há duas teorias que dispõem sobre o fundamento do dever de indenizar.

A teoria da responsabilidade civil subjetiva fundamenta a obrigação de indenizar (reparar o dano) "quando o agente causador do dano atuar com violação de um dever jurídico, normalmente de cuidado (como se verifica nas modalidades de negligência ou imprudência), conforme consta do art. 186 do Código Civil de 2002" (GAGLIANO, PAMPLONA FILHO, 2017, p. 862).

Isso significa que, para ser indenizada por um dano sofrido, a vítima deve comprovar a culpa do causador do dano, que se revela na conduta negligente, imprudente ou imperita, a ensejar o ato ilícito. Essa fórmula (ato ilícito e obrigação de reparar) é resultado da leitura dos arts. 186 e 927, caput, do Código Civil, assim:

> Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.
>
> Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.

Nesse cenário, os elementos caracterizadores da responsabilidade civil subjetiva são a conduta culposa do agente, o dano e o nexo de causalidade entre a conduta e o dano. Em sua concepção clássica, a culpa é entendida como a "violação de dever preexistente, para cuja configuração se exige o elemento subjetivo, identificado na manifestação volitiva livre e consciente do agente, bem como na previsibilidade do resultado" (GUEDES; TEPEDINO; TERRA, 2020, p. 104). Caio Mário da Silva Pereira sintetiza "em face do art. 186 do Código Civil, o elemento subjetivo do ato ilícito, como gerador do dever de indenizar, está na imputabilidade da conduta à consciência do agente" (PEREIRA, 2018, p. 55). Desse modo, o que se avalia, na violação do dever preexistente, é a vontade de agir do causador do dano e a previsibilidade do resultado danoso.

Importante destacar que o ato ilícito pode existir mesmo quando não associado à violação de um dever preexistente, como no caso do abuso de direito, que é situação em que "o agente atua formalmente de acordo com a regra jurídica, mas ofende materialmente as finalidades do ordenamento jurídico" (BRAGA NETTO; FARIAS; ROSENVALD, 2019, p. 190).

Entendida nestes termos, o conceito de culpa está arraigado a uma forte concepção moral, de modo que "ao definir a noção jurídica de culpa, muitos autores se valiam – e ainda hoje se valem – de elementos psicológicos ou anímicos, típicos de uma avaliação moral e

subjetiva da conduta individual" (SCHREIBER, 2015, p. 14). Essa concepção moral de culpa traz para a vítima o ônus de demonstrar o elemento subjetivo do autor do dano, o que nem sempre é possível.

Sobre esse ponto, a literatura jurídica processualista conceitua essa prova de difícil produção de "prova diabólica", "expressão que se encontra na doutrina para fazer referência àqueles casos em que a prova da veracidade da alegação a respeito de um fato é extremamente difícil, nenhum meio de prova sendo capaz de permitir tal demonstração" (CÂMARA, 2005, p. 12).

Contudo, com o passar do tempo, esse modelo de comprovação da culpa do ofensor se mostrou insuficiente, pois levaria a situações em que o causador do dano não poderia ser responsabilizado. Sobre o ponto, a literatura jurídica destaca que

> De início, a dificuldade de demonstração da culpa atendia, em boa medida, ao interesse liberal que rejeitava a limitação da autonomia privada, salvo nas hipóteses de uso flagrantemente inaceitável da liberdade individual. Entretanto, com o desenvolvimento do capitalismo industrial e a proliferação de acidentes ligados às novas tecnologias, tal dificuldade intensificou-se ao extremo, atraindo a intolerância social e a rejeição do próprio Poder Judiciário. A exigência de que a vítima demonstrasse a culpa em acidentes desta natureza – basta pensar em acidentes de transporte ferroviário ou em acidentes de trabalho ocorridos no interior das fábricas – tornava-se verdadeiramente odiosa diante do seu desconhecimento sobre o maquinismo empregado, da sua condição de vulnerabilidade no momento do acidente e de outros tantos fatores que acabaram por assegurar à prova da culpa alcunha de *probatio diabolica* (SCHREIBER, 2015, p. 17).

Para evitar situações em que a vítima restasse irressarcida ante a impossibilidade de comprovação de culpa, a jurisprudência passou a alargar o conceito de culpa e até dispensá-la como requisito essencial para o dever de indenizar (VENOSA, 2017). Passou-se no Brasil a admitir situações em que a culpa fosse presumida, fundada no princípio de não causar dano (*neminem laedere*).

E isso tem uma razão de ser: a responsabilidade civil tradicional estava exclusivamente baseada na proteção ou tutela do direito de propriedade e dos demais direitos subjetivos patrimoniais. Contudo, passou-se a admitir a dignidade da pessoa humana, a solidariedade social e a justiça distributiva como elementos decisivos no dever de ressarcir (SCHREIBER, 2015).

A superação de uma noção de culpa calcada na tutela do direito patrimonial foi lenta e gradual, tendo os tribunais, primeiramente, admitido a facilitação da prova da culpa por parte

das vítimas e, em um segundo momento, admitido a presunção de culpa, com inversão do ônus da prova (CAVALIERI FILHO, 2019). Na fase de presunção de culpa, há um maior favorecimento da vítima, pois o causador do dano se presume culpado pelo evento danoso. Por fim, caminha-se para uma fase em que se admite a responsabilização sem culpa em determinados casos (CAVALIERI FILHO, 2019).

Nesse sentido, Henri De Page bem sintetiza a questão

> É possível melhorar sensivelmente a situação da vítima invertendo a ordem da prova. Se em certas circunstâncias, ou na fé de certas situações, o dano é em princípio imputado ao seu aturo, a vítima será infinitamente melhor tratada, porque não terá ela de provar senão o fato material do dano e sua origem; e o autor do dano não poderá escapar à responsabilização senão demonstrando que nenhuma culpa cometeu (1974 *apud* DA SILVA PEREIRA, 2018, p. 103).

O desgaste da culpa como elemento balizador da responsabilização, aliado à multiplicação de acidentes devido ao desenvolvimento industrial, levou ao surgimento da teoria do risco, que figura como fundamento para a responsabilização objetiva, ou independente de culpa. Em que pesem os demais mecanismos de mitigação da culpa – "admissão fácil da existência da culpa pela aplicação da teoria do abuso do direito e da culpa negativa; o reconhecimento da presunção de culpa; [...]; a transformação da responsabilidade aquiliana em contratual" (SCHREIBER, 2015, p. 18), – para facilitar o acesso da vítima à reparação, a teoria do risco como fundamento de responsabilização obteve maior sucesso na definição de elementos objetivos para imputação de responsabilidade (SCHREIBER, 2015).

A responsabilização objetiva, portanto, desconsidera o elemento subjetivo, ou seja, trata como "irrelevante o nexo psicológico entre o fato ou atividade e a vontade de quem a pratica, bem como o juízo de censura moral ou de aprovação da conduta" (CAVALIERI FILHO, 2019, p. 227). Importante destacar, porém, que a evolução para a doutrina objetiva e a aceitação de teorias do risco não afastaram a responsabilidade subjetiva, calcada na ideia de culpa, de modo que ambas subsistem no ordenamento jurídico brasileiro, aplicadas a situações distintas.

Assim, a responsabilidade civil objetiva, ou doutrina do risco, surge em um contexto de superação da culpa como elemento de imputação de responsabilidade, centrada no dever de indenizar independentemente da comprovação da culpa do ofensor, trazendo para a responsabilidade civil uma perspectiva solidarista e de repartição de riscos, sobretudo a partir da Constituição Federal de 1988, comprometida com a solidariedade social e com a justiça distributiva (CF, art. 3º, I e II) (GUEDES; TEPEDINO; TERRA, 2020, p. 5). A Constituição

Federal não apenas previu hipóteses de responsabilidade civil objetiva (art. 7º, XXVIII; art. 21. XXIII, "d"; art. 37, §6º) (GUEDES; TEPEDINO; TERRA, 2020, p. 6), como também é o vértice a partir do qual o sistema jurídico se organiza e recebe influência.

Nesse sentido, essa perspectiva de socialização de riscos se espalha para outros diplomas normativos, como o Código de Defesa do Consumidor (Lei nº 8.078/1990), que dispôs a responsabilidade objetiva do fornecedor de produtos e serviços (art. 12 e 18) e o Código Civil de 2002, que institui no parágrafo único do art. 927 a cláusula geral de responsabilidade objetiva para atividades de risco, "conferindo ao Poder Judiciário discricionariedade na avaliação das hipóteses de incidência da responsabilidade sem culpa" (GUEDES; TEPEDINO; TERRA, 2020, p. 6).

O conceito de "atividade de risco" merece atenção, por ser o cerne da responsabilidade civil objetiva, ao lado de outras hipóteses previstas em lei (art. 927, §único). A atividade de risco pode ser definida como aquela cuja potencialidade de causar danos às pessoas seja superior ao "normal". Cumpre saber, portanto, se a atividade de tratamento de dados pessoais poderia ser identificada como uma atividade de risco a ensejar a responsabilização objetiva. Nesse ponto, a Autoridade Nacional de Proteção de Dados Pessoais, assim que efetivamente instalada, terá um papel importante na definição do risco no tratamento de dados pessoais.

Para tentar identificar uma "atividade de risco", a literatura jurídica aponta algumas hipóteses e critérios de identificação. Nesse sentido, Maria Celina Bodin de Moraes anota que

> a atividade é considerada perigosa, portanto, quando, do ponto de vista estatístico, causa danos quantitativamente numerosos e qualitativamente graves. Esses critérios, a serem aproveitados em nosso ordenamento, criam um standard flexível que será definido, pela inter-relação destes dois elementos: a magnitude do dano e sua probabilidade. (BODIN DE MORAES, 2006, p. 28).

A doutrina do risco sustenta a ideia de que aqueles que exercem atividades que por sua natureza causem riscos às pessoas devem ser responsabilizados independentemente da verificação de culpa de sua parte. Resume-se, dessa forma, "nesta fórmula: "todo prejuízo deve ser atribuído ao seu autor e reparado por quem o causou" (PEREIRA, 2018, p. 41). Trata-se, como visto, da superação da necessidade da prova de culpa dos agentes causadores de danos, sem a ocorrer a eliminação da responsabilidade subjetiva.

A noção de risco se desdobra em algumas categorias cujas especificidades estabelecem fundamentos distintos de responsabilização, como o risco profissional, risco criado e risco proveito, por exemplo, sobre as quais há certa controvérsia sobre qual teria sido a concepção

de risco adotada pelo Código Civil. Para a teoria do risco profissional, responde pelos danos causados aqueles que tiverem proveitos da atividade empresarial desempenhada, que lhes fornece lucratividade ou benefício (GUEDES; TEPEDINO; TERRA, 2020). Já a teoria do risco criado estabelece que "se alguém põe em funcionamento uma qualquer atividade, responde pelos eventos danosos que esta atividade gera para os indivíduos" (PEREIRA, 2018 p. 353). Por fim, a teoria do risco proveito estatui que aquele que exerce atividade lucrativa, com considerável risco à coletividade, responde pelos danos causados quando o exercício da atividade representou vantagem ou benefício ao causador do dano (CAVALIERI FILHO, 2019).

Na atividade de tratamento de dados, a teoria do risco criado parece ser a melhor opção, pois ainda que a atividade seja exercida sem qualquer "proveito" ou "intuito lucrativo", o simples exercício é capaz de gerar riscos para os titulares de dados, comprometendo-lhes direitos e garantias constitucionalmente estabelecidas, como a privacidade, intimidade e vida privada, excetuadas as hipóteses previstas no art. 4º da LGPD[31]. E, adiantando-se o entendimento exposto no tópico "3.3" e em sede de conclusão, a atividade de tratamento de dados representa risco intrínseco aos direitos dos titulares de dados, de modo que o princípio da prevenção deverá ser o valor mais importante a ser seguido pelos agentes de tratamento, buscando antecipar os riscos à privacidade que possam ser causados pelo tratamento de dados, buscando preveni-los.

Assim, os agentes de tratamento devem assegurar que medidas de segurança sejam adotadas para se minimizar o risco do tratamento de dados, sendo este o dever jurídico cuja violação enseja o dever de indenizar civilmente.

3.2 Elementos Caracterizadores da Responsabilidade Civil Subjetiva dos Agentes de Tratamento

Embora a Lei Geral de Proteção de Dados Pessoais (LGPD) não tenha deixado claro qual regime de responsabilidade civil se aplica aos casos de violação de seus dispositivos, a

[31] LGPD. Art. **4º Esta Lei não se aplica ao tratamento de dados pessoais:** I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II - realizado para fins exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

literatura jurídica nacional tenta identificar os elementos que apontam para um tipo de responsabilização específica, seja ela subjetiva ou objetiva. Neste tópico, veremos os argumentos que apontam para a responsabilização civil subjetiva dos agentes de tratamento.

Como se percebe, o dispositivo legal não cita explicitamente a espécie de responsabilidade adotada pelo legislador, se objetiva ou subjetiva, como fundamento do regime de responsabilidade. Contudo, da análise sistemática da lei, é possível, argumenta parte da literatura jurídica, entender que o regime adotado foi o da responsabilidade civil subjetiva.

Nesse sentido, Gisela Sampaio e Rose Melo argumentam que toda a estrutura da lei é baseada na criação de deveres de cuidados, dirigidos aos agentes de tratamento, sob pena de responsabilização (GUEDES; VENCELAU MEIRELES, 2019). Assim, prosseguem as autoras, "se o que se pretende é responsabilizar os agentes, independentemente de culpa de fato, não faz sentido criar deveres a serem seguidos, tampouco responsabilizá-los quando tiverem cumprido perfeitamente todos esses deveres" (GUEDES; VENCELAU MEIRELES, 2019, p. 231). Com base no mesmo fundamento, (GUEDES; TEPEDINO; TERRA, 2020) entendem que

> [...] tudo isso está a indicar que, na sistemática da lei, o modelo adotado foi o da responsabilidade subjetiva. Afinal, como acima observado, não haveria razão para o legislador impor tantos deveres, fixando preciso padrão de conduta, se fosse para responsabilizar os agentes, independentemente de terem esses agido ou não com culpa.

A investigação a respeito do descumprimento de deveres e *standards* de conduta se aproxima de um modelo de responsabilização baseado na culpa. Isso porque, a noção atual de culpa aponta para a desconsideração da vontade do agente para o descumprimento da norma, levando-se em consideração o padrão de conduta que era esperado na situação concreta, revestindo o conceito de culpa de um conteúdo normativo. Nesse sentido,

> [...] as críticas à noção clássica conduziram à elaboração de conceito objetivado de culpa, designado *culpa normativa,* que se revela na ideia de desvio de conduta, e cuja apreciação desconsidera a análise do perfil subjetivo do agente que se pretende responsabilizar, mas leva em conta o comportamento exigível diante das especiais circunstâncias do caso concreto. Não se investiga o direcionamento da vontade do agente para o descumprimento da ordem jurídica *in abstrato*, e sim, ao revés, a adequação (ou não) de sua conduta ao padrão de comportamento esperado *in concreto*. Esse *standard* de comportamento desejado para o caso concreto serve a normatizar objetivamente a investigação da culpa, dando-lhe contornos consentâneos com a especificidade fática e circunstancial da hipótese em exame. (GUEDES; TEPEDINO; TERRA, 2020, p. 4).

É importante destacar que a "tutela prioritária da vítima, prevista em sede constitucional, que impõe a ampliação dos mecanismos de imputação de responsabilidade, incrementando suas

chances de obter o ressarcimento pelo dano sofrido" (GUEDES; TEPEDINO; TERRA, 2020, p. 7), de modo que, mesmo na teoria subjetiva, o conceito de culpa ganha uma nova roupagem, tornando-a mais "objetivada" (GUEDES; TEPEDINO; TERRA, 2020).

Trata-se do conceito de culpa normativa, que se revela quando o comportamento do agente destoa do padrão de comportamento esperado na situação concreta. Para aferição da conduta culposa, basta comparar a conduta do ofensor com o padrão de comportamento (*standards*) que dele era esperado. Esse conceito assume especial relevância na Lei Geral de Proteção de Dados, que estipula aos agentes de tratamento regras de comportamento que devem ser seguidas durante todo o tratamento de dados pessoais.

Desse modo, concluem as autoras, "não se investiga mais o direcionamento da vontade do agente para o descumprimento da ordem jurídica em termos abstratos, mas, sim, a sua adequação (ou não) ao padrão de comportamento esperado naquelas circunstâncias concretas" (GUEDES; VENCELAU MEIRELES, 2019, p. 233). Importante destacar que a LGPD se estrutura em torno da criação de deveres aos agentes de tratamento, como por exemplo nos incisos VI, VII e VII, do art. 6º.

Ainda, o inciso X do referido artigo, ao conceituar o princípio da "responsabilização e prestação de contas", dispõe que os agentes deverão demonstrar a "a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas". Essa é mais uma "pista" de que o regime adotado pela legislação foi mesmo o da responsabilidade subjetiva, pois

> do ponto de vista do controlador, do que adianta "prestar contas", se, ao final, se houver incidente, por mais diligente que tenha sido, ele será responsabilizado da mesma forma e independentemente de culpa? (GUEDES; VENCELAU MEIRELES, 2019, p. 233).

Importante destacar, também, o fato de a LGPD ter dedicado um capítulo à "segurança e boas práticas", dividido em duas seções: "da segurança e do sigilo dos dados" e "das boas práticas e da governança". As duas seções estabelecem verdadeiro *standard* de conduta a ser seguido pelos agentes de tratamento, oferecendo, inclusive, a possibilidade de se associarem para formular regras de boas práticas e de governança (art. 50, caput) (GUEDES; VENCELAU MEIRELES, 2019).

No mesmo sentido, Fernando Antônio Tasso entende que o regime adotado foi o da responsabilidade civil subjetiva, porque a lei, ao exigir dos agentes de tratamento de dados um padrão de conduta, afasta a responsabilidade objetiva. Desse modo,

> [...] à evidência, tais regras não consistem em meras recomendações tendentes a evitar incidentes de segurança. Antes, o legislador estabeleceu um standard de conduta e cobra o cumprimento desses deveres. O tratamento regular de dados consiste em uma obrigação de resultado e não de meio. Assim sendo, caso o sistema de responsabilidade civil fosse da modalidade objetiva, a prescrição exaustiva e detalhada dos deveres seria algo absolutamente inócuo, sobretudo porque redundaria na conclusão de que de nada adiantaria o cumprimento dos deveres se, qualquer que fosse o incidente, a responsabilidade pela reparação estivesse configurada, o que é um contrassenso. (TASSO, 2020, p. 108).

Como se vê, a lei confere aos agentes a possibilidade de se autorregular, ou seja, estabelecer regras para a atividade que desempenham. Trata-se de medida louvável, pois

> [...] a autorregulação assegura eficácia, flexibilidade e economia aos agentes de mercado. Como os regulados desempenham o papel disciplinador, as normas são elaboradas por pessoas capacitadas, que conhecem o objeto da regulação e a vivência do mercado. A *expertise* tende a assegurar a melhor qualidade da regulação e, via de consequência, goza de boa reputação e maior receptividade ou aderência pelo público alvo. Este benefício diz respeito também à legitimidade da norma, pois, ao ser emanada de uma entidade privada especializada, seu conteúdo não se sujeita às mesmas críticas deferidas ao processo legislativo ou instruções de órgãos governamentais. (RIBEIRO DIAS; FADEL BECUE, 2012, p. 7.368).

Há, ainda, dois outros fatores que apontam, segundo Gisela Sampaio e Rose Melo, para a adoção do regime subjetivo de responsabilidade. Primeiramente, o histórico de tramitação do projeto de lei que originou a LGPD demonstra uma preferência pelo regime subjetivo ao se excluir a menção expressa à responsabilidade civil (GUEDES; VENCELAU MEIRELES, 2019). Ademais, o inciso II, do art. 43, remete à ideia de culpa como fundamento da responsabilidade civil, ao contrário dos incisos I e III, que afastam o nexo de causalidade e reconhecem a culpa exclusiva do titular de dados, respectivamente.

A regra do inciso II exclui a responsabilidade do agente de tratamento ainda que haja nexo de causalidade entre a conduta e o dano,

> se ele conseguir provar que cumpriu todos os deveres impostos pela LGPD, tomando as medidas de segurança recomendadas (cumprindo programas, políticas internas, procedimentos, mecanismos de supervisão, internos e externos, padrões técnicos etc), não será responsabilizado. (GUEDES; VENCELAU MEIRELES, 2019, p. 235).

Assim, observando-se que o agente cumpriu aquilo que era esperado e mesmo assim ocorreu o evento danoso, "não foi em razão de sua conduta culposa" (GUEDES; VENCELAU MEIRELES, 2019, p. 237). Por fim, importante frisar que as autoras admitem a aplicação da responsabilidade civil objetiva em relação aos incidentes que envolvem dados sensíveis, tendo

por base a atividade dos agentes, e com fundamento na cláusula geral de responsabilidade civil objetiva do Código Civil, segundo a qual

> Art. 927. [...] 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.**

Do mesmo modo, Diogo Ramos Ferreira entende que o regime adotado pela LGPD foi o da responsabilidade subjetiva, admitindo-se a aplicação da responsabilidade objetiva "quando a atividade de tratamento, em razão de sua natureza ou elementos, apresentar graves riscos aos titulares", em razão da teoria do risco criado (FERREIRA, 2019). Ademais, segundo destaca Fernando Tasso, o sistema adotado pela LGPD está em consonância com o Código Civil, segundo o qual, no âmbito das relações privadas, aplica-se a responsabilidade civil subjetiva, excepcionando-se em hipóteses específicas e no caso de exercício de atividade de risco, na forma do parágrafo único do art. 927 (TASSO, 2020).

Verifica-se, portanto, que parte da literatura jurídica entende ter a LGPD adotado o regime de responsabilidade civil subjetivo, ante a previsão de deveres específicos que devem ser seguidos pelos agentes de tratamento, configurando verdadeiro standard de conduta esperado. A violação a esse padrão de comportamento demandaria a prova de culpa do agente para eventual responsabilização.

Como se observa, o argumento de maior relevo para a adoção do regime subjetivo é o fato da lei estabelecer deveres aos agentes de tratamento. Contudo, em que pese o entendimento dos autores e autoras citados, entende-se que o simples estabelecimento de deveres aos agentes de tratamento não é elemento apto a definir como subjetivo o regime de responsabilização previsto na LGPD.

Isso porque, a teoria subjetiva, calcada na ideia moderna de culpa normativa, não é a única a estabelecer um padrão de comportamento a ser seguido. Na seara da responsabilização ambiental, aplica-se a teoria do risco integral, segundo a qual o causador do dano responde objetivamente ainda que tenha cumprido todos os deveres impostos para o desempenho normal de sua atividade. Percebe-se que, ocorrendo o dano, o causador não poderá alegar que o fato de ter cumprido com as exigências legais e regulamentares o isentará de responsabilidade.

A esse respeito, Nelson Nery Júnior dispõe que

> ainda que a indústria tenha tomado todas as precauções para evitar acidentes danosos ao meio ambiente, se, por exemplo, explode um reator controlador da emissão de agentes químicos poluidores (caso fortuito), subsiste o dever de indenizar. Do mesmo modo, se por um fato da natureza ocorrer derramamento de substância tóxica existente no depósito de uma indústria (força maior), pelo simples fato de existir a atividade há o dever de indenizar (NERY JÚNIO, 1984, p. 172).

O estabelecimento de deveres por normas regulatórias é usual em diversos setores econômicos, nos quais a responsabilidade ainda assim é objetiva ante os danos causados aos usuários dos serviços (eg. fornecimento de energia elétrica, abastecimento de água e esgotamento sanitário, telefonia etc.).

Por fim, estando a atividade de tratamento de dados ligada diretamente a valores constitucionais tão caros aos cidadãos como a autodeterminação informativa, a inviolabilidade da intimidade e o respeito à privacidade, o estabelecimento de deveres ou *standards* de comportamento que visem a proteção desses direitos é uma medida importante para salvaguarda-los de quaisquer danos. Ocorrendo o dano, a demonstração de observância de tais deveres não pode ensejar a exoneração da responsabilidade do causador, pois os princípios de segurança, prevenção e mitigação do risco foram instituídos como contraposto ao risco intrínseco da atividade de tratamento de dados. Não possuem, portanto, efeito liberatório de responsabilização civil, funcionando como elementos balizadores da atividade, de observância obrigatória, podendo atenuar, quando efetivamente observados pelo agente de tratamento causador do dano, eventual multa administrativa que possa ser aplicada por parte da Autoridade Nacional de Proteção de Dados Pessoais (ANPD)[32].

3.3 Elementos Caracterizadores da Responsabilidade Civil Objetiva dos Agentes de Tratamento

Como visto, o regime de responsabilidade civil objetivo se caracteriza pela ausência de investigação de culpa e pelo desempenho de uma atividade caracterizada como de "risco". Cumpre saber, portanto, se a atividade de tratamento de dados pessoais poderia ser identificada como uma atividade de risco.

[32] Nesse sentido, observe-se o art. 52, §1º: § 1º **As sanções serão aplicadas após procedimento administrativo** que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto **e considerados os seguintes parâmetros e critérios**: [...] VIII – a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei.

Nesse sentido, a LGPD "tem como um de seus fundamentos principais a diminuição do risco, levando-se em conta que o tratamento de dados apresenta risco intrínseco aos seus titulares" (MENDES; DONEDA, 2018, p. 469). Ainda, as semelhanças com o Código de Defesa do Consumidor (CDC) poderiam levar a crer que se adotou, à semelhança do código consumerista, o regime de responsabilidade objetivo.

Isso porque, algumas disposições da LGPD seriam semelhantes às disposições do CDC, como o disposto no art. 42, §2º[33], da LGPD e art. 6º, inciso VIII, do CDC, que tratam da inversão do ônus da prova, o art. 43[34] se assemelha ao §3º, do art. 12[35], do CDC, excetuando-se o inciso II, do art. 43 que, como visto anteriormente, remete à ideia de não ocorrência de ato ilícito, cerne do regime subjetivo.

Importante destacar que o tratamento de dados realizado em um contexto de uma relação de consumo atrairá a responsabilidade objetiva, por força da regra do art. 14 do CDC, segundo a qual

> Ar. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.

Nesse sentido, o Superior Tribunal de Justiça, quando do julgamento do Tema 710 (Recurso Especial 1419697/RS), por meio de Recurso Representativo de Controvérsia, em controvérsia envolvendo o sistema de "credit scoring", consignou que

> RECURSO ESPECIAL REPRESENTATIVO DE CONTROVÉRSIA (ART. 543-C DO CPC). TEMA 710/STJ. DIREITO DO CONSUMIDOR. ARQUIVOS DE CRÉDITO. SISTEMA "CREDIT SCORING". COMPATIBILIDADE COM O DIREITO BRASILEIRO. LIMITES. DANO MORAL. I - TESES: 1) O sistema "credit scoring" é um método desenvolvido para avaliação do risco de concessão de crédito, a partir de modelos estatísticos, considerando diversas variáveis, com atribuição de uma

[33] 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. [...] § 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 (BRASIL, 2020d).

[34] 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, 2020d).

[35] Art. 12. O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos. [...] § 3° O fabricante, o construtor, o produtor ou importador só não será responsabilizado quando provar: I - que não colocou o produto no mercado; II - que, embora haja colocado o produto no mercado, o defeito inexiste; III - a culpa exclusiva do consumidor ou de terceiro (BRASIL, 2020d).

> pontuação ao consumidor avaliado (nota do risco de crédito). 2) Essa prática comercial é lícita, estando autorizada pelo art. 5º, IV, e pelo art. 7º, I, da Lei n. 12.414/2011 (lei do cadastro positivo). 3) Na avaliação do risco de crédito, devem ser respeitados os limites estabelecidos pelo sistema de proteção do consumidor no sentido da tutela da privacidade e da máxima transparência nas relações negociais, conforme previsão do CDC e da Lei n. 12.414/2011. 4) Apesar de desnecessário o consentimento do consumidor consultado, devem ser a ele fornecidos esclarecimentos, caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem como as informações pessoais valoradas. **5) O desrespeito aos limites legais na utilização do sistema "credit scoring", configurando abuso no exercício desse direito (art. 187 do CC), pode ensejar a responsabilidade objetiva e solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente (art. 16 da Lei n. 12.414/2011) pela ocorrência de danos morais nas hipóteses de utilização de informações excessivas ou sensíveis (art. 3º, § 3º, I e II, da Lei n. 12.414/2011), bem como nos casos de comprovada recusa indevida de crédito pelo uso de dados incorretos ou desatualizados.** [...] (REsp 1419697/RS, Rel. Ministro PAULO DE TARSO SANSEVERINO, SEGUNDA SEÇÃO, julgado em 12/11/2014, DJe 17/11/2014) (BRASIL. Superior Tribunal de Justiça. Recurso Especial 1419697/RS).

No que diz respeito à atividade de tratamento de dados como uma atividade de risco, Laura Schertel e Danilo Doneda apontam que a LGPD procurou restringir as hipóteses de tratamento de dados, com atendimento à finalidade, adequação e necessidade do tratamento, além de indicar a necessidade de se levar em consideração o risco presente no tratamento de dados, buscando "minimizar as hipóteses de tratamento àquelas que sejam, em um sentido geral, úteis e necessárias, e que mesmo estas possam ser limitadas quando da verificação de risco aos direitos e liberdades do titular de dados" (MENDES; DONEDA, 2018, p. 477). O mesmo raciocínio, embora não tenha citado a LGPD expressamente, foi adotado pela Ministra Rosa Weber no julgamento da Medida Cautelar em Ação Direta de Inconstitucionalidade (ADI) 6387, proposta pelo Conselho Federal da Ordem dos Advogados do Brasil – CFOAB contra o inteiro teor da Medida Provisória n. 954, de 17 de abril de 2020.

Naquela oportunidade, a ministra apontou importantes princípios relacionados à minimização de riscos no tratamento de dados, como adequação e necessidade. Nesse sentido,

> [...] não emerge da Medida Provisória n. 954/2020, nos moldes em que posta, **interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia, considerados a necessidade, a adequação e a proporcionalidade da medida**. E tal dever competia ao Poder Executivo ao editá-la. Nessa linha, **ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP n. 954/2020 não oferece condições para avaliação da sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas**

> **finalidades**. Desatende, assim, a garantia do devido processo legal (art. 5º, LIV, da Lei Maior), em sua dimensão substantiva. (Grifos meus) (BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade 6387).

Desse modo, "justifica-se o legislador optar por um regime de responsabilidade objetiva no art. 42, vinculando a obrigação de reparação do dano ao exercício de atividade de tratamento de dados pessoais" (MENDES; DONEDA, 2018, p. 477). No mesmo sentido, Caitlin Mulholland argumenta pela adoção do regime objetivo, pois tanto na hipótese do art. 42 quanto do art. 44, parágrafo único,

> o legislador quis identificar nessa hipótese situações danosas que decorrem especificamente de incidentes de segurança que são, por sua vez, acontecimentos que se relacionam ao **risco inerente ao desenvolvimento da atividade de tratamento de dados**, como vazamentos não intencionais e invasão de sistemas e bases de dados por terceiros não autorizados. Neste sentido, esses riscos devem ser necessariamente situados como intrínsecos à atividade de tratamento de dados e, portanto, considerados, em última análise, como hipótese de fortuito interno, incapazes de afastar a obrigação dos agentes de tratamento de indenizar os danos causados pelos incidentes. (MULHOLLAND, 2020, grifos meus).

Em relação à análise de risco prevista na LGPD, é importante destacar o posicionamento de Maria Cecília Oliveira Gomes, segundo o qual tal análise não deve se prender a um simples *"check list de compliance"*, ou seja, cumprir o maior número de obrigações impostas pela lei para demonstrar conformidade. Segundo a autora, uma vez que o risco é inerente ao tratamento de dados, deve-se identificá-lo, compreendê-lo e avaliar seu impacto para assim mitigá-lo, de modo a preservar e proteger os direitos dos titulares de dados, o que nem sempre é feito em algumas metodologias baseada em risco, que servem para demonstrar conformidade ao regulamento de dados, "mas não para avaliar possíveis violações aos direitos dos titulares de dados" (GOMES, 2020, p. 263-264).

Ainda segundo a autora, a análise de risco deverá ter como norte as liberdades civis e direitos fundamentais dos titulares de dados e deverá ser baseada em metodologias de avaliação de risco, "fundamentadas em indicadores e métodos de análise que levem em consideração as características do risco" (GOMES, 2020, p. 265). Assim, destaca a autora

> [...] considerando essas questões, o importante em uma avaliação de risco é estabelecer método (escolha de metodologia, justificativa para essa escolha, desenvolvimento de matriz de risco com indicadores e elaboração de procedimento interno de avaliação de impacto para verificar a necessidade do relatório). Para isso, é necessário estabelecer indicadores mínimos de análise. Volume de dados, espécie dos dados (pessoal e/ou sensível) e tipo de titulares de dados, são, por exemplo, indicadores na avaliação do risco em operações de tratamento. Se uma operação de tratamento possui um grande volume de dados, provenientes de crianças e que são sensíveis (dados de saúde, p. ex.), é

> possível qualificar essa operação de tratamento de dados como de alto risco. E, a partir disso, analisar qual é o impacto delas nas liberdades civis e nos direitos fundamentais desses titulares. (GOMES, 2020, p. 265).

Em sede de conclusão, é importante destacar que a estrutura da lei é voltada para uma análise preventiva de riscos, buscando a mitigação de danos, explicitando a natureza intrínseca do risco na atividade de tratamento de dados. E isso se evidencia na análise dos princípios e fundamentos que demandam dos agentes de tratamento uma atuação preventiva para o cumprimento das normas de proteção de dados pessoais.

Nesse sentido, Maria Celina Bodin de Moraes acredita que a LGPD adotou um regime de responsabilização civil dito "proativo". Trata-se de um regime especial, que reflete a determinação do disposto no inciso X, art. 6º da lei[36], de modo que é exigido do agente de tratamento não apenas o ressarcimento dos danos causados mas, principalmente, que evitem a ocorrência desses danos.

Desse modo, destaca a autora, "não descumprir a lei não é suficiente; é preciso 'proativamente' prevenir a ocorrência de danos" (BODIN DE MORAES, 2019, p. 5). Tal posicionamento parece se adequar ao pretendido pelo legislador, que destacou nos princípios da lei a prevenção de danos como valor máximo a ser perseguido pelos agentes de tratamento, de modo que o regime de responsabilidade a ser adotado deve refletir esse posicionamento. E isso pode ser observado no capítulo referente aos direitos dos titulares de dados (e bem antes, como demonstrado no capítulo próprio) e nas regras concernentes ao tratamento de dados pessoais.

No que diz respeito à adoção de medidas proativas, pode-se afirmar que a LGPD, embora não o tenha feito de maneira explícita, adotou os princípios da Privacidade por Concepção (*Privacy by desing*) e da Privacidade por Padrão (*Privacy by default*). Tais princípios foram expressamente incorporados pela legislação europeia (*Genaral Data Protection Regulation – GDPR*), no art. 25, no capítulo referente a "*Data protection by design and by default*".

Ambos os princípios se relacionam com a ideia de coleta mínima de dados para a realização das finalidades informadas ao titular de dados. Na LGPD, esse é o conteúdo do princípio da necessidade, segundo o qual, o tratamento de dados deve ser limitado "ao mínimo

[36] Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. (BRASIL, 2020d).

necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados" (art. 6º, III).

A privacidade por concepção promove a ideia de que a privacidade dos indivíduos não pode ser objeto de preocupação apenas para fins de compliance com as exigências regulatórias, devendo, antes de tudo, ser objeto de preocupação de toda a estrutura organizacional, como um padrão de comportamento na elaboração de produtos e serviços (CAVOUKIAN, 2011). A privacidade e a segurança dos dados, portanto, devem estar presentes desde a fase de concepção do produto, como estabelece o §2º, do art. 46, ao tratar da segurança e do sigilo de dados[37].

O princípio da privacidade por concepção se aproxima do princípio da prevenção, pois ambos buscam a evitar a ocorrência de danos à privacidade, sendo a prevenção um dos princípios fundacionais da privacidade por concepção[38]. Nesse sentido, Ann Cavoukian, ex Comissária de Informação e Privacidade da província de Ontário, Canadá, estabelece em importante artigo que a privacidade por concepção é baseada no estabelecimento de medidas proativas ao invés de medidas reativas, prevenindo eventos de invasão à privacidade antes que aconteçam[39].

Além disso, o crescente número de violações à segurança de dados pessoais aumenta a necessidade da promoção e respeito a este tão relevante princípio, de modo que

> violações de segurança podem ser um problema estrutural para uma sociedade da informação que depende cada vez mais do bom desempenho tecnologias

[37] Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. [...] § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. Além disso, outros artigos também sustentam a ideia de privacidade por concepção, como por exemplo: **Art. 6°, VIII – prevenção**: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais**; Art. 49.** Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares. **Art. 50.** Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais**. § 2º** Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá: [...].

[38] 1. Proactive not Reactive; Preventative not Remedial. The Privacy by Design (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after. CAVOUKIAN, Ann. **Privacy by design: The 7 Fundational Principles**. Disponível em: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf. Acesso em: 15 de nov. de 2020.

[39] CAVOUKIAN, Ann. Op. Cit.

> de informação e comunicação. Portanto, isso também deve ser visto como uma oportunidade para a "Privacy by design" (HUSTINX, 2010, p. 254)[40].

A privacidade por padrão ou *Privacy by Default* estabelece a ideia de que nenhuma ação precise ser tomada por parte do titular de dados para proteger sua privacidade, pois a proteção de dados pessoais deve ser uma "configuração padrão" para o fornecimento de produtos e serviços que utilizam dados pessoais. Sobre o tema, a GDPR estabeleceu, no §2º, do art. 25, que

> O responsável pelo tratamento deve implementar medidas técnicas e organizacionais adequadas para garantir que, por padrão, apenas sejam tratados os dados pessoais necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao período de armazenamento e à acessibilidade. Em particular, tais medidas devem assegurar que, por padrão, os dados pessoais não sejam disponibilizados sem a intervenção do indivíduo a um número indefinido de pessoas naturais[41].

Desse modo, a GDPR estabelece que os responsáveis pelo tratamento de dados devem definir uma configuração padrão que respeite os princípios da proteção de dados, em especial a minimização de processos intrusivos, tais como a minimização de quantidade de dados pessoais, minimização da extensão do processamento, minimização do tempo de armazenamento dos dados e mínimo acesso aos dados pessoais (AEPD, 2020).

Importante destacar que os princípios de mitigação de risco e adoção de mecanismos preventivos para evitar danos aos titulares de dados, previstos na LGPD, já vêm sendo acatados para o convencimento judicial. Nesse sentido, veja-se o decidido pela 1ª Vara da Fazenda Pública de São Paulo, ao deferir em parte pedido de produção antecipada de provas para que a Companhia do Metropolitano de São Paulo - Metrô de São Paulo, preste informações a respeito da implementação de um sistema de reconhecimento facial, objeto de processo de licitação, nos autos do processo nº 1006616-14.2020.8.26.0053. A ação foi ajuizada para justificar a instruir eventual demanda a ser ajuizada.

O pedido fora ajuizado pela Defensoria Pública de São Paulo (DPSP), pela Defensoria Pública da União (DPU), pelo Instituto Brasileiro de Defesa do Consumidor (IDEC) e Artigo

[40] No original: "In fact, security breaches may well be a structural problem for an information society that is increasingly dependent on the good performance of ICT. This should therefore also be seen as an opportunity for "Privacy by Design".

[41] No original: "The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.".

19 Brasil, questionando a implementação da tecnologia, amparado no Código de Defesa do Consumidor (CDC) e na Lei Geral de Proteção de Dados Pessoais (LGPD), antes mesmo da entrada em vigor da lei. Os autores apontaram o potencial violador de direitos constitucionais pelo sistema de reconhecimento facial, como direito à privacidade e à autodeterminação informativa. O Metrô-SP não teria revelado a finalidade do tratamento, a forma de obtenção de consentimento, especialmente no caso de pais e responsáveis pelos dados pessoais de crianças e adolescentes, além de não informar as ações de mitigação do risco envolvido ou a proposta de compartilhamento da base de dados com outras entidades, públicas ou privadas.

Chama atenção a menção ao risco que é feita para o deferimento do pedido de produção antecipada de prova. Assim, a magistrada determina que o Metrô-SP apresente

> Prova documental sobre análise de impacto de proteção de dados, contendo quais dados serão coletados e tratados, a base legal para essa coleta (art. 7º, LGPD), a finalidade desse tratamento, análise à luz do princípio da minimização e da proporcionalidade, se há dentre os dados que serão coletados algum que seja definido como sensível pela LGPD, o período de retenção dos dados, o grau de risco e **finalmente as ações para a mitigação do risco envolvido**. Na Sua ausência, prova documental com **i) descrição do processo de tratamento de dados pessoais que podem gerar riscos aos titulares e que possam impor restrições não previstas em lei aos usuários de serviços públicos, conforme previsto na LGPD e decorrente do sistema normativo protetor dos consumidores e dos usuários de serviços públicos (art. 6º, I e III, do CDC; Art. 5º, inc. IV, CDURP;art. 7º, V, da Lei Estadual 10.294/1999; ii) medidas e mecanismos voltados a mitigar os riscos identificados (**BRASIL. Tribunal de Justiça do Estado de São Paulo. Processo nº 1006616-14.2020.8.26.0053).

O único pedido não acatado foi o relativo à provisão orçamentária da ré para arcar com eventuais danos decorrentes de falhas e vazamentos na atividade de monitoração, pois os requerentes não cumpriram os requisitos da legislação processual[42] quanto a esse ponto. Desse modo, tem-se que o legislador buscou proteger os direitos dos titulares de dados de maneira ativa, ora apontando para a atuação preventiva dos agentes de tratamento, ora apontando para o risco envolvido no tratamento de dados pessoais, mas sempre primando pela efetiva proteção dos direitos dos titulares de dados.

Em sede de conclusão, foi visto que o legislador optou por um sistema de proteção que privilegia a prevenção e reparação de danos, por meio da adoção de mecanismos capazes de mitigar os prejuízos causados aos usuários dos serviços. O princípio da prevenção adotado pelo legislador acompanha a importância atribuída a esse princípio na responsabilidade civil. A

[42] Art. 382. Na petição, o requerente apresentará as razões que justificam a necessidade de antecipação da prova e mencionará com precisão os fatos sobre os quais a prova há de recair. (BRASIL. Código de Processo Civil).

crescente expansão dos danos trouxe para a responsabilidade civil não só o dilema de como melhor reparar os danos, mas também se a reparação era o melhor caminho (SCHREIBER, 2015).

Os riscos associados ao exercício de certas atividades demandam a adoção de outros mecanismos, além da responsabilidade civil, para evitar a ocorrência de danos. Nesse sentido, o princípio da prevenção traduz a ideia de adoção de medidas aptas a evitar ou reduzir os prejuízos causados por atividades tidas por perigosas e produtoras de risco.

No tratamento de dados, os riscos, conforme vistos, são intrínsecos a essa atividade, de modo que o reforço do legislador ao princípio da prevenção é compreensível. O que se busca com o protagonismo desse princípio na LGPD é a máxima proteção dos direitos dos titulares de dados, do mesmo modo que na responsabilidade civil atual o que se busca é a máxima reparação do dano e a proteção da vítima.

Assim, os conceitos de risco e prevenção devem ser levados em consideração na atividade de tratamento de dados, de modo que a adoção do regime de responsabilidade civil objetivo parece ser o meio mais adequado para se garantir a proteção dos direitos dos titulares de dados pessoais.

4 CONSIDERAÇÕES FINAIS

O presente trabalho dispôs-se a analisar como problema principal a identificação do regime de responsabilização civil dos agentes de tratamento de dados na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, 14 de agosto de 2018). Embora seja um importante marco regulatório que sistematiza o tratamento de dados pessoais no Brasil, a lei foi omissa quanto ao regime de responsabilização civil dos agentes de tratamento de dados pessoais, se subjetivo, calcado na culpa, ou objetivo, calcado no risco da atividade.

Os dados pessoais são os insumos da economia moderna, cuja relevância, porém, pode ser verificada para além dos cenários econômicos. Exercem influência sobre as liberdades civis e direitos fundamentais, razão pela qual a LGPD determina aos agentes de tratamento a elaboração de relatório de impacto à proteção de dados quando o tratamento realizado puder gerar riscos a tais liberdades e direitos. Em suma, os dados pessoais possuem uma importância transversal e impactam indivíduos e sociedade de maneiras diversas, do ponto de vista econômico e social.

Inicialmente, adotou-se como hipótese de pesquisa as seguintes afirmações: a) a LGPD adotou a prevenção de danos como valor máximo a ser perseguido pelos agentes de tratamento, de modo que o regime de responsabilidade a ser adotado deve refletir esse posicionamento; e b) o risco criado pelos agentes de tratamento enseja a objetivação da responsabilidade civil e é o regime mais adequado para se garantir a proteção dos direitos dos titulares de dados pessoais.

Após a realização das pesquisas, encontrou-se elementos que puderam confirmar as hipóteses inicialmente levantadas. Primeiramente, destaca-se que a LGPD se insere em um sistema de proteção de dados pessoais, para aperfeiçoar o arcabouço normativo e permitir maior robustez aos direitos dos titulares de dados. Isso já pode ser observado desde o art. 1º da lei, ao dispor como objetivo "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural".

A concepção de privacidade adotada pelo legislador aponta para uma noção segundo a qual o desenvolvimento da personalidade é a essência desse conceito. Nesse sentido, a proteção de dados deixa de ser apenas uma forma de tutela de dados pessoais para se tornar uma forma de anteparo à autodeterminação do indivíduo.

Durante o estudo aqui desenvolvido, verificou-se que a LGPD, com vistas a maior proteção dessa concepção de privacidade, adotou mecanismos de proteção dos titulares de dados que se compatibilizam com a preocupação segundo a qual o tratamento de dados pode representar riscos à individualidade, autonomia e liberdade. A exposição a respeito dos direitos dos titulares (tópico 2.4) ressalta que o tratamento de dados deve levar em consideração os fundamentos da proteção de dados, estabelecidos no art. 2º, que representam verdadeiro *ethos* da lei.

No que diz respeito às regras relativas ao tratamento de dados (tópico 2.5), evidencia-se uma preocupação com a prevenção de danos, especialmente ao se analisar os princípios de "segurança", "prevenção" e a "responsabilização e prestação de contas". A lei previu mecanismos de mitigação do risco de dano a serem adotados pelos agentes de tratamento, a fim de garantir o cumprimento das normas de proteção de dados pessoais e salvaguardar os direitos dos titulares de dados.

Assim, percebe-se que as palavras "risco" e "prevenção" se repetem ao longo da legislação, na medida em que se fala sobre o estabelecimento de padrões de conduta a serem observados pelos agentes de tratamento com vistas a não ocorrência de danos. Nesse ponto, o regime de responsabilidade civil adotado pela lei parece se clarificar e ganhar maior visualização.

No que diz respeito ao regime subjetivo, demonstrou-se que a concepção atual de culpa desconsidera a vontade do agente para o descumprimento da norma, levando-se em conta apenas o padrão de conduta esperado na situação concreta. E esse padrão de conduta é exposto ao longo da lei, baseando-se na criação de deveres aos agentes de tratamento, prezando pela conduta preventiva e visando sempre a não ocorrência de danos ou a mitigação do risco de dano, o que aponta para a hipótese (a), acima apresentada.

Para o regime de responsabilidade civil objetivo, o risco da atividade é um dos fatores que fazem incidir a sistemática objetiva. Conforme se analisou, na LGPD, o risco é inerente ao desenvolvimento da atividade de tratamento de dados, devendo-se analisá-lo para avaliar seu impacto e preservar e proteger os direitos dos titulares de dados pessoais. A adoção de um regime objetivo, conforme verificado, parece ser o caminho mais adequado, na medida em que a LGPD disciplinou de maneira bastante vigorosa a adoção de um comportamento proativo dos agentes de tratamento.

Assim, considerando todo o exposto, a pesquisa demonstrou que a estrutura da lei é voltada para uma análise preventiva, buscando a minimização da ocorrência de riscos e a mitigação de danos, explicitando a natureza intrínseca do risco na atividade de tratamento de dados, o que aponta para a hipótese (b), acima apresentada. Ademais, decisões judiciais já levam em consideração a LGPD, antes mesmo de sua vigência, apontando importantes princípios relacionados à minimização de riscos no tratamento de dados, como adequação e necessidade, conforme demonstrado no julgamento da ADI 6387, o que se permite concluir que o regime mais adequado para a proteção dos direitos dos titulares de dados é o regime da responsabilidade civil objetiva.

REFERÊNCIAS BIBLIOGRÁFICAS

ACCESS NOW. Recommendations on Privacy and Data Protection in the Fight against COVID-19. Disponível em: https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf. 2020. Acesso em: 16 jun. 2020.

ALMEIDA, Ursula Ribeiro de. Tutela de Urgência e Princípio da Precaução. *In:* **Tutela de Urgência no Direito Ambiental**: Instrumento de Efetivação do Princípio da Precaução. Coord. Carlos Alberto Carmona. São Paulo: Atlas, 2015. p. 168-198. (Coleção Atlas de Processo Civil).

BELLIZZE OLIVEIRA, Marco Aurélio; PEREIRA LOPES, Isabela Maria. Os princípios norteadores da proteção de dados pessoais no Brasil. *In:* FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena DONATO. **Lei Geral de Proteção de Dados Pessoais e Suas Repercussões no Direito Brasileiro**. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 53-83.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BIONI, Bruno Ricardo. **Xeque-Mate, o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. São Paulo: GPoPAI/USP, 2015.

BODIN DE MORAES, Maria Celina de. Risco, solidariedade e responsabilidade objetiva. **Revista dos Tribunais**, São Paulo, v. 854, p. 11-37, dez. 2006.

BODIN DE MORAES, Maria Celine. LGPD: um novo regime de responsabilização dito "proativo", **Civilistica.com**, Rio de Janeiro, ano 8, n. 3, 2019. Disponível em: http://civilistica.com/lgpd-um-novo-regime/. Acesso em: 4 out. 2020.

BRAGA NETTO, Felipe Peixoto; FARIAS, Cristiano Chaves de; ROSENVALD, Nelson. **Novo tratado de responsabilidade civil**. 4. ed. São Paulo: Saraiva Educação, 2019. v. 1.

BRASIL. **Código de Processo Civil**. Lei nº 13.105, de 16 de março de 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 09 out. 2020.

BRASIL. **Guia de Boas Práticas** – Lei Geral de Proteção de Dados. 2020a. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd. Acesso em: 4 out. 2020.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, 2020b. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 22 fev. 2020.

BRASIL. **Marco Civil Da Internet**. Lei nº 12.965, de 23 de abril de 2014. Brasília, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 fev. 2020.

BRASIL. **Lei nº 14.058, de 17 de setembro de 2020**. Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Lei nº 14.020, de 06 de julho de 2020. Brasília, 2020c. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Lei/L14058.htm. Acesso em: 4 out. 2020.

BRASIL. **Lei Geral de Proteção de Dados (LGPD)**. Lei nº 13.709, de 14 de agosto de 2018. Brasília, 2020d. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 4 out. 2020.

BRASIL. **Superior Tribunal de Justiça. Recurso Especial 1419697/RS**. Brasília, DF. Superior Tribunal de Justiça, [2014]. Disponível em: https://scon.stj.jus.br/SCON/jurisprudencia/toc.jsp?i=1&b=ACOR&livre=(%27RESP%27.clas.+e+@num=%271419697%27)&thesaurus=JURIDICO&fr=veja. Acesso em: 09 out. 2020.

BRASIL. **Superior Tribunal de Justiça. Recurso Especial 1450434 [2018].** Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201400583712&dt_publicacao=09/11/2018. Acesso em: 11 nov. 2020.

BRASIL. **Supremo Tribunal Federal**. Ação Direta de Inconstitucionalidade 6387. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165. Acesso em: 09. Out. 2020.

BRASIL. **Tribunal de Justiça do Estado de São Paulo**. Processo nº 1006616-14.2020.8.26.0053. Disponível em: https://www.jota.info/wp-content/uploads/2020/02/doc-76725029.pdf. Acesso em: 09 out. 2020).

CÂMARA, Alexandre Freitas. Doenças Preexistentes e ônus da Prova: o Problema da Prova Diabólica e uma Possível Solução. **Revista Dialética de Direito Processual**, São Paulo, n. 31, v. 222. p. 9-18, 2005.

CAVALIERI FILHO, Sério. Programa de Responsabilidade Civil. 13ª ed. São Paulo: Atlas. 2019.

CAVOUKIAN, Ann. **Privacy by design: The 7 Fundational Principles**. Disponível em: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf. Acesso em: 15 nov. 2020.

CHEN, Adrian. *Cambridge Analytica and our lives inside the surveillance machine*. Disponível em: http://personal-computing.coryarcangel.com/Cambridge-Analytic.pdf. Acesso em: 10 nov. 2020.

CIVILISTICA.COM: Revista eletrônica de Direito Civil. Disponível em: http://civilistica.com/. Acesso em: 4 out. 2020.

CONFESSORE, Nicholas. **Cambridge Analytica and Facebook**: The Scandal and the Fallout So Far. Revelations that digital consultants to the Trump campaign misused the data of millions of Facebook users set off a furor on both sides of the Atlantic. This is how The Times covered it. Nova York, 2018. Disponível em: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html. Acesso em: 4 out. 2020.

CUEVA, Ricardo Villas Bôas. A insuficiente proteção de dados pessoais no Brasil. **Revista de Direito Civil Contemporâneo**, São Paulo, v. 13, ano 4, p. 59-67, out.-dez. 2017.

DAVID, Cleber Cilli. Lei Geral de Proteção de Dados. **Revista Fórum de Direito na Economia Digital** – RFDED, Belo Horizonte, ano 3, n. 5, p. 61-85, jul./dez. 2019.

DE PAGE, Henri. *Traité* élémentaire *de droit civil belge*. Bruxelles: E. Bruylant, 1974. v. 2. De Page. *Traité élémentaire de droit civil belge*. Cit. n. 932. (1974 *apud* DA SILVA PEREIRA, 2018, p. 103).

DIAS, José de Aguiar. Da Responsabilidade Civil. 12ª ed. Rio de Janeiro: Editora Lumen Juris, 2012.

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

ESPANHA. Agencia Española Protección Datos. Guidelines for Data Protection by Defaut.

FARIAS, Cristiano Chaves de; ROSELVALD, Nelson; BRAGA NETO, Felipe. **Manual de Direito Civil**. 1. ed. Salvador: Juspodivm, 2017.

FERREIRA, Diogo Ramos. **Responsabilidade civil dos agentes de tratamento de dados**: subjetiva ou objetiva? 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/responsabilidade-civil-dos-agentes-de-tratamento-de-dados-subjetiva-ou-objetiva-20112019. Acesso em: 4 out. 2020.

FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais – Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados Pessoais. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e Suas Repercussões no Direito Brasileiro.** 1. ed. São Paulo: Thomson Reuters Brasil, 2019a. p. 23-49.

FRAZÃO, Ana. **Nova LGPD**: os direitos dos titulares de dados pessoais. Parte VIII. 2018a. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-os-direitos-dos-titulares-de-dados-pessoais-17102018. Acesso em: 4 out. 2020.

FRAZÃO, ANA. **Nova LGPD**: os direitos dos titulares de dados pessoais. Parte IX. 2018b. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-direitos-dos-titulares-de-dados-pessoais-24102018. Acesso em: 4 out. 2020.

FRAZÃO, Ana. **Responsabilidade Civil na Lei Geral de Proteção de Dados Pessoais**. Palestra proferida no Escola Judicial Desembargador Edésio Fernandes, Tribunal de Justiça de Minas Gerais, set. 2019b. 32 min. Disponível em: https://www.youtube.com/watch?v=1VYnDXn81Rc. Acesso em: 23 fev. 2020.

FRAZÃO, Ana. **Objetivos e alcance da Lei Geral de Proteção de Dados**. *In:* FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena DONATO (coord.). **Lei Geral de Proteção de Dados Pessoais e Suas Repercussões no Direito Brasileiro**. 1. ed. São Paulo, Thomson Reuters Brasil, 2019c. p. 99-119.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena DONATO (coord.). **Lei Geral de Proteção de Dados Pessoais e Suas Repercussões no Direito Brasileiro**. 1. ed. São Paulo: Thomson Reuters Brasil, 2019.

GARCIA, Lara Rocha *et al.* **Lei Geral de Proteção de Dados Pessoais (LGPD)** – Guia de Implementação. São Paulo: Blucher, 2020.

GOMES, Maria Cecília Oliveira. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. *In*: PALHARES, Felipe (coord.). **Temas Atuais de Proteção de Dados**. São Paulo: Thomsom Reuters Brasil, 2020. p. 245-273.

GONZÁLEZ, Mariana. **Conheça o cenário das leis de proteção de dados ao redor do mundo**. IdBlog., 14 fev. de 2020. Disponível em <https://blog.idwall.co/protecao-de-dados-cenario-mundial-das-leis/#:~:text=Na%20Col%C3%B4mbia%2C%20a%20quest%C3%A3o%20da,de%20processamento%20de%20dados%20pessoais.>. Acesso em 10 nov. 2020.

GUEDES, Gisela Sampaio da Cruz; TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde. **Fundamentos do Direito Civil**. Rio de Janeiro: Forense, 2020. v. 4 – Responsabilidade Civil.

GUEDES, Gisela Sampaio da Cruz; VENCELAU MEIRELES, Rose Melo. Término do Tratamento de Dados. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena DONATO. **Lei Geral de Proteção de Dados Pessoais e Suas Repercussões no Direito Brasileiro**. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 219-241.

HANNA, Mina J.; ISAAK, Jim. *User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection*. Disponível em: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8436400. Acesso em: 10 nov. 2020.

HUSTINX, Peter. Privacy by design: delivering the promises. Disponível em: https://link.springer.com/article/10.1007/s12394-010-0061-z#citeas. Acesso em: 15. nov. 2020.

KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da lei 13.709/2018. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena DONATO. **Lei Geral de Proteção**

de Dados Pessoais e Suas Repercussões no Direito Brasileiro. 1. ed. São Paulo, Thomson Reuters Brasil, 2019. p. 445-460.

KOZLOWSKA, Iga. Facebook and Data Privacy in the Age of Cambridge Analytica. Disponível em: https://jsis.washington.edu/news/facebook-data-privacy-age-cambridge-analytica/. Acesso em: 10 nov. 2020;

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, São Paulo, v. 120, ano 27, p. 469-483, nov.-dez. 2018.

MIRAGEM, BRUNO. O contrato de seguro e a lei geral de proteção de dados. **Revista dos Tribunais**, v. 1.018, ago, pgs. 1-35, 2020. Disponível em: http://www.brunomiragem.com.br/wp-content/uploads/2020/06/005-contrato-de-seguro-e-a-LGPD.pdf. Acesso em: 4 out. 2020.

MONOKHA, Ivan. Surveillance: *The DNA of Platform Capital – The Case of Cambridge Analytica Put into Perspective*. Disponível em: https://ora.ox.ac.uk/objects/uuid:15e74c10-225f-4bd7-b086-8e1fdb1b79e8/download_file?file_format=pdf&safe_filename=Manokha%252C%2BSurveillance%252C%2BAAM.pdf&type_of_work=Journal+article. Acesso em: 10 nov. 2020.

MPF. **Nota Técnica Conjunta elaborada pela Procuradoria Federal dos Direitos do Cidadão e Câmara Criminal, do Ministério Público Federal, sobre o PLS (Substitutivo) nº 1179/2020**: Manutenção do prazo de entrada em vigor da LGPD (ressalvadas as sanções administrativas). 2020. Disponível em: http://www.mpf.mp.br/pgr/documentos/PRSP00039100.2020.pdf. Acesso em 16 jun. 2020.

MULHOLLAND, Caitlin Sampaio. Responsabilidade Civil por Danos Causados pela Violação de Dados Sensíveis e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018). *In*: MARTELETO GODINHO, Adriano *et al.* **Responsabilidade civil e novas tecnologias**. Indaiatuba, SP: Foco, 2020. p. 109-125.

MULHOLLAND, Caitlin. **Migalhas de Responsabilidade Civil**. A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco? jun. 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-de-dados-pessoais-culpa-ou-risco. Acesso em: 4 out. 2020.

NERY Jr., Nelson. **Responsabilidade civil por dano ecológico e a ação civil pública**. In: Revista Justitia, n. 126, São Paulo, jul./set. 1984.

NUNES DE SOUZA, Eduardo. GUIA SILVA, Rodrigo da. Direitos do titular de dados pessoais na Lei 13.709/2018: uma abordagem sistemática. *In:* FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena DONATO. **Lei Geral de Proteção de Dados Pessoais e Suas Repercussões no Direito Brasileiro**. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 243-281.

PAMPLONA FILHO, Rodolfo; STOLZE GAGLIANO, Pablo. Manual de Direito Civil: Volume Único. São Paulo: Saraiva, 2017.

PALHARES, Felipe (org.). **Temas Atuais de Proteção de Dados**. São Paulo: Thomsom Reuters Brasil, 2020.

PEREIRA, Caio Mário da Silva. Responsabilidade Civil. 12ª ed. rev., atual. e ampl. Rio de Janeiro: Forense, 2018.

PEREIRA, Luiz Fernando. A Lei Geral de Proteção de Dados Pessoais: uma teoria finalística. *In*: **Revista Jus Navegandi**, 13 set. 2018. Disponível em: https://jus.com.br/artigos/68967/a-lei-geral-de-protecaode-dados-pessoais-uma-teoria-finalistica. Acesso em: 4 nov. 2018.

PERUZZI, *Antonio et al. How News May Affect Markets' Complex Structure: The Case of Cambridge Analytica. D*isponível em: https://www.mdpi.com/1099-4300/20/10/765?type=check_update&version=2. Acesso em: 10 nov. 2020.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

REVISTA BRASILEIRA DE DIREITO CIVIL. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc. Acesso em: 4 out. 2020.

REVISTA DO INSTITUTO BRASILEIRO DE RESPONSABILIDADE CIVIL. Disponível em: http://revistaiberc.responsabilidadecivil.org/iberc. Acesso em: 4 out. 2020.

REVISTA PENSAR. Disponível em: https://periodicos.unifor.br/rpen/about. Acesso em: 4 out. 2020.

RIBEIRO DIAS, Leonardo Adriano; FADEL BECUE, Sabrina Maria. Regulação e Autorregulação do Mercado de Valores Mobiliários Brasileiro: Limites da Autorregulação. **RIDB**, ano 1, n. 12, p. 7.357-7.388, 2012. Disponível em: http://www.cidp.pt/revistas/ridb/2012/12/2012_12_7357_7388.pdf. Acesso em: 4 out. 2020.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Org. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

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

SCHREIBER, Anderson. **Manual de Direito Civil Contemporâneo**. São Paulo: Saraiva Educação, 2018.

SCHREIBER, Anderson. **Novos Paradigmas Da Responsabilidade Civil**: Da Erosão Dos Filtros Da Reparação à Diluição Dos Danos. 6. ed. São Paulo: Atlas, 2015.

SERPRO. **Proteção de dados ao redor do mundo**. Disponível em: https://www.serpro.gov.br/lgpd/menu/arquivos/mapa-sobre-protecao-de-dados-no-mundo. Acesso em: 23 fev. 2020.

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.

VENOSA, Sílvio de Salvo. Direito Civil: Obrigações e Responsabilidade Civil. 17ª ed. São Paulo, Atlas, 2017.