UNIVERSIDADE FEDERAL DE ALAGOAS – UFAL
FACULDADE DE DIREITO DE ALAGOAS – FDA
GRADUAÇÃO EM DIREITO

LARISSA DANTAS COUTO MONTENEGRO

A RESPONSABILIDADE CIVIL À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS

MACEIÓ/AL
2021

LARISSA DANTAS COUTO MONTENEGRO

UFAL

A RESPONSABILIDADE CIVIL À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS

Monografia de conclusão de curso, apresentada à Faculdade de Direito de Alagoas como requisito parcial para obtenção do grau de Bacharel em Direito.

Orientador: Prof. Marcos Augusto de Albuquerque Ehrhardt Júnior.

MARCOS AUGUSTO DE ALBUQUERQUE EHRHARDT J

Assinado de forma digital por MARCOS AUGUSTO DE ALBUQUERQUE EHRHARDT J
Dados: 2021.07.30 10:49:05 -03'00'

_____

Professor-Orientador

MACEIÓ/AL
2021

Catalogação na Fonte
Universidade Federal de Alagoas
Biblioteca Central
Divisão de Tratamento Técnico

Bibliotecário: Marcelino de Carvalho Freitas Neto – CRB-4 – 1767

M777r Montenegro, Larissa Dantas Couto.
A responsabilidade civil à luz da Lei Geral de Proteção de Dados / Larissa Dantas Couto Montenegro. – 2021.
83 f.

Orientador: Marcos Augusto de Albuquerque Ehrhardt Júnior.
Monografia (Trabalho de Conclusão de Curso em Direito) – Universidade Federal de Alagoas. Faculdade de Direito de Alagoas. Maceió, 2021.

Bibliografia: f. 73-83.

1. Brasil. Lei geral de proteção de dados pessoais (2018). 2. Responsabilidade civil. 3. Risco. 4. Prevenção de dano. I. Título.

CDU: 347.51

Folha de Aprovação

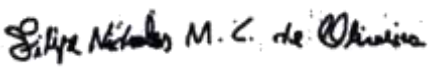
AUTORA: LARISSA DANTAS COUTO MONTENEGRO

A Responsabilidade Civil à Luz da Lei Geral de Proteção de Dados

Trabalho de Conclusão de Curso apresentado à banca examinadora na Faculdade de Direito de Alagoas da Universidade Federal de Alagoas (UFAL) e aprovado em 08 de setembro de 2021.

Banca Examinadora:

Presidente: Prof. Dr. Querino Mallmann



Membro: Mestrando Filipe Nicholas Moreira Cavalcante de Oliveira

Coordenador do NPE: Prof. Hugo Leonardo Santos

À minha avó Zuleide, que tanto se emociona com todas as minhas conquistas acadêmicas e com todo o seu entusiasmo de avó segue torcendo, com fé e amor, pelo meu contínuo sucesso nos estudos e na vida.

AGRADECIMENTOS

O desenvolvimento deste trabalho de conclusão de curso contou com a importante contribuição de pessoas queridas às quais devo meus sinceros agradecimentos:

Ao professor-Orientador, Marcos Ehrhardt Júnior, pela assistência, pelas suas correções e por todo o auxílio na elaboração desta monografia.

Aos professores Everilda Brandão, Rafael Dresch e Chiara de Teffé, por compartilharem comigo suas opiniões pessoais sobre a matéria, além das fontes bibliográficas indicadas.

À minha família, especialmente aos meus pais, Deise e Alexandre, que sempre me deram todo o suporte e não mediram esforços para que eu pudesse dedicar ao máximo meu tempo aos estudos e realizasse o sonho da graduação em Direito.

Ao meu irmão, Nicolas, pela motivação e força diárias.

Ao meu namorado, Victor, que me incentivou em todos os momentos.

Às minhas amigas da Universidade, especialmente Débora, Tamires, Marília, Gabriela e Alícia, pelo encorajamento mútuo e troca de experiência durante a elaboração de grande parte deste trabalho. À minha amiga Gabriela Buarque, pelas dicas, conhecimentos e materiais bibliográficos partilhados.

Aos graduados da turma de 2020, Nathalia Aciole e Rodrigo Souza, pelas referências partilhadas sobre a Lei Geral de Proteção de Dados, que me ajudaram a dar os primeiros passos nessa pesquisa.

Por fim, aos professores do curso, que ao longo desses cinco anos contribuíram diretamente na formação do meu conhecimento jurídico.

RESUMO

Esta monografia versa sobre o regime de responsabilidade civil compreendido na Lei Geral de Proteção de Dados e todas as suas peculiaridades, visando demonstrar o risco existente nas atividades de tratamento e a necessidade de prevenção aos danos, sem deixar de lado o estímulo ao desenvolvimento econômico, garantindo a plena conformidade com os ditames constitucionais de dignidade da pessoa humana, solidariedade social e justiça distributiva, por meio das multifunções que a responsabilidade pode incorporar. Assim, demonstrar-se-á que é preciso a adoção de um modelo híbrido de responsabilidade civil, caracterizado pela combinação entre as teorias objetiva e subjetiva, a partir do dever objetivo de reparar o dano, somado à observância de *standards* de conduta na etapa de quantificação da indenização, a fim de que haja o devido incentivo ao implemento de programas de *compliance* e proteção dos titulares de dados, considerados tanto individualmente quanto coletividade. Por fim, será discutida a possibilidade de responsabilização por mera violação de dados e risco de dano, cujo posicionamento é pelo não cabimento da indenização por dano *in re ipsa*, mas, por outro lado, defendendo a consagração das tutelas de urgência como instrumentos aliados à responsabilidade preventiva.

Palavras-chave: Lei Geral de Proteção de Dados. Responsabilidade Civil. Risco. Prevenção de danos. Multifunções da responsabilidade civil.

ABSTRACT

This monograph deals with the civil responsibility regime included in the General Data Protection Law and all its peculiarities, aiming to demonstrate the existing risk in processing activities and the need to prevent damage, without neglecting the stimulus to economic development, ensuring full compliance with the constitutional dictates of human dignity, social solidarity and distributive justice, through the multifunctions that responsibility can incorporate. Thus, it will be demonstrated that it is necessary to adopt a hybrid model of civil responsibility, distinguished by the combination of objective and subjective theories, from the objective duty to repair the damage, summed to the observance of standards of conduct in the stage of quantification of indemnity, in order to ensure that there is due incentive to implement compliance and protection programs for data subjects, considered both individually and collectively. Lastly, the possibility of responsibilization for mere data breach and risk of damage will be discussed, whose position is that the indemnity for damage in re ipsa is not appropriate, but, on the other hand, defending the consecration of emergency reliefs as allied instruments of responsibility preventive.

Key-words: General Data Protection Law. Civil Responsibility. Risk. Damage prevention. Multifunctions of civil liability.

LISTA DE ABREVIATURAS E SIGLAS

ACP – Ação Civil Pública
ADI – Ação Direta de Inconstitucionalidade
CC – Código Civil
CDC – Código de Defesa do Consumidor
GDPR – *General Data Protection Regulation*
IA – Inteligência Artificial
IBGE – Instituto Brasileiro de Geografia e Estatística
LGPD – Lei Geral de Proteção de Dados
MPDFT – Ministério Público do Distrito Federal e Territórios
OCDE - Organização para a Cooperação e Desenvolvimento Econômico
PL – Projeto de Lei
STF – Supremo Tribunal Federal
STJ – Superior Tribunal de Justiça
TJ – Tribunal de Justiça

SUMÁRIO

1. **INTRODUÇÃO** 9
2. **ASPECTOS DA LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA** 11
2.1 **Origem e Escopo de Aplicação** 11
2.2 **Os Sujeitos do Tratamento de Dados**.....17
2.3 **Os Princípios** 23
3. **A CLASSIFICAÇÃO DO TRATAMENTO IRREGULAR NA LGPD** 29
3.1 **Os Deveres Específicos da LGPD**.....30
3.1.1 Autodeterminação e a bases legais legitimadoras do tratamento.....30
3.1.2 Direitos do titular, princípios e obrigações dos agentes de tratamento.....37
3.2 **O Dever Geral de Segurança**.....39
4. **O SISTEMA DE RESPONSABILIDADE CIVIL DA LGPD**.....46
4.1 A Natureza da Imputação da Responsabilidade.....46
4.1.1 O dano na Lei Geral da Proteção de Dados.....46
4.1.2 Divergências doutrinárias acerca da responsabilidade na LGPD.....48
4.1.3 A presença da imputação objetiva na estrutura normativa.....52
4.2 **A Análise Constitucional**.....55
4.2.1 O reforço constitucional na interpretação de um nexo de imputação objetiva.....55
4.2.2 Responsabilidade proativa: tendência a um sistema híbrido de responsabilidade?.....56
4.3 **A Atuação *Ex Ante* da Responsabilidade Civil: Responsabilidade Sem Dano**.....61
5. **CONCLUSÃO**.....70
6. **REFERÊNCIAS**.....73

INTRODUÇÃO

O conceito de privacidade já não é mais aquele percebido em décadas passadas. Em uma era digital, caracterizada pela hiperconectividade, novas formas de interação entre os indivíduos são criadas, acarretando profundas mudanças nos hábitos e comportamentos humanos. Dois dos principais campos afetados por esse processo de desenvolvimento tecnológico foram a privacidade e a proteção dos dados pessoais.

O capitalismo do século XXI passou a centrar-se na extração e no uso de dados pessoais, sendo eles o insumo presente em praticamente todas as atividades econômicas. Entretanto, a coleta de dados, cada vez mais maciça, é muitas vezes realizada sem a observância dos dispositivos legais e procedimentos de segurança, preterindo, até mesmo, o consentimento de seus titulares. Se os cidadãos não conseguirem sequer acesso sobre quais dados pessoais estão sendo coletados, terão dificuldade ainda maior para compreender as inúmeras destinações que a eles pode ser dada e a extensão do impacto destas em suas vidas.

Diante desse cenário, torna-se cada vez mais necessário o estudo sobre os reflexos jurídicos de questões intrínsecas ao uso dessas informações, de forma a oferecer bases introdutórias para a reflexão em torno dos fundamentos que justificam a proteção de dados na atualidade, visando encontrar um equilíbrio entre o desenvolvimento econômico, por um lado, e a preservação dos direitos dos indivíduos e da própria sociedade, por outro.

Dessa forma, com o objetivo de tutelar com maior especificidade os direitos da personalidade humana em face dos possíveis riscos gerados pelo tratamento desses dados, nasceu a Lei n.º 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD). Inspirada nas normas de proteção de dados internacionais, sobretudo o regulamento europeu, a lei brasileira, dentre outros feitos, criou as figuras do controlador e do operador para poder delimitar direitos e obrigações, aclarando a posição de cada personagem que participa do tratamento de dados, definição essa que será bastante útil para a responsabilização dos agentes.

Confirmando a importância acerca do tema, recorda-se que em meados de maio de 2020, por meio de decisão histórica, a Suprema Corte brasileira passou a enquadrar expressamente a proteção de dados como um direito fundamental autônomo a ser tutelado, reconhecendo o dever do Estado de não apenas se abster de infringir esse direito, como também a obrigação de impor medidas positivas em favor dessa proteção.

O objetivo primaz desta monografia consiste em evidenciar o papel dos atores incumbidos nas tarefas de prevenir a ocorrência de danos e de garantir a segurança dos dados,

bem como a análise de sua responsabilidade civil em face de possíveis incidentes que poderão acarretar danos aos titulares.

Utilizando-se do método dedutivo, o presente trabalho partirá do estudo bibliográfico acerca das posições doutrinárias de maior destaque na atualidade e a análise de artigos, buscando acompanhar os debates mais recentes sobre a matéria. Ao longo desta monografia, será exibida a legislação brasileira a respeito da proteção de dados pessoais, servindo-se, também, de exemplos práticos que auxiliem no entendimento do tema.

Na primeira parte do trabalho, será feita uma abordagem geral sobre a Lei Geral de Proteção de Dados, porquanto para adentrar nos aspectos relativos à responsabilidade civil é importante saber primeiramente as principais características da referida lei. Assim, convém apresentar o seu âmbito de aplicação, os seus objetivos, fundamentos, princípios e direitos previstos, bem como o papel dos sujeitos envolvidos na atividade de tratamento de dados.

O segundo capítulo terá por objetivo classificar as hipóteses de violação da legislação de proteção de dados pessoais, adentrando nas particularidades dessas categorias sobre as quais se concentra maior risco de dano aos titulares e, consequentemente, maior probabilidade de judicialização.

A terceira parte consistirá na análise minuciosa acerca da responsabilidade civil versada na LGPD. Serão apresentadas as principais teses que vêm sendo defendidas pela doutrina brasileira, cuja preocupação volta-se, especialmente, em responder se a natureza da responsabilidade é objetiva ou subjetiva. Nesse contexto, cumpre refletir até que ponto é eficaz a discussão sobre um modelo que seja puramente objetivo ou puramente subjetivo, ou seja, restrito à classificação dualista tradicional e, por vezes, antiquada.

A partir disso, serão abordados os aspectos que tornam especialíssima a responsabilidade civil da LGPD, principalmente quando considerado o seu intuito primaz de estimular condutas de prevenção a danos e mitigação de riscos, devendo ser interpretada em conjunto com a Constituição Federal, Código Civil, Código de Defesa do Consumidor e demais normas que formam o ordenamento jurídico brasileiro.

Por fim, será avaliada a possibilidade de utilização de outros instrumentos jurídicos que incentivem a adoção de práticas preventivas pelos agentes de tratamento e auxiliem os titulares de dados na busca por resguardar os seus direitos.

2 ASPECTOS DA LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA

2.1 Origem e Escopo de Aplicação

Diante da crescente importância atribuída aos dados pessoais, considerados na modernidade a principal matéria-prima propulsora de negócios em todo o mundo, não subsistem dúvidas de que sua contribuição para um ambiente econômico mais seguro e eficiente perpassa pela regulação de seu tratamento.

Nesse sentido, as principais democracias do globo já compreenderam a imprescindibilidade da construção de um sistema jurídico de proteção da privacidade e passaram a criar legislações para regular a matéria.

Com certo atraso, após oito anos de discussões legislativas e consultas públicas acerca da proteção de dados pessoais, o então presidente Michel Temer, em 14 de agosto de 2018, sancionou a Lei nº 13.709/2018, mais conhecida como Lei Geral de Proteção de Dados (LGPD), inserindo o Brasil no rol de países que possuem diretrizes protetivas sobre o tema[1].

Conforme bem pontuado no Projeto de Lei Complementar 53 que deu origem à LGPD, um significativo propulsor de sua criação foi o Regulamento Geral de Proteção de Dados (*General Data Protection Regulation* – GDPR), a mais recente e importante norma europeia para tratamento de dados, cuja entrada em vigor ocorreu em 25 de maio de 2018 e tem provocado profundas mudanças na comunidade internacional, em razão de sua forte extraterritorialidade[2].

Segundo exigência expressa do art. 45 do GDPR[3], a partir da entrada em vigor da lei, empresas europeias somente poderiam contratar empresas estrangeiras se essas estivessem localizadas em países que possuíssem nível adequado de proteção de dados, comparável ao estabelecido em seu território, segundo critérios estipulados pela Comissão Europeia. Em função disso, houve uma clara preocupação do legislador brasileiro com a perda de oportunidades de investimento financeiro internacional no país, ante o isolamento jurídico[4] em que se encontrava por não dispor, até aquele momento, da LGPD.

---

[1] SENADO FEDERAL. Sancionada com vetos lei geral de proteção de dados pessoais. **Agência Senado**, 15 out. 2018. Disponível em: <https://www12.senado.leg.br/noticias/materias/2018/08/15/sancionada-com-vetos-lei-geral-de-protecao-de-dados-pessoais >. Acesso em: 26 fev. 2020.

[2] BRASÍLIA. Parecer sobre o Projeto de Lei da Câmara nº 53, de 2018, p. 10. **Agência Senado.** Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7751566&ts=1571776637073&disposition=inline>. Acesso em: 26 fev. 2020.

[3] UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, 23 abr. 2016 (*General Data Protection Regulation*). ***Intersoft Consulting*.** Disponível em: <https://gdpr-info.eu/art-45-gdpr/>. Acesso em: 26 fev. 2020.

[4] Parecer sobre o Projeto de Lei da Câmara nº 53, de 2018, *op. cit.* p. 03.

Ademais, no processo de produção da LGPD é possível afirmar que houve a importação da experiência e do conhecimento europeu no que diz respeito ao tratamento de dados, sem ter deixado de lado, contudo, a preocupação em adaptar as regras às características do Estado e da sociedade brasileira[5].

Outro fator preponderante na aprovação da lei foi a necessidade de o Brasil possuir uma legislação nacional adequada à proteção da privacidade e da liberdade individual em matéria de dados pessoais[6] para poder, minimamente, ser um candidato sério a integrar a Organização para a Cooperação e Desenvolvimento Econômico – OCDE, desejo do Governo brasileiro há alguns anos[7].

Logo, muitas foram as razões que reivindicaram uma lei especialmente orientada à proteção de dados no Brasil. No entanto, sem menosprezar as peculiaridades e inovações por ela trazidas, não se afigura razoável, muito menos justo, afirmar que os dados pessoais e a privacidade do cidadão estiveram completamente desamparados pelo ordenamento jurídico brasileiro até sua edição.

Isso porque a LGPD faz parte de um sistema que já se encontrava em formação e que se preocupou, tanto no plano constitucional, quanto por meio de leis de caráter público e privado, em assegurar certo grau de proteção à privacidade das pessoas. Portanto, será mais proveitoso que sua observância pelos juristas seja feita levando em conta sua integração a esse sistema normativo, de forma a evitar que o assunto seja tratado apenas sob a óptica dos dispositivos novos e, consequentemente, limitar a proteção a esse diploma legal, transformando-o na resposta para todas as inquirições próprias da disciplina dos dados[8].

Nesse viés, a Constituição Federal, nos incisos X e XII do art. 5º, trata da inviolabilidade da intimidade e da vida privada, bem como do sigilo de correspondências e comunicações telefônicas. Também merece alusão, a ação constitucional do *Habeas Data*, regulamentada pela Lei 9.507/97, cujo art. 7º dispõe sobre as hipóteses de cabimento, as quais, em síntese, referem-se ao conhecimento, retificação e esclarecimento sobre dado ou informação do impetrante constante em banco de dados público.

---

[5] Parecer sobre o Projeto de Lei da Câmara nº 53, de 2018, *op. cit.*, p. 10.

[6] **Síntese Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais**. *Rights and Translation unit, Public Affairs and Communications Directorate*, 2002. Disponível em: <http://www.oecd.org/sti/ieconomy/15590254.pdf>. Acesso em 26 fev. 2020.

[7] OLIVEIRA, Ricardo Alexandre. **Lei Geral de Proteção de Dados Pessoais e seus impactos no ordenamento jurídico**. Revista dos Tribunais. vol. 998/2018. p. 241 – 261. Dez/2018, p. 03.

[8] OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria. Capítulo 2. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018; Introdução. *In:* FRAZÃO, Ana *et al* (org.). **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** São Paulo: Thomson Reuters, 2019. Não paginado [livro digital].

Tal sistema também se refletiu na atuação de tribunais superiores ainda na década de 1990. A título de exemplo, cita-se o julgamento do RHD 22/DF, ocasião na qual o Ministro Celso de Mello enfatizou a relevância do *Habeas Data* como instrumento de concreção efetiva de direito fundamental, porquanto "a garantia de acesso a informações de caráter pessoal, registradas em órgãos do Estado, constitui um natural consectário do dever estatal de respeitar a esfera de autonomia individual, que torna imperativa a proteção da intimidade"[9].

No âmbito do direito privado, o Código de Defesa do Consumidor - Lei 8.078/1990 - é indicado como o precursor de uma série de diretrizes que vieram a sucedê-lo. Por meio de seu art. 43, ficou estabelecido que o funcionamento de bancos de dados e cadastros de consumidores estaria autorizado, desde que respeitadas determinadas condições para a proteção da sua privacidade[10].

Ainda na seara dos bancos de dados, merecem atenção os preceitos advindos com a Lei do Cadastro Positivo – Lei 12.414/2011, principalmente o maior rigor na limitação da coleta e uso de informações àquelas estritamente necessárias à análise de risco de crédito ao consumidor (art. 3º, §3º), o direito do cadastrado solicitar uma revisão de decisão baseada exclusivamente em dados automatizados (art. 5º, VI) e a preocupação voltada em resguardar a classe das "informações sensíveis" (art. 3º, §3º, II) – dimensão que também mereceu tratamento especial na LGPD, representada pelos "dados pessoais sensíveis", conforme será analisado adiante.

Mais recentemente, sobreveio o Marco Civil da Internet – Lei 12.965/2014 –, que estabeleceu princípios, garantias, direitos e deveres para o uso da internet no Brasil, situando-se o principal deles no inciso III do art. 3º, referente à proteção conferida aos dados pessoais digitais. Esse instrumento normativo já sinalizava um grande avanço para a formação de um sistema brasileiro de proteção de dados, mesmo que restrito ao meio virtual.

A criação da Lei nº 13.709/2018, simboliza, nessa conjuntura, uma referência para a organização formal desse sistema, respaldado pelo fato de que, por meio dela, permitiu-se a reunião e reprodução de muitos desses preceitos legais [11], contidos dispersamente no ordenamento jurídico, e que foram recebidos, inclusive, com *status* principiológico.

Conforme expresso em seu art. 1º, a LGPD ocupa-se do tratamento de dados pessoais, seja no meio virtual ou físico (*off-line*), praticado por pessoa natural ou por pessoa jurídica de

---

[9] BRASIL. Supremo Tribunal Federal (STF). **RHD 22/DF**, Pleno, j. 19.09.1991, m. v., rel. Min. Marco Aurélio, rel. p/ acórdão Ministro Celso de Mello, DJ 01.09.1995.

[10] OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria. Capítulo 2. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018; 1.O sistema legal de proteção de dados no Brasil e seus princípios. *In:* FRAZÃO, Ana *et al* (org.). **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** São Paulo: Thomson Reuters, 2019. Não paginado [livro digital].

[11] *Ibidem.*

direito público ou privado, buscando a proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. O conceito de "tratamento" está disposto no art. 5º, X, da lei, *in verbis*:

> Art. 5º [...] X - tratamento: 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;

Os fundamentos da LGPD, contidos em seu art. 2º, englobam o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, de informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico e tecnológico e a inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor, e, por fim, os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

O *caput* do art. 3º da LGPD dispõe sobre a sua aplicação territorial e extraterritorial, especificando que a lei será aplicada às operações de tratamento de dados, realizadas no território nacional, bem como nas atividades de tratamento que tenham por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional, ou quando os dados pessoais objeto de tratamento tenham sido coletados em território nacional – considerado aquele em que seu titular se encontra no momento da coleta.

No entanto, para entender o escopo de aplicação da LGPD é preciso ter em mente, antes de tudo, o que é o dado pessoal nos termos da referida lei.

O dado pessoal é conceituado no art. 5º da LGPD como sendo a "informação relacionada a pessoa natural identificada ou identificável". Por esse dispositivo, fica clara a escolha brasileira em adotar o conceito expansionista[12] europeu de dado pessoal, modelo no qual todos os dados, tanto aqueles relacionados às pessoas diretamente identificadas, como aqueles com potencial de identificar seu titular, serão protegidos de forma equivalente pela lei.

Nesse viés, para ser qualificado como dado pessoal e obter a proteção legal, deverá existir, necessariamente, um vínculo objetivo com uma pessoa natural, de modo que, direta ou

---

[12] Paul Schwartz e Daniel Solove desenvolveram o conceito de PII 2.0, criando duas categorias de *Personally Identifiable Information* (Informações de Identificação Pessoal) - PII, quais sejam, os dados "identificados" e "identificáveis", visando tratá-los de maneira distinta. Esse modelo evita tanto a visão reducionista dos Estados Unidos quanto a visão expansionista da União Europeia. Na visão reducionista, são protegidos apenas dados identificados, deixando, portanto, muitas informações pessoais sem proteção legal. Na abordagem expansionista, é irrelevante a diferenciação entre aqueles dados, os quais são tratados como equivalentes. Pelo modelo PII 2.0, defende-se que as proteções legais necessárias devem ser diferentes para dados identificados e identificáveis. SCHWARTZ, Paul M.; SOLOVE, Daniel J. ***The PII Problem: Privacy and a New Concept of Personally Identifiable Information*****.** In: *New York University Law Review*, [s. l.], v. 86, n. *December*, p. 1814–1894, 2011, p. 1817. Disponível em: <https://lawcat.berkeley.edu/record/1124577?ln=en>. Acesso em: 21 mar. 2020.

indiretamente, seja possível identificá-la. Nos ensinamentos de Lawrence Lessig, a identidade é algo maior do que apenas quem a pessoa é, ou seja, ela também inclui os atributos e todos os fatos verdadeiros sobre o sujeito, como o nome, o sexo, onde mora, qual o nível de escolaridade, o número da carteira de motorista, número de previdência social, compras em *site*, profissão, e assim por diante[13].

A proteção legal da LGPD, do mesmo modo que o regulamento europeu, não alcança dados ou informações de pessoas jurídicas, isto é, essencialmente empresariais, sejam de caráter público ou privado, a exemplo de planejamentos estratégicos, balanços financeiros, sistemas em desenvolvimento, protótipos, fórmulas, outras inovações ou qualquer outro tipo de documento corporativo. No caso de possuírem dados pessoais em seu conteúdo, somente estes serão considerados para fins de proteção dessa norma, de modo que o titular de dados sempre será uma pessoa física[14].

À vista disso, pela óptica do potencial de identificação de um indivíduo, os dados pessoais serão classificados em: i) dados pessoais diretos, os quais identificam diretamente uma pessoa natural, a exemplo do CPF, RG, título eleitoral, nomes não homônimos; ii) dados pessoais indiretos, que tornam a pessoa natural identificável, uma vez que necessitam de informações suplementares para identificá-la, por exemplo, gostos, interesses, hábitos de consumo, profissão, sexo, idade e geolocalização[15].

Outrossim, a LGPD também traz o conceito de dano anonimizado, como sendo, nos termos do art. 5º, III, aquele "relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento", os quais, portanto, conforme o art. 12 da mesma lei, encontram-se excluídos de sua proteção normativa, "salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido".

Nesse cenário, é concebida a ideia de dado pseudonimizado, enquadrado como uma gradação entre o dado pessoal e o dado anônimo[16]. A própria LGPD reconhece essa diferença, conceituando a técnica da pseudonimização, no art. 13, §4º, como sendo "o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão

---

[13] LESSIG, Lawrence. *Code, version* 2.0. Nova York: *Basic Books*, 2006. p. 39. Disponível em: <http://codev2.cc/download+remix/Lessig-Codev2.pdf>. Acesso em: 21 mar. 2020.

[14] VAINZOF, Rony. Capítulo I, disposições preliminares, art. 5º. *In*: MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (org.). **LGPD: Lei Geral de Proteção de Dados Comentada**. 2ª ed. São Paulo: Revista dos Tribunais, 2019. Não paginado [livro digital].

[15] *Ibidem.*

[16] DONEDA, Danilo. Parte III. 2.Dado pessoal: contornos conceituais e normativos. *In:* **A criptografia no direito brasileiro**. São Paulo: Revista dos Tribunais, 2019. Não paginado [livro digital].

pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro", voltado principalmente para a realização de estudos e pesquisas em saúde pública.

No que concerne aos dados sensíveis, a LGPD os define em seu art. 5º, II, como o "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".

Vale destacar que a LGPD estatui que o tratamento desses dados (art. 11) somente poderá ocorrer nas hipóteses de consentimento do titular, de forma expressa e destacada, para finalidades específicas. Contudo, estabelece exceções nas quais o tratamento poderá ser realizado sem o respectivo consentimento, mas desde que relativas ao cumprimento de obrigação legal ou regulatória, à execução de políticas públicas, aos estudos por órgãos de pesquisa, ao exercício regular de direitos, à proteção da vida ou da incolumidade física do titular ou de terceiros, à tutela da saúde e à garantia da prevenção à fraude e à segurança do titular.

Em tempos de pandemia provocada pela Covid-19, questões concernentes à proteção de dados de saúde têm suscitado uma série de questionamentos, principalmente diante de notícias de que países em todo o mundo vêm utilizando o tratamento de dados sensíveis para geolocalização, identificação e rastreamento de pacientes, gerenciamento do risco de contágio, dentre outras práticas, buscando auxiliar os mecanismos de combate à pandemia[17], a exemplo de Taiwan [18] e Israel [19] que programaram *smartphones* para monitorar os pacientes no cumprimento da quarentena. No Brasil, de forma semelhante, uma operadora de telefonia já manifestou o mesmo interesse[20].

Apesar da compatibilidade entre a LGPD e o acesso aos dados sensíveis para a tutela da saúde, restrito à finalidade de conter a disseminação do vírus e resguardado o direito ao sigilo das informações pessoais, é imprescindível afastar alternativas extremadas para não perder de

---

[17]EHRHARDT JR., Marcos; SILVA, Gabriela Buarque. **Privacidade e proteção de dados pessoais durante a pandemia da Covid-19.** JusBrasil. Disponível em: <https://marcosehrhardtjr.jusbrasil.com.br/artigos/824475623/privacidade-e-protecao-de-dados-pessoais-durante-a-pandemia-da-covid-19?ref=feed>. Acesso em: 26 mar. 2020.

[18] SMITH, Nicola. *Taiwan uses smartphones monitor patients quarantined vírus scare.* ***The Telegraph***, 03 fev. 2020. Disponível em: <https://www.telegraph.co.uk/news/2020/02/03/taiwan-uses-smartphones-monitor-patients-quarantined-virus-scare/>. Acesso em: 27 mar. 2020.

[19] *Israel government approves mobile tracking monitor coronavírus quarentine enforcement.* ***Data Guidance***, 2020. Disponível em: <https://platform.dataguidance.com/news/israel-government-approves-mobile-tracking-monitor-coronavirus-quarantine-enforcement>. Acesso em: 27 mar. 2020.

[20]Tim quer rastrear celular para monitorar se doente de Covid-19 sai de casa. **UOL**, 2020. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2020/03/26/tim-quer-rastrear-celular-para-monitorar-se-doente-de-covid-19-sai-de-casa.htm>. Acesso em 27 mar. 2020.

vista princípios que há anos são desenvolvidos pela doutrina e jurisprudência e que foram adotados pela lei de dados, os quais também deverão ser observados num contexto de pós-pandemia[21].

Noutro giro, é importante ter em mente a linha tênue que separa informações consideradas comuns das sensíveis. É possível identificar aspectos particulares mais íntimos dos indivíduos a partir de uma série de dados triviais que são correlacionados para prever comportamentos e acontecimentos[22], a exemplo da Target[23], uma loja de departamentos que, por meio de operações estatísticas, analisava o comportamento de compra das clientes para identificar quais estariam grávidas, buscando direcionar campanhas de *marketing* para esse público.

Bruno Bioni menciona um estudo realizado pela Universidade de Cambridge, cuja conclusão foi a de que, a partir de "curtidas" em uma rede social, é possível criar um retrato fiel dos gostos e predileções dos usuários. A pesquisa demonstrou com precisão a porcentagem dos usuários homossexuais e heterossexuais, os usuários brancos e negros e, ainda, a preferência partidária republicana ou democrata. Igualmente, outros registros digitais, tais como o histórico de navegação, os termos de pesquisa ou as compras realizadas por um consumidor "têm o potencial de revelar muitos atributos da personalidade de um indivíduo, dentre os quais informações sensíveis a seu respeito" [24].

À vista do que foi exposto, depreende-se que o tratamento diferenciado dedicado aos dados sensíveis é justificável, porquanto a probabilidade de uso discriminatório da informação é potencialmente maior, sem olvidar daqueles casos cuja discriminação poderá ocorrer ainda sem a coleta de dados considerados sensíveis ou diante de situações nas quais estes foram tratados mesmo sob o amparo de fins legítimos e lícitos[25].

2.2 Os Sujeitos do Tratamento de Dados

---

[21] EHRHARDT JR., Marcos; SILVA, Gabriela Buarque. **Privacidade e proteção de dados pessoais durante a pandemia da Covid-19.** JusBrasil. Disponível em: <https://marcosehrhardtjr.jusbrasil.com.br/artigos/824475623/privacidade-e-protecao-de-dados-pessoais-durante-a-pandemia-da-covid-19?ref=feed>. Acesso em: 26 mar. 2020.

[22] BIONI, Bruno. 2.3.1 Dados sensíveis e o tratamento sensível de dados triviais: a interface com o direito de isonomia e não discriminação. L.83 [livro digital, Kindle]. *In:* **Proteção de dados pessoais. A função e os limites do consentimento**. 2ª ed. Rio de Janeiro: Forense, 2019.

[23] REDAÇÃO. Proteção de dados: relembre seis casos de vazamentos. **Conecta Já**, 27 jan. 2020. Disponível em: <https://conectaja.proteste.org.br/casos-de-vazamentos-de-dados/>. Acesso em: 26 mar. 2020.

[24] BIONI, Bruno. *Op. cit*.

[25] DONEDA, Danilo. Cap. 2 Privacidade e Informação. 3 Bancos de dados e os dados sensíveis. *In:* **Da privacidade à proteção de dados pessoais:** Fundamentos da lei geral de proteção. 2ª ed. São Paulo: Revista dos Tribunais. 2020. Não paginado [livro digital].

A diferenciação dos sujeitos que participam do tratamento de dados é imprescindível para determinar quem deve ser responsável pelo cumprimento de determinadas regras de proteção de dados e de que forma os titulares podem exercer seus direitos.

A LGPD enuncia as definições de "controlador" e "operador" em seu art. 5º, incisos VI e VII, figuras essas que, em associação, dão origem ao conceito de "agentes de tratamento", no inciso IX. Seu conteúdo está assim disposto:

> Art. 5º Para os fins desta Lei, considera-se: [...]
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; [...]
> IX - agentes de tratamento: o controlador e o operador;

Antes de tudo é preciso reconhecer, porém, as dificuldades em aplicar as definições da LGPD em um ambiente complexo, onde muitos cenários podem ser previstos envolvendo agentes de tratamento, sozinhos ou em conjunto, com diferentes graus de autonomia e responsabilidade[26]. Assim, devido à tendência de entidades serem e proverem serviços multidisciplinares, tanto no setor privado quanto no público, haverá situações em que uma mesma pessoa jurídica será controladora e operadora[27].

Para Rony Vainzof[28], a noção de controlador abarca absolutamente todas as decisões sobre as atividades que representam o ciclo de vida dos dados pessoais, desde o projeto, passando pela coleta ou recepção, por todas as formas de processamento, até o descarte, motivo pelo qual a LGPD delegou maiores responsabilidades a esta função.

Assim, em síntese, sua competência consiste em determinar quais espécies de dados serão tratados, para quais propósitos, com quem serão compartilhados, por quanto tempo eles serão mantidos, quais são os requisitos de segurança necessários, entre outros.[29]

Há casos em que a lei, mesmo sem designar diretamente o controlador, impõe o dever de alguém coletar e processar certos dados. Esse seria o caso de uma entidade encarregada de determinadas tarefas públicas, como o Instituto Nacional do Seguro Social (INSS), por

---

[26] *Article* 29. ***Opinion* 1/2010 *on the concepts of "controller" and "processor".*** 16 de fevereiro de 2010. p. 01. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf>. Acesso em: 18 mar. 2020. A Autoridade Nacional de Proteção de Dados manifestou-se sobre o assunto no Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.

[27] VAINZOF, Rony. Capítulo I, disposições preliminares, art. 5º. *In*: MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (org.). **LGPD: Lei Geral de Proteção de Dados Comentada**. 2ª ed. São Paulo: Revista dos Tribunais, 2019. Não paginado [livro digital].

[28] *Ibidem.*

[29] VAINZOF, Rony. Capítulo I, disposições preliminares, art. 5º. *In*: MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (org.). **LGPD: Lei Geral de Proteção de Dados Comentada**. 2ª ed. São Paulo: Revista dos Tribunais, 2019. Não paginado [livro digital].

exemplo, que não poderia cumprir suas funções sem coletar e registrar pelo menos alguns dados pessoais[30]. Nesse caso, emana explicitamente da lei quem é o controlador[31].

Também há o controle derivado de uma competência implícita, decorrente de práticas legais comuns a diversas áreas, como Direito Civil e Direito do Trabalho, nas quais o papel funcional do sujeito revela quem é o controlador, a exemplo do empregador em relação aos dados de seus funcionários, o corretor de imóveis (pessoa física) pelos dados de seus clientes, o editor em relação aos dados sobre assinantes, a associação em relação aos dados de seus membros ou colaboradores[32].

Contudo, ser um controlador é principalmente a consequência da circunstância factual pela qual uma entidade optou por processar dados pessoais para seus próprios fins. Por certo, um critério meramente formal não seria suficiente, pelo fato de que, em alguns casos, a nomeação expressa de um controlador de dados - estabelecida, por exemplo, mediante lei ou contrato - poderia não refletir a realidade, confiando formalmente o papel de controlador a uma organização que na verdade não está em posição de "determinar"[33].

Nesse contexto, outros elementos poderão ser considerados em caso de dúvida, os quais podem ser úteis para identificar um controlador, a exemplo do grau de controle real exercido por uma parte, a imagem passada aos titulares de dados e expectativas razoáveis destes últimos com base nessa visibilidade[34].

Não obstante, o controlador poderá nomear um operador, buscando maior segurança, eficácia e organização no tratamento dos dados, exigindo-se dele confidencialidade no exercício da função. Assim, a atividade desenvolvida pelo operador está inserida no âmbito da execução dos meios técnicos e organizacionais do tratamento, devendo agir conforme as orientações recebidas do controlador, uma vez que, a depender do caso, estará sob sua autoridade direta, ou será pessoa física ou jurídica terceirizada para agir em seu nome.

A LGPD, em seu art. 39, reforça esse caráter de subordinação da atividade desempenhada pelo operador em relação às orientações fixadas pelo controlador, do seguinte modo:

---

[30] Decreto nº 9.746, de 8 de abril de 2019. "Art. 14. À Diretoria de Benefícios compete: I - gerenciar: a) as bases de dados cadastrais, os vínculos, as remunerações e as contribuições dos segurados da Previdência Social, com vistas ao reconhecimento automático do direito".

[31] *Article* 29. ***Opinion* 1/2010 *on the concepts of "controller" and "processor"*.** 16 de fevereiro de 2010. p. 10. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf>. Acesso em: 18 mar. 2020. A Autoridade Nacional de Proteção de Dados manifestou-se sobre o assunto no Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.

[32] *Ibidem*, p. 10.

[33] *Ibidem*, p. 08.

[34] *Ibidem*, p. 11-12.

> Art. 39. 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.

Um exemplo de operador seria uma empresa de *call center*, contratada por um banco, qualificado como controlador. Nesse contexto, a empresa está apenas autorizada a colher informações de um correntista que se referem ao negócio da instituição bancária, de modo que o tratamento de dados para o qual aquela foi designada está adstrito aos limites estabelecidos pelo controlador, com obediência à lei[35].

Em resumo, a definição da finalidade dos dados é reservada à competência do controlador, por serem questões substanciais e ligadas ao núcleo de legalidade do tratamento. Já a opção pelos meios nos quais serão tratados os dados pode ser delegada pelo controlador ao operador, no que concerne a questões técnicas ou organizacionais, a exemplo de qual *hardware* ou *software* deverá ser usado e o oferecimento de consultoria sobre o horário de maior abertura de *e-mail marketing*[36].

Nesta perspectiva, é bem possível que tais meios técnicos e organizacionais sejam determinados exclusivamente pelo operador de dados[37]. Porém, esse tipo de decisão não modifica a qualificação da empresa de operadora para controladora, exceto se utilizar o tratamento das informações para outras finalidades, visando ao seu próprio benefício, com a intenção de gerar serviços de valor agregado de forma ilícita[38], momento a partir do qual, automaticamente, passará a responder como controladora diante de seus atos.

Ademais, em que pese a previsão contida na LGPD acerca da plena possibilidade de o controlador ou o operador serem pessoas naturais, tal hipótese não se confunde com o CEO (*Chief Executive Officer*)[39] da empresa, com o encarregado, ou com os demais funcionários incumbidos de tarefas decisórias dentro do tratamento de dados, uma vez que estarão laborando em nome da pessoa jurídica, a qual permanecerá respondendo como controladora ou operadora.

---

[35] LIMA, Mariana. **Titular, Operador e Controlador – o que isso quer dizer?.** Disponível em: <https://triplait.com/titular-operador-e-controlador/>. Acesso em: 19. Mar. 2020.

[36] VAINZOF, Rony. Capítulo I, disposições preliminares, art. 5º. *In*: MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (org.). **LGPD: Lei Geral de Proteção de Dados Comentada**. 2ª ed. São Paulo: Revista dos Tribunais, 2019. Não paginado [livro digital].

[37] *Article* 29. ***Opinion* 1/2010 *on the concepts of "controller" and "processor".*** 16 de fevereiro de 2010. p. 14. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf>. Acesso em: 18 mar. 2020. A Autoridade Nacional de Proteção de Dados manifestou-se sobre o assunto no Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.

[38] VAINZOF, Rony. Capítulo I, disposições preliminares, art. 5º. *In*: MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (org.). **LGPD: Lei Geral de Proteção de Dados Comentada**. 2ª ed. São Paulo: Revista dos Tribunais, 2019. Não paginado [livro digital].

[39] O termo "CEO é a sigla inglesa de *Chief Executive Officer*, que significa Diretor Executivo em português. CEO é a pessoa com maior autoridade na hierarquia operacional de uma organização. É o responsável pelas estratégias e pela visão da empresa". Disponível em:< https://www.significados.com.br/ceo/>. Acesso em: 18 mar. 2020.

Todavia, se aquela mesma pessoa física usufruir dos dados, visando finalidades pessoais que são externas às atividades da empresa, será classificada como um controlador de fato e responsável como tal.[40]

Já o encarregado é definido como a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a autoridade nacional.

Suas funções incluem, em síntese, o recebimento de reclamações dos titulares e comunicados da autoridade nacional, para que sejam prestados esclarecimentos e adotadas as devidas providências, bem como a orientação de funcionários e contratados da entidade a respeito das práticas contidas na LGPD, e a execução as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Além disso, a obrigatoriedade da indicação de um encarregado ainda é uma questão em aberto na LGPD, uma vez que, a depender da natureza e do porte da entidade ou do volume de operações de tratamento de dados, poderá ter sua presença dispensada, problemas estes ainda pendentes de resolução, cabendo a ANPD a edição de normas complementares.

Neste contexto, será fundamental lidar com a multiplicidade de arranjos possíveis nos quais vários sujeitos podem interagir ou ser ligados entre si no decorrer do tratamento de dados, de forma que seja possível ao operador do direito responder a determinados questionamentos, dentre eles a definição da responsabilidade civil, seja entre controladores e operadores, seja em uma cadeia de controladores – exercendo controle conjunto ou parcial -, compreendida em uma relação de consumo ou não.

Nota-se que a expectativa da presença de inúmeros sujeitos envolvidos nesse ciclo do uso de dados pessoais está naturalmente ligada aos vários tipos de atividades que, de acordo com o art. 5º, inciso X[41], da LGPD, podem significar "tratamento". Nesse viés, será de suma importância reconhecer que, em razão dos diferentes graus de tratamento em que os sujeitos podem interagir, incidirão diferentes graus de responsabilidade, havendo a necessidade de aferição em cada caso concreto[42].

---

[40] VAINZOF, Rony. *Op. cit*.

[41] Art. 5º [...] X - tratamento: 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. BRASÍLIA. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm#art65 >. Acesso em: 18 mar. 2020.

[42] *Article* 29. ***Opinion* 1/2010 *on the concepts of "controller" and "processor"*.** 16 de fevereiro de 2010. p. 18. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf>. Acesso em: 18 mar. 2020. A Autoridade Nacional de Proteção de

Somando-se a esses sujeitos, consoante estabelecido na Lei nº 13.853/19, cuja promulgação alterou alguns pontos da Lei nº 13.709/18 (LGPD), a Autoridade Nacional de Proteção de Dados (ANPD) é o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. Apesar da autonomia técnica, está vinculada à Presidência da República e terá, como órgão máximo de direção, o Conselho Diretor, formado por cinco membros que serão nomeados pelo presidente.

No que diz respeito a importância da Autoridade Nacional, cumpre salientar sua função precípua de interpretação da LGPD e do estabelecimento de normas e diretrizes para a sua implementação, além de articular sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afeitas à temática de proteção de dados pessoais (parágrafo único, art. 55-K).

Merece relevo a sua responsabilidade em regulamentar determinadas disposições legais e esclarecer obrigações dos agentes de tratamento, como, por exemplo, a base legal do legítimo interesse para o tratamento de dados, padrões e técnicas utilizados em processos de anonimização (art. 13, § 3°), padrões técnicos mínimos para segurança e sigilo dos dados pessoais (art. 46, § 1°), prazo para comunicação de incidente de segurança (art. 48, § 1°), além de normas, orientações e procedimentos simplificados e diferenciados para adequação à lei por microempresas, empresas de pequeno porte e startups (art. 55-J, inc. XVIII), entre muitas outras[43].

Para a professora Chiara de Teffé[44], a ANPD traz junto com ela certas expectativas, principalmente ligadas a decisões técnicas e consistentes, provindas de um corpo técnico, multidisciplinar e intimamente afeto à temática, além da independência funcional e autonomias administrativa, financeira e decisória do órgão, que deverá ter o compromisso de promover de forma ampla a conscientização e a transparência no tratamento de dados, realizar consultas públicas e tratar os regulados como parceiros e não adversários.

Contudo, mesmo após a vigência da LGPD, o cenário brasileiro é de grande indefinição, uma vez que, até o presente momento, aguarda-se uma postura mais assertiva por parte da

Dados manifestou-se sobre o assunto no Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.

[43] ALVES, Fabrício da Mota; VIEIRA, Gustavo Afonso Sabóia. **Sem a ANPD, a LGPD é um problema, não uma solução.** JOTA. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/anpd-lgpd-problema-solucao-06012020>. Acesso em: 20 mar. 2020.

[44] TEFFÉ, Chiara Spadaccini de. **Por que precisamos de uma Autoridade Nacional de Proteção de Dados?** JOTA. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/por-que-precisamos-de-uma-autoridade-nacional-de-protecao-de-dados-07012020#sdfootnote5anc>. Acesso em: 20 mar. 2020.

Autoridade Nacional de Proteção de Dados no sentido de efetivar a aplicação da lei[45]. Insta salientar que a ANPD poderá aplicar sanções administrativas a partir de 1º de agosto de 2021, com "multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração" (art. 52, II).

Para Fabricio da Mota Alves e Gustavo Afonso Sabóia Vieira[46], ambos indicados pelo Senado Federal para o Conselho Nacional da Proteção de Dados Pessoais e da Privacidade[47], grande parcela desses dispositivos legais não terá eficácia plena enquanto pendentes de regulamentação, pois "sem a Autoridade, o sistema é incompleto, falho e potencialmente prejudicial à sociedade brasileira", produzindo uma enorme insegurança jurídica para todos os agentes envolvidos, seja no setor privado, seja no setor público.

Portanto, não há dúvidas sobre a necessidade de uma maior atuação da Autoridade Nacional de Dados Pessoais, visando à regulamentação de inúmeros pontos da LGPD, sem a qual prolongar-se-á a atual insegurança jurídica, configurando-se como um dos grandes desafios para a proteção de dados no Brasil em pelos próximos anos[48].

2.3 Os Princípios

Fundamentado na reflexão acerca do sistema de proteção de dados no país, é acentuada a importância da LGPD na tarefa de consolidar os preceitos que já despontavam de outras leis que, apesar de forma não exclusiva, atuavam pela proteção de dados. Nesse aspecto, merece especial atenção o rol de princípios do art. 6º. Vejamos:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - **finalidade**: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - **adequação**: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - **necessidade**: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> 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;

---

[45] DE CASTRO, André Zanatta Fernandes; MARQUES, Fernanda Mascarenhas. Segurança, competitividade e a necessária adequação à LGPD. **Conjur**, 2021. Disponível em: https://www.conjur.com.br/2021-mar-26/opiniao-seguranca-competitividade-adequacao-lgpd. Acesso em: 26 mar. 2021.

[46] ALVES, Fabrício da Mota; VIEIRA, Gustavo Afonso Sabóia. *Op. cit.*

[47] BUCCO, Rafael. Senado indica seus represente no Conselho Nacional de Proteção de Dados Pessoais. **Tele.síntese**, 06 nov. 2019. Disponível em: <https://www.telesintese.com.br/senado-indica-seus-representantes-no-conselho-nacional-de-protecao-de-dados-pessoais/>. Acesso em: 20 mar. 2020.

[48] TEFFÉ, Chiara Spadaccini de. Por que precisamos de uma Autoridade Nacional de Proteção de Dados? **JOTA**. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/por-que-precisamos-de-uma-autoridade-nacional-de-protecao-de-dados-07012020#sdfootnote5anc>. Acesso em: 20 mar. 2020.

> V - **qualidade dos dados**: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - **transparência**: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - **segurança**: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - **prevenção**: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - **não discriminação**: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - **responsabilização e prestação de contas**: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. (Grifo nosso)

Quanto aos três primeiros princípios apontados na LGPD - finalidade, adequação e necessidade -, associados à transparência, cumpre salientar que, por estarem intimamente relacionados, poderão ser conceituados, muitas vezes, de forma entrelaçada, em razão do maior esforço para analisá-los em apartado.

Inicialmente, para estar de acordo com o princípio da finalidade, o titular deverá ser prévia e plenamente esclarecido sobre quais os fins se desejam alcançar com a coleta de seus dados pessoais, inclusive se terceiros terão ou não acesso, de forma a garantir-lhe que a utilização das informações por ele cedidas estará adstrita a esse propósito. Referido princípio também está presente no RGPD, denominado de forma similar como "Limitação da Finalidade" (*Purpose Limitation*), insculpido em seu art. 5º, 1, "b"[49].

As orientações do Grupo de Trabalho do Artigo 29 (*Article 29 Working Party*), na *Opinion* 03/2013[50], ainda na vigência da Diretiva 95/46/CE, foram cruciais para a interpretação dos elementos formadores da *Purpose Limitation*, quais sejam, os termos "legítimo", "específico" e "explícito", conceitos também presentes na LGPD, como visto acima. Tal parecer foi acolhido pelo Conselho Europeu de Proteção de Dados (*European Data Protection Board* - EDPB)[51], que sucedeu ao Grupo do Artigo 29 com a entrada em vigor do RGPD.

---

[49]UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, 23 abr. 2016 (*General Data Protection Regulation*). **Intersoft Consulting.** Disponível em: https://gdpr-info.eu/art-5-gdpr/. Acesso em: 09 mar. 2020.

[50] Referido grupo de trabalho foi instituído pelo artigo 29º da Diretiva 95/46/CE. Trata-se um órgão consultivo europeu independente sobre proteção de dados e privacidade. Este parecer analisa o princípio da limitação de objetivos. pp. 15-19. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. Acesso em: 08 mar. 2020.

[51] O Regulamento Geral de Proteção de Dados (RGPD) estabelece que o EDPB é responsável por garantir a consistência da sua aplicação em toda a União Europeia. Para tanto, o EDPB está habilitado a emitir orientações sobre questões relativas à interpretação e aplicação do RGPD. pp. 5-6. Disponível em: <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_draft_guidelines-art_6-1-b final_public_consultation_version_en.pdf>. Acesso em 08 mar. 2020.

Conforme interpretação europeia, para ser legítimo, o processamento deverá sempre estar "de acordo com a lei" em sentido mais amplo. Isso compreende todas as formas de direito conhecidas, o que inclui os princípios constitucionais, jurisprudência e outros elementos, como costumes, códigos de conduta, códigos de ética, acordos contratuais e o contexto geral dos fatos do caso. A legitimidade de um determinado objetivo também pode mudar ao longo do tempo, dependendo de fatores científicos, desenvolvimento tecnológico e mudanças culturais na sociedade[52].

Já a especificidade será atendida se, antes ou durante a coleta de dados pessoais, as finalidades forem suficientemente definidas para permitir que a conformidade com a lei possa ser avaliada e delimitar o escopo do processamento. Por esses motivos, um objetivo vago ou geral, tais quais “melhorar experiência”, “fins de marketing”, “fins de segurança de TI” ou “pesquisa futura” dos usuários – sem maiores detalhes – geralmente não atendem aos critérios de ser "específico"[53].

Para serem explícitos, os objetivos não poderão conter imprecisão ou ambiguidade quanto ao seu significado ou intenção. Deverão ser expressos de modo a serem entendidos da mesma maneira, não apenas pelo controlador (incluindo toda a equipe) e quaisquer processadores de terceiros, mas também pela Autoridade de Proteção de Dados e titulares dos dados em questão, independentemente de suas origens culturais, linguísticas, nível de entendimento ou necessidades especiais[54].

No que diz respeito ao princípio da adequação, este encontra-se intrinsecamente ligado ao princípio da finalidade, pois se consubstancia na utilização dos dados de modo compatível com a finalidade previamente apresentada e consentida pelo proprietário das informações. Isso significa dizer que haverá a necessidade de solicitar uma nova autorização do titular sempre que a intenção original do controlador se transmutar.

Assim, para exemplificar, imagine-se um aplicativo que monitora os níveis de concentração de açúcar no sangue para ajudar pacientes com diabetes, recomendando o momento certo de tomar a medicação. Pela Lei, não poderá ser feita a venda dessas informações aos fornecedores de medicamentos voltados para esse público. A exploração comercial de

---

[52] *Article* 29. ***Opinion* 03/2013 *on purpose limitation*.** 02 de abril de 2013. p. 19-20. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>. Acesso em: 18 mar. 2020.

[53] *Ibidem*, p. 15-16.

[54] *Article* 29. ***Opinion* 03/2013 *on purpose limitation*.** 02 de abril de 2013. p. 17-19. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>. Acesso em: 18 mar. 2020.

dados relativos à saúde por terceiros não é compatível com o objetivo original de prestar assistência a pacientes com diabetes[55].

Em arremate, se os dados pessoais tiverem que ser utilizados para uma finalidade distinta daquela originalmente informada, será necessário obter um consentimento adicional, livre, informado e explícito dos usuários sobre o novo uso, sendo-lhe garantido o direito de revogar o consentimento, caso discorde das alterações. Em ambos os casos, o usuário deverá ser notificado sobre qualquer modificação na finalidade dos dados coletados[56].

O princípio da necessidade, por seu turno, reduz o universo das informações coletadas ao mínimo necessário para o cumprimento da finalidade pretendida, inclusive quando o tratamento for baseado no legítimo interesse do controlador, conforme previsto no art. 10, § 1º, da LGPD.

De forma semelhante ao regulamento europeu, a lei brasileira ainda prevê que o controlador, ao verificar que a finalidade foi alcançada ou que os dados deixaram de ser necessários ao alcance da finalidade específica almejada (art. 15, I), bem como diante de requerimento do titular (art. 18, VI), terá de eliminar os dados em razão do término do tratamento, ressalvadas as hipóteses previstas no art. 16, tais quais o cumprimento de obrigação legal ou regulatória, estudo por órgão de pesquisa, transferência a terceiro, desde que respeitados os requisitos de tratamento de dados, e para o uso exclusivo do controlador com a devida anonimização.

A não discriminação é um princípio reservado à proibição do tratamento com objetivos discriminatórios, ilícitos e abusivos, vinculados principalmente à classe dos dados sensíveis, mas também àquelas informações pessoais que, apesar de aparentemente triviais, a depender do tratamento que recebem, podem revelar aspectos íntimos do titular e passíveis de discriminação, como origem étnica, religião, orientação sexual e posição política.

Quanto ao princípio do livre acesso, poderá ser conceituado como o direito de requisição e acesso facilitado e gratuito do titular às informações sobre o tratamento de seus dados, tais como a forma e duração do tratamento, identificação do controlador e informações de contato, compartilhamento dos dados, entre outras (art. 9º).

O princípio da qualidade diz respeito a exigibilidade de que os dados deverão ser precisos e atualizados. Seu fundamento consiste no fato de que dados pessoais, ao serem

---

[55] UNIÃO EUROPEIA. *Draft Code of Conduct on privacy for mobile health applications* (“Projeto de código de conduta sobre privacidade para aplicativos móveis de saúde”). Publicado em 07.06.2016. pp. 07-08. Disponível em: file:///C:/Users/LeNovo/Downloads/CodeofConductfinaldraft.pdf. Acesso em: 10 mar. 2020.
[56] *Ibidem.*

colocados em conjunto e processados por meio de dispositivos notavelmente desenvolvidos, refletem a personalidade de seu titular e representam, perante terceiros, inúmeras características. Por consequência, qualquer inexatidão, seja por uma informação pessoal equivocada ou desatualizada, poderá impactar profundamente sua vida privada e relações sociais, ocasionando sérios danos ao indivíduo[57].

Portanto, existe, por um lado, o dever por parte das empresas de manter dados completos, exatos e atualizados e, por outro, o direito assegurado aos titulares de solicitar a correção de quaisquer informações incorretas a seu respeito. Nesse sentido, confira-se o inciso III do art. 18 da LGPD:

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: [...] III – correção de dados incompletos, inexatos ou desatualizados.

Há, ainda, a possibilidade de requerer a correção de equívocos ou revisão de decisões subsidiadas em procedimentos exclusivamente automatizados sobre seus dados, em semelhança à previsão já contida na Lei do Cadastro Positivo, citada anteriormente.

Outro princípio muito presente na LGPD é a transparência, porquanto sua observância se estende não só ao momento da coleta de informações, mas a toda a atividade de tratamento[58]. Os dados disponíveis à análise pelo titular não se restringem àqueles coletados, mas também os que foram transformados. Na LGPD, entre outros dispositivos, é encontrada no art. 10, § 2º e no art. 18, I, II, VII e VIII:

> Art. 10. [...] § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I – confirmação da existência de tratamento; II – acesso aos dados; [...] VII – informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII – informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

Em resumo, é perceptível o forte vínculo existente entre esses três últimos princípios, uma vez que a transparência se consubstancia no conhecimento de todo e qualquer conteúdo relativo ao titular e o livre acesso corresponde aos meios de se obter essas informações, ao passo

---

[57] VAINZOF, Rony. Capítulo I, disposições preliminares, art. 6º. *In*: MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (org.). **LGPD: Lei Geral de Proteção de Dados Comentada**. 2ª ed. São Paulo: Revista dos Tribunais, 2019. Não paginado. [Livro digital].

[58] OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria. Capítulo 2. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. Introdução. *In:* FRAZÃO, Ana *et al* (org.). **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** São Paulo: Thomson Reuters, 2019. Não paginado [livro digital].

que o princípio da qualidade significa o dever de a empresa manter dados corretos, bem como o direito do titular de corrigi-los em caso de equívoco[59].

Do mesmo modo, os princípios da segurança, da prevenção e da responsabilização ou prestação de contas caminham lado a lado, sendo representados na legislação, muitas vezes, por um mesmo dispositivo[60]. Isso se deve ao fato de que, pelo princípio da segurança, os agentes de tratamento devem utilizar medidas que objetivem, desde a fase de concepção do produto ou serviço (*privacy by design)* até a sua execução, impedir eventuais violações – dolosas ou acidentais –, de forma que os sistemas sejam estruturados para atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na LGPD e demais normas regulamentares.

Já a prevenção está ligada ao conjunto de procedimentos que deve ser adotado para prevenir situações de dano no decorrer do tratamento, incluindo o dever de o controlador comunicar, no menor prazo possível (art. 48, § 1º), não apenas à autoridade nacional, mas também ao titular, qualquer ocorrência de incidente de segurança que possa acarretar risco ou dano relevante ao titular, como tentativa de revertê-lo ou mitigá-lo[61].

Com efeito, o ato ilícito juntamente com a ocorrência do dano são conceitos próprios da responsabilidade. Os meios para estimular a responsabilidade podem ser proativos e reativos. No primeiro caso, devem garantir uma implementação eficaz de medidas de proteção de dados e meios suficientes de responsabilização dos agentes, juntamente com a prestação de contas. No segundo caso, podem envolver ações de responsabilidade civil e sanções, a fim de garantir que qualquer dano relevante seja compensado e que sejam tomadas medidas adequadas para corrigir erros ou irregularidades[62].

Não obstante, tendo em vista que o objetivo primaz do presente estudo é voltado para questões atinentes à responsabilidade civil dos agentes de tratamento conforme a Lei Geral de Proteção de Dados, este assunto será melhor abordado no decorrer do trabalho, com maior profundidade e em conjunto com os seus demais princípios e dispositivos, bem como em observância ao sistema nacional e internacional de proteção de dados.

---

[59] *Ibidem.*
[60] *Ibidem.*
[61] COTS, Márcio; OLIVEIRA, Ricardo. Da segurança e das boas práticas. Sessão I: Da segurança e do sigilo de dados, art. 48. *In:* **Lei Geral de Proteção de Dados Pessoais comentada.** 2ª ed. São Paulo: Revista dos Tribunais, 2019. Não paginado [livro digital].
[62] *Article* 29. ***Opinion* 1/2010 *on the concepts of "controller" and "processor".*** 16 de fevereiro de 2010. p. 05. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf. Acesso em: 18 mar. 2020.

3 A CLASSIFICAÇÃO DO TRATAMENTO IRREGULAR NA LGPD

À medida que é reforçado o entendimento de que os dados são, hoje, o recurso mais valioso do mundo[63], responsáveis pelo fomento de uma indústria lucrativa e de rápido crescimento, sendo imprescindíveis para os novos negócios, desponta, por outro lado, a preocupação quanto a superexposição daqueles que se valem dos recursos tecnológicos e, em contrapartida, cedem seus dados pessoais.

Tencionando coibir práticas danosas, a LGPD inovou ao trazer como destaque um sistema de responsabilidade civil dito especialíssimo[64], ressaltado nos artigos 42 a 45, cuja compreensão encontra-se diretamente ligada ao princípio da responsabilização e prestação de contas, delineado anteriormente no inciso X do art. 6º da lei, isto é, a "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". Nota-se, assim, a intenção do legislador de não se limitar a impor o ressarcimento do titular, mas, sobretudo, querer prevenir a ocorrência de ilícitos e danos.

A análise dessa responsabilidade civil, em consonância com a legislação protecionista internacional, deverá partir da soma de três pontos fundamentais, organizados de modo sistematizado: a) dano; b) violação da legislação de proteção dos dados por parte do controlador e/ou operador; e c) reparação. Dessa forma, fixa-se a premissa de que, ocorrendo um dano decorrente do descumprimento da LGPD e que tenha sido comprovadamente causado pela atividade do agente de tratamento de dados, parte-se, então, para a etapa final de ressarcimento da parte lesada[65].

Para a compreensão do que seria um descumprimento da LGPD capaz de gerar um dano ao titular e, consequentemente, a imputação da responsabilidade civil dos agentes de tratamento, o art. 44 da lei trouxe a importante definição de "tratamento irregular", conceituado como aquele que "deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar", considerando, para tanto, as circunstâncias presentes nos incisos, os

---

[63] THE ECONOMIST. *The world's most valuable resource is no longer oil, but data.* ***The Economist***, 06 maio 2017. Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em: 20 abr. 2020.

[64] MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. **Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD**. *In*: Cadernos Adenauer, volume 3, Ano XX, 2019. p. 126.

[65] *Ibidem*.

quais fazem uma adequada correlação entre a regularidade do tratamento e o avanço tecnológico de determinada época[66].

A partir dessa leitura, extrai-se que a violação da legislação de proteção de dados pessoais poderá ocorrer por duas formas: i) por meio de ilícitos específicos, representados pela inobservância de deveres expressamente previstos em lei para o tratamento de dados; e ii) mediante o cometimento de um ilícito geral, próprio desse sistema protetivo, compreendido como a falta ao dever de segurança que legitimamente se pode esperar[67].

Portanto, faz-se necessário adentrar nas particularidades dessas categorias de violação da LGPD sobre as quais se concentra maior risco de dano aos titulares. Por uma questão metodológica, inicia-se pelas hipóteses de inobservância da legislação que, em conjunto, formam a categoria dos ilícitos específicos, com enfoque nas questões com maior probabilidade de judicialização, tais como a exigência de bases legais para a legitimidade do tratamento, os direitos dos titulares e obrigações dos agentes de tratamento. Ao final deste capítulo, analisar-se-á o dever geral de segurança.

3.1 Os Deveres Específicos da LGPD

3.1.1 Autodeterminação e a bases legais legitimadoras do tratamento

Segundo lições de Bobbio, em função das inovações técnicas no campo da transmissão e difusão das informações e do possível abuso que se pode fazer dessas inovações, a esfera dos direitos do homem foi sendo modificada e ampliada[68], transcendendo a fase dos direitos de liberdade, ditos negativos, no sentido do não-impedimento ou de não sofrer interferência, para consagrar também os direitos positivos, marcados pela autonomia e participação ativa de seus proprietários[69]. Portanto, com a crescente e cada vez mais forte oposição ao tratamento desenfreado de dados pessoais, é reforçada a ideia de que os seus legítimos titulares devem ocupar um papel central na tarefa de limitar as informações que desejam, ou não, tornar públicas, com o escopo de exercer a tutela sobre sua privacidade.[70]

---

[66] BRUNO, Marcos Gomes da Silva. Capítulo VI, dos agentes de tratamento de dados pessoais, art. 44. *In*: MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (org.). **LGPD: Lei Geral de Proteção de Dados Comentada**. 2ª ed. São Paulo: Revista dos Tribunais, 2019. Não paginado. [Livro digital].

[67] DRESCH, Rafael. **A especial responsabilidade civil na Lei Geral de Proteção de Dados**. Migalhas. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/330019/a-especial-responsabilidade-civil-na-lei-geral-de-protecao-de-dados > Acesso em: 31 jul. 2020.

[68] BOBBIO, Norberto (traduzido por Carlos Nelson Coutinho). **A Era dos Direitos**. 8ª ed. Rio de Janeiro: Campus, 1992. P. 76-77.

[69] BOBBIO, Norberto (traduzido por Carlos Nelson Coutinho). *Op. cit***,** p. 32-33.

[70] BARRETO JUNIOR, Irineu Francisco; NASPOLINI, Samyra Haydêe Dal Farra. **Proteção de informações no mundo virtual: a LGPD e a determinação de consentimento do titular para tratamento de dados pessoais.** *In*: Cadernos Adenauer, volume 3, Ano XX, 2019. p. 142-143.

Nessa mesma linha de pensamento, Stefano Rodotá direciona sua abordagem para a evolução do direito à privacidade, cujo conceito passou daquela concepção original de ser deixado em paz para uma definição mais atualizada e ampla do *right of privacy,* sinalizando "o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada"[71], qualificado como o direito à autodeterminação informativa:

> No âmbito da União Européia, graças a diversas diretivas e suas transposições aos ordenamentos nacionais, nasceu um modelo diverso. O seu ponto de partida é representado pelo reconhecimento do direito à autodeterminação informativa, o que não significa simplesmente atribuir a cada um o poder de impedir determinados usos das informações a si relacionadas, segundo a ótica originária do direito a ser deixado só. Significa acima de tudo o poder de controlar, a cada momento, o uso que outros façam das minhas informações[72].

Reconhecendo sua relevância, a LGPD incorporou ao art. 2º, II, a autodeterminação informativa como um de seus fundamentos. A partir dessa ideia central, desenvolveram-se os seus elementos constitutivos, especialmente o consentimento do interessado e o seu direito de acesso a totalidade de informações a seu respeito, classificados como um poder difuso, que não necessita de mediações burocráticas, sendo exercido diretamente pelo titular face a todos os sujeitos, públicos e privados, que coletam dados pessoais[73].

Dessa forma, volta-se a atenção para a importância de fixar as balizas do tratamento de dados e estabelecer a legitimidade para tomada de medidas, visando criar uma atmosfera de confiança que atenda às legítimas expectativas dos usuários, especialmente quando são levados a abrir mão de suas informações pessoais em troca das aplicações e serviços[74].

Por essa razão, é requisito essencial e inafastável da lei a exigência de que o tratamento de dados somente poderá ser realizado se estiver amparado em uma base normativa que o autorize. Será legítimo somente aquele tratamento que atenda ao menos uma das 10 hipóteses autorizativas para o tratamento de dados pessoais, especificamente aquelas contidas no rol taxativo do art. 7º da LGPD, sendo possível a cumulação entre elas.

Ocupando posição de destaque no referido artigo, a primeira base legal diz respeito ao fornecimento de consentimento pelo titular (art. 7º, I), cujo conceito é extraído do inciso XII, do art. 5º da lei, compreendido como uma "manifestação livre, informada e inequívoca pela

---

[71] RODOTÀ, Stefano. (traduzido por: DONEDA, Danilo; MORAES, Maria Celina Bodin) **A Vida na Sociedade da Vigilância: A privacidade hoje.** Rio de Janeiro: Renovar, 2008. P. 109.
[72] *Ibidem*, p. 148.
[73] *Ibidem*, p. 148.
[74] BARRETO JUNIOR, Irineu Francisco; NASPOLINI, Samyra Haydêe Dal Farra. **Proteção de informações no mundo virtual: a LGPD e a determinação de consentimento do titular para tratamento de dados pessoais.** *In*: Cadernos Adenauer, volume 3, Ano XX, 2019. p. 142-143.

qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". Impende destacar que o Marco Civil da Internet (MCI), Lei 12.965 de 2014, buscando assegurar e garantir os direitos dos cidadãos no âmbito virtual, já havia determinado expressamente em seu art. 7º, IX, a necessidade do consentimento do usuário para "coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais".

Apesar de a LGPD não tecer maiores considerações acerca do que seria um consentimento "livre, informado e inequívoco", é possível compreender melhor seus elementos por meio da interpretação feita pelo *Article* 29, encontrada na *Guideline* 259/2017[75], que analisou a aplicação do consentimento no contexto do GDPR, sendo oportuna sua análise para fins de referência no cenário brasileiro.

Nesse quadro, será "livre" o consentimento que possibilita a escolha e o controle reais para os titulares dos dados. Em outras palavras, se o titular se sentir compelido a consentir ou sofrer consequências negativas se não consentir, tal consentimento não será válido. Da mesma forma, se o consentimento for agrupado como parte inegociável dos termos e condições, ou se o titular dos dados for incapaz de recusar ou retirar seu consentimento sem prejuízo, presume-se que não tenha sido concedido livremente[76].

Situação bastante comum é aquela no qual o titular, ao instalar aplicativos em seu aparelho, depara-se com termos de uso unilaterais, solicitando o acesso irrestrito a certas funcionalidades do dispositivo que não guardam relação com a finalidade buscada, sob pena de não permitir o acesso a produtos e serviços. Ou seja, o indivíduo vê-se diante de um "tudo ou nada"[77]. Seria o exemplo de um aplicativo de edição de fotos que solicita ao seu usuário o acesso a geolocalização para o uso dos serviços, bem como os informa que utilizará os dados coletados para fins de publicidade comportamental. Nesse contexto, nem a localização geográfica nem a publicidade comportamental *on-line* são necessárias ao correto funcionamento do aplicativo e vão além da entrega do serviço principal ofertado[78].

---

[75] UNIÃO EUROPEIA. *Guidelines on Consent under Regulation* 2016/679. Disponível em: http://portaldaprivacidade.com.br/wp-content/uploads/2017/12/wp29_consent-12-12-17.pdf. Acesso em 19 jul. 2020.

[76] *Ibidem*, p. 06.

[77] MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. **Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD**. *In*: Cadernos Adenauer, volume 3, Ano XX, 2019. p. 122-123.

[78] *Guidelines on Consent under Regulation* 2016/679. *Op. cit*., p. 07.

Sendo assim, corroborado pelo considerando 43[79] do GDPR, conclui-se que, se a execução de um contrato, incluindo a prestação de um serviço, estiver condicionada a autorização integral de acesso a um conjunto de dados, sobre os quais o titular não tenha poder de optar se, realmente, deseja ou não ter esses dados tratados quando não forem necessários ao propósito buscado, esse consentimento não poderá ser considerado livre.

Ademais, um serviço pode ainda envolver várias atividades de tratamento para mais de uma finalidade. Nesses casos, entra em cena a característica de "granularidade" do consentimento, ou seja, seguindo o que prescreve o considerando 32 do GDPR, quando o tratamento tem vários propósitos, o consentimento deve ser dado para todos eles. Outro ponto interessante é que o responsável pelo tratamento precisa demonstrar que é possível para o titular recusar ou retirar o consentimento sem prejuízo (considerando 42).

Dentre as questões elencadas na *Guideline* 259 sobre o tema, chama a atenção a que diz respeito ao "desequilibro de poder", em consequência da posição hierarquicamente superior do controlador em relação ao titular, percebida sobretudo, mas não somente, nas relações de emprego e no tratamento de dados exercido pelo poder público. Assim, nesses casos, poderá não existir alternativas realistas para o titular aceitar os termos de tratamento deste controlador ou negar seu consentimento sem experimentar o medo ou o risco real de efeitos prejudiciais como resultado de uma recusa. Portanto, em razão dessa natureza, guardadas as exceções, a base legal não pode e não deve ser o consentimento[80].

Já o consentimento informado está intimamente ligado ao princípio da transparência e preceitua que o titular dos dados realmente possa entender as atividades de tratamento em questão, de forma clara, inteligível e facilmente acessível[81], além de traduzida para o português, consoante prescrito no art. 224 do código civil. Assim, deverão ser fornecidas ao titular as informações elencadas nos incisos do art. 9º da LGPD, a exemplo da identificação do controlador, finalidade específica, forma e duração do tratamento e informações acerca do uso compartilhado de dados pelo controlador.

Quanto ao elemento "inequívoco", este exige que, conforme previsão do art. 8º da LGPD, caberá ao controlador lançar mão de meios idôneos para demonstrar que houve manifestação de vontade do titular, isto é, por meio de um "ato afirmativo claro"[82], sendo

---

[79] UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, 23 abr. 2016 (*General Data Protection Regulation*). *Recital* 43. **GDPR *Text***. Disponível em: <https://gdpr-text.com/pt/read/recital-43/ >. Acesso em: 21 jul. 2020.

[80] *Guidelines on Consent under Regulation* 2016/679. *Op. cit*., p. 6-7.

[81] *Guidelines on Consent under Regulation* 2016/679. *Op. cit*., p. 13.

[82] *Guidelines on Consent under Regulation* 2016/679. *Op. cit*., p. 16.

inválido, por exemplo, o uso de caixas de autorização pré-selecionadas, bem como não deve ser considerada como indicação ativa de escolha o silêncio ou inatividade por parte do titular dos dados.

No julgamento do Recurso Especial n.º 1.758.799, a Terceira Turma do Superior Tribunal de Justiça (STJ) decidiu, por unanimidade, que configura dano moral *in re ipsa* a ausência de comunicação acerca da disponibilização/comercialização de informações pessoais em bancos de dados do consumidor. A Corte Superior firmou esse entendimento ao negar provimento ao recurso de uma empresa gestora de dados, condenada a indenizar um consumidor em R$ 8.000,00 (oito mil reais) pela comercialização indevida de seus dados pessoais[83]. Foi utilizado o diálogo entre a Lei do cadastro positivo (Lei n.º 12.414/2011) e o Código de Defesa do Consumidor (Lei n.º 8.078/1990) para fundamentar a decisão que, embora seja anterior à vigência da LGPD, está em consonância com seus mandamentos. Confira-se trecho da ementa:

> RECURSO ESPECIAL. FUNDAMENTO NÃO IMPUGNADO. SÚM. 283/STF. AÇÃO DE COMPENSAÇÃO DE DANO MORAL. BANCO DE DADOS. COMPARTILHAMENTO DE INFORMAÇÕES PESSOAIS. DEVER DE INFORMAÇÃO. VIOLAÇÃO. DANO MORAL *IN RE IPSA*. JULGAMENTO: CPC/15. [...] 7. **A inobservância dos deveres associados ao tratamento (que inclui a coleta, o armazenamento e a transferência a terceiros) dos dados do consumidor – dentre os quais se inclui o dever de informar – faz nascer para este a pretensão de indenização pelos danos causados e a de fazer cessar, imediatamente, a ofensa aos direitos da personalidade.** 8. Em se tratando de compartilhamento das informações do consumidor pelos bancos de dados, prática essa autorizada pela Lei 12.414/2011 em seus arts. 4º, III, e 9º, deve ser observado o disposto no art. 5º, V, da Lei 12.414/2011, o qual prevê o direito do cadastrado ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais 9. O fato, por si só, de se tratarem de dados usualmente fornecidos pelos próprios consumidores quando da realização de qualquer compra no comércio, não afasta a responsabilidade do gestor do banco de dados, na medida em que, quando o consumidor o faz não está, implícita e automaticamente, autorizando o comerciante a divulgá-los no mercado; está apenas cumprindo as condições necessárias à concretização do respectivo negócio jurídico entabulado apenas entre as duas partes, confiando ao fornecedor a proteção de suas informações pessoais. 10. Do mesmo modo, o fato de alguém publicar em rede social uma informação de caráter pessoal não implica o consentimento, aos usuários que acessam o conteúdo, de utilização de seus dados para qualquer outra finalidade, ainda mais com fins lucrativos. 11. **Hipótese em que se configura o dano moral *in re ipsa*.** [...].
>
> STJ – REsp: 1758799 MG 2017 / 0006521-9, Relator: Ministra NANCY ANDRIGHI, Data de Julgamento: 12/11/2019, T3 – TERCEIRA TURMA, Data de Publicação: DJe 19/11//2019). (grifo nosso).

De forma semelhante, o Juízo da 13ª Vara Cível de São Paulo condenou a Cyrela, empresa do ramo imobiliário, a indenizar em R$ 10.000,00 (dez mil reais) um cliente que teve

[83] CONJUR. Banco de dados deve notificar compartilhamento de informações. **Conjur,** 26 fev. 2020. Disponível em: https://www.conjur.com.br/2020-fev-26/banco-dados-notificar-compartilhamento-informacoes. Acesso em: 05 out. 2020.

informações pessoais compartilhadas com outras empresas sem o seu consentimento. O autor comprou um apartamento em novembro de 2018 e, no mesmo ano, passou a ser assediado por instituições financeiras e firmas de decoração que citavam sua recente aquisição com a parte ré. A magistrada Tonia Yuka Koroku entendeu pela configuração do dano moral *in re ipsa*, utilizando-se, por meio do diálogo das fontes, de dispositivos da LGPD, do Código de Defesa do Consumidor e da Constituição Federal[84].

Portanto, será necessário que, na prática, seja garantido ao usuário o acesso a bens, serviços e facilidades tecnológicas imprescindíveis à vida moderna sem exigir, em contrapartida, a renúncia pelo titular de todo e qualquer dado pessoal, sob pena de a autodeterminação informativa fazer-se inócua, indicando um dos principais desafios a serem enfrentados pela LGPD[85] e que motivará inúmeras demandas no judiciário brasileiro.

Não obstante a importância do consentimento como meio de manifestação da vontade do titular, não se pode perder de vista a existência de outras bases autorizativas que, de forma semelhante, atendem a legitimidade do tratamento. Em síntese, também será legítimo o tratamento nas hipóteses de cumprimento de obrigação legal ou regulatória pelo controlador (art. 7º, II), para a execução de políticas públicas (art. 7º, III), para a realização de estudos por órgão de pesquisa (art. 7º, IV), quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular (art. 7º, V), para o exercício regular de direitos em processo judicial, administrativo ou arbitral (art. 7º, VI), para a proteção da vida ou da incolumidade física do titular ou de terceiro (art. 7º, VII), para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (art. 7º, VIII), quando necessário para atender aos interesses legítimos do controlador ou de terceiro (art. 7º, IX) e para a proteção do crédito (art. 7º, X).

Dentre essas demais bases, merece atenção a hipótese legal do legítimo interesse do controlador, termo jurídico com alto grau de subjetividade e bastante controvertido na LGPD. Apresenta-se como exceção à regra geral do consentimento, sendo a opção a ser utilizada quando se constatar que todas as outras bases legais não são adequadas ao contexto e desde que presentes os requisitos. Seu escopo de aplicação está delineado em rol meramente exemplificativo nos incisos I e II, art. 10, da LGPD, *ipsis litteris*:

---

[84] ANGELO, Tiago. Decisão pioneira: Juíza aplica LGPD e condena construtora que não protegeu dados de cliente. Revista **Consultor Jurídico**, 2020. Disponível em: https://www.conjur.com.br/2020-set-30/compartilhar-dados-consumidor-terceiros-gera-indenizacao. Acesso em: 06 out. 2020.

[85] MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. **Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD**. *In*: Cadernos Adenauer, volume 3, Ano XX, 2019. p. 122-145.

> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
> I - apoio e promoção de atividades do controlador; e
> II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

Inclui-se, aqui, o tratamento no qual, após coletados os dados, é conferido um uso adicional a eles pelo controlador sem se buscar um novo consentimento do titular. Contudo, conforme ensina Bruno Bioni, "tal hipótese não se dá no vácuo, mas dentro da dinâmica de regra geral em que há uma relação pré-estabelecida na qual o titular consentiu para um uso específico ou para uma finalidade determinada de seus dados"[86]. Logo, a legitimidade dessa medida é avaliada pela correspondência entre o novo propósito e aquele que originou a coleta dos dados pessoais, exigindo-se uma análise contextual da relação, para averiguar se o proveito secundário está em consonância com as legítimas expectativas do titular.

Por ser um termo em formação, competirá especialmente a Autoridade Nacional de Proteção de Dados (ANPD) e ao Poder Judiciário compreendê-lo no caso concreto. No entanto, o Parecer 06/2014[87] sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados, elaborado pelo *Working Party* 29, trouxe exemplos de alguns objetivos que podem constituir um interesse legítimo, destacando-se: a) prevenção de fraudes; b) garantia da segurança da rede e da informação; c) indicação de possíveis atos criminosos ou ameaças à segurança pública; d) processamento de dados de funcionários ou clientes; e e) transferências administrativas dentro de um grupo de empresas.

Ademais, o mesmo documento propõe a utilização de um teste: o *legitimate interest assessment* (LIA). Nele são apontadas quatro etapas que devem ser seguidas, visando garantir o preenchimento do requisito do legítimo interesse, são elas: (i) avaliação dos interesses legítimos; (ii) impacto sobre o titular do dado; (iii) equilíbrio entre os interesses legítimos do controlador e o impacto sobre o titular; e (iv) salvaguardas desenvolvidas para proteger o titular dos dados e evitar qualquer impacto indesejado[88].

---

[86] BIONI, Bruno. **Xequemate**, o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. São Paulo: GPOPAI USP, 2015. p. 49. Disponível em: https://www.academia.edu/28752561/Xeque-Mate_o_trip%C3%A9_de_prote%C3%A7%C3%A3o_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil. Acesso em: 19 mar. 2020.

[87] Grupo de trabalho do artigo 29.º para a proteção de dados. Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva 95/46/CE. Adotado em 9 de abril de 2014. Disponível em: <https://ec.europa.eu/justice/article29/documentation/opinion-recommendation/files/2014/wp217_pt.pdf >acesso em 28 jul. 2020.

[88] BUCAR, Daniel; VIOLA, Mario. Tratamento de dados pessoais por "legítimo interesse do controlador": primeiras questões e apontamentos. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. Editora Revista dos Tribunais, 2019. Não paginado [livro digital].

O fato é que, embora a amplitude desse conceito tenha a função de abranger diversas situações necessárias para o desenvolvimento econômico e da inovação no país, uma vez que simples funções administrativas se tornariam inexequíveis se dependentes de um consentimento do titular, é latente a possibilidade de que, na prática, ela possa ser utilizada como instrumento legitimador em qualquer circunstância[89]. Nesse sentido, Bruno Bioni reforça a importância do consentimento como regra geral a ser efetivada por meio do que ele chama de sistema de "freios e contrapesos":

> A hipótese de interesses legítimos deve ser desenhada de forma cuidadosa para que o consentimento permaneça sendo a regra geral da dinâmica da proteção dos dados pessoais, sob pena de tornar, de forma incoerente, artificial a mencionada adjetivação a ele empregada.
> [...]
> Sob o ponto de vista de coerência normativa centrada na regra geral do consentimento e da autodeterminação informacional, um sistema de freios e contrapesos mais rígido acaba por não esvaziar a promessa de que o cidadão deve exercer controle sobre seus dados pessoais.[90]

Portanto, no caso concreto, será necessário fazer uma ponderação entre os interesses legítimos do controlador e os direitos e liberdades fundamentais do titular dos dados[91]. Ademais, de acordo com a LGPD, somente os dados estritamente necessários poderão ser tratados (art. 10, §1º) e, sempre que possível, deverão ser anonimizados, bem como exige-se dos agentes de tratamento o dever de transparência (art. 10, §2º) e de registro das operações de tratamento (art. 37).

3.1.2 Direitos do titular, princípios e obrigações dos agentes de tratamento

A LGPD para além de traçar diretrizes para o tratamento de dados pessoais de forma direcionada aos operadores e controladores, também relaciona os direitos dos titulares em seus artigos 17 a 22. Entretanto, nota-se que antes mesmo de concentrar-se no capítulo reservado aos direitos do titular, referida lei já havia delineado um robusto conjunto de direitos e garantias, o qual, em consonância com os princípios, precisa ser considerado de forma sistematizada para se compreender a real extensão do Capítulo III[92]. Esses direitos estão listados, principalmente, no art. 18 da LGPD:

---

[89] CARNEIRO, Isabelle *et al*. Tratamento de dados pessoais. 1.4. Legítimo interesse do controlador. *In:* FEIGELSON, Bruno *et al* (org.). **Comentários à Lei Geral de Proteção de Dados – Lei 13.709/2018.** São Paulo: Revista dos Tribunais, 2019. Não paginado [livro digital].

[90] BIONI, Bruno. **Xequemate**, o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. São Paulo: GPOPAI USP, 2015. p. 50. Disponível em: https://www.academia.edu/28752561/Xeque-Mate_o_trip%C3%A9_de_prote%C3%A7%C3%A3o_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil. Acesso em: 19 mar. 2020.

[91] CARNEIRO, Isabelle *et al*. *Op. cit*.

[92] FRAZÃO, Ana. **Nova LGPD: direitos dos titulares de dados pessoais.** A 9ª parte de uma série sobre as repercussões para a atividade empresarial. JOTA. 24/10/2018. Disponível em: <https://www.jota.info/opiniao-e-

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> I - confirmação da existência de tratamento;
> II - acesso aos dados;
> III - correção de dados incompletos, inexatos ou desatualizados;
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
> VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
> VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

Diante disso, constata-se que praticamente todos os direitos elencados, exceto a portabilidade, já haviam sido abordados e conceituados indiretamente, muitos deles extraídos a partir dos princípios inseridos no art. 6º da LGPD, especialmente os princípios do livre acesso, da qualidade dos dados e da transparência, razão pela qual predomina neste art. 18 a sua função sistematizadora[93].

Segundo as diversas legislações nacionais e tratados internacionais, os direitos mais básicos atribuídos ao titular dos dados para o controle do fluxo de suas informações pessoais são classificados pela sigla "ARCO", referente à abreviação dos direitos de: i) acesso – o titular deve possuir livre acesso aos seus dados; ii) retificação – o poder de corrigir dados equivocados ou desatualizados; iii) cancelamento – possibilidade de revogar o consentimento ou eliminar dados indevidamente armazenados; e iv) oposição – direito de se opor ao tratamento quando realizado em desconformidade com a LGPD[94].

Outros direitos importantes são aqueles concedidos ao titular que teve seus dados submetidos a decisões tomadas unicamente com base em tratamento automatizado, consoante previsão do art. 20 da LGPD, pelo qual revelam-se ao menos três direitos do titular: direito à revisão em procedimentos decisórios automatizados (*caput*), direito à explicação (§ 1º), e direito à auditoria pela autoridade para verificação de aspectos discriminatórios face ao titular[95]. Mais uma vez é constatada a influência de princípios, tais como a transparência e não discriminação.

---

analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-direitos-dos-titulares-de-dados-pessoais-24102018#sdfootnote1sym> . Acesso em: 29 jul. 2020.

[93] *Ibidem.*

[94] MENDES, Laura Schertel. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. **Caderno Especial LGPD**. p. 35-56. São Paulo: Revista dos Tribunais, novembro 2019.

[95] MENDES, Laura Schertel. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. **Caderno Especial LGPD**. p. 35-56. São Paulo: Revista dos Tribunais, novembro 2019.

É preciso mencionar, ainda, as obrigações fixadas para todos aqueles que participam das atividades de tratamento, a exemplo da obrigação do controlador de instituir um encarregado pelo tratamento de dados (art. 41) e a manutenção do registro das operações pelos agentes de tratamento (art. 37), principalmente quando amparado no legítimo interesse.

Por fim, é valido salientar a importância de atender aos princípios defendidos pela LGPD em qualquer fase do processo de tratamento de dados, de forma a garantir que a relação entre titular e agentes de tratamento seja sempre pautada por princípios como a boa-fé objetiva, a finalidade e a necessidade.

3.2 O Dever Geral de Segurança

A respeito do ilícito geral na LGPD, é possível compreendê-lo buscando sua similitude com a disciplina adotada no Código de Defesa do Consumidor (CDC), porquanto o tratamento irregular, pela falta ao dever de segurança, adquire, no contexto da legislação consumerista, os mesmos contornos do defeito do produto ou serviço, ensejador da responsabilidade pelo fato do serviço. Sobre o assunto, Rafael de Freitas Valle Dresch elucida:

> No direito do consumidor o dever geral de segurança está fundado no elemento defeito, pois o produto ou serviço é considerado defeituoso e, assim, ensejador da responsabilidade civil do fornecedor, quando não oferece a segurança que legitimamente se pode esperar. Do mesmo modo, mantendo a coerência sistemática, o tratamento irregular previsto no art. 44 da LGPD ocorre quando da quebra de legítimas expectativas quanto à segurança dos processos de tratamento de dados. Poderia se falar, por conseguinte, de um defeito no tratamento de dados pessoais ou, caso se queira manter a nomenclatura da própria LGPD, de um tratamento irregular[96].

À vista disso, a LGPD prevê que os agentes de tratamento devem implementar medidas técnicas e procedimentos organizacionais aptos a garantir a segurança adequada aos dados pessoais, incluindo a proteção contra tratamento não autorizado ou ilegal, sob pena de serem responsabilizados pelos danos decorrentes dessas violações.

Assim, para garantir um nível de segurança compatível ao risco representado pelos dados pessoais em decorrência do tratamento, controlador e operador devem levar em consideração a natureza das informações tratadas, as características específicas do tratamento, o estado atual da tecnologia, custo e tempo necessários, bem como a probabilidade e magnitude dos riscos aos direitos dos titulares.

Para além disso, o controlador deverá comunicar à autoridade nacional e ao titular, em prazo razoável, a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (art. 48). Para isso, a LGPD requer todo aparato tecnológico e

---

[96] DRESCH, Rafael. **A especial responsabilidade civil na Lei Geral de Proteção de Dados**. Migalhas. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/330019/a-especial-responsabilidade-civil-na-lei-geral-de-protecao-de-dados > Acesso em: 31 jul. 2020.

procedimentos organizacionais para que se possa detectar, rapidamente, se houve uma violação de dados, questão essa determinante para saber se haverá o dever de notificação envolvido.

Portanto, um elemento-chave de qualquer política de segurança de dados é poder, sempre que possível, impedir uma violação e, quando ocorrer, reagir a ela em tempo hábil. Mas, primeiramente, é necessário compreender o que seria uma violação de dados pessoais.

O regulamento europeu, em seu rol de definições do art. 4º (12), define, expressamente, que uma violação de dados pessoais (*personal data breach)* significa uma violação da segurança que leva à destruição, perda, alteração, divulgação não autorizada ou acidental ou ilegal de dados pessoais transmitidos, armazenados ou processados de outra forma.

Por outro lado, observa-se curiosamente que na LGPD não há um conceito taxativo do que seria uma violação de dados pessoais. Porém, extrai-se essa definição a partir de alguns artigos específicos. No primeiro deles, ao tratar sobre o princípio da segurança no art. 6º, VII, o legislador antecipa o contorno geral daquilo que, em um segundo momento, seria melhor definido como um dever dos agentes de tratamento, no capítulo destinado à "segurança e boas práticas", mais especificamente no art. 46 da lei, assim disposto:

> 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.

A princípio, cabe salientar que, longe de ser uma mera faculdade, o verbo "devem" indica uma obrigação legal, cujo não cumprimento poderá acarretar a aplicação de sanções administrativas e responsabilidade civil[97], sendo esta última o objeto de estudo do presente trabalho. Nesse aspecto, é imprescindível analisar pormenorizadamente o sentido de cada um dos termos utilizados no dispositivo supracitado, de modo a extrair a interpretação mais adequada e justa do que seria uma violação de dados para a LGPD.

Primeiramente, quanto as medidas de segurança a serem adotadas, compreende-se, no entendimento do legislador, que tais mecanismos têm natureza híbrida, uma vez que contemplariam medidas técnicas e administrativas[98].

Sobre as medidas técnicas, Camilla do Vale Jimene conceitua que "são aquelas adotadas no âmbito da Tecnologia da Informação, com o uso de recursos informáticos dotados de

---

[97]COTS, Márcio; OLIVEIRA, Ricardo. Da segurança e das boas práticas. Sessão I: Da segurança e do sigilo de dados, art. 46. *In*: **Lei Geral de Proteção de Dados Pessoais comentada.** 2ª ed. São Paulo: Revista dos Tribunais, 2019. Não paginado [livro digital].

[98]JIMENE, Camilla do Vale. Capítulo VII, da segurança e das boas práticas, art. 46. *In*: MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (org.). **LGPD: Lei Geral de Proteção de Dados Comentada**. 2ª ed. São Paulo: Revista dos Tribunais, 2019. Não paginado. [Livro digital].

funcionalidades voltadas à garantia da segurança da informação"[99]. A autora traz como exemplos as ferramentas de autenticação de acesso a sistemas, os métodos de segurança em *softwares* e *hardwares*, os recursos de controle de tráfego de dados em rede, os meios para detectar invasões de sistemas, a criptografia, a segregação de servidores, os dispositivos de prevenção à perda de dados, os testes de vulnerabilidade, as cópias de segurança, dentre outros.

Por seu turno, as medidas administrativas são os procedimentos executados no campo administrativo-gerencial dos agentes de tratamento, inclusive de ordem jurídica, tais como as políticas de privacidade de *sites* e aplicativos, a capacitação dos profissionais envolvidos no tratamento, políticas corporativas de proteção dos dados pessoais, contratos de confidencialidade e o controle de acesso aos arquivos de armazenamento de dados[100].

Portanto, todo esse aparato técnico e organizacional tem como função precípua evitar, justamente, que ocorram quaisquer das hipóteses de violação de dados previstas na lei, sejam elas cometidas por acidente (negligência, imperícia ou imprudência) ou intencionalmente (dolo), tais como os acessos não autorizados, as situações de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Em síntese, são três os pilares que fundamentam a matéria da segurança da informação, formando o objeto da LGPD: i) confidencialidade; ii) disponibilidade; e iii) integridade.

O *Computer Fraud and Abuse Act* (CFAA)[101], ao tutelar a defesa de sistemas de computadores estatais norte-americanos, descreve que um "acesso indevido" compreende não apenas uma invasão por parte de pessoas de fora do sistema que ganham acesso sem permissão dos agentes de tratamento, a exemplo do que faz um *hacker*, mas também daqueles que, já dentro do sistema e possuindo autorização para ingressar em parte dele, aproveitam-se das credenciais de acesso de um outro funcionário, para adentrar em área restrita, que lhe era defesa[102].

Nesse ponto, vale recordar o episódio de violação de dados ocorrido no Centro Hospitalar Barreiro-Montijo, multado em 400 mil euros por permitir acessos indevidos a processos clínicos por profissionais não autorizados. Segundo a Comissão Nacional de Proteção de Dados portuguesa - CNPD, apesar de o quadro do hospital contar apenas com 296 médicos,

---

[99] *Ibidem.*
[100] *Ibidem.*
[101] A "Lei de Fraude e Abuso de Computador" - *Computer Fraud and Abuse Act* (CFAA) foi um ato do Congresso dos Estados Unidos em 1986 para tratar de revisão elaborada das leis criminais a respeito de crimes cometidos com auxílio de computador, visando regulamentar o seu uso e definir o que são e como julgar ações tomadas na rede de computadores.
[102] ESTADOS UNIDOS. *18 U.S. Code § 1030 - Fraud and related activity in connection with computers.* ***Legal Information Institute*** **[LII].** Disponível em: https://www.law.cornell.edu/uscode/text/18/1030. Acesso em: 01 maio 2020

havia 985 profissionais com contas ativas que davam acesso aos ficheiros clínicos, grande parte relacionada a médicos que não trabalhavam mais no hospital, além de profissionais com funções na área técnica com possibilidade de acesso que deveria ser de exclusividade dos médicos[103].

Por outro lado, ocorrerá a "comunicação" indevida ou ilícita de dados quando informações que não deveriam ser públicas são disponibilizadas, expostas, difundidas ou transmitidas a terceiros, a exemplo da ocorrência de um ataque cibernético a um mercado *on-line* no qual nomes de usuário, senhas e histórico de compras são publicados na *web* pelo invasor[104].

Nesses dois casos, o propósito da lei em evitar o acesso e a comunicação não autorizados é prezar pela confidencialidade dos dados pessoais, de modo que sejam conhecidos apenas por aqueles que podem conhecê-los.

Em sequência, o que se entende por "destruição", conforme consignado pelo *Article 29 Working Party* nas "*Guidelines on Personal data breach notification under Regulation* 2016/679"[105], de 03 de outubro de 2017, diz respeito aos dados que não existem mais ou não existem de uma forma que sejam úteis ao controlador, ao passo que "perda" de dados pessoais deve ser interpretado como os dados que ainda podem existir, mas o controlador perdeu o comando ou acesso a eles, ou não os possui mais[106]. Interpreta-se, então, que a intenção da lei é assegurar a disponibilidade dos dados pessoais sempre que necessários.

Quanto ao conceito de "alteração" de dados, pode-se dizer tratar da "hipótese de modificação do dado pessoal por pessoas não autorizadas ou modificação indevida realizada por pessoas autorizadas"[107], de modo que sejam adulterados, corrompidos ou tornem-se incompletos, de modo acidental ou visando ao cometimento de fraudes contra o titular. Assim, por meio da aplicação da lei, busca-se garantir a integridade da informação e, consequentemente, elevar ao máximo o seu grau de confiabilidade.

---

[103] SÉNECA, Hugo. CNPD: Hospital do Barreiro multado em 400 mil euros por permitir acessos indevidos a processos clínicos. **Exame Informática**, 19 de outubro de 2018. Disponível em: <https://visao.sapo.pt/exameinformatica/noticias-ei/mercados/2018-10-19-cnpd-hospital-do-barreiro-multado-em-400-mil-euros-por-permitir-acessos-indevidos-a-processos-clinicos/>. Acesso em: 02 ago. 2020.

[104] UNIÃO EUROPEIA. *Guidelines on Personal data breach notification under Regulation 2016/679.* ***European Commission***. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052. Acesso em: 18 maio 2020.

[105] Tradução nossa: Diretrizes sobre a notificação de violação de dados pessoais nos termos do Regulamento 2016/679.

[106] *Guidelines on Personal data breach notification under Regulation 2016/679. Op. cit.*

[107] JIMENE, Camilla do Vale. Capítulo VII, da segurança e das boas práticas, art. 46. *In*: MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (org.). **LGPD: Lei Geral de Proteção de Dados Comentada**. 2ª ed. São Paulo: Revista dos Tribunais, 2019. Não paginado. [Livro digital].

Dentre os principais problemas que envolvem qualquer situação relacionada a uma violação de dados, há também o dano à reputação da empresa, decorrente da não execução de um trabalho preventivo ou de gerenciamento de crise para mitigação de risco ou dano, tal como ocorreu em novembro de 2016, quando a Uber, em decorrência de um acesso indevido a dados pessoais de 57 milhões de contas da sua plataforma, incluindo 600.000 números de carteira de motorista, pagou aos *hackers* a quantia de US$ 100.000 para que destruíssem os dados roubados, optando por não denunciar o assunto às vítimas ou autoridades. A decisão da Uber, revelada mais de um ano após a invasão da empresa, foi taxada como uma "flagrante violação da confiança do público", segundo afirmou o procurador-geral da Califórnia, Xavier Becerra. Além da repercussão negativa, a empresa foi condenada a pagar US$ 148 milhões por não ter divulgado às autoridades reguladoras no momento em que foi descoberto, sendo considerado um dos maiores constrangimentos legais sofridos pela empresa[108].

Ademais, a respeito da mitigação de riscos nas atividades de processamento de dados, esta poderá ser obtida por meio de técnicas como a "pseudonimização" de dados pessoais que, apesar de não tornar o dado anônimo, pode obstaculizar a identificação do titular, e a "anonimização", compreendida como a "retirada de vínculo da informação com a pessoa a qual se refere"[109], motivo pelo qual a LGPD entendeu pela desnecessidade de incluir os dados anonimizados em sua proteção normativa, consoante determinação do art. 12 da lei.

Contudo, significativos estudos promovidos nas últimas duas décadas, no campo da ciência da computação, a exemplo das pesquisas realizadas por Latanya Sweeney[110], Arvind Narayanan e Vitaly Shmatikov[111], revelaram graves falhas em técnicas de anonimização de dados consideradas seguras até então. Por efeito, esses resultados afastaram a ideia de uma anonimização resistente, fazendo com que, hoje em dia, haja o reconhecimento de que sempre haverá fatores de risco de identificação ou reidentificação de titulares.

---

[108] SOMERVILLE, Heather. *Uber to pay $148 million to settle data breach cover-up with U.S. states.* **Discovery Thomson Reuters**, 26 de setembro de 2018. Disponível em: https://www.reuters.com/article/us-uber-databreach/uber-settles-for-148-million-with-50-us-states-over-2016-data-breach-idUSKCN1M62AJ. Acesso em: 02 abr. 2020.

[109] DONEDA, Danilo. Cap. 2 Privacidade e Informação; 2 Classificação. *In:* **Da privacidade à proteção de dados pessoais:** Fundamentos da lei geral de proteção. 2ª ed. São Paulo: Revista dos Tribunais. 2020. Não paginado [livro digital].

[110] Para mais informações sobre este estudo, vide: SWEENEY, Latanya. ***Simple Demographics Often Identify People Uniquely***. Carnegie Mellon University, DataPrivacy Working Paper 3. Pittsburgh 2000. Disponível em: https://dataprivacylab.org/projects/identifiability/paper1.pdf. Acesso em: 06 out. 2020.

[111]Para mais informações sobre este estudo, vide: NARAYANAN, Arvind; SHMATIKOV, Vitaly. ***Robust De-anonymization of Large Sparse Datasets***. Universidade do Texas em Austin, 2008. Disponível em: https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf. Acesso em 06 out. 2020.

Entre dezenas de diferentes técnicas de anonimização[112], Paul Ohm elege um subconjunto importante e usual delas, denominado por ele como "Liberação e Esquecimento" (*release-and-forget*), tecendo uma análise crítica a seu respeito. Com essa técnica, o controlador realiza algumas modificações nos dados, por meio da retirada de certos identificadores e os libera – publicamente, em particular para terceiros ou internamente dentro de sua própria organização – e então o esquece, ou seja, não há mais a tentativa de rastreio, por parte daquele, do que acontece com os registros após o lançamento. A concentração de interesse de Ohm no estudo dessa técnica se justifica por dois motivos, quais sejam, a promessa de privacidade ao titular enquanto permite ampla divulgação de dados anônimos sem compromisso, e os riscos de falha.

Paul Ohm explica que o problema da reidentificação surge a partir da possibilidade de se realizar uma sequência de vinculações (*linkability*) entre bancos de dados anônimos, os quais, isoladamente, funcionam como elos intermediários na formação de uma cadeia de inferências que busca por informações correspondentes, visando conectar a pessoa ao fato[113]. Assim, toda reidentificação bem sucedida, mesmo aquela na qual são revelados dados aparentemente sem sentido, como classificações de filmes, poderá ajudar a desbloquear outros bancos de dados anônimos, aproximando-se daquilo que o autor denomina "bancos de dados de ruína" – segredos e informações sigilosas que um inimigo poderia usar para causar um grande dano ao seu titular[114].

A crítica de Ohm é no sentido de que, face a atual regulamentação de privacidade, tende-se a manter a responsabilidade dos controladores, após anonimização, somente em dois casos: i) quando a reversibilidade do banco de dados anônimos, para poder identificar o titular, demande menor grau de entropia, ou seja, menos esforço para ligação de dados; e ii) diante da ocorrência do fato danoso. Nessa perspectiva, a defesa do autor volta-se para a necessidade de regular com antecedência os dados intermediários, que se encontram no meio desses dois extremos, pois a esperança de regular o fato somente após concretizado o dano seria o mesmo que não regular nada[115].

---

[112]Paul Ohm cita outros meios de tornar os dados mais anônimos, os quais incluem: liberar apenas estatísticas agregadas; técnicas interativas, nas quais os administradores respondem perguntas direcionadas em nome dos pesquisadores; liberação de dados em sua totalidade; e técnicas de "privacidade diferencial", que protegem a privacidade adicionando ruído cuidadosamente calibrado para os dados. OHM, Paul. ***Broken promises of privacy: responding to the surprising failure of anonymization***. In: UCLA *Law Review*, [s. l.], v. 57, n. 6, p. 1701–1777, 2010, p. 1711.

[113] OHM, Paul. ***Broken promises of privacy: responding to the surprising failure of anonymization***. In: UCLA *Law Review*, [s. l.], v. 57, n. 6, p. 1701–1777, 2010, p. 1746.

[114] OHM, Paul. ***Broken promises of privacy: responding to the surprising failure of anonymization***. In: UCLA *Law Review*, [s. l.], v. 57, n. 6, p. 1701–1777, 2010, p. 1705.

[115] *Ibidem*, p. 1750.

Portanto, é válida a reflexão sobre a viabilidade de tutelar de alguma forma os dados anonimizados, ante os riscos de dano que a quebra de um anonimato poderá causar. Todavia, em que pesem as consequências do modelo *release-and-forget*, a escolha legislativa para proteger dados desvinculados de seu titular ainda parece algo distante[116].

Fixadas as premissas, reitera-se a importância de se ter em mente que a segurança é apenas um dos princípios instituídos no art. 6º da LGPD para orientar as atividades de tratamento de dados pessoais, devendo estar sempre em diálogo com os outros princípios para que, de forma conjunta, atendam integralmente aos objetivos da lei.

[116] EHRHARDT JR, Marcos; PEIXOTO, Erick. **Os desafios da compreensão do direito à privacidade no sistema jurídico brasileiro em face das novas tecnologias.** *In:* RJLB. Pp. 389-418, ano 6 (2020), nº 2. p. 414.

4. O SISTEMA DE RESPONSABILIDADE CIVIL DA LGPD

4.1 A Natureza da Imputação da Responsabilidade

4.1.1 O dano na Lei Geral da Proteção de Dados

Conforme já visto, o tratamento irregular de dados pessoais poderá resultar em danos de elevada proporção e a um grande número de pessoas, restando às vítimas buscarem guarida judicial. A Lei Geral de Proteção de Dados (LGPD), em matéria de responsabilidade civil, definiu as modalidades de danos indenizáveis em razão do exercício da atividade de tratamento de dados, tais quais o dano patrimonial, moral, individual ou coletivo (art. 42, *caput*).

Sabe-se que o dano patrimonial compreende os danos emergentes (aquilo que efetivamente se perdeu) e lucros cessantes (aquilo que deixou de lucrar). Do mesmo modo, a legislação menciona o dano moral, entendido pela doutrina e jurisprudência pátrias não somente em sua concepção original mais restrita, isto é, pela ocorrência expressiva e anormal de angústia, dor, sofrimento, tristeza ou humilhação à vítima, mas também pela ofensa a direitos personalíssimos, como a liberdade, a honra, a atividade profissional, a reputação, as manifestações culturais e intelectuais[117], nos quais prescinde a prova da dor[118].

Há, ainda, a possibilidade de que os efeitos de incidentes nas atividades de tratamento de dados irradiem para uma coletividade de pessoas simultaneamente, causando pequenas lesões, razão pela qual é assegurado na LGPD a tutela do dano coletivo, seja ele de cunho patrimonial ou extrapatrimonial.

Cogita-se, até mesmo, a possibilidade de aplicação da noção do dano estético associado ao perfil digital, ou seja, o corpo eletrônico como vítima de ofensas, de modo a desfigurar a forma pela qual os indivíduos se apresentam e são identificados no mundo virtual, importando em "ranqueamento desfavorável do usuário, em prejuízo de sua aparência binária"[119].

A partir disso, é importante ter em mente que ações judiciais de reparação em virtude de incidentes de segurança, envolvendo dados pessoais, serão cada vez mais comuns, a exemplo de falhas técnicas que permitam o acesso indevido a banco de dados[120], vazamentos de

---

[117] MORAES, Maria Celina Bodin. **Dano à Pessoa Humana: uma leitura Civil-Constitucional dos danos morais.** São Paulo: Renovar, 2003, p. 157/158.

[118] Enunciado 445, da V Jornada de Direito Civil do Conselho da Justiça Federal, de 2012: "O dano moral indenizável não pressupõe necessariamente a verificação de sentimentos humanos desagradáveis como dor ou sofrimento".

[119] Sobre o tema, vide: COLOMBO, Cristiano; FACCHINI NETO, Eugênio. **"Corpo Elettronico" como vítima de ofensas em matéria de tratamento de dados pessoais: reflexões acerca da responsabilidade civil por danos à luz da Lei Geral de Proteção de Dados pessoais brasileira e a viabilidade da aplicação da noção de dano estético ao mundo digital.** *In*: ROSENVALD, Nelson; DRESCH, Rafael de Freitas Valle; WESENDONCK, Tula (coord.). Responsabilidade civil: novos riscos. Indaiatuba: Foco, 2019. p. 45-64.

[120] GLOBO. *Site* brasileiro de classificados de empregos revela que invasores tiveram acesso indevido a banco de dados. **Globo.com**. Disponível em: https://g1.globo.com/economia/tecnologia/blog/altieres-

informações pessoais por determinada empresa, tais quais o nome, data de nascimento, *e-mail*, endereço residencial e histórico de compra do consumidor[121], ou mesmo a indisponibilidade de registros médicos sobre paciente devido a pane no sistema, seja de forma temporária ou definitiva.

A princípio, caberá à jurisprudência – mas não somente a ela – a tarefa de distinguir uma ocorrência geradora de dano passível de ser indenizado, de um episódio tipificado como mero aborrecimento, sob pena de banalização do instituto do dano, mormente do dano moral, e sobrecarga do Poder Judiciário com inúmeras demandas desprovidas de motivação. De outro lado, há também uma tendência de que novas modalidades de prejuízo venham a ser reconhecidas, ensejando inclusive discussões sobre o cabimento da presunção *in re ipsa*, visando sobretudo coibir práticas indevidas e reiteradas do mercado[122].

No entanto, não há aqui a pretensão de adentrar nas hipóteses em que restará configurado um dano, mas busca-se, nesse estágio metodológico, refletir sobre a necessidade de uma responsabilidade civil que acompanhe as demandas coletivas e esteja em conformidade com os ditames constitucionais. Além disso, faz-se imprescindível uma responsabilidade que se antecipe ao dano, combatendo o risco, motivado pela probabilidade e severidade potencial do impacto das atividades de tratamento de dados sobre o indivíduo. O debate contemporâneo, então, volta-se à possibilidade de desenvolver uma responsabilidade civil multifuncional que vá além do modelo tradicional de reparação a posteriori, visando oferecer respostas aos anseios de uma sociedade de risco antes mesmo da concretização do dano, a fim de estimular ações preventivas.

À vista disso, a Lei Geral de Proteção de Dados, em sua Seção III, intitulada "Da Responsabilidade e do Ressarcimento de Danos", apresenta as principais regras que irão nortear o sistema de responsabilidade civil dos agentes de tratamento de dados.

Em primeiro lugar, por meio da proposição alternativa empregada no *caput* do art. 42, observa-se a previsão de eventual solidariedade entre controladores e operadores na assunção da responsabilidade. A explicação vem logo em seguida, em seu §1º, o qual descreve o raciocínio a ser seguido: (i) é o controlador quem possui vasto controle pelo tratamento de dados

---

rohr/post/2020/06/10/site-brasileiro-de-classificados-de-empregos-revela-que-invasores-tiveram-acesso-indevido-a-banco-de-dados.ghtml. Acesso em: 28 ago. 2020.

[121] RIGUES, Rafael. Dados de 250 mil consumidores da Natura são expostos em vazamento. **Olhar Digital**, 19 de maio de 2020. Disponível em: https://olhardigital.com.br/noticia/dados-de-250-mil-consumidores-da-natura-sao-expostos-em-vazamento/100957. Acesso em: 27 ago. 2020.

[122] Cita-se, como exemplo, o seguinte julgado: CONFIGURA DANO MORAL *IN RE IPSA* a ausência de comunicação acerca da disponibilização/comercialização de informações pessoais em bancos de dados do consumidor." (REsp 1.758.799-MG, Rel. Min. Nancy Andrighi, Terceira Turma, por unanimidade, julgado em 12/11/2019, DJe 19/11/2019).

pessoais e, por consequência, ampla responsabilidade; (ii) o controlador terá o dever de repassar instruções ao operador, o qual igualmente está obrigado a observar os mandamentos impressos na LGPD; (iii) caso o operador descumpra os regramentos legais ou as instruções que lhe foram repassadas, responderá de forma solidária com o controlador por eventuais danos aos titulares[123].

Apesar de a redação dos artigos 42 a 45 não ser explícita quanto a natureza da responsabilidade desses sujeitos, se objetiva ou subjetiva - consubstanciando, inclusive, uma das principais críticas remetidas à lei - é inquestionável que importantes debates doutrinários vêm sendo impulsionados a partir dessa lacuna deixada pelo legislador.

4.1.2 Divergências doutrinárias acerca da responsabilidade na LGPD

Como é sabido, muitos critérios foram utilizados no decorrer da história para respaldar a pretensão reparatória da vítima. Para aqueles que se filiam ao modelo de responsabilidade pautado na culpa, somente haveria obrigação de ressarcir os prejuízos na circunstância de o ofendido comprovar que o autor do dano agiu intencionalmente ou em descumprimento a um dever de cuidado, quando lhe era possível exigir, naquela oportunidade, um comportamento diligente[124].

Nessa conjuntura, percebe-se que há implicitamente um pretexto moral para justificar a imputação de responsabilidade, associado a um ato ilícito, socialmente reprovável e eticamente corrompido. Assim, a ideia de culpa termina por assumir uma conotação pejorativa, atraindo o sentimento de punição, de sorte que a responsabilidade subjetiva teria como pressuposto não apenas a reparação do dano, mas igualmente a função de penalizar a conduta do ofensor. Por consequência, inexistindo prova do cometimento de erro, não haveria fundamento jurídico para impor o dever ressarcitório, tendo como resultado danos sem indenização[125].

Contudo, em razão das mudanças ocorridas na civilização moderna, decorrentes principalmente da expansão dos danos advindos da revolução industrial, ganhou espaço um novo modelo de responsabilidade civil, cuja preocupação deixa de ser a análise subjetiva da

---

[123] DRESCH, Rafael de Freitas Valle; FALEIROS JÚNIOR, José Luiz de Moura. **Reflexões sobre a responsabilidade civil na Lei Geral de Proteção de Dados (Lei nº 13.709/2018)**. *In*: ROSENVALD, Nelson; DRESCH, Rafael de Freitas Valle; WESENDONCK, Tula (coord.). Responsabilidade civil: novos riscos. Indaiatuba: Foco, 2019. p. 65-89.

[124] EHRHARDT JR., Marcos. **Responsabilidade civil pelo inadimplemento da boa-fé.** Belo Horizonte: Fórum, 2017. 2 ed. p. 131.

[125] RODOVALHO, Thiago. Responsabilidade civil objetiva: da culpa à objetivação da responsabilidade - responsável, mas não culpado. **Migalhas**, 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/336454/responsabilidade-civil-objetiva--da-culpa-a-objetivacao-da-responsabilidade---responsavel--mas-nao-culpado. Acesso em: 13 mar. 2020.

conduta do ofensor e volta-se à necessidade de proteção da vítima, sujeito vulnerável em face dos "criadores de risco"[126].

Surgiu, então, a responsabilidade civil objetiva, alicerçada na ideia de que "os danos deveriam ser suportados por seu causador, ainda que sem nenhuma culpa, se os prejuízos tivessem conexão com as atividades por ele desenvolvidas"[127]. Nesse mesmo sentido, Alvino Lima prelecionava que a teoria objetiva está firmada no critério do risco criado pelas múltiplas atividades humanas, risco este que, sendo intrínseco à normalidade de seu desempenho, deverá ser suportado por seu criador, e não pelo ofendido que em nada contribuiu para a sua ocorrência. *Ipsis litteris:*

> Partindo da necessidade da segurança da vítima, que sofreu o dano, sem para ele concorrer, os seus defensores sustentam que "*les faiseurs d'actes*", nas suas múltiplas atividades, são os criadores de riscos, na busca de proveitos individuais. Se destas atividades colhem os seus autores todos os proventos, ou pelo menos agem para consegui-los, é justo e racional que suportem os encargos, que carreguem com os ônus, que respondam pelos riscos disseminados - *Ubi emolumentum, ibi onus*. Não é justo, nem racional, nem tampouco eqüitativo e humano, que a vítima, que não lhe colhe os proveitos da atividade criadora dos riscos e que para tais riscos não concorreu, suporte os azares da atividade alheia[128].

Como bem pontuado por Marcos Ehrhardt, embora haja uma tendência moderna em considerar o critério do risco como o "mais adequado às necessidades de segurança jurídica de uma sociedade marcada pelo desenvolvimento tecnológico que necessita de estabilidade nas relações econômicas entre os indivíduos"[129], ainda é bem visível a coexistência das duas vertentes no sistema civilista brasileiro.

Sem prejuízo de uma classificação dualista, Maria Celina Bodin de Morais[130] chama a atenção para uma possível confluência entre as duas teorias, em virtude de uma tendência de reunificação do sistema que tem origem na indefinição atual dos conceitos de culpa e de risco. Explica a autora que, com o tempo, parte da doutrina abandonou a interpretação da culpa sob o ponto de vista psicológico e passou a enxergá-la mais próxima de um conceito normativo, pautado em *standards* ou padrões de conduta, pretendendo tornar sua aferição mais "objetiva", ou seja, configurada a partir do descumprimento de um dever de cuidado ou de diligência previsto em norma própria. O inverso também ocorre, principalmente no momento de definição do *quantum* indenizatório, quando os tribunais, muitas vezes, fazem uso de uma espécie de

---

[126] LIMA, Alvino. **Culpa e risco**. São Paulo: Revista dos Tribunais, 1998. 2 ed. p. 116.
[127] EHRHARDT JR., Marcos. **Responsabilidade civil pelo inadimplemento da boa-fé.** Belo Horizonte: Fórum, 2017. 2 ed. p. 131.
[128] LIMA, Alvino. *Op. cit.,* p. 119.
[129] EHRHARDT JR., Marcos. *Op. cit.,* p. 131.
[130] BODIN DE MORAES, Maria Celina. Risco, solidariedade e responsabilidade objetiva. **Revista dos Tribunais**, São Paulo, v. 854, ano 95, dez. 2006, p. 11-37.

escala com origem no comportamento de maior ou menor grau de cautela dispensada pelo agente, com o intuito de estipular o valor do dano para mais ou para menos, ainda que a responsabilidade aplicada ao caso tenha sido a objetiva.

Em suma, havendo uma convergência entre eles ou não, são dois os nexos de imputação de responsabilidade destacados pela doutrina: a culpa, como elemento configurador do ato ilícito da responsabilidade subjetiva, e o risco, critério-base da responsabilidade civil objetiva. No Código Civil de 2002, a teoria da responsabilidade subjetiva está positivada, de forma genérica, no *caput* do art. 927, ao passo que a cláusula geral de responsabilidade objetiva está situada logo em seguida no parágrafo único, art. 927, do referido código, *in verbis*:

> Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.
> 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.** (grifo nosso)

No tocante à Lei Geral de Proteção de Dados, essa tradicional dicotomia persiste. Para os defensores da responsabilidade subjetiva, é possível visualizar essa espécie por meio da própria estrutura da LGPD, a qual foi organizada estabelecendo uma série de deveres de cuidado, reforçando a tese de que o legislador não teria criado diversas obrigações para os agentes de tratamento se não fosse com o propósito de implantar um regime de responsabilidade pautado na análise da culpa.

Sustentam essa posição, na doutrina brasileira, Gisela Sampaio da Cruz Guedes e Rose Melo Vencelau, para as quais, "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"[131]. Assim, em virtude da excludente de responsabilidade prevista no inciso II do art. 43, no sentido de que os agentes de tratamento não serão responsabilizados quando provarem "que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados" (art. 43, II), bastaria, no entendimento das autoras, a prova do implemento de *standards* a serem estabelecidos pela Autoridade Nacional, conforme previsão do §1º[132], art. 46, da lei, ainda que sua observância não tenha sido suficiente para evitar o dano.

---

[131] GUEDES, Gisela Sampaio da Cruz; VENCELAU, Rose Melo. Término do tratamento de dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. Editora Revista dos Tribunais, 2019. Não paginado [livro digital].

[132] 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. **§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no *caput* deste artigo,**

Em outras palavras, a imputação de responsabilidade aos agentes de tratamento dependeria da aferição, caso a caso, do descumprimento de padrões técnicos mínimos de segurança no decorrer da atividade, cujo resultado tenha sido a ruptura da proteção dos dados e consequente dano ao seu titular. Ademais, as autoras ainda destacam que, ao contrário do Código de Defesa do Consumidor, o qual expressamente indica a opção do legislador pela natureza objetiva da responsabilidade por meio da locução "independentemente de culpa"[133], contida nos arts. 12 e 14, não haveria qualquer norma análoga na LGPD[134].

Já no entendimento de Rafael de Freitas Valle Dresch e Lílian Brandt Stein[135], a LGPD não adotou o risco e, tampouco, a culpa como critério de imputação de responsabilidade civil, mas, em verdade, instituiu um regime novo e diverso, denominado de responsabilidade objetiva especial, configurada a partir do cometimento de um ilícito, qual seja, o não cumprimento de deveres impostos pela legislação de proteção de dados, sobretudo o dever geral de segurança por parte do agente de tratamento, ante a legítima expectativa do titular sobre a conduta do agente.

Na visão dos autores, o ilícito previsto nos arts. 42 e 44 não estaria centrado na análise subjetiva do sujeito segundo sua intenção ou falta de cuidado, ou seja, por negligência, imprudência ou imperícia, como ocorre no artigo 186[136] do Código Civil, mas sim no ilícito objetivo, previsto no artigo 187[137] do aludido código, exigindo somente a análise externa e objetiva das práticas do controlador e operador, "para verificar se tal conduta está em

---

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. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm#art65 >. Acesso em: 07 mar. 2021.

[133] BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor (CDC)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Acesso em: 06 jan. 2021.

[134] GUEDES, Gisela Sampaio da Cruz; VENCELAU, Rose Melo. Término do tratamento de dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. Editora Revista dos Tribunais, 2019. Não paginado [livro digital].

[135] DRESCH, Rafael de Freitas Valle; STEIN, Lílian Brandt. Direito fundamental à proteção de dados e responsabilidade civil. **Revista de Direito da Responsabilidade**. Portugal: ano 3, 2021. p. 224-241. Disponível em: https://revistadireitoresponsabilidade.pt/2021/direito-fundamental-a-protecao-de-dados-e-responsabilidade-civil-rafael-de-freitas-valle-dresch-lilian-brandt-stein/. Acesso em: 07 mar. 2021.

[136] 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. BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. **Código Civil.** Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm>. Acesso em: 07 mar. 2021.

[137] Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes. BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. **Código Civil.** Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm>. Acesso em: 07 mar. 2021.

conformidade (*compliance*) ou não com o padrão de conduta que se pode exigir de um agente de tratamento com base em *standards* técnicos de mercado e regulatórios"[138].

Todavia, insta salientar que ao se propor um modelo de responsabilidade civil pautado no cumprimento de deveres, *in casu*, os *standards* de conduta, o que estará sendo questionado é se o agente de tratamento atuou ou não com culpa, evidenciando a similitude existente entre o novo regime proposto pelos autores, denominado "objetivo especial", e a teoria subjetivista da responsabilidade. Logo, para fins deste trabalho, as duas teses supracitadas serão consideradas equivalentes, insertas na teoria subjetiva.

Por outro lado, a corrente aliada à responsabilidade objetiva sustenta que há um perigo de dano intrínseco nas operações destinadas ao tratamento de dados. Nesse viés, Danilo Doneda e Laura Schertel Mendes sugerem que o ponto de partida para compreender a intenção do legislador por um sistema de responsabilidade objetiva, nos moldes do parágrafo único do art. 927 do Código Civil, consiste na interpretação do corpo normativo da LGPD, por meio do qual estaria sinalizada a natureza de risco da atividade. Isso porque a Lei trouxe diversas limitações às operações de tratamento, procurando "restringir às hipóteses com fundamento legal (art. 7º) e que não compreendam mais dados do que o estritamente necessário (princípio da finalidade, art. 6º, III) nem sejam inadequadas ou desproporcionais em relação à sua finalidade (art. 6º, II)"[139], somando-se ao fato de que, em diversos dispositivos, o risco é figura central do texto.

Como característica principal da LGPD, destacam, então, o seu papel em positivar condutas voltadas à diminuição de um risco que é inerente à atividade de tratamento de dados. Desta feita, diante de tantos alertas feitos pelo legislador acerca das possibilidades de ocorrerem incidentes de segurança, restaria justificada a sua vontade de empregar um regime de responsabilidade objetiva, tornando a obrigação de reparar o dano vinculada ao mero exercício da atividade de tratamento de dados pessoais[140].

Em face de todas as considerações acima esposadas e dos argumentos a seguir expostos, chegar-se-á à conclusão de que os critérios da imputação objetiva são os que conduzem para uma melhor interpretação e aplicação do sistema de responsabilidade da Lei Geral de Proteção de Dados brasileira.

4.1.3 A presença da imputação objetiva na estrutura normativa

---

[138] DRESCH, Rafael de Freitas Valle; STEIN, Lílian Brandt. Direito fundamental à proteção de dados e responsabilidade civil. **Revista de Direito da Responsabilidade.** Portugal: ano 3, 2021. p. 224-241. Disponível em: https://revistadireitoresponsabilidade.pt/2021/direito-fundamental-a-protecao-de-dados-e-responsabilidade-civil-rafael-de-freitas-valle-dresch-lilian-brandt-stein/. Acesso em: 07 mar. 2021.

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

[140] MENDES, Laura Schertel; DONEDA, Danilo. *Op cit.*

Partindo-se da leitura atenta da Seção "Da Responsabilidade e do Ressarcimento de Danos", iniciando pelo comando geral do art. 42 da LGPD, depreende-se primeiramente que o referido dispositivo não faz qualquer menção à culpa, em sentido *lato* ou estrito, assinalando, em verdade, que haverá obrigação de indenizar eventuais danos, ressalte-se, "em razão do exercício de atividade de tratamento de dados pessoais". Nesse sentido, torna-se despicienda a comprovação da existência de culpa na atuação do controlador ou operador, porquanto o nexo de imputação não provém do ilícito, mas tem origem no risco inerente à própria atividade desenvolvida pelo agente de tratamento, cuja prática, evidentemente, traz riscos aos direitos dos titulares de dados.

Em segundo lugar, ao analisar as excludentes de responsabilidade previstas no art. 43 e incisos, constata-se a impossibilidade de os agentes eximirem-se da responsabilidade somente alegando e provando não terem agido com culpa. Corroboram esse entendimento, Cristiano Colombo e Eugênio Facchini Neto, para os quais a LGPD adotou, no mencionado dispositivo, a mesma técnica utilizada pelo legislador do CDC nos arts. 12, §3º e 14, §3º, referentes à responsabilidade do fabricante e do fornecedor de serviços pelo fato do produto ou do serviço. Seguindo esse raciocínio, se as excludentes de responsabilidade contidas no CDC levam, inequivocadamente, a um modelo de responsabilidade objetiva, não haverá outro caminho senão o da aplicação da mesma regra sobre o art. 43 da LGPD.

Ademais, convém salientar que a excludente do inciso II, do art. 43, ao estabelecer que os agentes não serão responsabilizados quando provarem que, embora tenham realizado o tratamento, "não houve violação à legislação de proteção de dados", prevê a hipótese de a conduta do agente não ter relação causal com o resultado dano, embora este exista. Não se refere, portanto, a razão jurídica da obrigação, mas tão somente aponta uma circunstância fática capaz de afastar o nexo de causalidade, semelhante ao que ocorre no CDC quando cita a excludente de que "o defeito inexiste" (arts. 12, §3º, II e 14, §3º, I). Em síntese, se houve um dano, este não decorreu da realização do tratamento em análise, porquanto teve origem noutra causa alheia à atividade do agente, caracterizando a quebra do nexo de causalidade.

Com vistas a esclarecer o assunto, Adalberto Pasqualotto elucida as diferenças entre o nexo de imputação e o nexo de causalidade, pois enquanto a causalidade abarca a relação entre um fato e sua causa, a imputação é decorrente de uma certa razão jurídica para se atribuir a responsabilidade a alguém, que pode ser a culpa do ofensor ou o risco por ele provocado no exercício da sua atividade. Desse modo, a relação causal deverá ser verificada antes do nexo de

imputação, a fim de se ter certeza de que houve um dano e que este seja efetivamente a consequência de determinado fato[141].

Outra interpretação possível para o mencionado dispositivo são as hipóteses em que é afastada a aplicação da lei, previstas no art. 4º, referentes ao tratamento realizado por pessoa natural para fins exclusivamente particulares e não econômicos, jornalísticos, artísticos, acadêmicos, segurança pública, defesa nacional, segurança do Estado, atividades de investigação e repressão de infrações penais ou provenientes de fora do território nacional.

Ato contínuo, percebe-se da leitura do art. 44 que o tratamento de dados será irregular diante de duas hipóteses, quais sejam, a não observância de deveres específicos da lei ou pela quebra do dever geral de segurança, circunstâncias estas já explanadas no segundo capítulo deste trabalho. Nesse sentido, o parágrafo único do art. 44, ao prescrever que responderá "pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano", pretendeu destinar uma maior atenção à responsabilidade decorrente de incidentes de segurança. Este foi mais um artifício utilizado pelo legislador para advertir sobre os riscos e a necessidade de se adotar medidas técnicas e administrativas (art. 46) para evitar danos, assumindo uma postura proativa.

A partir disso, é preciso ter em mente que a condição de "deixar de adotar as medidas de segurança" é uma causa fática do dano. O nexo de causalidade entre esse dano e a conduta do agente consiste na falta de êxito no momento de concretização das medidas de segurança, que por algum motivo, alheio ou não a sua vontade e empenho, não foram aptas a evitar um incidente de segurança, ainda que tenham sido aplicadas todas as diligências mínimas exigidas pela lei ou até mesmo ido além delas. Por tanto, trata-se, aqui, de uma circunstância fática que originou o dano, relativa ao nexo de causalidade, e não de uma razão jurídica de imputação de responsabilidade. Não será a conduta do agente levada em consideração nesta etapa, mas sim a consequência de sua conduta (o dano) e o risco por ele assumido.

Sobre o assunto, Caitlin Mulholland assevera que tais incidentes são acontecimentos intimamente relacionados ao risco, o qual deverá ser visto, necessariamente, como intrínseco à atividade de tratamento de dados, "considerados, em última análise, como hipótese de fortuito interno, incapazes de afastar a obrigação dos agentes de tratamento de indenizar os danos

[141] PASQUALOTTO, Adalberto. **Causalidade e imputação na responsabilidade civil objetiva**. *In*: ROSENVALD, Nelson; DRESCH, Rafael de Freitas Valle; WESENDONCK, Tula (coord.). Responsabilidade civil: novos riscos. Indaiatuba: Foco, 2019. p. 199-217.

causados pelos incidentes"[142]. Em sua conclusão, a autora argumenta que tais danos possuem a característica de serem quantitativamente elevados e qualitativamente graves, podendo atingir direitos difusos, fato este que, por si mesmo, fundamenta a necessidade de aplicação da responsabilidade objetiva[143].

4.2 A Análise Constitucional

4.2.1 O reforço constitucional na interpretação de um nexo de imputação objetiva

Somando-se à análise da estrutura normativa da Lei Geral de Proteção de Dados, a qual se acredita conduzir para uma imputação objetiva, é preciso ainda estar atento ao fortalecimento dos debates doutrinários desenvolvidos a partir da última década do século XX, acerca da imprescindibilidade do processo de constitucionalização do direito civil brasileiro. Esse fenômeno nasceu a partir da preocupação entre os juristas com a necessidade de readequação do direito civil aos valores consagrados na Constituição de 1988, no intuito de acompanhar as mudanças sociais[144].

Nas palavras de Paulo Lôbo, "a constitucionalização é o processo de elevação ao plano constitucional dos princípios fundamentais do direito civil, que passam a condicionar a observância pelos cidadãos, e a aplicação pelos tribunais, da legislação infraconstitucional"[145]. Sua finalidade consiste no fortalecimento do Estado Democrático e Social de Direito, promovendo os ideais da justiça social e da solidariedade, consagrados no art. 3º, I, da Constituição, bem como a aplicação de valores fundados na dignidade da pessoa humana (art. 1º, III, CF/88)[146], de modo a superar os arcaicos juízos do modelo liberal do século XIX de hipervalorização do individualismo e da primazia do patrimônio em detrimento do sujeito de direito[147].

---

[142] MULHOLLAND, Caitlin. A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco? **Migalhas**, 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: 14 set. 2020.

[143] *Ibidem*.

[144] LÔBO, Paulo. Novas perspectivas da constitucionalização do direito civil. **Jus Navigandi**, Teresina, ano 18 (/revista/edicoes/2013), n. 3754 (/revista/edicoes/2013/10/11), 11 (/revista/edicoes/2013/10/11) out. (/revista/edicoes/2013/10) 2013 (/revista/edicoes/2013). Disponível em: <http://jus.com.br/artigos/25361>. Acesso em: 25 mar. 2021.

[145] *Ibidem.*

[146] BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**: promulgada em 05 de outubro de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm >. Acesso em: 05 mar. 2021.

[147] LÔBO, Paulo. Novas perspectivas da constitucionalização do direito civil. **Jus Navigandi**, Teresina, ano 18 (/revista/edicoes/2013), n. 3754 (/revista/edicoes/2013/10/11), 11 (/revista/edicoes/2013/10/11) out. (/revista/edicoes/2013/10) 2013 (/revista/edicoes/2013). Disponível em: <http://jus.com.br/artigos/25361>. Acesso em: 25 mar. 2021.

É do mesmo pensamento Maria Celina Bodin de Moraes, para quem a responsabilidade civil, como instituto do direito civil que é, deverá ser aplicada de forma sistematizada com os valores e princípios constitucionais. Nesse desiderato, consolida-se o entendimento de que a vítima não deve ficar sem o devido ressarcimento e que o sistema da responsabilidade deverá atuar, destaque-se, como "um mecanismo de controle e distribuição dos riscos da vida em sociedade"[148].

Por consequência, com a implantação do modelo solidarista constitucional, ampliam-se as funções e objetivos da responsabilidade, abandonando-se cada vez mais o pressuposto da culpa, ao tempo em que é fortalecido o princípio da justiça distributiva no tocante à reparação de qualquer dano injusto, ainda que não haja ilicitude na conduta danosa[149].

Outrossim, é preciso ter em mente que, independentemente de qual natureza de responsabilidade tenha sido adotada para LGPD, muito provavelmente a grande maioria dos casos a serem levados ao judiciário estará inserida no âmbito das relações consumeristas, as quais, como já se sabe, seguem a regra da responsabilidade objetiva prevista no CDC, baseada no defeito do produto ou serviço. É justamente o que prevê o art. 45 da LGPD, ao dispor que "as hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente" (art. 45).

Neste passo, como bem alerta Aline de Miranda Valverde Terra, caberá ao intérprete o papel de aplicar as regras do CDC em harmonia com as determinações da LGPD e peculiaridades do meio digital, a fim de que a legislação consumerista acompanhe a evolução da ciência e da tecnologia dos últimos 30 anos desde a sua edição. Dessa forma, se a responsabilidade pelo fato do produto ou do serviço pressupõe acidente de consumo por quebra do dever de segurança, e a responsabilidade pelo vício ocorrerá quando o produto ou serviço for inadequado às suas finalidades e funções, será plenamente possível e necessário integrar tal classificação ao contexto e circunstâncias fáticas do tratamento de dados[150].

Além de tudo o que foi dito, o assunto não é pacífico, existem outras perspectivas e visões, como as que serão analisadas na sequência, voltadas à ampliação das funções da responsabilidade civil, principalmente em seu âmbito preventivo.

4.2.2 Responsabilidade proativa: tendência a um sistema híbrido de responsabilidade?

---

[148] DE MORAES, Maria Celina Bodin. A constitucionalização do direito civil e seus efeitos sobre a responsabilidade civil. *In*: **Direito, Estado e Sociedade**, v.9, n. 29, p. 233/258, jul/dez de 2006.

[149] *Ibidem*

[150] TERRA, Aline de Miranda Valverde. Hackeamento de dados pessoais e responsabilidade do fornecedor: releitura do CDC pela óptica da LGPD. **Migalhas**, 09 jul. 2021. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-patrimoniais/348292/hackeamento-de-dados-pessoais-e-responsabilidade-do-fornecedor >. Acesso em: 18 jul. 2021.

Fortalecendo o debate, Maria Celina Bodin de Moraes pontua que o sistema de responsabilidade civil da LGPD não é subjetivo e nem objetivo, mas se mostra especialíssimo, porquanto instaurou uma mudança profunda no tocante à responsabilização *lato sensu* ao fixar deveres voltados à prevenção de danos. Esse modelo é intitulado de "responsabilização ativa" ou "proativa", e dentro dele torna-se insuficiente a mera abdicação de descumprir a lei, exigindo-se, ainda, atitudes conscientes, diligentes e proativas por parte das empresas quanto à utilização dos dados pessoais, buscando "proativamente" prevenir a ocorrência de danos[151]. Sustenta a autora, *in verbis*:

> Em conclusão, vê-se que o legislador, embora tenha flertado com o regime subjetivo, elaborou a um novo sistema, de prevenção, e que se baseia justamente no risco da atividade. Tampouco optou pelo regime da responsabilidade objetiva, que seria talvez mais adequado à matéria dos dados pessoais, porque buscou ir além na prevenção, ao aventurar-se em um sistema que tenta, acima de tudo, evitar que danos sejam causados[152].

Como fundamento, Maria Celina Bodin destaca o fato de que a LGPD traz um rol de princípios positivados expressamente em seu texto, dentre eles os princípios da boa-fé (art. 6º, *caput*), segurança (art. 6º, VII), responsabilização/prestação de contas (art. 6º, X) e sobretudo da prevenção (art. 6º, VIII), determinando a "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais" (art. 6º, VIII).

A partir disso, pode-se inferir que uma das formas de concretização desses princípios partirá do desenvolvimento de efetivos programas de *compliance* por partes dos empresários, ou seja, a busca pela conformidade com a lei e padrões de mercado, visando à mitigação de riscos. O *compliance,* aliás, extrapola essa definição, porquanto, "em verdade, trata-se de verdadeira mudança cultural multidisciplinar nas empresas envolvendo as áreas jurídicas, de tecnologia e segurança da informação, recursos humanos, marketing, entre outras, bem como os ideais de ética empresarial e responsabilidade social"[153]. Nesse aspecto, é preciso ter em vista que qualquer projeto de adequação à LGPD dependerá, necessariamente, do dispêndio de recursos humanos e financeiros.

No entanto, parte da doutrina passou a indagar como seria possível estimular uma conduta proativa por parte dos agentes de tratamento, com forte investimento em *compliance* e

---

[151] BODIN DE MORAES, Maria Celina. LGPD: um novo regime de responsabilização civil dito "proativo". **Civilistica.com**. Rio de Janeiro: a. 8, n. 3, 2019. Disponível em: <http://civilistica.com/lgpd-um-novo-regime/>. Acesso em: 15 mar. 2020.

[152] *Ibidem.*

[153] TAMER, Maurício Antonio; VAINZOF, Rony; LIMA, Caio César Carvalho. Compliance e LGPD: Plano de adequação como ferramenta de mitigação de riscos legais. **Jota**, 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/compliance-e-lgpd-plano-de-adequacao-como-ferramenta-de-mitigacao-de-riscos-legais-07042019. Acesso em: 12 maio 2021.

práticas que transcendam os padrões mínimos estipulados em lei, quando o nexo da imputação objetiva dispensa qualquer valoração de tais esforços. Nesse viés, se fixada a tese de que nem mesmo as melhores técnicas aplicadas pelo empresário – ainda que superando a média do mercado - terão aptidão de afastar o dever reparatório em caso de dano, questiona-se por qual razão haveria interesse de investimento em um padrão de excelência na atividade se a resposta dada a ele pelo Poder Judiciário será a mesma propiciada àquele concorrente que pouco ou nada se empenhou.

É nesse cenário de dúvidas e incertezas que Nelson Rosenvald[154] lança uma necessária reflexão acerca da possibilidade de ampliação das funções da responsabilidade civil, sobretudo sua função promocional, a qual teria como pressuposto o estímulo a condutas proativas de prevenção ao dano mediante "sanções premiais" aos agentes de tratamento, no intuito de alcançar, por via difusa, uma maior proteção aos titulares de dados, mantendo o alinhamento com os ditames constitucionais.

Em seu texto "O *compliance* e a redução equitativa da indenização na LGPD", o autor traça um modelo no qual faz uso da exceção ao princípio da reparação integral, representada pelo parágrafo único do art. 944 do Código Civil, cujo teor prevê a hipótese de que, "se houver excessiva desproporção entre a gravidade da culpa e o dano, poderá o juiz reduzir, eqüitativamente, a indenização" (sic). Nas palavras do autor,

> [...] o referido dispositivo é um ponto de partida para aproveitarmos as enormes potencialidades do *compliance*, alargando os horizontes da responsabilidade civil, destacando a sua "função promocional", na qual a tônica será a aplicação das sanções premiais, tão decantadas por Norberto Bobbio. Para além de compensar, punir e prevenir danos, a responsabilidade civil deve criteriosamente recompensar a virtude e os comportamentos benevolentes de pessoas naturais e jurídicas[155].

No entanto, embora parte da doutrina entenda pela incompatibilidade da supracitada norma com a teoria objetiva da responsabilidade, sob o argumento de que o seu nexo de imputação afasta qualquer discussão sobre culpa, o autor acredita que "a incidência da cláusula não pode fechar as portas para a responsabilidade objetiva, sob pena de frustrar o seu próprio escopo de equidade"[156], sendo necessário, portanto, amoldar a aplicação do dispositivo a determinados casos de responsabilidade objetiva.

---

[154] ROSENVALD, Nelson. O *compliance* e a redução equitativa da indenização na LGPD. *In*: **Migalhas**, 2021. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/342032/o-compliance-e-a-reducao-equitativa-da-indenizacao-na-lgpd. Acesso em: 12 maio 2021.

[155] *Ibidem.*

[156] ROSENVALD, Nelson. O *compliance* e a redução equitativa da indenização na LGPD. *In*: **Migalhas**, 2021. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/342032/o-compliance-e-a-reducao-equitativa-da-indenizacao-na-lgpd. Acesso em: 12 maio 2021.

Em face dessas questões, Nelson Rosenvald propõe um esquema de aplicação da norma à LGPD, orientado a partir da observância de três graus ou *standards* de diligência no contexto da atividade de risco. São eles: (a) ausência de diligência; (b) diligência ordinária; e (c) diligência extraordinária.

A resposta ao primeiro deles encontra-se limitada à esfera de atuação administrativa, em razão da ausência de previsão legal no Brasil de um modelo similar aos *punitive damages*, de forma que o magistrado, mesmo diante de condutas negligentes ou imprudentes, não poderá aumentar o *quantum* devido a título de indenização, havendo permissão apenas para a aplicação de sanções administrativas e quantificação de multas por parte da Autoridade Nacional de Proteção de Dados (ANPD), em consonância com o art. 52 da LGPD[157]. Quanto ao segundo *standard*, por se tratar de diligência ordinária, sendo constatado que as medidas de segurança empregadas pelos agentes de tratamentos estão no padrão médio do setor de mercado, ou seja, quando não foi preenchida a condição de "excessividade" a que se refere o parágrafo único do 944 do CC, o resultado será neutro do ponto de vista punitivo, mantendo-se a regra da reparação integral do dano.

A respeito do terceiro *standard*, Rosenvald explica que a excepcional diligência do sujeito responsável pelo tratamento poderá ser constatada "não apenas pela conformidade à regulação de gestão de riscos, como por práticas proativas de sua mitigação"[158], a exemplo do teor o art. 50 da LGPD[159], quando preconiza que os agentes de tratamento, no âmbito de suas competências, poderão formular regras de boas práticas e de governança para mitigação de riscos. Em razão do caráter meramente facultativo da norma, sinalizado pelo uso do vocábulo "poderão", desponta a necessidade de um incentivo para a efetivação das medidas recomendadas, sob pena de ficarem restritas ao plano da abstração.

---

[157] Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: [...]. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm#art65 >. Acesso em: 12 maio 2021.

[158] ROSENVALD, Nelson. O *compliance* e a redução equitativa da indenização na LGPD. *In*: **Migalhas**, 2021. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/342032/o-compliance-e-a-reducao-equitativa-da-indenizacao-na-lgpd. Acesso em: 12 maio 2021.

[159] 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. (grifo nosso). BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm#art65 >. Acesso em: 12 maio 2021.

O ponto de intersecção entre o *compliance* e a sua concretude consistiria justamente na aplicabilidade do parágrafo único do art. 944 do CC, pois, conforme assinalado por Rosenvald, "através da mitigação equitativa da obrigação de indenizar, o dispositivo atua como uma forma desejável de estímulo a todo e qualquer agente econômico que, não obstante o risco inerente à sua atividade, não meça esforços para refrear a possibilidade de causação de danos a terceiros"[160].

Ademais, se a LGPD menciona que os aspectos relacionados à culpa do agente de tratamento serão tomados como parâmetros para fins de quantificação da multa administrativa, consoante rol do §1º do art. 52, abrem-se as portas para o debate acerca da possibilidade de adoção de métodos similares de estímulo também na seara judicial, ampliando-se as funções da responsabilidade civil.

Todavia, importa reiterar que a discussão aqui pretendida gira em torno da possibilidade de aferição da culpa tão somente com a finalidade de redução do *quantum* indenizatório, ou seja, após a fase de imputabilidade, não sendo tal conduta proativa suficiente, por si só, para atingir o plano existencial da responsabilidade objetiva, porquanto, do ponto de vista constitucional, o direito da vítima de ser ressarcida pelo dano sofrido, ainda que parcialmente, sobrepõe-se à tese da inexistência de culpa do seu agente causador.

Trata-se, portanto, da proposta de um modelo híbrido de responsabilidade, consistente na utilização do nexo de imputação objetiva para firmar o dever reparatório do ofensor, pautado no risco da atividade, seguido da verificação de diligência extraordinária que justifique a redução equitativa do *quantum debeatur*, funcionando como uma espécie de sanção premial, cujo intuito, segundo Silvio de Salvo Venosa, é o de servir de "instrumento de educação social, direcionando os indivíduos para um modelo desejado"[161].

À vista do exposto, embora o assunto não seja pacífico, a exceção ao princípio da restituição integral do dano em casos de excepcional diligência aparenta ser uma contribuição promissora na tarefa de pôr em prática os ideais da responsabilidade proativa da LGPD, beneficiando um número indeterminado de titulares dados, com efeito *erga omnes* na redução de danos, e evitando a judicialização de inúmeras demandas de caráter indenizatório.

Além disso, com o propósito de coibir ações ou omissões que ponham em flagrante risco os dados pessoais dos titulares, cogita-se a possibilidade de utilização de outras ferramentas da

---

[160] ROSENVALD, Nelson. O *compliance* e a redução equitativa da indenização na LGPD. *In*: **Migalhas**, 2021. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/342032/o-compliance-e-a-reducao-equitativa-da-indenizacao-na-lgpd. Acesso em: 12 maio 2021.

[161] VENOSA, Sílvio de Salvo. Sanção premial. *In*: **Migalhas**, 2019. Disponível em: https://www.migalhas.com.br/depeso/298207/sancao-premial. Acesso em: 06 jun. 2021.

responsabilidade civil, em caráter *ex ante* ao dano. Esse último ponto será analisado na sequência.

4.3 A Atuação *Ex Ante* da Responsabilidade Civil: Responsabilidade Sem Dano

Dano e responsabilidade civil sempre estiveram intrinsecamente ligados entre si, analisados sob a ótica reparatória, proveniente da relação de causa e efeito. A ideia de que não há responsabilidade civil sem a existência de um dano esteve presente na doutrina e jurisprudência desde a elaboração do Código Civil francês de 1804, manifestada pela interpretação de seus arts. 1382 e 1383, dos quais extraiu-se o princípio entendido comumente por: "*san dommage subi par la victime, il n'y a pas de responsabilité"*[162].

Em que pese a aparente suficiência do modelo reparatório de responsabilidade para lidar com as demandas até então existentes, com o progresso advindo da revolução industrial e tecnológica, a sociedade passou a vivenciar novas formas de acidentes e riscos, abrindo espaço para uma significativa expansão dos danos e de sua potencialidade lesiva, de modo a pôr em xeque a capacidade dos parâmetros daquele instituto para regular toda e qualquer atividade que implique riscos a outrem por sua própria natureza[163]. Nesse cenário, novas circunstâncias ganharam força e passaram a ser consideradas para a criação de um "modelo de responsabilidade civil diferente"[164].

Foi a partir da necessidade de adaptação do Direito às demandas de uma sociedade de risco que parte da doutrina passou a defender a refundação das bases teóricas da responsabilidade civil. Na qualidade de instrumento para proteção de direitos fundamentais e diante de uma variedade de fontes normativas, a responsabilidade não deveria estar limitada ao binômio dano-reparação, de sorte que, nas palavras de Marcos Ehrhardt Júnior, "o papel do direito de danos não se limita apenas à reparação dos prejuízos, mas se estende à prevenção de resultados socialmente indesejados"[165].

---

[162] Tradução nossa: "sem danos sofridos pela vítima, não há responsabilidade". CARRÁ, Bruno Leonardo Câmara. É possível uma responsabilidade civil sem dano? (I). Revista **Consultor Jurídico**, 2016. Disponível em: https://www.conjur.com.br/2016-abr-18/direito-civil-atual-possivel-responsabilidade-civil-dano. Acesso em: 15 set. 2020.

[163] RODRIGUES, Cássio Monteiro. Reparação de danos e função preventiva da responsabilidade civil: parâmetros para o ressarcimento de despesas preventivas ao dano. **Civilistica.com.** Rio de Janeiro, a. 9, n. 1, 2020. p. 04-05. Disponível em: <http://civilistica.com/reparacao-por-danos-e-funcao-preventiva/>. Acesso em: 16 set. 2020.

[164] CARRÁ, Bruno Leonardo Câmara. É possível uma responsabilidade civil sem dano? (I). Revista **Consultor Jurídico**, 2016. Disponível em: https://www.conjur.com.br/2016-abr-18/direito-civil-atual-possivel-responsabilidade-civil-dano. Acesso em: 15 set. 2020.

[165] EHRHARDT JR., Marcos. Responsabilidade civil ou direito de danos? Breves reflexões sobre a inadequação do modelo tradicional sob o prisma do direito civil constitucional. pp. 303-314. *In*: RUZYK, Carlos Eduardo Pianovski *et al*. (Org.). **Direito civil constitucional: a ressignificação da função dos institutos fundamentais do direito civil contemporâneo e suas consequências.** Florianópolis: Conceito Editorial, 2014. p. 312.

Essa construção teórica mais abrangente está atrelada ao anseio por um sistema de justiça civilista dito constitucionalizado, na medida em que "o direito civil deixa de ser o centro de regulação da ordem privada e o intérprete passa a se valer dos princípios constitucionais para a reunificação do sistema, especialmente a dignidade humana e a solidariedade"[166]. Nesse contexto, a ameaça de um dano já permitiria o uso de sanções jurídicas que passariam a ser incorporadas pela responsabilidade civil, buscando tutelar integralmente a vítima e restituí-la ao *status quo ante*.

Corroborando esse entendimento, Paulo Luiz Netto Lôbo aduz que a Constituição reservou uma série de dispositivos legais voltados para a responsabilidade civil, por meio dos quais se acredita que a intenção do legislador constituinte foi a de não restringir o instituto à tradicional responsabilidade por danos, de caráter negativo e voltado à reparação, mas compreenderia, também, o que se convencionou chamar de "responsabilidade sem danos", com viés positivo, tendente ao acolhimento dos deveres de prevenção, cuidado, preservação e precaução, possibilitando uma interpretação que informa e conforma a legislação aplicável, sobretudo o Código Civil. Assim, ao defender que, além da reparação, a responsabilidade deve preocupar-se igualmente em evitar o dano, seja por meio da abstenção de condutas ou de uma atuação positiva, o autor sintetiza:

> A ideia de reparação, que domina a concepção clássica de responsabilidade civil, ancora-se no fato passado, como consequência ao dano já consumado. Contudo, para certos danos, especialmente os que ultrapassam sujeitos determinados e atingem coletividades, como os danos nas relações de consumo e os danos ambientais, além dos decorrentes de conflitos de vizinhança, ou de concorrência desleal, ou de direitos da personalidade, notadamente os relativos à privacidade, os deveres de prevenção, precaução e preservação, que se voltam ao futuro, são imprescindíveis. Os antigos romanos já tinham criado a caução de dano infecto, voltada para prevenir o dano futuro[167].

Por outro lado, há quem apresente resistência à expansão das funções da responsabilidade proposta por esse novo modelo, sob pena de ocorrer sua descaracterização[168]. Para Bruno Leonardo Câmara Carrá, esse novo conceito de responsabilidade civil preventiva trouxe, em parte, algum benefício, na medida em que chamou a atenção para o crescimento dos danos nos tempos atuais e para a necessidade de controlar sua expansão por meio de instrumentos jurídicos[169].

---

[166] *Ibidem*, p. 305.
[167] LÔBO, Paulo Luiz Netto. Direito Civil: **Obrigações,** volume II. 7ª ed. São Paulo: Saraiva, 2019. p. 46.
[168] RODRIGUES, Cássio Monteiro. Reparação de danos e função preventiva da responsabilidade civil: parâmetros para o ressarcimento de despesas preventivas ao dano. **Civilistica.com.** Rio de Janeiro, a. 9, n. 1, 2020. p. 03. Disponível em: <http://civilistica.com/reparacao-por-danos-e-funcao-preventiva/>. Acesso em: 16 set. 2020.
[169] CARRÁ, Bruno Leonardo Câmara. É possível uma responsabilidade civil sem dano? (I). Revista **Consultor Jurídico**, 2016. Disponível em: https://www.conjur.com.br/2016-abr-18/direito-civil-atual-possivel-responsabilidade-civil-dano. Acesso em: 15 set. 2020.

Todavia, o autor julga inconcebível a vertente mais "radical" e "extremada" da responsabilidade sem danos, consubstanciada na função punitiva, ou seja, a hipótese de considerar a mera conduta humana como fator de imputação para incidência de condenações civis, em verdadeiro *punitive damages*. Segundo Carrá, "a responsabilidade civil, completamente alterada em sua essência, teria por finalidade o estabelecimento de regras de comportamento e de modo consequencial a aplicação de sanções eficazes para aqueles que viessem a transgredi-las"[170], asseverando, ainda:

> [...] A gestão do dano na sociedade de risco não precisa ser realizada apenas por meio da responsabilidade civil, que é como uma espécie de mantra para seus defensores. Outros ramos do Direito também possuem vocação para isso e só uma atuação coordenada e conjugada entre eles se revelaria capaz de dar algum efetivo alento às potenciais vítimas do progresso tecnológico. Ao invés de uma cisão da responsabilidade civil, uma gestão "global" dos riscos por meio de um diálogo interdisciplinar entre os vários ramos do Direito destinados a enfrentá-los, cada qual com suas peculiaridades e mantendo seus respectivos constitutivos ontológicos, vem a ser uma opção bem mais ponderada.[171]

Nesse contexto, emerge a questão do dano moral *in re ipsa*, entendido como aquele em que não se faz necessária a prova da ofensa moral à pessoa, sendo este dano presumido porquanto está vinculado à existência do próprio fato ilícito.

Sobre o assunto, Jonas Sales e Paulo Roque Khouri questionam se diante do descumprimento de normas da LGPD o dever de reparação por dano moral seria automático, ou seja, *in re ipsa*. Após a análise de jurisprudências, os autores chegam à conclusão de que "têm andado bem os tribunais pátrios [...] no sentido de não permitir caracterização de dano moral *in re ipsa* pelo simples fato de ocorrer vazamento de dados"[172].

Para eles, neste caso, não incumbe à responsabilidade civil o papel de autorizar a indenização pecuniária pela mera expectativa de dano, sendo mais prudente fazer uso das sanções administrativas previstas na LGPD, pois a "condenação por reparação moral sem demonstração de dano teria tão somente caráter punitivo, o que, como sabido, não é permitido pelo ordenamento jurídico pátrio"[173].

---

[170] *Idem.* É possível uma responsabilidade civil sem dano? (III). Revista **Consultor Jurídico**, 2016. Disponível em: https://www.conjur.com.br/2016-mai-02/direito-civil-atual-possivel-responsabilidade-civil-dano-iii. Acesso em: 15 set. 2020.

[171] *Idem.* É possível uma responsabilidade civil sem dano? (IV). Revista **Consultor Jurídico**, 2016. Disponível em: https://www.conjur.com.br/2016-mai-09/direito-civil-atual-possivel-responsabilidade-civil-dano-iv. Acesso em: 15 set. 2020.

[172] SALES, Jonas; KHOURI, Paulo Roque. Dano moral e LGPD: não se indeniza expectativa de dano. **Migalhas**, 8 jul. 2021. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/348230/dano-moral-e-lgpd-nao-se-indeniza-expectativa-de-dano >. Acesso em: 18 jul. 2021.

[173] SALES, Jonas; KHOURI, Paulo Roque. Dano moral e LGPD: não se indeniza expectativa de dano. **Migalhas**, 8 jul. 2021. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/348230/dano-moral-e-lgpd-nao-se-indeniza-expectativa-de-dano >. Acesso em: 18 jul. 2021.

Corroborando esse entendimento, Aline de Miranda Valverde Terra assevera que "não existe responsabilidade sem dano, nem responsabilidade por mero risco de dano, como se poderia pretender extrair do *caput* do já mencionado artigo 48"[174] da LGPD. Em sua concepção, se não houver danos decorrentes do incidente de segurança, não há que se falar em responsabilidade civil, embora seja possível fazer uso de outras medidas que visem não apenas restabelecer a segurança, mas também prevenir a ocorrência de danos aos titulares.

De forma semelhante, Cássio Monteiro Rodrigues sustenta a impossibilidade de responsabilizar civilmente alguém por mera conduta, seja ela lícita ou ilícita, que não cause prejuízo à esfera jurídica de outrem, sendo inadmissível a indenização do dano hipotético e, pela mesma razão, do perigo ou ameaça de dano[175], considerando a vedação ao enriquecimento sem causa e a determinação legal do art. 944 do Código Civil[176].

Entretanto, na busca por um ponto de intersecção entre a função reparatória e preventiva, defende o autor a possibilidade de ressarcimento de despesas injustas custeadas pela vítima na tentativa de prevenção ao dano, porquanto representaria um significativo avanço do instituto da responsabilidade civil em seu propósito de tutelar a pessoa humana frente aos novos riscos[177].

Afastando-se da esfera reparatória e passando a examinar a possibilidade de utilização de demais mecanismos processuais face aos ilícitos, entende o supracitado autor que "medidas de tutela inibitória material e multas civis não podem ser considerados instrumentos da responsabilidade civil, que deve se ocupar justamente do momento patológico da ilicitude, o dano, e não da simples ilicitude"[178].

Noutra vertente, a respeito das tutelas inibitórias, Marcos Ehrhardt Júnior e Andrey Bruno Cavalcante Vieira[179] sustentam sua qualidade de instrumento voltado ao combate da prática, manutenção ou reiteração de condutas lesivas, circunstância apta para atrair a responsabilização, independentemente da existência de dano. Assim, acreditam que o melhor

---

[174] TERRA, Aline de Miranda Valverde. Hackeamento de dados pessoais e responsabilidade do fornecedor: releitura do CDC pela óptica da LGPD. **Migalhas**, 09 jul. 2021. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-patrimoniais/348292/hackeamento-de-dados-pessoais-e-responsabilidade-do-fornecedor >. Acesso em: 18 jul. 2021.

[175] RODRIGUES, Cássio Monteiro. Reparação de danos e função preventiva da responsabilidade civil: parâmetros para o ressarcimento de despesas preventivas ao dano. **Civilistica.com.** Rio de Janeiro, a. 9, n. 1, 2020. p. 22. Disponível em: <http://civilistica.com/reparacao-por-danos-e-funcao-preventiva/>. Acesso em: 16 set. 2020.

[176] Art. 944. A indenização mede-se pela extensão do dano. BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. **Código Civil.** Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm>. Acesso em: 16 set. 2020.

[177] RODRIGUES, Cássio Monteiro. *Op. cit.*, p. 34.

[178] RODRIGUES, Cássio Monteiro. *Op. cit.*, p. 33.

[179] VIEIRA, Andrey Bruno Cavalcante; EHRHARDT JUNIOR, Marcos. **O direito de danos e a função preventiva: desafios de sua efetivação a partir da tutela inibitória em casos de colisão de direitos fundamentais.** Revista IBERC, Minas Gerais, v. 2, n. 2, p. 01-30, mai-ago./2019.

caminho é a evolução para um sistema jurídico protetor da pessoa humana e de seus direitos fundamentais mediante a união entre os meios inibitórios de direito material e processual, buscando ressignificar a responsabilidade civil. Destacam, ainda, que:

> A tutela inibitória deve assumir posição preferencial em relação à simples tutela reparatória do dano, pois intenta garantir a proteção integral do direito, evitando a ocorrência da lesão e direcionando-se aos consequenciais futuros da conduta, sendo a tutela jurisdicional mais adequada à proteção de direitos não patrimoniais[180].

No tocante à LGPD, podem ser citados alguns exemplos interessantes de atuação preventiva por meio de tutela inibitória. O primeiro deles diz respeito a Ação Civil Pública nº 0733785-39.2020.8.07.0001, ajuizada pelo Ministério Público do Distrito Federal e Territórios (MPDFT), requerendo a concessão de tutela de urgência para determinar que certo anunciante se abstivesse de comercializar dados pessoais de brasileiros, tratados de forma contrária às exigências da LGPD, bem como a suspensão do anúncio e o fornecimento de dados cadastrais do anunciante pelo portal Mercado Livre, plataforma digital de vendas na qual foi veiculado o conteúdo.

Na petição inicial, o MPDFT alegou que a sua Unidade Especial de Proteção de Dados e Inteligência Artificial identificou a comercialização maciça de dados pessoais de brasileiros por meio do *website*, destacando que "pelo teor do anúncio o vendedor deixa claro que possui bases de dados contendo nome, CPF, telefone fixo, telefone celular, *e-mail* e endereço", além de "números de telefones celulares, de todas as operadoras, para uso em *callcenters*, torpedos de voz, SMS e disparos de *WhatsApp*"[181].

Em sede de decisão interlocutória, o Juízo da 17ª Vara Cível de Brasília deferiu a tutela de urgência postulada, valendo-se de princípios da legislação de proteção de dados, destacando a ausência de indícios de que tenha havido consentimento dos titulares, de forma a caracterizar a irregularidade no negócio, em patente violação ao art. 44 da LGPD. Ressaltou, ainda, o confronto de tal prática com o princípio constitucional da inviolabilidade do sigilo de dados, situado no art. 5º, XII, da Constituição Federal e o fundamento do respeito à privacidade, insculpido no art. 2º, I, da Lei 13.709/18.

Em contrapartida, outra ação muito semelhante teve desfecho distinto. Trata-se da ACP nº 0730600-90.2020.8.07.0001 que tramitou perante o Juízo da 5ª Vara Cível de Brasília, julgada extinta sem resolução de mérito, com fundamento na ausência de interesse processual,

---

[180] *Ibidem*.

[181] BRASÍLIA. Cópia da petição inicial relativa à Ação Civil Pública com Pedido de Tutela de Urgência, ajuizada pelo MPDFT [documento alterado para suprimir a presença de dados pessoais]. Disponível em: https://www.mpdft.mp.br/portal/pdf/comunicacao/outubro_2020/ACP_Venda_Mercado_Livre_XXXXXXXXXX.pdf. Acesso em: 18 jun. 2021.

tendo em vista que o *site* acusado de comercializar dados pessoais de milhares de brasileiros estaria em manutenção à época. Tal fato levou o magistrado a supor que os seus responsáveis provavelmente estariam "buscando adequar os seus serviços às normas jurídicas de proteção de dados pessoais"[182], tornada vigente poucos dias antes da sentença, afastando qualquer justificativa para a pretensão de tutela inibitória.

Sobre o caso, convém salientar, primeiramente, que a mera manutenção do *site* não significa o início de um programa de adequação à LGPD, sendo imprescindível a apresentação de provas mais consistentes, tais como esclarecimentos a respeito da política de segurança da informação, regras de mapeamento de dados (*data mapping*), ou mesmo sobre a criação de um comitê interno de *compliance*[183]. Em segundo lugar, a ação foi extinta quando a ré ainda se encontrava na posse dos dados, em situação de flagrante irregularidade ante a ausência de base legal, evidenciando o risco de que ocorram novas violações à privacidade de seus titulares.

Ainda como exemplo, cita-se o pedido de medida cautelar na Ação Direta de Inconstitucionalidade 6.387[184] contra o inteiro teor da Medida Provisória nº 954/2020, por meio da qual as operadoras de telefonia estavam obrigadas a repassar ao Instituto Brasileiro de Geografia e Estatística (IBGE) as relações de nomes, números de telefone e endereços de seus consumidores, pessoas físicas ou jurídicas, com o intuito de manter a continuidade de pesquisas estatísticas durante o período de pandemia causado pela Covid-19.

Pela interpretação da Suprema Corte, a referida MP não definiu apropriadamente de que forma os dados seriam coletados, impossibilitando a aferição quanto a sua adequação e necessidade, além de não ter apresentado mecanismo técnico ou administrativo hábil a proteger o banco de dados de acessos não autorizados, vazamentos acidentais ou utilização indevida. Por essa razão, restaram demonstrados o *fumus boni juris* e *periculum in mora* para possibilitar o deferimento da medida cautelar, suspendendo a eficácia da MP nº 954/2020, "a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel"[185].

---

[182] BRASÍLIA. 5ª Vara Cível de Brasília. Ação Civil Pública nº 0730600-90.2020.8.07.0001. Juiz: Wagner Pessoa Vieira. Brasília, 22 de setembro de 2020. **Migalhas**. Disponível em: https://www.migalhas.com.br/arquivos/2020/9/2AF3CAD38469F2_sentenca_.pdf. Acesso em: 24 jun. 2021.

[183] RODRIGUES, Matheus. Primeiras impressões sobre o uso da LGPD. **ConJur**, 2020. Disponível em: https://www.conjur.com.br/2020-set-27/matheus-rodrigues-primeiras-impressoes-uso-lgpd. Acesso em: 22 jun. 2021.

[184] BRASIL. **Supremo Tribunal Federal.** ADI nº 6.387/DF. Relatora: Ministra Rosa Weber. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629. Acesso em: 24 jun. 2021.

[185] BRASIL. **Supremo Tribunal Federal**. ADI nº 6.387/DF. Relatora: Ministra Rosa Weber. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629. Acesso em: 24 jun. 2021.

Sob o mesmo fundamento de inobservância dos princípios da transparência e do livre acesso, outras demandas vêm sendo propostas, tais como a ação ajuizada no estado de Pernambuco por um estudante, usuário de transporte público, em face do Consórcio de Transportes municipal e do Sindicato das Empresas de Transportes estadual. Em razão da exigência de cadastramento biométrico facial para recarga do bilhete eletrônico, o demandante alegou ter questionado um funcionário acerca da política de privacidade e proteção de dados pessoais da empresa. Como não houve qualquer esclarecimento, o estudante decidiu não consentir em fornecer sua biometria, fato que o impossibilitou de fazer uso de transporte público na condição de estudante. Dessa forma, requereu a concessão da tutela de urgência antecipada para determinar a atualização do cadastro do autor sem o registro de sua biometria facial[186].

Convém lembrar que, embora o agente de tratamento possa se valer do legítimo interesse em algumas hipóteses (art. 11, II e alíneas), prescindindo do consentimento, a exemplo de quando tais dados forem indispensáveis à execução de políticas públicas, persistirá o dever de adotar medidas para garantir a transparência do tratamento de dados e o livre acesso do titular às informações de forma clara, adequada e ostensiva sobre os mecanismos de proteção e segurança desses dados.

Em setembro de 2018, o Tribunal de Justiça de São Paulo deferiu a tutela provisória de urgência pleiteada pelo Instituto brasileiro de Defesa do Consumidor (IDEC) e pela Defensoria Pública Paulista, determinando à ViaQuatro, concessionária da linha 4-Amarela do Metrô de São Paulo, o desligamento das câmeras para reconhecimento facial dos passageiros, por meio de sistema instalado para fins publicitários[187], e captados sem o devido consentimento e sequer ciência dos usuários.

Já no corrente ano, foi proferida a sentença, confirmando a tutela provisória anteriormente concedida e condenando a concessionária ao pagamento de multa de R$ 100 mil[188]. Consoante informações prestadas pela ré nos autos do processo, o sistema não captaria imagens atribuídas a pessoas identificadas, mas tão somente rostos e expressões por meio de algoritmos matemáticos. A empresa argumentou, ainda, que a tecnologia "se limita a contar as

---

[186] PERNAMBUCO. **Processo n.º 0060336-35.2020.8.17.2001.** Petição Inicial. **Conjur**. Disponível em: https://www.conjur.com.br/dl/inicial-bilhete-lgpd.pdf. Acesso em: 22 jun. 2021.

[187] GROSSMANN, Luís Osvaldo. Justiça manda metrô de SP parar coleta de dados e multa em R$ 50 mil por dia. **Convergência Digital**, 17 set. 2018. Disponível em: < https://www.convergenciadigital.com.br/Seguranca/Justica-manda-metro-de-SP-parar-coleta-de-dados-e-multa-em-R$-50-mil-por-dia-48974.html?UserActiveTemplate=site&UserActiveTemplate=mobile%252Csite >. Acesso em: 25 jul. 2021.

[188] POMPEU, Ana; BRITO, Débora. TJSP proíbe captura de dados por câmeras do Metrô de SP e aplica multa de R$ 100 mil. **Jota**, 10 maio 2021. Disponível em: < https://www.jota.info/justica/tjsp-proibe-captura-de-dados-por-cameras-do-metro-de-sp-e-aplica-multa-de-r-100-mil-10052021 >. Acesso em: 25 jul. 2021.

pessoas, visualizações, tempo de permanência, tempo de atenção, gênero, faixas etárias, emoções, fator de visão, horas de pico de visualizações e distância de detecção", de modo que, segundo alegou, "apenas são gerados dados meramente estatísticos"[189].

Para a magistrada Patrícia Martins Conceição, titular da 37ª Vara do Foro Central Cível de São Paulo:

> [...] o reconhecimento facial ou mesmo a mera detecção facial, sem que seja possível a identificação concreta do indivíduo, mas com acesso à sua imagem e face, parece já esbarrar no conceito de dado biométrico, legalmente considerado como dado pessoal sensível, daí porque merece tratamento especial à luz da Lei nº 13.709/2018[190].

É preciso estar atento ao fato de que o uso de tecnologias de reconhecimento facial pode provocar um estado de vigilância constante. Com relação aos sistemas de Inteligência Artificial (IA), caracterizados como de risco elevado, faz-se indispensável o desenvolvimento de uma gestão de riscos contínua, ao longo de todo o período de utilização do sistema, inclusive antes mesmo de sua colocação no mercado, acompanhada de medidas de transparência que possibilitem a aferição do seu grau de segurança[191].

Nesse ponto, Sergio Marcos Carvalho de Àvila Negri traz uma importante reflexão acerca da problemática envolvendo grupos historicamente submetidos a opressões e violências, os quais "podem se mostrar mais expostos a um risco maior de vigilância e de outros danos ocasionados pelo uso de novas tecnologias", concluindo que "a efetiva construção de um modelo pautado na alocação diferencial pressupõe a percepção de que os riscos [...] podem não se distribuir de forma linear entre pessoas e grupos"[192]. Trata-se de tecnologia que impacta diretamente os direitos humanos, devendo seguir uma lógica própria de gestão de riscos, sobretudo no que concerne ao respeito dos direitos dos titulares das informações tratadas.

Assim, ao utilizar-se de princípios que, por sua natureza, possuem extensão semântica e mutabilidade, a LGPD permite uma interpretação em compasso com o vertiginoso avanço da tecnologia, favorecendo, por consequência, a implantação de procedimentos flexíveis de regulação, buscando adequá-la aos ditames constitucionais e preencher lacunas existentes[193].

---

[189] SÃO PAULO. 37ª Vara Cível da Comarca de São Paulo. Ação Civil Pública nº 1090663-42.2018.8.26.0100. Juíza: Patrícia Martins Conceição. 07 de maio de 2021. **Jota.** Disponível em: < https://images.jota.info/wp-content/uploads/2021/05/doc-87156787.pdf?x93516 >. Acesso em: 25 jul. 2021.

[190] *Ibidem.*

[191] NEGRI, Sergio Marcos Carvalho de Ávila. Personalidade, responsabilidade e classificação dos riscos na Inteligência Artificial e na robótica. **Migalhas**, 01 jul. 2021. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/347862/personalidade-responsabilidade-e-classificacao-dos-riscos-na-ia >. Acesso em: 25 jul. 2021.

[192] *Ibidem.*

[193] BUSATTA, Eduardo Luiz. **Do dever de prevenção em matéria de proteção de dados pessoais.** *In*: EHRHARDT JÚNIOR, Marcos; CATALAN, Marcos; MALHEIROS, Pablo (Coord.). Direito Civil e tecnologia. Belo Horizonte: Fórum, 2020. p. 25-56.

Em suma, a lei não trouxe uma resposta concreta e absoluta passível de solucionar as divergências doutrinárias e jurisprudenciais acerca do tema, mas é certo que, ao impor um dever jurídico de prevenção aos agentes de tratamento, sob a forma de princípios e dispositivos esparsos, pretendeu chamar atenção especial para a necessidade de evolução do ordenamento jurídico face aos riscos da atividade de tratamento de dados. Nesse viés, é preciso impulsionar o debate doutrinário e jurisprudencial na busca de soluções que, de algum modo, façam frente às demandas que serão cada vez mais comuns no cotidiano forense.

CONCLUSÃO

O presente trabalho teve por escopo a análise acerca dos diversos aspectos que permeiam a responsabilidade civil retratada na Lei nº 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados – LGPD. Inicialmente, fez-se necessária uma abordagem geral sobre as peculiaridades existentes na lei, sobretudo o seu âmbito de aplicação, os seus objetivos, fundamentos, princípios e direitos previstos, bem como o papel dos sujeitos envolvidos na atividade de tratamento de dados.

A respeito do sistema de responsabilidade civil inaugurado pela LGPD, pode-se classificá-lo como especialíssimo, cuja compreensão encontra-se diretamente ligada aos princípios encartados na lei, especialmente os princípios da segurança, da prevenção e da responsabilização e prestação de contas.

Em síntese, há duas formas de ocorrer a violação da legislação de proteção de dados, seja por meio de ilícitos específicos, relacionados ao descumprimento de deveres contidos expressamente na legislação, seja por meio do ilícito geral, por quebra do dever de segurança que legitimamente é esperado.

Embora a Lei Geral de Proteção de Dados não tenha sido expressa a respeito de qual seria a natureza da responsabilidade dos agentes de tratamento, se objetiva ou subjetiva, depreende-se da interpretação conjunta dos artigos 42 a 45 com todo o corpo normativo da lei, que o legislador pretendeu imputar aos agentes de tratamento o dever de reparação de danos de forma objetiva, alicerçado no fundamento do risco da atividade que é intrínseco ao tratamento de dados.

O risco, configurado como critério-base da responsabilidade civil objetiva, é identificado por meio de diversas limitações às operações de tratamento de dados dispostas ao longo da estrutura da LGPD, exigindo dos sujeitos responsáveis a adoção de medidas aptas a garantir a segurança da atividade.

Para além da avaliação estrutural da Lei Geral de Proteção de Dados, cujos elementos apontam para uma imputação objetiva, é imprescindível estar atento à influência dos ditames constitucionais na responsabilidade civil. A partir do modelo solidarista implantado pela Constituição Federal, despontou a necessidade de ampliar as funções e objetivos da responsabilidade, renunciando cada vez mais aos pressupostos da culpa, a fim de estimular o princípio da justiça distributiva no que concerne ao dever de reparar qualquer dano injusto, mesmo diante da ausência de ilícito na conduta danosa.

Outrossim, não se pode olvidar que as relações consumeristas permanecem sujeitas às regras do Código de Defesa do Consumidor, o qual adota a responsabilidade objetiva, cabendo

ao intérprete necessariamente fazer uso dos princípios, fundamentos e demais preceitos da LGPD no momento de prestar a tutela jurisdicional.

Nesse panorama de crescente evolução tecnológica, é cada vez maior o anseio pela multifuncionalização da responsabilidade civil, fazendo emergir novas perspectivas que fortalecem o debate doutrinário na busca por soluções para os problemas ligados ao tratamento de dados, especialmente por meio da consolidação da função preventiva. Não há dúvidas de que a LGPD se preocupou, por meio de diversos dispositivos ao longo do seu texto, em evitar a ocorrência de danos.

O chamado modelo de "responsabilidade proativa", que aqui se filia, fortalece a noção de que não basta a mera abdicação em descumprir a lei, mas, para muito além disso, exige-se dos agentes de tratamento atitudes proativas e diligentes voltadas à diminuição dos riscos.

A fim de concretizar a ideia de proatividade, a LGPD prevê que os agentes de tratamento poderão desenvolver programas de *compliance*, formulando regras de boas práticas e de governança que estabeleçam, dentre outras coisas, normas de segurança, padrões técnicos, ações educativas e mecanismos internos de supervisão e de mitigação de riscos. No entanto, em razão da facultatividade da norma, faz-se necessária a criação de incentivos para o investimento em tais ações.

Um ponto de partida para essa questão se consubstancia no estímulo a condutas proativas por meio de sanções premiais, representada pela aplicação do parágrafo único do artigo 944 do Código Civil, o qual se apresenta como uma exceção ao princípio da reparação integral diante da hipótese de haver excessiva desproporção entre a culpa do ofensor e o dano, prevendo a possibilidade de redução equitativa da indenização. Trata-se de *standard* de diligência extraordinária praticada pelo agente ofensor que, no intuito de evitar o dano e transcendendo os padrões mínimos estipulados na lei, autoriza o julgador a reduzir o valor devido a título de indenização.

Ao tempo em que o dispositivo atua como forma de estímulo aos agentes econômicos, irradia os seus efeitos positivos para toda a sociedade titular de dados, assegurando uma menor exposição ao risco de dano, em plena conformidade com os preceitos constitucionais e infraconstitucionais, valendo-se da função promocional da responsabilidade civil.

Em suma, depreende-se que, ainda na hipótese de aplicação correta de medidas técnicas e administrativas de segurança e prevenção ao dano, tal fato, por si só, não será o bastante para suprimir a responsabilidade do ofensor, imputada de forma objetiva. Mas, por outro lado, defende-se que uma conduta com alto grau de diligência por parte do agente de tratamento

poderá repercutir em um segundo plano da responsabilidade civil, qual seja, o momento de definição do *quantum* indenizatório.

Tal conclusão culmina na propositura de um modelo híbrido de responsabilidade, caracterizado pela combinação das teorias objetiva e subjetiva. Seguindo esse modelo, a responsabilidade do ofensor deverá ser primeiramente fixada com fundamento no risco da atividade, valendo-se no nexo da imputação objetiva, a fim de resguardar o direito constitucional da vítima de ser indenizada pelo dano sofrido. Já na fase seguinte de definição do *quantum debeatur*, filia-se à tese doutrinária menos tradicional, porém a mais promissora, cuja ideia central é a redução equitativa da indenização na hipótese de cumprimento do *standard* de diligência extraordinária por parte do agente de tratamento, pautado na culpa, visando pôr em prática os princípios da responsabilidade proativa.

Além disso, a função preventiva da responsabilidade pode ser fomentada por meio de outros mecanismos, ainda que antecedentes ao dano. Embora seja aqui adotado o posicionamento de que a mera conduta humana não poderá ser considerada fator de imputação do dever de indenizar, sendo descabível a caracterização de dano moral *in re ipsa* por violação à LGPD, não restam dúvidas de que outros instrumentos terão grande relevância no papel de combater condutas potencialmente danosas e que estejam em desacordo com a norma.

Ganha destaque, nesse cenário, o uso da tutela inibitória como ferramenta processual de combate à execução, continuidade ou reiteração de atos danosos, em aliança com a função preventiva da responsabilidade. Nesse desiderato, os titulares poderão exercer o seu direito à autodeterminação informativa em face de todos os sujeitos que de alguma forma estejam em posse ou controle de seus dados pessoais, exigindo deles a transparência e o livre acesso às informações de forma clara, adequada e ostensiva sobre a forma de tratamento e medidas empregadas na proteção e segurança de dados, a fim de prevenir a ocorrência de lesões irreparáveis aos direitos da personalidade.

Portanto, a interpretação da Lei Geral de Proteção de Dados deverá estar sempre em diálogo com as demais fontes do direito, atenta às modificações sociais e inovações tecnológicas, lançando mão de todas as normas protetivas em favor da pessoa humana, buscando sempre conformar o Direito Civil com a Constituição, de forma a assentar que os pilares da dignidade da pessoa humana, solidariedade social e justiça distributiva deverão guiar toda a sistemática do dever de reparação e prevenção de danos.

REFERÊNCIAS

ALVES, Fabrício da Mota; VIEIRA, Gustavo Afonso Sabóia. Sem a ANPD, a LGPD é um problema, não uma solução. **JOTA**, 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/anpd-lgpd-problema-solucao-06012020>. Acesso em: 20 mar. 2020.

ANGELO, Tiago. Decisão pioneira: Juíza aplica LGPD e condena construtora que não protegeu dados de cliente. Revista **Consultor Jurídico**, 2020. Disponível em: https://www.conjur.com.br/2020-set-30/compartilhar-dados-consumidor-terceiros-gera-indenizacao. Acesso em: 06 out. 2020.

ARTICLE 29. ***Opinion* 03/2013 *on purpose limitation*.** 02 de abril de 2013. p. 19-20. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>. Acesso em: 18 mar. 2020.

_____. ***Opinion* 1/2010 *on the concepts of "controller" and "processor".*** 16 de fevereiro de 2010. p. 01. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf>. Acesso em: 18 mar. 2020.

BARRETO JUNIOR, Irineu Francisco; NASPOLINI, Samyra Haydêe Dal Farra. Proteção de informações no mundo virtual: a LGPD e a determinação de consentimento do titular para tratamento de dados pessoais. *In*: **Cadernos Adenauer**, volume 3, Ano XX, 2019. p. 142-143.

BIONI, Bruno. 2.3.1 Dados sensíveis e o tratamento sensível de dados triviais: a interface com o direito de isonomia e não discriminação. L.83 [livro digital, Kindle]. *In:* **Proteção de dados pessoais. A função e os limites do consentimento**. 2ª ed. Rio de Janeiro: Forense, 2019.

_____. **Xequemate**, o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. São Paulo: GPOPAI USP, 2015. Disponível em: https://www.academia.edu/28752561/Xeque-Mate_o_trip%C3%A9_de_prote%C3%A7%C3%A3o_de_dados_pessoais_no_xadrez_das_iniciativas_legislativas_no_Brasil. Acesso em: 19 mar. 2020.

BOBBIO, Norberto (traduzido por Carlos Nelson Coutinho). **A Era dos Direitos**. 8ª ed. Rio de Janeiro: Campus, 1992.

BODIN DE MORAES, Maria Celina. A constitucionalização do direito civil e seus efeitos sobre a responsabilidade civil. *In*: **Direito, Estado e Sociedade**, v.9, n. 29, p. 233/258, jul/dez de 2006.

_____. **Dano à Pessoa Humana: uma leitura Civil-Constitucional dos danos morais.** São Paulo: Renovar, 2003, p. 157/158.

_____. LGPD: um novo regime de responsabilização civil dito "proativo". **Civilistica.com**. Rio de Janeiro: a. 8, n. 3, 2019. Disponível em: <http://civilistica.com/lgpd-um-novo-regime/>. Acesso em: 15 mar. 2020.

_____. Risco, solidariedade e responsabilidade objetiva. **Revista dos Tribunais**, São Paulo, v. 854, ano 95, dez. 2006, p. 11-37.

BODIN DE MORAES, Maria Celina; QUEIROZ, João Quinelato de. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD. *In*: **Cadernos Adenauer**, volume 3, Ano XX, 2019. p. 126.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**: promulgada em 05 de outubro de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm >. Acesso em: 05 mar. 2021.

_____. Lei nº 10.406, de 10 de janeiro de 2002. **Código Civil.** Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm>. Acesso em: 07 mar. 2021.

_____. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm#art65 >. Acesso em: 07 mar. 2020.

_____. Lei nº 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor (CDC).** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm . Acesso em: 06 jan. 2021.

_____. Supremo Tribunal Federal (STF). **RHD 22/DF**, Pleno, j. 19.09.1991, m. v., rel. Min. Marco Aurélio, rel. p/ acórdão Ministro Celso de Mello, DJ 01.09.1995.

_____. Supremo Tribunal Federal. **ADI nº 6.387/DF**. Relatora: Ministra Rosa Weber. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629. Acesso em: 24 jun. 2021.

BRASÍLIA. 5ª Vara Cível de Brasília. Ação Civil Pública nº 0730600-90.2020.8.07.0001. Juiz: Wagner Pessoa Vieira. Brasília, 22 de setembro de 2020. **Migalhas**. Disponível em: https://www.migalhas.com.br/arquivos/2020/9/2AF3CAD38469F2_sentenca__.pdf. Acesso em: 24 jun. 2021.

_____. Cópia da petição inicial relativa à Ação Civil Pública com Pedido de Tutela de Urgência, ajuizada pelo MPDFT [documento alterado para suprimir a presença de dados pessoais]. Disponível em: https://www.mpdft.mp.br/portal/pdf/comunicacao/outubro_2020/ACP_Venda_Mercado_Livre_XXXXXXXXXX.pdf. Acesso em: 18 jun. 2021.

_____. Parecer sobre o Projeto de Lei da Câmara nº 53, de 2018, p. 10. **Agência Senado.** Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7751566&ts=1571776637073&disposition=inline>. Acesso em: 26 fev. 2020.

BRUNO, Marcos Gomes da Silva. Capítulo VI, dos agentes de tratamento de dados pessoais, art. 44. *In*: MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (org.). **LGPD: Lei Geral de Proteção de Dados Comentada**. 2ª ed. São Paulo: Revista dos Tribunais, 2019. Não paginado. [Livro digital].

BUCAR, Daniel; VIOLA, Mario. Tratamento de dados pessoais por "legítimo interesse do controlador": primeiras questões e apontamentos. In: FRAZÃO, Ana; TEPEDINO, Gustavo;

OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. Editora Revista dos Tribunais, 2019. Não paginado [livro digital].

BUCCO, Rafael. Senado indica seus representes no Conselho Nacional de Proteção de Dados Pessoais. **Tele.síntese**, 06 nov. 2019. Disponível em: <https://www.telesintese.com.br/senado-indica-seus-representantes-no-conselho-nacional-de-protecao-de-dados-pessoais/>. Acesso em: 20 mar. 2020.

BUSATTA, Eduardo Luiz. Do dever de prevenção em matéria de proteção de dados pessoais. *In*: EHRHARDT JÚNIOR, Marcos; CATALAN, Marcos; MALHEIROS, Pablo (Coord.). **Direito Civil e tecnologia**. Belo Horizonte: Fórum, 2020. p. 25-56.

CARNEIRO, Isabelle *et al*. Tratamento de dados pessoais. 1.4. Legítimo interesse do controlador. *In:* FEIGELSON, Bruno *et al* (org.). **Comentários à Lei Geral de Proteção de Dados – Lei 13.709/2018.** São Paulo: Revista dos Tribunais, 2019. Não paginado [livro digital].

CARRÁ, Bruno Leonardo Câmara. É possível uma responsabilidade civil sem dano? (I). Revista **Consultor Jurídico**, 2016. Disponível em: https://www.conjur.com.br/2016-abr-18/direito-civil-atual-possivel-responsabilidade-civil-dano. Acesso em: 15 set. 2020.

_____. É possível uma responsabilidade civil sem dano? (III). Revista **Consultor Jurídico**, 2016. Disponível em: https://www.conjur.com.br/2016-mai-02/direito-civil-atual-possivel-responsabilidade-civil-dano-iii. Acesso em: 15 set. 2020.

_____. É possível uma responsabilidade civil sem dano? (IV). Revista **Consultor Jurídico**, 2016. Disponível em: https://www.conjur.com.br/2016-mai-09/direito-civil-atual-possivel-responsabilidade-civil-dano-iv. Acesso em: 15 set. 2020.

COLOMBO, Cristiano; FACCHINI NETO, Eugênio. "Corpo Elettronico" como vítima de ofensas em matéria de tratamento de dados pessoais: reflexões acerca da responsabilidade civil por danos à luz da Lei Geral de Proteção de Dados pessoais brasileira e a viabilidade da aplicação da noção de dano estético ao mundo digital. *In*: ROSENVALD, Nelson; DRESCH, Rafael de Freitas Valle; WESENDONCK, Tula (coord.). **Responsabilidade civil: novos riscos.** Indaiatuba: Foco, 2019. p. 45-64.

CONJUR. Banco de dados deve notificar compartilhamento de informações. Revista **Consultor Jurídico,** 26 fev. 2020. Disponível em: https://www.conjur.com.br/2020-fev-26/banco-dados-notificar-compartilhamento-informacoes. Acesso em: 05 out. 2020.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais comentada.** 2ª ed. São Paulo: Revista dos Tribunais, 2019. Não paginado [livro digital].

DATA GUIDANCE. *Israel government approves mobile tracking monitor coronavírus quarentine enforcement. **Data Guidance**,* 2020. Disponível em: <https://platform.dataguidance.com/news/israel-government-approves-mobile-tracking-monitor-coronavirus-quarantine-enforcement>. Acesso em: 27 mar. 2020.

DE CASTRO, André Zanatta Fernandes; MARQUES, Fernanda Mascarenhas. Segurança, competitividade e a necessária adequação à LGPD. **Conjur**, 2021. Disponível em: https://www.conjur.com.br/2021-mar-26/opiniao-seguranca-competitividade-adequacao-lgpd. Acesso em: 26 mar. 2021.

DONEDA, Danilo. **A criptografia no direito brasileiro**. São Paulo: Revista dos Tribunais, 2019. Não paginado [livro digital].

_____. **Da privacidade à proteção de dados pessoais:** Fundamentos da lei geral de proteção. 2ª ed. São Paulo: Revista dos Tribunais. 2020. Não paginado [livro digital].

DRESCH, Rafael de Freitas Valle; FALEIROS JÚNIOR, José Luiz de Moura. **Reflexões sobre a responsabilidade civil na Lei Geral de Proteção de Dados (Lei nº 13.709/2018)**. *In*: ROSENVALD, Nelson; DRESCH, Rafael de Freitas Valle; WESENDONCK, Tula (coord.). Responsabilidade civil: novos riscos. Indaiatuba: Foco, 2019. p. 65-89.

DRESCH, Rafael de Freitas Valle; STEIN, Lílian Brandt. Direito fundamental à proteção de dados e responsabilidade civil. **Revista de Direito da Responsabilidade**. Portugal: ano 3, 2021. p. 224-241. Disponível em: https://revistadireitoresponsabilidade.pt/2021/direito-fundamental-a-protecao-de-dados-e-responsabilidade-civil-rafael-de-freitas-valle-dresch-lilian-brandt-stein/. Acesso em: 07 mar. 2021.

DRESCH, Rafael. A especial responsabilidade civil na Lei Geral de Proteção de Dados. **Migalhas,** 2020. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/330019/a-especial-responsabilidade-civil-na-lei-geral-de-protecao-de-dados > Acesso em: 31 jul. 2020.

EHRHARDT JR, Marcos; PEIXOTO, Erick. **Os desafios da compreensão do direito à privacidade no sistema jurídico brasileiro em face das novas tecnologias.** *In:* RJLB. Pp. 389-418, ano 6 (2020), nº 2. p. 414.

EHRHARDT JR., Marcos. Responsabilidade civil ou direito de danos? Breves reflexões sobre a inadequação do modelo tradicional sob o prisma do direito civil constitucional. pp. 303-314. *In*: RUZYK, Carlos Eduardo Pianovski *et al*. (Org.). **Direito civil constitucional: a ressignificação da função dos institutos fundamentais do direito civil contemporâneo e suas consequências.** Florianópolis: Conceito Editorial, 2014. p. 312.

EHRHARDT JR., Marcos. **Responsabilidade civil pelo inadimplemento da boa-fé.** Belo Horizonte: Fórum, 2017. 2 ed. p. 131.

EHRHARDT JR., Marcos; SILVA, Gabriela Buarque. **Privacidade e proteção de dados pessoais durante a pandemia da Covid-19.** JusBrasil. Disponível em: <https://marcosehrhardtjr.jusbrasil.com.br/artigos/824475623/privacidade-e-protecao-de-dados-pessoais-durante-a-pandemia-da-covid-19?ref=feed>. Acesso em: 26 mar. 2020.

EHRHARDT JR., Marcos; VIEIRA, Andrey Bruno Cavalcante. **O direito de danos e a função preventiva: desafios de sua efetivação a partir da tutela inibitória em casos de colisão de direitos fundamentais.** Revista IBERC, Minas Gerais, v. 2, n. 2, p. 01-30, mai-ago./2019.

ESTADOS UNIDOS. *18 U.S. Code § 1030 - Fraud and related activity in connection with computers*. ***Legal Information Institute*** **[LII].** Disponível em: https://www.law.cornell.edu/uscode/text/18/1030. Acesso em: 01 maio 2020

FRAZÃO, Ana. **Nova LGPD: direitos dos titulares de dados pessoais.** A 9ª parte de uma série sobre as repercussões para a atividade empresarial. JOTA. 24/10/2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-direitos-dos-titulares-de-dados-pessoais-24102018#sdfootnote1sym> . Acesso em: 29 jul. 2020.

GLOBO. *Site* brasileiro de classificados de empregos revela que invasores tiveram acesso indevido a banco de dados. **Globo.com**. Disponível em: https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2020/06/10/site-brasileiro-de-classificados-de-empregos-revela-que-invasores-tiveram-acesso-indevido-a-banco-de-dados.ghtml. Acesso em: 28 ago. 2020.

GOMES, Helton Simões. Tim quer rastrear celular para monitorar se doente de Covid-19 sai de casa. **UOL**, 2020. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2020/03/26/tim-quer-rastrear-celular-para-monitorar-se-doente-de-covid-19-sai-de-casa.htm>. Acesso em 27 mar. 2020.

GROSSMANN, Luís Osvaldo. Justiça manda metrô de SP parar coleta de dados e multa em R$ 50 mil por dia. **Convergência Digital**, 17 set. 2018. Disponível em: < https://www.convergenciadigital.com.br/Seguranca/Justica-manda-metro-de-SP-parar-coleta-de-dados-e-multa-em-R$-50-mil-por-dia-48974.html?UserActiveTemplate=site&UserActiveTemplate=mobile%252Csite >. Acesso em: 25 jul. 2021.

GUEDES, Gisela Sampaio da Cruz; VENCELAU, Rose Melo. Término do tratamento de dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. Editora Revista dos Tribunais, 2019. Não paginado [livro digital].

JIMENE, Camilla do Vale. Capítulo VII, da segurança e das boas práticas, art. 46. *In*: MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (org.). **LGPD: Lei Geral de Proteção de Dados Comentada**. 2ª ed. São Paulo: Revista dos Tribunais, 2019. Não paginado. [Livro digital].

LESSIG, Lawrence. *Code, version* 2.0. Nova York: *Basic Books*, 2006. p. 39. Disponível em: <http://codev2.cc/download+remix/Lessig-Codev2.pdf>. Acesso em: 21 mar. 2020.

LIMA, Alvino. **Culpa e risco**. São Paulo: Revista dos Tribunais, 1998. 2 ed. p. 116.

LIMA, Mariana. **Titular, Operador e Controlador – o que isso quer dizer?.** Disponível em: <https://triplait.com/titular-operador-e-controlador/>. Acesso em: 19. Mar. 2020.

LÔBO, Paulo Luiz Netto. Direito Civil: **Obrigações,** volume II. 7ª ed. São Paulo: Saraiva, 2019. p. 46.

_____. Novas perspectivas da constitucionalização do direito civil. **Jus Navigandi**, Teresina, ano 18 (/revista/edicoes/2013), n. 3754 (/revista/edicoes/2013/10/11), 11 (/revista/edicoes/2013/10/11) out. (/revista/edicoes/2013/10) 2013 (/revista/edicoes/2013). Disponível em: <http://jus.com.br/artigos/25361>. Acesso em: 25 mar. 2021.

MENDES, Laura Schertel. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. **Caderno Especial LGPD**. p. 35-56. São Paulo: Revista dos Tribunais, novembro 2019.

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

MULHOLLAND, Caitlin. A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco? **Migalhas**, 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: 14 set. 2020.

NEGRI, Sergio Marcos Carvalho de Ávila. Personalidade, responsabilidade e classificação dos riscos na Inteligência Artificial e na robótica. **Migalhas**, 01 jul. 2021. Disponível em: < https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/347862/personalidade-responsabilidade-e-classificacao-dos-riscos-na-ia >. Acesso em: 25 jul. 2021.

OHM, Paul. *Broken promises of privacy: responding to the surprising failure of anonymization*. In: **UCLA *Law Review***, [s. l.], v. 57, n. 6, p. 1701–1777, 2010.

OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria. Capítulo 2. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018; Introdução. *In:* FRAZÃO, Ana *et al* (org.). **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** São Paulo: Thomson Reuters, 2019. Não paginado [livro digital].

OLIVEIRA, Ricardo Alexandre. Lei Geral de Proteção de Dados Pessoais e seus impactos no ordenamento jurídico. **Revista dos Tribunais**. vol. 998/2018. p. 241 – 261. Dez/2018, p. 03.

PASQUALOTTO, Adalberto. Causalidade e imputação na responsabilidade civil objetiva. *In*: ROSENVALD, Nelson; DRESCH, Rafael de Freitas Valle; WESENDONCK, Tula (coord.). **Responsabilidade civil: novos riscos.** Indaiatuba: Foco, 2019. p. 199-217.

PERNAMBUCO. **Processo n.º 0060336-35.2020.8.17.2001.** Petição Inicial. Conjur. Disponível em: https://www.conjur.com.br/dl/inicial-bilhete-lgpd.pdf. Acesso em: 22 jun. 2021.

POMPEU, Ana; BRITO, Débora. TJSP proíbe captura de dados por câmeras do Metrô de SP e aplica multa de R$ 100 mil. **Jota**, 10 maio 2021. Disponível em: < https://www.jota.info/justica/tjsp-proibe-captura-de-dados-por-cameras-do-metro-de-sp-e-aplica-multa-de-r-100-mil-10052021 >. Acesso em: 25 jul. 2021.

REDAÇÃO. Proteção de dados: relembre seis casos de vazamentos. **Conecta Já**, 27 jan. 2020. Disponível em: <https://conectaja.proteste.org.br/casos-de-vazamentos-de-dados/>. Acesso em: 26 mar. 2020.

RIGUES, Rafael. Dados de 250 mil consumidores da Natura são expostos em vazamento. **Olhar Digital**, 19 de maio de 2020. Disponível em: https://olhardigital.com.br/noticia/dados-de-250-mil-consumidores-da-natura-sao-expostos-em-vazamento/100957. Acesso em: 27 ago. 2020.

RODOTÀ, Stefano. (traduzido por: DONEDA, Danilo; MORAES, Maria Celina Bodin) **A Vida na Sociedade da Vigilância: A privacidade hoje.** Rio de Janeiro: Renovar, 2008.

RODOVALHO, Thiago. Responsabilidade civil objetiva: da culpa à objetivação da responsabilidade - responsável, mas não culpado. **Migalhas**, 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/336454/responsabilidade-civil-objetiva--da-culpa-a-objetivacao-da-responsabilidade---responsavel--mas-nao-culpado. Acesso em: 13 mar. 2020.

RODRIGUES, Cássio Monteiro. Reparação de danos e função preventiva da responsabilidade civil: parâmetros para o ressarcimento de despesas preventivas ao dano. **Civilistica.com.** Rio de Janeiro, a. 9, n. 1, 2020. Disponível em: <http://civilistica.com/reparacao-por-danos-e-funcao-preventiva/>. Acesso em: 16 set. 2020.

RODRIGUES, Matheus. Primeiras impressões sobre o uso da LGPD. **ConJur**, 2020. Disponível em: https://www.conjur.com.br/2020-set-27/matheus-rodrigues-primeiras-impressoes-uso-lgpd. Acesso em: 22 jun. 2021.

ROSENVALD, Nelson. O *compliance* e a redução equitativa da indenização na LGPD. *In*: **Migalhas**, 2021. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/342032/o-compliance-e-a-reducao-equitativa-da-indenizacao-na-lgpd. Acesso em: 12 maio 2021.

SALES, Jonas; KHOURI, Paulo Roque. Dano moral e LGPD: não se indeniza expectativa de dano. **Migalhas**, 8 jul. 2021. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/348230/dano-moral-e-lgpd-nao-se-indeniza-expectativa-de-dano >. Acesso em: 18 jul. 2021.

SÃO PAULO. 37ª Vara Cível da Comarca de São Paulo. Ação Civil Pública nº 1090663-42.2018.8.26.0100. Juíza: Patrícia Martins Conceição. 07 de maio de 2021. **Jota.** Disponível em: < https://images.jota.info/wp-content/uploads/2021/05/doc-87156787.pdf?x93516 >. Acesso em: 25 jul. 2021.

SCHWARTZ, Paul M.; SOLOVE, Daniel J. ***The PII Problem: Privacy and a New Concept of Personally Identifiable Information*.** In: *New York University Law Review*, [s. l.], v. 86, n. *December*, p. 1814–1894, 2011, p. 1817. Disponível em: <https://lawcat.berkeley.edu/record/1124577?ln=en>. Acesso em: 21 mar. 2020.

SENADO FEDERAL. Sancionada com vetos lei geral de proteção de dados pessoais. **Agência Senado**, 15 out. 2018. Disponível em: <https://www12.senado.leg.br/noticias/materias/2018/08/15/sancionada-com-vetos-lei-geral-de-protecao-de-dados-pessoais >. Acesso em: 26 fev. 2020.

SÉNECA, Hugo. CNPD: Hospital do Barreiro multado em 400 mil euros por permitir acessos indevidos a processos clínicos. **Exame Informática**, 19 de outubro de 2018. Disponível em: <https://visao.sapo.pt/exameinformatica/noticias-ei/mercados/2018-10-19-cnpd-hospital-do-barreiro-multado-em-400-mil-euros-por-permitir-acessos-indevidos-a-processos-clinicos/>. Acesso em: 02 ago. 2020.

SMITH, Nicola. *Taiwan uses smartphones monitor patients quarantined vírus scare.* ***The Telegraph***, 03 fev. 2020. Disponível em: <https://www.telegraph.co.uk/news/2020/02/03/taiwan-uses-smartphones-monitor-patients-quarantined-virus-scare/>. Acesso em: 27 mar. 2020.

SOMERVILLE, Heather. *Uber to pay $148 million to settle data breach cover-up with U.S. states.* **Discovery Thomson Reuters**, 26 de setembro de 2018. Disponível em:

https://www.reuters.com/article/us-uber-databreach/uber-settles-for-148-million-with-50-us-states-over-2016-data-breach-idUSKCN1M62AJ. Acesso em: 02 abr. 2020.

TAMER, Maurício Antonio; VAINZOF, Rony; LIMA, Caio César Carvalho. Compliance e LGPD: Plano de adequação como ferramenta de mitigação de riscos legais. **Jota**, 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/compliance-e-lgpd-plano-de-adequacao-como-ferramenta-de-mitigacao-de-riscos-legais-07042019. Acesso em: 12 maio 2021.

TEFFÉ, Chiara Spadaccini de. Por que precisamos de uma Autoridade Nacional de Proteção de Dados? **JOTA**, 2020. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/por-que-precisamos-de-uma-autoridade-nacional-de-protecao-de-dados-07012020#sdfootnote5anc>. Acesso em: 20 mar. 2020.

TERRA, Aline de Miranda Valverde. Hackeamento de dados pessoais e responsabilidade do fornecedor: releitura do CDC pela óptica da LGPD. **Migalhas**, 09 jul. 2021. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-patrimoniais/348292/hackeamento-de-dados-pessoais-e-responsabilidade-do-fornecedor >. Acesso em: 18 jul. 2021.

THE ECONOMIST. *The world's most valuable resource is no longer oil, but data.* ***The Economist****,* 06 maio 2017. Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em: 20 abr. 2020.

UNIÃO EUROPEIA. ***Draft Code of Conduct on privacy for mobile health applications*** ("Projeto de código de conduta sobre privacidade para aplicativos móveis de saúde"). Publicado em 07.06.2016. pp. 07-08. Disponível em: file:///C:/Users/LeNovo/Downloads/CodeofConductfinaldraft.pdf. Acesso em: 10 mar. 2020.

UNIÃO EUROPEIA. ***Guidelines on Consent under Regulation* 2016/679**. Disponível em: http://portaldaprivacidade.com.br/wp-content/uploads/2017/12/wp29_consent-12-12-17.pdf. Acesso em 19 jul. 2020.

UNIÃO EUROPEIA. ***Guidelines on Personal data breach notification under Regulation 2016/679.*** *European Commission.* Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052. Acesso em: 18 maio 2020.

UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, 23 abr. 2016 (*General Data Protection Regulation*). ***Intersoft Consulting*****.** Disponível em: < https://gdpr-info.eu//>.

UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, 23 abr. 2016 (*General Data Protection Regulation*). *Recital* 43. **GDPR *Text***. Disponível em: <https://gdpr-text.com/pt/read/recital-43/ >. Acesso em: 21 jul. 2020.

UNIÃO EUROPEIA. **Síntese Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais**. *Rights and Translation unit, Public Affairs and Communications Directorate*, 2002. Disponível em: <http://www.oecd.org/sti/ieconomy/15590254.pdf>. Acesso em 26 fev. 2020.

VAINZOF, Rony. Capítulo I, disposições preliminares, art. 5º. *In*: MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (org.). **LGPD: Lei Geral de Proteção de Dados Comentada**. 2ª ed. São Paulo: Revista dos Tribunais, 2019. Não paginado [livro digital].

VENOSA, Sílvio de Salvo. Sanção premial. *In*: **Migalhas**, 2019. Disponível em: https://www.migalhas.com.br/depeso/298207/sancao-premial. Acesso em: 06 jun. 2021.