UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS

FACULDADE DE DIREITO

A LGPD E O FUNDAMENTO DA RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS: UMA ANÁLISE SOBRE O DANO MORAL DECORRENTE DE VAZAMENTO DE DADOS

MARIA EDUARDA LANA MEDINA

Rio de Janeiro

2021

MARIA EDUARDA LANA MEDINA

A LGPD E O FUNDAMENTO DA RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS: UMA ANÁLISE SOBRE O DANO MORAL DECORRENTE DE VAZAMENTO DE DADOS

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do **Professor Dr. Carlos Augusto Silva dos Santos Thomaz.**

Rio de Janeiro

2021

Medina, Maria Eduarda Lana
MM491l A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: uma análise sobre o dano moral decorrente de vazamento de dados / Maria Eduarda Lana Medina. -- Rio de Janeiro, 2021.
66 f.

Orientador: Carlos Augusto Silva dos Santos Thomaz.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade Nacional de Direito, Bacharel em Direito, 2021.

1. Lei 13.709/2018. 2. Proteção de dados pessoais. 3. Vazamento de dados. 4. Responsabilidade Civil Subjetiva. I. Thomaz, Carlos Augusto Silva dos Santos , orient. II. Título.

MARIA EDUARDA LANA MEDINA

A LGPD E O FUNDAMENTO DA RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS: UMA ANÁLISE SOBRE O DANO MORAL DECORRENTE DE VAZAMENTO DE DADOS

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do **Professor Dr. Carlos Augusto Silva dos Santos Thomaz.**

Data da Aprovação: 04/06/2021.

Banca Examinadora:

_____

Professor Dr. Carlos Augusto Silva dos Santos Thomaz
Orientador

_____

Professor Dr. Carlos Eduardo Mendes de Azevedo
Membro da Banca

Rio de Janeiro,

2021

AGRADECIMENTOS

É com muita felicidade que encerro mais um ciclo em minha vida: a conclusão desta monografia e consequente formatura na Universidade Federal do Rio de Janeiro. Ao longo desses cinco anos, estive acompanhada de pessoas que foram essenciais para que alcançasse as minhas metas.

Agradeço, primeiramente, à minha família, pelo apoio incondicional e por estarem sempre ao meu lado. À minha mãe, por ser a minha fonte inesgotável de amor e cumplicidade que recarregou as minhas energias todos os dias ao longo dessa etapa. Ao meu pai, por sempre estar presente me incentivando com um conselho certeiro ou uma palavra de descontração, me mostrando o equilíbrio com que devo levar as adversidades. Ao meu irmão, mais novo calouro desta faculdade em que me formo, por ser meu exemplo de garra e determinação nos estudos. Obrigada por serem a minha fonte de motivação na busca pelos meus objetivos. Sem vocês a realização deste sonho não seria possível!

Agradeço também aos meus amigos, que, estando ao meu lado durante toda a graduação, vivenciaram comigo momentos que estarão guardados na memória. Da divisão de cadernos de transcrição à divisão de barracas em jogos jurídicos, vocês fizeram com que a faculdade fosse uma das melhores fases da minha vida.

À todos aqueles com os quais tive a oportunidade de trabalhar e que foram fundamentais para o meu crescimento pessoal e profissional, através das instituições em que estagiei: a Defensoria Pública do Estado do Rio de Janeiro, o escritório Saud Advogados, o Tribunal de Justiça do Estado do Rio de Janeiro, o Tribunal Regional do Trabalho e a Procuradoria Geral do Estado do Rio de Janeiro. Em especial, faço questão de destacar a gratidão à minha chefe no Núcleo do Sistema Penitenciário, Dra. Lisete, com a qual mantive uma relação de amizade, além do campo profissional.

Agradeço ao professor Carlos Augusto, pela orientação e atenção dedicada a este trabalho e ao meu amigo Tarcísio, agora colega de profissão, que auxiliou na escolha deste tema e contribuiu para a pesquisa.

Por último, agradeço à Faculdade Nacional de Direito e ao seu corpo docente, instituição que me possibilitou um enorme aprendizado durante toda a graduação e da qual me despeço com um imenso carinho que levarei para sempre no meu coração.

RESUMO

A presente monografia apresenta uma análise sobre o instituto da responsabilidade civil na Lei Federal nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados, com enfoque na defesa da responsabilidade subjetiva e da culpa como fundamento do regime estabelecido pela LGPD, em que o dano moral decorrente de vazamento de dados não deve ser considerado *in re ipsa*. O principal objetivo deste trabalho é demonstrar que o simples vazamento de dados, por si só, não deve implicar a imediata responsabilização dos agentes de tratamento. Não desconhece que é dever daqueles que tratam dados pessoais envidar os melhores esforços para sua proteção, contudo, far-se-ia necessária a prova da lesão efetiva para ocorrência dos danos morais. A pesquisa aborda o instituto da responsabilidade civil desde antes da entrada em vigor da LGPD até o debate travado atualmente quanto ao regime adotado pelo legislador, demonstrando os argumentos favoráveis às duas correntes formadas. Por se tratar de uma legislação visivelmente recente, este estudo não tem a pretensão de esgotar o tema tratado. Apesar da Lei nº 13.709/2018 ter entrado em vigor em 16 de agosto de 2020, os artigos das sanções entrarão em vigor apenas em 1º de agosto de 2021, nos termos da Lei 14.010/2020. Entretanto, busca-se com este trabalho de conclusão de curso contribuir para a discussão acadêmica e compartilhar os conhecimentos adquiridos ao longo de seu desenvolvimento.

Palavras-chave: Lei 13.709/2018; Proteção de dados pessoais; Vazamento de dados; Responsabilidade Civil Subjetiva.

ABSTRACT

This undergraduate thesis presents an analysis of the civil liability institute in Law 13.709/2018, known as the General Data Protection Law, with a focus on the defense of subjective liability and guilt as the foundation of the type established by the mentioned Law, in which the moral damage resulting from data breach should not be considered *in re ipsa*. The main purpose of this work is to demonstrate that the simple breach of data should not imply the immediate responsibility of the data processing agents. It is common knowledge that it is the duty of those who deal with personal data to make the best efforts to protect them, however, it would be necessary to prove the actual lesion in order for moral damages to occur. The research addresses the institute of civil liability from before the implementation of the mentioned Law until the debate currently held on the regime adopted by the legislator, demonstrating the arguments in favor of the two currents constituted. As it is a visibly recent legislation, this study does not intend to exhaust the topic discussed. Although Law 13.709/2018 came into force on August 16, 2020, the articles of the sanctions will only come into effect on August 1, 2021, under the terms of Law 14.010/2020. However, this work aims to contribute to the academic discussion and share the knowledge acquired throughout its development.

Keywords: Law 13.709/2018; Protection of personal data; Data breach; Subjective Civil Liability.

SUMÁRIO

1. INTRODUÇÃO.....09

2. A EVOLUÇÃO HISTÓRICA DA PROTEÇÃO DE DADOS NO BRASIL.....13

2.1. As Mudanças da Responsabilidade Civil no Tratamento de Dados Pré-LGPD.....17

3. RESPONSABILIDADE CIVIL NA LGPD.....22

3.1. Noções Propedêuticas da Responsabilidade Civil.....22

3.2. Agentes de Tratamento de Dados.....26

3.3. Responsabilidade Civil na Lei Geral de Proteção de Dados.....31

3.4. Responsabilidade Objetiva.....34

3.5. Responsabilidade Subjetiva.....39

4. O DANO MORAL DECORRENTE DE VAZAMENTO DE DADOS.....45

4.1. A Frequência dos Vazamentos de Dados e a Fragilidade das Medidas de Segurança.....45

4.2. O Dano Moral Decorrente de Vazamento de Dados não deve ser considerado *In Re Ipsa*.....46

4.3. Culpa Exclusiva de Terceiro.....47

4.4. Os Direitos da Personalidade não podem servir como Instrumento de Mercantilização do Instituto do Dano Moral.....50

4.5. A Jurisprudência Comparada e os Danos Morais Decorrentes da Violação de Dados Pessoais.....51

4.5.1. A Experiência Canadense – Dicotomia Da Prova Dos Danos.....52

4.5.1.1. Precedente Li versus Equifax.....52

4.5.1.2 Precedente Bourbonnière versus Yahoo!.....53

4.5.2. A Jurisprudência Norte-Americana – Sem Prova do Dano, não há Processo.....54

4.5.3 A Experiência Europeia – *General Data Protection Regulation*.....55

5. CONCLUSÃO.....59

6. REFERÊNCIAS BIBLIOGRÁFICAS.....61

1. INTRODUÇÃO

Este trabalho de conclusão de curso tem como objetivo traçar uma análise sobre o instituto da responsabilidade civil à luz da Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709, sancionada em 14 de agosto de 2018 e em vigor a partir de agosto de 2020.

Busca-se com o presente estudo discutir acerca da natureza jurídica de responsabilidade civil adotada pelo legislador demonstrando que, embora a Lei Geral de Proteção de Dados não seja explícita, diversos motivos levam a crer que o regime adotado, como regra, é o da responsabilidade subjetiva, devendo haver a prova da conduta culposa do agente de tratamento na ocasião do dano.

Indubitavelmente, a revolução tecnológica concentrada nas tecnologias da informação proporcionou não somente a facilidade na coleta, tratamento e desfecho de dados, como sua essencialidade em todos os ramos. Como bem nos aponta Demócrito:

> "A disseminação do uso de computadores fez com que, nos dias atuais, não somente as agências governamentais que tradicionalmente coletavam dados pessoais, a exemplo dos Correios, os Departamentos de Trânsito e as repartições do Fisco, funcionassem como poderosos centros de processamento de informações pessoais, mas também todas as empresas privadas hoje adquiriram os meios para coletar, manipular, armazenar e transmitir dados de uma forma simples e a um custo relativamente baixo."[1]

Na era digital, é praticamente unanimidade que todos possuem o acesso a internet ou possuirão alguma vez na vida. O Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), em sua última pesquisa TIC Domicílios[2], que trata do uso das tecnologias de informação e comunicação nos domicílios brasileiros, observou que a proporção de usuários de Internet no Brasil segue uma tendência de crescimento observada nos últimos anos, chegando a 70% em 2018. Isso representa uma estimativa de aproximadamente 127 milhões de indivíduos.

Ademais, em 2020, a pandemia da Covid-19 levou a um aumento inevitável no uso de tecnologias digitais devido às medidas de restrição de circulação de pessoas adotadas no

---

[1] REINALDO, Demócrito. **Direito da Informática: Temas Polêmicos**. Bauru/SP: EDIPRO, 2002. P. 26.

[2] TIC Domicílios. Publicado pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br). 2018. Disponível em <https://www.cetic.br/media/docs/publicacoes/2/12225320191028-tic_dom_2018_livro_eletronico.pdf > Acesso em 03/04/2021.

enfrentamento da doença. A internet tornou-se uma ferramenta fundamental para lidar com o isolamento e mitigar os efeitos do isolamento, tornando-se indispensável para garantir a comunicação, o acesso à informação, o comércio eletrônico, a prestação de serviços públicos, o trabalho remoto e o ensino a distância.

Devido ao aumento exponencial do uso da Internet e da dependência da sociedade nas comunicações digitais, consequentemente os dados tornaram-se cada vez mais relevantes. Em abril de 2020, Martin McKeay, Diretor editorial da Akamai Technologies, Inc. publicou um artigo de blog[3] relatando que a empresa observou um aumento de 30% no tráfego da internet quando os confinamentos da pandemia começaram, o que desencadeia um maior consumo de dados.

Os dados encontram-se em qualquer lugar, numa pesquisa no Google, num cadastro de perfil no Instagram, na procura por um destino no Waze ou numa compra no Ifood. Tudo que é feito virtualmente é convertido em dados que podem ser coletados seja para fins comerciais e empresariais, como para fins educacionais, de pesquisa e lazer. Essa realidade foi resumida em uma frase que agitou o mundo dos negócios citada por Clive Humby, um matemático londrino especializado em ciência de dados: "Os dados são o novo petróleo", em tradução livre para o significado original, "*Data is the new oil*"[4].

Com efeito, surgiu a expressão *data driven economy*, ou, em outras palavras, a economia movida a dados, para ilustrar o fato de que a fase atual do capitalismo está baseada na extração e uso de dados pessoais, como bem descreve Nick Srnicek[5].

Diante dessa realidade de dependência virtual, a internet foi elevada ao patamar de ferramenta tecnológica mais eficaz de comunicação sendo quase que obrigatório que todos a usem para realização de alguma tarefa no seu cotidiano. Lamentavelmente, junto com os avanços e benefícios percebidos com a evolução da internet, tornaram-se cada vez mais corriqueiros os ataques de terceiros mal-intencionados.

---

[3] Disponível em < https://blogs.akamai.com/sitr/2020/04/the-building-wave-of-internet-traffic.html >. Acesso em 12/04/2021.
[4] Disponível em < https://bakertillybr.com.br/dados-novo-petroleo/ > Acesso em 12/04/2021.
[5] SRNICEK, Nick. ***Platform capitalism***. Cambridge: Polity Press, 2018. P. 39.

Inegavelmente o tratamento de informações na internet em âmbito empresarial, dentre as quais dados pessoais, se dá de forma muito fluída, de modo que o seu armazenamento em provedores de nuvem é uma prática deveras usual. Conforme alerta o advogado David G. Ries, em artigo publicado no site da *American Bar Association*:

> "Falhas de segurança se tornaram tão prevalentes que há um novo mantra em cibersegurança atualmente: 'É quando e não se', um escritório de advocacia ou alguma outra empresa sofrerá um vazamento."[6]

Ilustrando o que ora se aduz, oportuno pontuar o estudo[7] realizado pela empresa Akamai Technologies, Inc., por meio do qual foi identificada a ocorrência de mais de 28 bilhões de ataques cibernéticos ocorridos entre maio e dezembro de 2018, o que se traduz em mais de 115 milhões de ataques por dia.

Recentemente, grandes corporações como Dunkin Donuts[8], Dailymotion[9], Nest[10], Reddit[11] e AdGuard[12] foram alvo de ataques que culminaram com vazamento de dados de seus usuários. Em janeiro de 2021, um ataque creditado ao banco de dados da Serasa Experian culminou com pacotes de dados com informações pessoais, como CPF, número de celular, fotos, salário e a pontuação no score de inadimplência da empresa, de mais de 223 milhões de brasileiros disponíveis em fóruns usados por criminosos digitais. O caso é considerado o mais grave do tipo já ocorrido no Brasil[13].

Nesse diapasão, ganha especial relevância a discussão acerca da responsabilidade dos agentes de tratamento, em virtude de vazamento de dados decorrentes de ataques cibernéticos,

---

[6] Livre tradução de: "Security breaches are becoming so prevalent that there is a new mantra in cybersecurity today: *"It's when not if," a law firm or other entity will suffer a breach".* Disponível em <https://www.americanbar.org/groups/law_practice/publications/techreport/2017/security/>. Acesso em 26/08/2020.

[7] Disponível em <https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-retail-attacks-and-api-traffic-report-2019.pdf>. Acesso em 26/08/2020.

[8] Disponível em <https://oglobo.globo.com/economia/cibercriminosos-fazem-planos-de-fidelizacao-perderem-us-1-bilhao-por-ano-nos-eua-23662569>. Acesso em 26/08/2020.

[9] Disponível em <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/dados-de-milhoes-de-usuarios-do-site-dailymotion-vazam-na-web.html>. Acesso em 26/08/2020.

[10] Disponível em <https://tecnoblog.net/351638/google-nest-speaker-alto-falante-inteligente-confirmado/>. Acesso em 26/08/2020.

[11] Disponível em <https://www.tecmundo.com.br/seguranca/132813-reddit-assume-invasao-vazamento-dados.htm>. Acesso em 26/08/2020.

[12] Disponível em <https://sensorstechforum.com/pt/adguard-ad-blocker-hacked-reset-passwords/>. Acesso em 26/08/2020.

[13] Disponível em < https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2021/01/25/vazamentos-de-dados-expoem-informacoes-de-223-milhoes-de-numeros-de-cpf.ghtml > Acessado em 12/04/2021.

estipulada pela nova Lei Geral de Proteção de Dados. Não desconhece que é dever daqueles que tratam dados pessoais envidar os melhores esforços para sua salvaguarda e proteção.

Contudo, como demonstrado, a ocorrência cada vez mais frequente de ataques aos dados pessoais de usuários na rede mundial de computadores é um fardo decorrente da evolução tecnológica. Resta notória a dicotomia entre os benefícios pela troca de informações instantâneas e o surgimento de novos problemas a serem solucionados pelo Direito.

É necessário entender que, neste cenário, segurança absoluta não existe[14]. Uma empresa pode adotar as melhores e mais sofisticadas práticas de Segurança da Informação, investir em tecnologia de ponta, estabelecer as melhores políticas de conduta em seu Programa de Governança em Privacidade e, ainda assim, ser vítima de falhas ou invasões acarretando incidentes de segurança.

Diante disso, o vazamento de informações cadastrais, sem nenhuma repercussão específica na esfera do titular, não deve implicar na imediata responsabilização e dever de indenizar dos agentes de tratamento de dados, pois não gera dano moral na medida em que não ofende a dignidade humana.

Pontua-se que a metodologia utilizada é a do método dedutivo, consubstanciado no critério qualitativo, em pesquisa doutrinária, legal e jurisprudencial. Todo argumento dedutivo reformula ou enuncia de modo explícito a informação já contida nas premissas.[15]

Por fim, salienta-se que, por se tratar de uma legislação visivelmente recente, este estudo não tem a pretensão de esgotar o tema tratado. Apesar da Lei nº 13.709/2018 ter entrado em vigor em 16 de agosto de 2020, os artigos das sanções entrarão em vigor apenas em 1º de agosto de 2021, nos termos da Lei 14.010/2020. Entretanto, busca-se com este trabalho de conclusão de curso contribuir para a discussão acadêmica e compartilhar os conhecimentos adquiridos ao longo de seu desenvolvimento.

---

[14] JIMENE, Camilla do Vale. **Da Importância da Segurança da Informação para Adequação à LGPD**. In: BLUM, Renato Opice (Organizador). **Proteção de Dados: Desafios e Soluções na Adequação à Lei**. Rio de Janeiro: Editora Forense, 2020. P. 47.

[15] LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas, 2003. P. 91.

2. A EVOLUÇÃO HISTÓRICA DA PROTEÇÃO DE DADOS NO BRASIL

Apesar de parecer uma temática recente dada a popularidade crescente nos últimos anos, a proteção de dados já é debatida há mais tempo do que aparenta, tendo em vista que a primeira lei sobre o tema surgiu na Alemanha, ainda em 1970, em pleno século XX.

A partir da década de 1970, o rápido avanço da informática e da indústria nos países mais desenvolvidos e, consequentemente, as crescentes ameaças à privacidade teria impulsionado os estados a criarem normas para regular a proteção de dados, como, por exemplo, a lei de dados da Suécia (1973), a lei federal de proteção de dados da Alemanha (1977), o *Privacy Act* nos Estados Unidos da América (1974).

Até agosto de 2018, o Brasil não dispunha de legislação específica para a proteção de dados pessoais. Verificavam-se apenas legislações esparsas que tangenciavam o tema de proteção de dados pessoais e das consequências do vazamento indevido para terceiros não autorizados.

Entre nós, a proteção de dados poderia ser tutelada, ainda que em grau insuficiente, com base em dispositivos estabelecidos na Constituição Federal, como a inviolabilidade da intimidade e da vida privada[16], o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas[17] e a previsão do remédio constitucional habeas data[18].

Além disso, um dos primeiros diplomas legais a tratar do assunto é o Código de Defesa do Consumidor, que disciplinou regras específicas a respeito de bancos de dados e cadastros de consumidores, em seu artigo 43[19]. Cabe registrar também a Lei nº 12.414/2011, que disciplina

---

[16] Art. 5º da CF, inciso X: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação."

[17] Art. 5º da CF, inciso XII: "é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal."

[18] Art. 5º da CF, inciso LXXII: "conceder-se-á 'habeas-data': a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;"

[19] Art. 43 do CDC: "O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. § 3º O consumidor, sempre que encontrar inexatidão nos seus dados

o cadastro positivo e tem como objetivo regulamentar o disposto no CDC, e a Lei nº 12.527/2011, que regula o acesso a informações públicas.

A Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que dispõe sobre a tipificação criminal de delitos cibernéticos, introduziu no Código Penal o artigo 154-A, estabelecendo ser crime "invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita".

Todos esses diplomas servem de base para a proteção de dados, entretanto não previam, e nem seria possível, a dimensão que tomaria o mercado de dados, como se encontra hodiernamente.

Apenas com o Marco Civil da Internet, instituído como Lei nº 12.965/2014, é que se tem propriamente uma lei que trate da proteção de dados pessoais em todas as esferas, prevendo que o uso da internet no Brasil tem como princípios a proteção da privacidade e a proteção de dados pessoais.

Nessa perspectiva, aponta a doutrina[20] que o país já dispunha de mais de 40 normas que direta e indiretamente tratavam da proteção à privacidade e aos dados pessoais. Todavia, a Lei Geral de Proteção de Dados vem substituir e/ou complementar esse arcabouço regulatório, que por vezes trazia insegurança jurídica e não oferecia garantias adequadas às partes.

Com o desenvolvimento de tecnologias cada vez mais sofisticadas para o tratamento de dados e a ampliação da capacidade de armazenamento de informações, o Direito enquanto ciência se viu obrigado a editar e atualizar no ordenamento jurídico instrumentos legais específicos capazes de garantir efetiva proteção aos dados pessoais.

---

e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. § 4º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público. § 5º Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores. § 6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor."

[20] MONTEIRO, Renato Leite. **Lei Geral de Proteção de Dados do Brasil: análise contextual detalhada**. *Jota*, 14 de julho de 2018. Disponível em < https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada-14072018 > Acesso em 13/04/2021.

Nesse cenário em que há uma atenção maior à destinação que é dada aos dados, seguindo a tendência mundial e acompanhando a necessidade do mercado nacional de apresentar compatibilidade com a legislação europeia para continuar suas atividades, o Brasil estabeleceu a Lei Geral de Proteção de Dados.

Essa lei resulta de um árduo trabalho de quase oito anos. O processo legislativo começou em 2010, com a abertura de uma consulta pública sobre o tema, promovida pelo Ministério da Justiça, que resultou, posteriormente, na propositura do PL 5.276/2016, anexado ao PL 4060/2012, perante a Câmara dos Deputados.

Após 2 anos de trâmite no Congresso Nacional (Câmara e Senado), duas consultas públicas, mais de 2500 contribuições de especialistas de todos os setores, a Lei Geral de Proteção de Dados foi sancionada em 14 de agosto de 2018.

O início da vigência seria em 18 meses desde a publicação, mas, em dezembro de 2018, o então Presidente Temer editou a Medida Provisória nº 869, de 27 de dezembro de 2018, prevendo a criação da ANPD e alterando o início da vigência da lei para agosto de 2020.

Importante ressaltar que, apesar da Lei nº 13.709/2018 ter entrado em vigor em 16 de agosto de 2020, os artigos das sanções entrarão em vigor apenas em 1º de agosto de 2021, nos termos da Lei nº 14.010/2020.

Patrícia Peck Pinheiro, em sua obra, leciona que:

> "A Lei nº 13.709/2018 é um novo marco legal brasileiro de grande impacto, tanto para as instituições privadas como para as públicas, por tratar da proteção dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais, por qualquer meio, seja por pessoa natural, seja por pessoa jurídica. É uma regulamentação que traz princípios, direitos e obrigações relacionadas ao uso de um dos ativos mais valiosos da sociedade digital, que são as bases de dados relacionadas as pessoas."[21]

A nova Lei Geral de Proteção de Dados foi uma resposta a lacuna até então presente, regulando a privacidade e o poder dos dados pessoais dos usuários da rede mundial de computadores, bem como garantindo a transparência sobre informações coletadas, o poder das

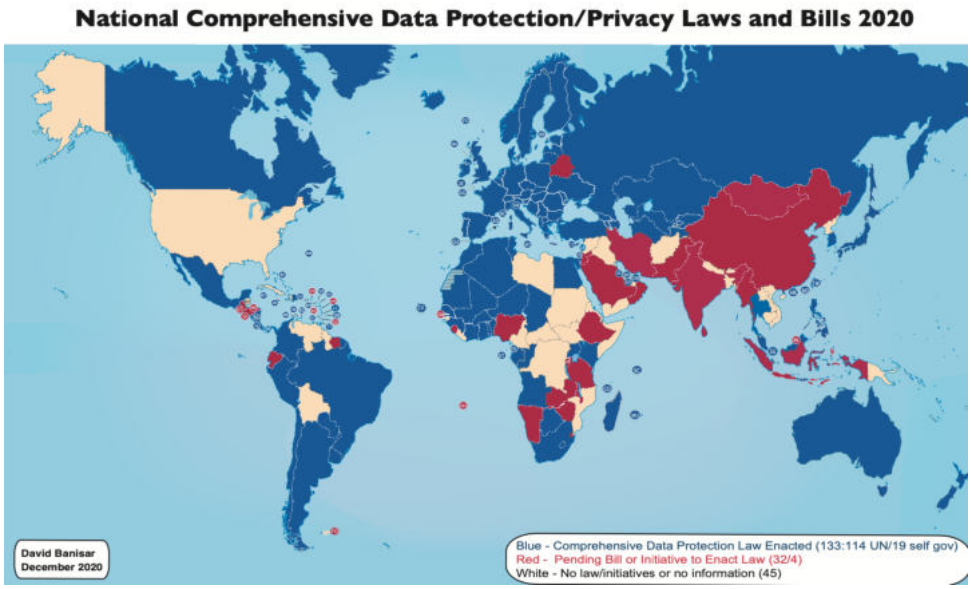
[21] PINHEIRO, Patrícia P. **Proteção de Dados Pessoais: Comentários à Lei nº 13.709/2018**. 1. ed. São Paulo: Saraiva Educação, 2018. P. 15.

entidades reguladoras que fiscalizam as organizações e empresas que lidam com esse tipo de conteúdo.

Fato é que se não houver maior cuidado em relação à proteção dos dados pessoais, é possível a consolidação do cenário descrito pelo historiador israelense Yuval Harari[22] ao apontar, em sua obra, que: "Se quisermos evitar a concentração de toda a riqueza e de todo o poder nas mãos de uma pequena elite, a chave é regulamentar a propriedade dos dados."

Destarte, com o sancionamento da Lei Geral de Proteção de Dados, ou apenas LGPD, o Brasil junta-se a diversos países que já possuíam legislação específica sobre o tema, tornando-se mais competitivo no contexto de uma sociedade cada vez mais movida a dados.

Mais de 130 países e jurisdições e territórios autônomos em todo o mundo já adotaram leis de proteção de dados. Outros quase 40 países e jurisdições, incluindo China, Nigéria, Irã e Indonésia, têm projetos de lei ou iniciativas pendentes, conforme pesquisa realizada pelo advogado David Banisar[23], em novembro de 2020:



A legislação brasileira, apesar de já contar com leis esparsas que tutelam a proteção de dados, agora conta com uma delimitação mais específica e precisa do tema, passando a

[22] HARARI, Yuval Noah. **21 Lições para o Século 21**. Trad. Paulo Geiger. São Paulo: Companhia das Letras, 2018. P. 107.
[23] Disponível em < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416 > Acesso em 12/04/2021.

disciplinar e proteger de forma eficiente e rigorosa o tratamento de dados pessoais no país, estipulando sanções para quando for constatado violações a essas regulamentações.

2.1 As mudanças da responsabilidade civil no tratamento de dados pré-LGPD

A responsabilidade civil é possivelmente o instituto que melhor dialoga com as mudanças sociais[24]. De forma geral, o dano causado pelo ilícito sempre foi combatido pelo Direito. No tocante ao tratamento de dados, somente teve sua previsão expressa com o Marco Civil da Internet.

Para uma melhor compreensão do tema, cumpre definir o que são provedores de serviços de internet, para em seguida explorar o que são provedores de aplicações de internet, bem como quais são os atos ilícitos de terceiros pelos quais estes últimos podem ser responsabilizados.

Marcel Leonardi, em sua obra[25], leciona que provedor de serviços de internet é gênero do qual as demais categorias são espécies. Portanto, provedor de internet é a pessoa natural ou jurídica que fornece serviços relacionados ao funcionamento da internet, ou por meio desta. Dentro do gênero dos provedores de serviços de internet encontram-se as algumas espécies, dentre as quais cabe mencionar: o provedor de informação, o provedor de conteúdo e o provedor de hospedagem.

Conforme define Leonardi, o provedor de informação é quem cria a informação[26]. Logo, é o efetivo autor da informação. Enquanto, o provedor de conteúdo e o provedor de hospedagem são definidos pelo jurista como:

> "O provedor de conteúdo é toda pessoa natural ou jurídica que disponibiliza na Internet as informações criadas ou desenvolvidas pelos provedores de informação, utilizando para armazená-las servidores próprios ou os serviços de um provedor de hospedagem."[27]

> "Provedor de hospedagem é a pessoa jurídica que fornece o serviço de armazenamento de dados em servidores próprios de acesso remoto, possibilitando o acesso de terceiros a esses dados, de acordo com as condições estabelecidas com o contratante do serviço."[28]

---

[24] CASTRONOVO, Carlo. **La nuova responsabilità civile**. Milano: Giuffrè, 2006. P. 102.
[25] LEONARDI, Marcel. **Responsabilidade Civil dos Provedores de Serviços de Internet**. São Paulo: Editora Juarez de Oliveira, 2005.
[26] Ibid. P. 30.
[27] Ibid. P. 30.
[28] Ibid. P. 30.

O Marco Civil da Internet classifica o provedor de conteúdo e o provedor de hospedagem como provedores de aplicações de internet[29]. O provedor de aplicação de internet pode ser definido como "qualquer pessoa jurídica que, através de um terminal conectado à internet, fornece um conjunto de funcionalidades que podem ser acessadas pelos usuários"[30].

Assim, o que se pretende analisar é a responsabilidade civil desses provedores de aplicações por atos ilícitos praticados por terceiros (provedores de informação), disponibilizados na internet em suas respectivas aplicações de internet: websites, portais, redes sociais, entre outros.

Anteriormente à promulgação do Marco Civil da Internet, o Superior Tribunal de Justiça consolidou o procedimento do *notice and take down*, que mencionava a necessidade de notificação extrajudicial do provedor de aplicação para a retirada de qualquer conteúdo que entendesse ilícito, a qual deveria ser atendida no prazo de 24 horas, sob pena de ser responsabilizado solidariamente com o terceiro autor do ilícito pelo dano causado.

O julgado que é por alguns considerado o *leading case* da matéria teria sido o REsp 1.193.764/SP[31], cujo julgamento foi realizado pela Terceira Turma, em que se restringiu a responsabilização à notificação prévia do provedor, conforme destaca a ementa:

> "4. O dano moral decorrente de mensagens com conteúdo ofensivo inseridas no site pelo usuário não constitui risco inerente à atividade dos provedores de conteúdo, de modo que não se lhes aplica a responsabilidade objetiva prevista no art. 927, parágrafo único, do CC/02.
>
> 5. Ao ser comunicado de que determinado texto ou imagem possui conteúdo ilícito, deve o provedor agir de forma enérgica, retirando o material do ar imediatamente, sob pena de responder solidariamente com o autor direto do dano, em virtude da omissão praticada."

Esse entendimento foi consolidado por diversos precedentes da Terceira e Quarta Turmas, como o AgRg no REsp 1402104/RJ[32], julgado pela Quarta Turma, cuja ementa afirma expressamente que:

> "2. A responsabilidade subjetiva do agravante se configura quando: I) ao ser comunicado de que determinado texto ou imagem tem conteúdo ilícito, por ser ofensivo, não atua de forma ágil, retirando o

---

[29] Art. 5º do Marco Civil da Internet: "VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet;"

[30] FLUMIGNAN, Wévertton Gabriel Gomes. **Responsabilidade civil dos provedores no Marco Civil da Internet (lei 12.965/14)**. Dissertação de Mestrado Faculdade de Direito, Universidade de São Paulo, 2018. P. 67.

[31] BRASIL. Superior Tribunal de Justiça. Recurso Especial 1.193.764/SP. Rel. Ministra Nancy Andrighi. Terceira Turma. Julgado em 08/08/2011.

[32] BRASIL. Superior Tribunal de Justiça. Agravo Regimental no Recurso Especial 1.402.104/RJ. Rel. Ministro Raul Araújo. Quarta Turma. Julgado em 27/05/2014.

material do ar imediatamente, passando a responder solidariamente com o autor direto do dano, em virtude da omissão em que incide; II) não mantiver um sistema ou não adotar providências, que estiverem tecnicamente ao seu alcance, de modo a possibilitar a identificação do usuário responsável pela divulgação ou a individuação dele, a fim de coibir o anonimato."

Percebe-se, portanto, que no cenário anterior ao Marco Civil da Internet, a única possibilidade remanescente de responsabilidade civil dos provedores de aplicações de internet por conteúdo de terceiros era a responsabilidade civil culposa prevista no art. 186 do Código Civil[33]. A referida culpa poderia se materializar de duas maneiras, ambas por atos omissivos: (i) por não promover a remoção do conteúdo ofensivo diante da ciência de sua publicação tempestivamente, e, (ii) por não tomar as medidas necessárias para permitir a identificação do usuário, autor do ilícito, e prevenir o seu anonimato.

O advento do Marco Civil da Internet foi um divisor de águas no que tange à responsabilidade civil para provedores de internet, com a responsabilidade dos provedores de aplicações de internet sofrendo as mudanças mais significativas.

O caput do art. 19 trouxe a previsão do *judicial notice and take down,* caso em que o provedor de aplicações de internet somente seria responsabilizado civilmente por danos advindos de conteúdo gerado por terceiros após deixar de cumprir em tempo hábil ordem judicial específica determinando sua retirada[34]. Esse dispositivo contraria anterior posicionamento de que esta notificação poderia ser extrajudicial.

Excepcionalmente, prevê o art. 21, que é dever do provedor de conteúdo remover conteúdo de nudez ou atos sexuais privados, publicados sem consentimento, mediante simples notificação extrajudicial, sob pena de ser subsidiariamente responsável[35].

---

[33] Art. 186 do CC: "Aquele que, por ação ou omissão voluntária, negligência ou imprudên- cia, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito."

[34] Art. 19, Lei 12.965/14: "Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário. (...)"

[35] Art. 21, Lei 12.965/14: "O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo. Parágrafo único. A notificação prevista no caput deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido."

Cabe ressaltar que o prévio monitoramento do conteúdo gerado por terceiros não faz parte dos serviços prestados pelos provedores de aplicação, pois seu exercício poderia implicar em censura e violação de garantias constitucionais dos usuários e certamente viria de encontro a um dos elementos essenciais do serviço prestado: a propagação da informação.

Atenta-se que em relação aos provedores de conexão, que são aqueles que exercem uma função intermediária fornecendo serviços que consistem em possibilitar o acesso de seus usuários à internet, não há que se falar em responsabilidade civil por eventual conteúdo disponibilizado por terceiros, visto que os serviços que presta são apenas instrumentais, e não há condições técnicas de avaliar as informações nem o direito de interceptá-las. É o que se aduz do art. 18[36].

Ainda assim, os provedores de conexão devem estar atentos aos artigos 13[37] e 15[38] da lei que tratam da sua responsabilidade no que diz respeito a preservar e fornecer os registros eletrônicos utilizados na prática ilícita. Deverão ser mantidos os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança pelo prazo de 6 (seis) meses, nos termos do art. 15 e pelo prazo de 1 (um) ano, nos termos do art. 13. Ao ser

---

[36] Art. 18, Lei 12.965/14: "O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros."

[37] Art. 13, Lei 12.965/14: "Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento. §1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros. §2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput. §3º Na hipótese do §2º, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no caput. §4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no §2º, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no §3º. §5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo. §6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência."

[38] Art. 15, Lei 12.965/14: "O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento. §1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no caput a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado. §2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no caput, observado o disposto nos §§3º e 4º do art. 13. §3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo. §4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência."

requisitado por ordem judicial, estes dados devem ser prontamente disponibilizados, evitando que o provedor de conexão seja responsabilizado por descumprimento da lei.

Deste modo, resta a responsabilidade do provedor como sendo subjetiva, pois para a caracterização da teoria da responsabilidade objetiva deveria ser estipulado como dever do provedor o controle do conteúdo postado pelos usuários, pois, assim, a divulgação das informações pelos provedores estaria caracterizada como atividade de risco inerente às atividades do provedor.

No âmbito da Lei Geral de Proteção de Dados, o instituto da responsabilidade civil está regulamentado na Seção III do Capítulo VI, sob o título "Da Responsabilidade e do Ressarcimento de Danos", trazendo as principais regras de responsabilidade civil que irão reger as relações que envolvem tratamento de dados pessoais. Entretanto, o legislador não foi explícito quanto à espécie de responsabilidade adotada, se objetiva ou subjetiva, gerando amplo debate na doutrina.

3. RESPONSABILIDADE CIVIL NA LGPD

3.1 Noções propedêuticas da responsabilidade civil

Tal como ocorre quando da adoção de novas tecnologias, também caminha a adequação da responsabilidade civil, ajustando-se às necessidades identificadas e surgidas com o progresso, com o aparecimento de novas atividades e da multiplicação das adversidades causadas pela vida moderna.

A noção da responsabilização ao reparar dano injustamente causado, por ser própria da natureza humana, existe desde os primórdios da civilização. Todavia, a maneira de reparação deste dano foi transformando-se ao longo do tempo, evoluindo conforme a dinâmica da sociedade.

Em rápidas pinceladas, o instituto da responsabilidade civil tem a sua previsão desde as mais primitivas expressões do Direito, tendo a sua trajetória iniciada juntamente com a responsabilidade penal, com base na regra de Talião – olho por olho, dente por dente – caracterizada por uma vingança privada e, finalmente, chegando aos dias de hoje, em que há um afastamento da sua função sancionatória e um enfoque na função reparatória, deslocando-se assim a ênfase outrora atribuída ao ofensor para o ofendido.

Sobre mais, esclarecem os autores Gagliano e Pamplona Filho[39] em sua obra que o conceito jurídico de responsabilidade pressupõe uma atividade danosa de alguém que, atuando, a priori ilicitamente, viola uma norma jurídica preexistente (legal ou contratual), subordinando-se, dessa forma, às consequências do seu ato (obrigação de reparar).

Na mesma esteira, ressaltando que sem a violação de um dever jurídico previamente existente, não há que se falar em responsabilidade civil, expõe Sergio Cavalieri Filho:

> "Em seu sentido etimológico, responsabilidade exprime a ideia de obrigação, encargo, contraprestação. Em sentido jurídico, o vocábulo não foge dessa ideia. A essência da responsabilidade está ligada à noção de desvio de conduta, ou seja, foi ela engendrada para alcançar as condutas praticadas de forma contraria ao direito e danosas a outrem. Designa o dever que alguém tem de reparar o prejuízo decorrente da violação

[39] GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo Curso de Direito Civil: Responsabilidade Civil**. 15. ed. São Paulo: Saraiva, 2017. P. 872.

> de um outro dever jurídico. Em apertada síntese, responsabilidade civil é um dever jurídico sucessivo que surge para recompor o dano decorrente da violação de um dever jurídico originário."[40]

O sistema jurídico brasileiro adotou, no Código Civil de 2002, o modelo dualista de responsabilidade civil, fixando tanto uma norma geral de responsabilidade civil subjetiva, quanto uma cláusula geral de responsabilidade civil objetiva. Com efeito, essas duas facetas da responsabilidade divergem no tocante aos fundamentos que justificam a incidência do dever de indenizar.

Em que pese haja essa distinção, os requisitos para que se reconheça a aplicabilidade do instituto da responsabilidade civil são os mesmos em ambas as classificações: a conduta, o dano e o nexo de causalidade entre os dois primeiros. Como se pode notar, as soluções serão idênticas, independentemente da modalidade empregada, pois uniformes são os seus efeitos: a reparação patrimonial do dano sofrido, cuja indenização é medida de acordo com a sua extensão[41].

Aspecto essencial para que se configure o dever de indenizar, o conceito jurídico de dano sofreu alterações no decorrer do tempo. Antes, baseado na Teoria da Diferença, em que, segundo Maria Celina Bodin:

> "Tradicionalmente, define-se dano patrimonial como a diferença entre o que se tem e o que se teria, não fosse o evento danoso. A assim chamada 'Teoria da Diferença', devida à reelaboração de Friedrich Mommsen, converteu o dano numa dimensão matemática e, portanto, objetiva e facilmente calculável." [42]

A definição cunhada pela Teoria da Diferença, em que se identificava o dano como uma diferença entre o patrimônio antes do evento danoso e após a sua ocorrência, foi abandonada em favor de uma noção normativa do dano.[43]

Nesse sentido, o dano passa a ser compreendido como a lesão a qualquer interesse jurídico merecedor de tutela. Expondo Clóvis Veríssimo do Couto e Silva que o conceito jurídico de interesse determina:

> "(...) a extensão do dano que alguém esteja obrigado a indenizar. Se a noção de dano fosse simplesmente um conceito naturalista, seriam as leis da física que dariam as regras próprias para a fixação dos limites do

---

[40] CAVALIERI FILHO, Sergio. **Programa de Responsabilidade Civil**. 10. ed. rev. e ampl. São Paulo: Atlas, 2012. P. 02.

[41] Art. 944 do CC: "A indenização mede-se pela extensão do dano. Parágrafo único. Se houver excessiva desproporção entre a gravidade da culpa e o dano, poderá o juiz reduzir, equitativamente, a indenização."

[42] MORAES, Maria Celina Bodin de. **Danos à pessoa humana - uma leitura civil-constitucional dos danos morais**. Rio de Janeiro: Renovar, 2003. P. 143.

[43] TERRA, Aline de Miranda. GUEDES, Gisela Sampaio da Cruz. TEPEDINO, Gustavo (Orgs.). **Responsabilidade Civil**. Rio de Janeiro: Forense, 2020. P. 30.

> dano indenizável. Entretanto, há uma noção física de dano e uma noção jurídica. Como sucede muitas vezes, a norma jurídica seleciona uma fração do fato social para transformá-lo numa situação jurídica. Alude-se esse propósito à noção de interesse violado"[44]

Em suma, com essa releitura do pressuposto central da responsabilidade civil, a tendência é a de que a indenização pelo dano gerado passa a ser medida tão somente pelos impactos da lesão na vítima, independentemente de qualquer consideração acerca do ofensor ou de seu patrimônio.

De igual importância, outro pressuposto para a imputação da responsabilidade civil é a conduta do ofensor, devendo-se analisar se fundamentada na culpa ou no risco.

Como observado, no modelo dualista consolidado no ordenamento jurídico pátrio, coexistem paralelamente a responsabilidade subjetiva, que tem como base a conduta ilícita, e a responsabilidade objetiva, fundada no exercício de determinada atividade considerada capaz de gerar riscos.

Silvio Rodrigues explica que "em rigor, não se pode afirmar serem espécies diversas de responsabilidade, mas sim maneiras diferentes de encarar a obrigação de reparar o dano".[45]

A regra geral de responsabilização consagrada na lei civil brasileira se dá por meio da aplicação da teoria subjetiva, que, conforme a classificação sugere, consiste no exame do comportamento do sujeito, observando se o dano causado ocorreu em decorrência de ato doloso ou culposo, ao praticar uma conduta ilícita. É, portanto, uma responsabilidade pautada na verificação de culpa em sentido amplo de culpa ou dolo, com base no artigo 927, caput, segundo os ditames dos artigos 186 e 187, ambos do Código Civil:

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

---

[44] COUTO E SILVA, Clóvis Veríssimo do. **O conceito de dano no direito brasileiro e comparado**. In: Revista dos Tribunais, v. 667, São Paulo: RT, maio/1991. P. 08.
[45] RODRIGUES, Sílvio. **Direito Civil: Responsabilidade Civil**. 19ª ed. São Paulo: Saraiva, 2002, v. 4. P. 11.

Caio Mário da Silva Pereira preceitua que a culpa é "como um erro de conduta, cometido pelo agente que, procedendo contra direito, causa dano a outrem, sem a intenção de prejudicar, e sem a consciência de que seu comportamento poderia causá-lo".[46]

Indicam Tepedino, Terra e Guedes[47] a formulação recente de uma concepção normativa da culpa, em que a valoração do ato ilícito ocorre não a partir de elementos intencionais do agente, mas com base em padrões de comportamento considerados razoáveis para o fato concreto. Deve-se comparar a conduta concretamente praticada pelo agente com o *standard* de conduta estabelecido pelo legislador.

De outra face, o parágrafo único do artigo 927 estabelece, como exceção à regra, a forma de responsabilização objetiva, admitindo-se a sua adoção nas hipóteses em que o agente causador do dano exerce determinada atividade perigosa com habitualidade que gere riscos aos direitos dos envolvidos:

> Art. 927. [...] Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.

Com fulcro no aludido dispositivo, vislumbra-se que as atividades consideradas perigosas são assim determinadas não apenas por expressa determinação legal, mas também por decorrência da aplicação da teoria do risco, instituindo verdadeira cláusula geral. Dessa forma, permite-se que a jurisprudência considere determinadas atividades já existentes, ou que vierem a existir, como perigosas ou de risco, assim atribuindo ao Poder Judiciário ampla discricionariedade para a incidência da responsabilidade sem culpa.[48]

Cabe ressaltar que existe um limite à discricionariedade do juiz consistente na verificação das normas jurídicas como padrões a serem seguidos pelos tribunais, obedecendo assim ao princípio da legalidade. Segundo Hart:

---

[46] PEREIRA, Caio Mário da Silva. **Responsabilidade civil**. 9. ed. rev. Rio de Janeiro: Forense, 1999. P. 69.
[47] TERRA, Aline de Miranda. GUEDES, Gisela Sampaio da Cruz. TEPEDINO, Gustavo (Orgs.). **Responsabilidade Civil**. Rio de Janeiro: Forense, 2020.
[48] GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro: Responsabilidade Civil**. 15. ed. São Paulo: Saraiva, 2020. v. 4. P. 29.

> "Os tribunais consideram as normas jurídicas não como previsões, mas como padrões que devem ser seguidos nas decisões – e como padrões suficientemente precisos, apesar de sua textura aberta, para limitar, embora não para excluir, a discricionariedade do tribunal." [49]

Apesar do fenômeno de objetivação da responsabilidade civil diante da insuficiência da teoria subjetiva com a explosão tecnológica, de modo geral, a interpretação de que a responsabilidade objetiva se dará apenas em casos excepcionais foi mantida pela jurisprudência brasileira.

Em derradeiro, o nexo de causalidade é o elemento de ligação entre os dois elementos qualificados anteriormente: a conduta e o dano causado.

O nexo de causalidade assume uma dupla função, conforme advertem Tepedino, Terra e Guedes:

> "No campo da responsabilidade civil, o nexo causal cumpre uma dupla função: por um lado, permite determinar a quem se deve atribuir o resultado danoso; por outro, é indispensável na verificação da extensão do dano a se indenizar, pois serve como medida da indenização. É, portanto, o nexo causal que determina até onde vai a responsabilidade do autor do dano, e não a culpa."[50]

Após a exposição destas noções propedêuticas, cumpre ainda aludir os agentes de tratamento de dados definidos pela Lei Geral de Proteção de Dados, para que, concluídas as premissas, seja possível adentrar no debate central.

3.2 Agentes de tratamento de dados

No ciclo de vida da informação, há importantes atores envolvidos. Assim, a Lei Geral de Proteção de Dados tratou de determinar claramente quem são estes atores, bem como os seus papéis, obrigações e responsabilidades no tratamento de dados.

O protagonista das relações jurídicas envolvendo o tratamento de dados é o chamado titular, definido em seu art. 5º, inciso V, como a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. A titularidade de seus dados pessoais[51] é o direito mais elementar da pessoa física em termos de proteção de dados, pois significa que, ao permitir o

---

[49] HART, Herbert. L. A. **O conceito de Direito**. Pós-escrito editado por Penélope A. Bulloch e Joseph Raz. Tradução de A. Ribeiro Mendes. 2.ed. São Paulo: Martins Fontes, 2012. P. 190.

[50] TERRA, Aline de Miranda. GUEDES, Gisela Sampaio da Cruz. TEPEDINO, Gustavo (Orgs.). **Responsabilidade Civil**. Rio de Janeiro: Forense, 2020. P. 85.

[51] Art. 17 da LGPD: "Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei."

tratamento de seus dados pessoais, de modo algum e em nenhuma circunstância, a pessoa transfere a outrem a condição de dono de seus próprios dados pessoais.

No âmbito de aplicação, a LGPD é imposta, de maneira ampla, a qualquer pessoa natural ou jurídica, de direito público ou privado, que proceda com o tratamento, direto ou indireto, de dados pessoais, que emprega tanto meios digitais, quanto meios analógicos[52].

A definição do termo tratamento pela LGPD é bastante abrangente, conceituando-o como "toda operação realizada com dados pessoais"[53], incluindo a coleta, o armazenamento, o processamento, a classificação, a utilização, a reprodução, a eliminação e uma outra variedade de atividades relacionadas a dados pessoais.

Cumpre, nesse ponto, fazer a ressalva de que a lei se aplicará até mesmo a empresas com sede no exterior caso haja o tratamento de dados de brasileiros, ou mesmo empresas brasileiras que realizem, no Brasil, tratamento de dados unicamente de estrangeiros[54]. Ainda, a lei não distingue as pequenas empresas das grandes corporações. Além disso, não faz qualquer menção à quantidade de dados que deverá ser submetida ao regime previsto na legislação.

Dessa forma, independente do porte da empresa ou do volume de dados manuseados por esta, todos deverão agir de acordo com um *compliance* seguro para buscar a adequação à Lei de Proteção de Dados Pessoais, ressalvadas as hipóteses de sua não incidência, explicitadas em seu art. 4º[55].

---

[52] Art. 1º da LGPD: "Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios."

[53] Art. 5º da LGPD, inciso 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;"

[54] Art. 3º da LGPD: "Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: I - a operação de tratamento seja realizada no território nacional; II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional. § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta. § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei."

[55] Art. 4º da LGPD: "Esta Lei não se aplica ao tratamento de dados pessoais: I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II - realizado para fins exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; III - realizado para fins

Os atores que exercem a atividade de tratamento de dados são os chamados agentes de tratamento de dados e subdividem-se, conforme o art. 5º, inciso IX, em: "Art. 5º. Para os fins desta Lei, considera-se: [...] IX - agentes de tratamento: o controlador e o operador; [...]".

Conforme conceitua Celso Ricardo de Oliveira Basílio:

> "Os agentes de proteção de dados pessoais são profissionais que dentro de uma determinada organização adotam medidas de segurança de dados com o objetivo de zelar pela proteção das informações pessoais e impedir os acessos não permitidos. Além disso, são os responsáveis por prevenir qualquer uso inadequado, perda ou furto de dados."[56]

Tanto o controlador, quanto o operador possuem escopos relevantes no tratamento de dados, contudo desempenham funções bem diferentes, uma vez que a um cabe decidir e ao outro executar.

O controlador é definido pela lei como aquele que exerce a decisão referente ao tratamento dos dados, ou seja, é quem utiliza os dados pessoais fornecidos pelo titular para determinado fim econômico, conforme previsto no art. 5º, VI, da referida lei: "Art. 5º. [...] VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; [...]".

É o controlador quem determina o que será feito no âmbito das operações de tratamento de dados, definindo, por exemplo, os propósitos do tratamento, quais dados serão submetidos ao tratamento e quem pode ter acesso a esses dados. Por ser o agente que toma as decisões elementares, a posição de controlador implica em mais obrigações e maior responsabilidade.

O operador é indicado pela lei como aquele que executa o tratamento de dados pessoais em nome do controlador, sob as ordens deste, encontrando respaldo no mesmo artigo, no inciso seguinte: "Art. 5º. [...] VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; [...]".

---

exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei. (...)"

[56] CASCAES, Amanda Celli, BRESEGHELLO, Fabíola Meira de Almeida, TUTIKIAN, Priscila David Sansone (Coord.). **Comentários à Lei Geral de Proteção de Dados à luz do Código de Defesa do Consumidor**. São Paulo: Ed. Singular, 1ª edição, 2019. P. 129.

Por ser o agente que realiza o tratamento em nome do controlador e de acordo com as suas instruções, detém uma posição menos rígida na cadeia de tratamento de dados. A função de operador dos dados pessoais pode ser desenvolvida diretamente pelo próprio empregador, por funcionário de sua empresa, por um setor específico da companhia ou ainda por terceiros, estranhos à relação.

Os agentes de tratamento de dados – controlador e operador – podem ser solidariamente responsabilizados pelos danos causados. Entretanto, a reponsabilidade do operador, que pratica o tratamento de dados em nome e sob as ordens do controlador, pode ser limitada às suas obrigações contratuais e de segurança da informação, caso não viole as regras impostas pela LGPD.

Segundo Sérgio Cavalieri Filho, o conceito de responsabilidade solidária tem uma de suas bases no art. 942 do CC/02, que dispõe que "se a ofensa tiver mais de um autor, todos responderão solidariamente pela reparação". Dessa forma, tem-se que "cada um dos agentes que concorrerem adequadamente para o evento é considerado pessoalmente causador do dano e, consequentemente, obrigado a indenizar"[57].

Outro ator participante da relação jurídica do tratamento de dados é o encarregado. Uma das exigências da LGPD é a de que o controlador e o operador devem indicar um encarregado de dados, também chamado de "*Data Protection Officer (DPO)*", para atuar como canal de comunicação entre o controlador, os titulares de dados e a Autoridade Nacional de Proteção de Dados, conforme o art. 5º, inciso VIII:

> "Art. 5º. [...] VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); [...]"

O encarregado deverá ter sua identidade e informações de contato divulgadas publicamente, de forma clara, objetiva e de fácil acesso.

Além da intermediação entre os atores, as atividades do encarregado envolvem aceitar reclamações, prestar esclarecimentos aos titulares, adotar providências necessárias, orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à

---

[57] CAVALIERI FILHO, Sergio. **Programa de Responsabilidade Civil**. 12ª ed. ver. e ampl. São Paulo: Atlas, 2015. P. 87.

proteção de dados pessoais, entre outras[58]. A Autoridade Nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive as hipóteses para sua dispensa.

Por fim, a Lei 13.853/19 trouxe algumas modificações à Lei Geral de Proteção de Dados e, dentre elas, providenciou criar uma autoridade nacional de proteção de dados para que os fundamentos sob os quais a LGPD foi estabelecida sejam realmente cumpridos.

A Autoridade Nacional de Proteção de Dados Pessoais (ANPD) é a responsável pela fiscalização e pela regulação da LGPD, vinculada à Presidência da República, dotada de autonomia técnica e decisória, com jurisdição no território nacional. A ANPD foi criada em 2020 e a sua estrutura organizacional encontra-se prevista no Decreto nº 10.474, de 26 de agosto de 2020.

Suas principais atribuições estão detalhadas no art. 2º do referido decreto e consistem em: zelar pela proteção de dados pessoais, elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, fiscalizar e aplicar sanções na hipótese de tratamento de dados realizado em descumprimento à legislação, orientar os agentes na aplicação das normas e regulamentos relacionados ao tema; cooperar com órgãos nacionais e internacionais de Proteção de Dados Pessoais.

Resta evidente que as atividades relacionadas a coleta e tratamento de dados envolvem agentes e titulares, de diversas origens dada a globalização, exercendo diferentes atividades, sendo imprescindível a diligência de uma lei regulando e fiscalizando tais relações.

Essa complexa relação de múltiplos atores, direitos e deveres salienta o desafio que as entidades encontrarão para se alinharem às disposições expressas na LGPD. Os efeitos do não-

---

[58] Art. 41 da LGPD: "O controlador deverá indicar encarregado pelo tratamento de dados pessoais. § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador. § 2º As atividades do encarregado consistem em: I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da autoridade nacional e adotar providências; III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. § 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados. § 4º (VETADO)."

atendimento passam não só pelas sanções administrativas que podem ser eventualmente impostas pela ANPD, mas em maior escala, por ações de responsabilidade civil.

Ao impor deveres, responsabilidades e punições cabíveis para o descumprimento do bom uso e sigilo das informações coletadas, a Lei Geral de Proteção de Dados torna-se uma "arma eficaz de âmbito civil que atua juntamente com penalidades e estabelece quem são os agentes responsáveis para que se crie com o sistema penal uma forte barreira para que os dados das pessoas físicas que estão sendo usados nas redes sociais, nas transferências de bancos e até mesmo nos órgãos de segurança nacional possam ser devidamente guardados e não atingidos pelos cibercriminosos" [59].

3.3 Responsabilidade civil na Lei Geral de Proteção de Dados

Não há dúvida de que uma garantia essencial para a efetividade do regime de proteção de dados consiste na possibilidade de se responsabilizarem civilmente os controladores e operadores que incorram na violação dos direitos das pessoas naturais. Nesse cenário, há uma evidente conexão entre o instituto da responsabilidade civil e a disciplina da proteção de dados.

Com efeito, como princípios norteadores da LGPD, encontram-se a segurança, a prevenção e a responsabilização do agente, previstos em seu art. 6º:

> "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...]
>
> 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; [...]
>
> 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. [...]"

Nota-se que a lei impõe ao agente de tratamento de dados o dever de garantir a segurança e de reduzir ao máximo os efeitos de um incidente de segurança, o que resta evidenciado pelo

---

[59] Disponível em <https://www.radloff.com.br/lei-geral-de-protecao-de-dados-e-o-direito-na-era-digital/>. Acesso em 20/04/2021.

fato de a lei não estabelecer um rol taxativo de medidas de segurança, apenas mencionando o objetivo de tornar tão difícil quanto possível o acesso não autorizado a informações pessoais[60].

Na Seção III, inserida no Capítulo VI "Dos agentes de tratamento de dados pessoais", sob o título "Da Responsabilidade e do Ressarcimento de Danos", a Lei Geral de Proteção de Dados trouxe as principais regras de responsabilidade civil e de ressarcimento de danos imputados aos agentes de tratamento.

O artigo 42, em seu caput, dispõe acerca da obrigação de reparação civil do agente de tratamento de dados por dano patrimonial, moral, individual ou coletivo por dois motivos, quais sejam, o exercício da atividade de tratamento de dados e a violação da legislação de proteção de dados:

> "Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. [...]"

Faz-se necessário realizar uma leitura conjunta com o artigo 44, que prevê as situações de irregularidade no tratamento de dados pessoais:

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

Da interpretação dos referidos dispositivos, percebe-se que a responsabilidade civil no âmbito da Lei Geral de Proteção de Dados resta caracterizada também caso o agente de tratamento de dados não forneça a segurança e proteção aos dados esperada pelo titular e imposta pela legislação pertinente, levando-se em conta as seguintes circunstâncias: o modo

---

[60] Art. 46 da LGPD: "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."

pelo qual o tratamento é realizado; o resultado e os riscos que razoavelmente dele se esperam; as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado[61].

Nos incisos do §1º do artigo 42, o legislador optou por estabelecer hipótese de responsabilidade solidária dos operadores e controladores, garantindo assim uma maior efetividade de reparação do dano ao titular lesado:

> "Art. 42. [...] § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
>
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
>
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei. [...]"

Nesse sentido, responde solidariamente pelos danos causados pelo tratamento de dados o operador quando descumprir a lei ou quando atuar em contrariedade com as ordens lícitas do controlador e os controladores, uma vez comprovado estarem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados.

Estas hipóteses de solidariedade estarão afastadas caso presentes as hipóteses de exclusão de responsabilidade previstas no art. 43 da Lei Geral de Proteção de Dados.

Ainda, consoante o §4º do art. 42[62], resta assegurado àquele que reparar o dano ao titular dos dados o direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Seguindo o raciocínio presente em outros diplomas legais, o §2º do art. 42[63] admite a inversão do ônus da prova a favor do titular de dados, contanto que verossímil a alegação, em

---

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

[62] Art. 42 da LGPD: "§4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso."

[63] Art. 42 da LGPD: "§ 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa."

caso de hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular for excessivamente onerosa.

Por sua vez, o artigo 43 estipula expressamente as hipóteses excludentes da responsabilidade civil dos agentes de tratamento:

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

Na dicção do artigo 45[64], restou positivada a relação da legislação de proteção de dados com o diploma legal de defesa do consumidor. Caso a relação jurídica do titular com o controlador e o operador tenha natureza consumerista, serão aplicadas as normas de responsabilidade civil dos artigos 12 e 14 do Código de Defesa do Consumidor.

À vista do exposto, percebe-se que o legislador não foi exatamente claro quanto ao sistema de responsabilidade civil a ser adotado, gerando verdadeiro embate doutrinário, em que alguns especialistas defendem a responsabilidade subjetiva, antes já adotada como regra pelo Marco Civil da Internet em relação aos provedores de internet, e outros defendem a responsabilidade objetiva, presente na legislação consumerista.

Apesar da ausência de previsão expressa, é possível perceber indicativos que levam a conclusão de que o sistema eleito na Lei Geral de Proteção de Dados foi o da responsabilidade subjetiva, inserindo-se de forma harmônica no mosaico legislativo e trazendo assim um equilíbrio entre a proteção do titular de dados e a promoção de um ambiente virtual de fluxo informacional livre e democrático.

3.4 Responsabilidade objetiva

Os defensores da modalidade de responsabilidade objetiva, fundamentada no risco da atividade desenvolvida, ou seja, que prescinde da discussão sobre a culpa do agente bastando

---

[64] Art. 45 da LGPD: "As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente."

que se comprove o dano e o nexo causal, argumentam que este modelo foi adotado pelo legislador com base em diversos aspectos.

Segundo esta corrente, os princípios já dão o tom do que se espera no tratamento de dados em eventuais danos ocasionados. Deste modo, ao se fazer uma digressão aos fundamentos principiológicos da Lei Geral de Proteção de Dados, que são justamente as bases por meio das quais é possível se identificar a *mens legis*, a intenção do legislador ao enumerar uma série de princípios que regulam e servem como um cobertor da lei foi proporcionar um arcabouço de direitos, sanções, regulamentações específicas com o objetivo de alcançar a máxima proteção do titular de dados.

Nesse sentido, Caitlin Mulholland[65] destaca três princípios da LGPD, quais sejam, segurança[66], prevenção[67]e responsabilização e prestação de contas[68], que trazem uma fundamentação que permite ao intérprete da LGPD considerar que se está diante de uma lei que protege o titular de dados o concedendo um direito a ser indenizado pelos danos sofridos com base na chamada teoria do risco.

Segundo ela, a transparência a ser adotada pelo agente acerca dos procedimentos que são tomados para a segurança e prevenção no tratamento de dados deve ser considerada como um dever ativo, gerando a obrigação ao agente de tratamento de prestar contas, onde serão evidenciadas as medidas que estão sendo tomadas para uma atuação em conformidade com as boas práticas impostas pela lei.

A favor da responsabilidade objetiva, alega-se que a atividade de tratamento de dados deve ser considerada como uma atividade de risco, em que a própria atividade frequentemente desenvolvida seria suficiente para ocasionar a verificação da responsabilidade independentemente de qualquer análise de culpa. A insegurança e a intangibilidade que são

---

[65] 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 21/03/2021.

[66]Art. 6º da LGPD: "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;"

[67] Art. 6º da LGPD: "VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;"

[68] Art. 6º da LGPD: "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."

inerentes ao tratamento de dados seriam suficientes para demandar o reforço do dever de segurança daqueles que se dedicam a ofícios que realizam o tratamento de dados pessoais e a responsabilização em caso de incidentes de segurança, devido a mera identificação do risco.

Nesse sentido, Danilo Doneda e Laura Mendes[69] consideram que o legislador, ao adotar o princípio da necessidade[70] trazendo limitações ao tratamento de dados pessoais ao mínimo necessário para a realização de suas finalidades, previu a potencialidade danosa considerável no exercício desta atividade, vinculando-a a um risco intrínseco e, portanto, optou por um regime de responsabilidade objetiva.

Ainda, o guia orientativo para a construção da governança pelas entidades fornecido pela LGPD tem como um de seus objetivos a "mitigação do risco", sendo esta expressão considerada um reconhecimento do próprio legislador da capacidade existente do pretenso ofensor de avaliar previamente os riscos relacionados à atividade que ele desenvolve e tomar as medidas para evitar o dano, numa antecipação que o controlador ou operador deverá considerar para evitar a obrigação de reparar[71].

Explica Pinheiro:

> "Para o Direito Digital, a teoria do risco tem maior aplicabilidade, uma vez que, nascida na era da industrialização, vem resolver os problemas de reparação do dano em que a culpa é um elemento dispensável, ou seja, onde há responsabilidade mesmo que sem culpa em determinadas situações, em virtude do princípio de equilíbrio de interesses e genérica equidade[72]."

Outro fator que leva à defesa da adoção da responsabilidade objetiva pela Lei Geral de Proteção de Dados é a sua similaridade com o Código de Defesa do Consumidor (Lei nº 8.078/ 1990), no tocante aos dispositivos de responsabilidade civil. Neste diploma legal, adota-se a responsabilidade objetiva do fornecedor vinculada à ideia de vulnerabilidade do consumidor e o consequente desequilíbrio na relação processual.

---

[69] MENDES, Laura Schertel; DONEDA, Danilo. **Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018), o novo paradigma da proteção de dados no Brasil**. REVISTA DE DIREITO DO CONSUMIDOR, v. 120, 2018, P. 555.

[70] Art. 6° da LGPD: "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;"

[71] 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 21/03/2021.

[72] PINHEIRO, Patrícia Peck. **Direito Digital**. 6ª Edição. São Paulo. Saraiva 2016. P. 514.

Neste raciocínio, demonstram os especialistas adeptos da teoria objetiva que o titular de dados é considerado presumidamente vulnerável, dada a clara dificuldade de controlar o fluxo dos seus dados pessoais, bem como de adotar medidas de autoproteção contra os riscos do tratamento dessas informações. Destaca Mendes:

> "A vulnerabilidade do consumidor nesse processo de coleta e tratamento de dados pessoais é tão patente que se cunhou a expressão "consumidor de vidro" para denotar a sua extrema fragilidade e exposição no mercado de consumo, diante de inúmeras empresas que tomam decisões e influenciam as suas chances de vida, a partir das informações pessoais armazenadas em bancos de dados."[73]

Diante do reconhecimento da vulnerabilidade e hipossuficiência do titular de dados, nota-se que há um desequilíbrio anterior calcado na produção de um risco pelo ofensor que não é recíproco, ensejando assim o emprego da responsabilidade objetiva como ferramenta para a busca da igualdade entre as partes[74].

De fato, ao analisar a Lei Geral de Proteção de Dados, percebe-se a semelhança dos dispositivos com o Código de Defesa do Consumidor.

Conforme visto anteriormente, da leitura conjunta do artigo 42, caput com o artigo 44, ambos da LGPD, a responsabilidade civil no âmbito da Lei Geral de Proteção de Dados resta caracterizada caso o agente de tratamento de dados viole a legislação de proteção e caso não forneça a segurança e proteção aos dados esperada pelo titular e imposta pela legislação pertinente.

Percebe-se que tais circunstâncias estabelecidas pela LGPD para conferir a regularidade do tratamento são as mesmas presentes nos artigos 12, §1º e 14, §1º do CDC, quando se trata de fato do produto ou serviço, em que a regra adotada é a da responsabilidade objetiva:

> "Art. 12. [...] §1º O produto é defeituoso quando não oferece a segurança que dele legitimamente se espera, levando-se em consideração as circunstâncias relevantes, entre as quais:
>
> I - sua apresentação;
>
> II - o uso e os riscos que razoavelmente dele se esperam;
>
> III - a época em que foi colocado em circulação. [...]

---

[73] MENDES, Laura Schertel. **A vulnerabilidade do consumidor quanto ao tratamento de dados pessoais**. In: MARQUES, Claudia Lima; GSELL, Beate. **Novas tendências do direito do consumidor: rede Alemanha-Brasil de pesquisas em direito do consumidor**. São Paulo: Ed. RT, 2015.

[74] MIRAGEM, Bruno. **Direito civil: responsabilidade civil**. São Paulo: Saraiva, 2015. Pp. 301-303.

> Art. 14. [...] § 1º O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais:
>
> I - o modo de seu fornecimento;
>
> II - o resultado e os riscos que razoavelmente dele se esperam;
>
> III - a época em que foi fornecido. [...]"

Na legislação consumerista, deve-se verificar se o fornecedor adotou ou não as medidas necessárias para que o produto ou serviço fornecesse a segurança adequada esperada pelo consumidor, levando-se em conta a época em que o produto ou serviço foi fornecido, tal qual a LGPD impõe ao agente de tratamento de dados.

Ainda, ao analisar o artigo 43 da LGPD, que estabelece as hipóteses de exclusão de responsabilidade civil, observa-se uma proximidade com o §3º do art. 12 do CDC:

Tabela Comparativa LGPD x CDC	
Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem: I - que não realizaram o tratamento de dados pessoais que lhes é atribuído; II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.	Art. 12. [...] §3º O fabricante, o construtor, o produtor ou importador só não será responsabilizado quando provar: I - que não colocou o produto no mercado; II - que, embora haja colocado o produto no mercado, o defeito inexiste; III - a culpa exclusiva do consumidor ou de terceiro.

Além disso, conforme expõe Lima, o emprego do advérbio de exclusão "só" é um indicativo de rol taxativo de excludentes de responsabilização, o qual não seria necessário em caso de responsabilização subjetiva, pois bastaria demonstrar que não houve o elemento culpa[75].

[75] LIMA, Cintia Rosa Pereira de. *In* **I Simpósio de Responsabilidade Civil e Proteção de Dados**. Evento realizado pelo Instituto Brasileiro de Estudos de Responsabilidade Civil – IBERC. Agosto, 2020. Disponível em < https://www.youtube.com/watch?v=igbbxkbqeKI&t=4213s>. Acesso em 03/04/2021.

Em que pese os argumentos expostos ensejam uma tentação em se adotar a teoria objetiva, não se pode olvidar que o objetivo da nova Lei Geral de Proteção de Dados é não somente proteger o titular dos dados, como também viabilizar o desenvolvimento das atividades na rede.

Em tom crítico, Orlando Gomes já expressava: "A teoria da responsabilidade objetiva tem criado situações excessivamente onerosas para os que são obrigados a indenizar". [76]

Não pode, evidentemente, a responsabilização ser um meio de impor um novo desequilíbrio na relação entre as partes, a tal ponto de atribuir ao agente de tratamento de dados deveres impossíveis de serem desempenhados, desmotivando assim a adoção de comportamento adequado.

3.5 Responsabilidade subjetiva

Apesar da indefinição acerca da modalidade de responsabilidade civil na Lei Geral de Proteção de Dados, revela-se de suma importância atentar para as pistas deixadas pelo legislador que apontam para o regime subjetivo e da culpa como fundamento, pelo menos como regra geral, conforme os argumentos dos defensores desta corrente a serem expostos.

Com base nos princípios da responsabilização e da prestação de contas expressos no artigo 6º da LGPD[77], os agentes deverão comprovar a adoção de medidas eficazes e capazes de demonstrar a observância, o cumprimento e a eficácia das normas de proteção de dados pessoais. Diante disso, indagam Guedes e Meireles[78]:

> "Do ponto de vista do controlador, do que adianta 'prestar contas', se, ao final, se houver incidente, por mais diligente que tenha sido, ele será responsabilizado da mesma forma e independentemente de culpa?"

Aqui, sublinhe-se a concepção normativa da culpa, mencionada anteriormente (capítulo 3.1), adotada hodiernamente por diversos autores, em que a valoração do ato ilícito ocorre com

---

[76] GOMES, Orlando. **Obrigações**. 8ª Edição. Rio de Janeiro: Forense, 1992. P. 343.

[77] Art. 6º da LGPD: "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."

[78] GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Venceslau. Término do Tratamento de Dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. *A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. São Paulo: Revista dos Tribunais, 2019. P. 231.

base em padrões de comportamento considerados razoáveis para o fato concreto conforme estabelecido pela legislação. Nesse sentido, explica Moraes:

> "O conceito de culpa também se encontra em estado de indefinição no atual direito da responsabilidade civil. Originalmente, culpa era apenas a situação contrária ao direito, porque negligente, imprudente, imperita ou dolosa, que acarretava danos aos direitos de outrem. Modernamente, todavia, diversos autores abandonaram esta conceituação, preferindo considerar a culpa o descumprimento de um standard de diligência razoável, diferenciando esta noção, dita 'normativa' ou 'objetiva', da outra, dita 'psicológica'".[79]

Com este entendimento, percebe-se claramente que a intenção do legislador, ao pautar a Lei Geral de Proteção de Dados na criação de deveres aos agentes de tratamento de dados estabelecendo um standard de conduta, é a de adoção da responsabilidade subjetiva.

Seria incongruente o legislador impor uma série de deveres de cuidado para, ao final, responsabilizar o controlador e o operador independentemente do cumprimento do padrão de comportamento exigível. Esta seria a lógica da responsabilidade objetiva, cuja concretização ocorre com a prática de atos lícitos que causam danos, independentemente da violação de qualquer dever jurídico por parte do agente[80].

As circunstâncias, portanto, ensejam a responsabilização subjetiva, fazendo-se necessária uma análise casuística investigando se o agente de tratamento agiu conforme o padrão de comportamento esperado pela lei, adotando as medidas de segurança e medidas preventivas para evitar ao máximo um vazamento de dados pessoais.

A avaliação da responsabilidade no caso concreto é importante também para identificar o risco da atividade de tratamento de dados, visto que a LGPD não prevê um nivelamento de toda e qualquer atividade como sendo de risco acentuado.

Com o estudo do caso concreto, é possível a realização de um juízo de valor sobre a forma pelo qual deveria ter sido realizado o tratamento de dados diante da identificação dos riscos que da atividade razoavelmente eram esperados.

---

[79] MORAES, Maria Celina Bodin de. **Risco, solidariedade e responsabilidade objetiva.** Revista dos Tribunais, São Paulo, Ed. Rt, V. 854, dez. 2006. P. 21.
[80] Ibid. P. 25.

Cabe aos agentes de tratamento de dados ajustar as suas medidas de segurança para corresponder à probabilidade e à gravidade das violações possivelmente resultantes da atividade.

Essencial se mostra a avaliação do caso concreto para que se garanta a segurança jurídica, minimizando a produção de danos causados aos titulares de dados e, paralelamente, proporcionando um ambiente estimulante para a atividade econômica.

Contra o argumento dos defensores da responsabilidade objetiva acerca da similaridade da LGPD com o CDC, alegam os defensores da responsabilidade subjetiva que há indícios de que o modelo objetivo é apenas uma tentação.

Repara-se inicialmente que não há qualquer artigo que estabeleça expressamente a responsabilidade objetiva ou, pelo menos, se valha da expressão "independentemente de culpa", como há no CDC, em que claramente foi adotado o regime da responsabilidade objetiva:

Tabela Comparativa LGPD x CDC		
Art. 42. LGPD. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, **em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo**. [...]	Art. 12. CDC. O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, **independentemente da existência de culpa**, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos. [...]	Art. 14. CDC. O fornecedor de serviços responde, **independentemente da existência de culpa**, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos. [...]

Além do mais, no Código Civil, em todos os dispositivos em que se encontra prevista a responsabilidade objetiva, há clareza na sua escolha, seja pelo uso da expressão "independentemente de culpa", como ocorre no art. 927, parágrafo único[81], que prevê a cláusula geral de responsabilidade objetiva, seja por outra expressão como, por exemplo, "ainda que não haja culpa de sua parte"[82] ou "salvo motivo de força maior"[83].

Outrossim, apesar da similaridade do artigo 43 da LGPD com o artigo 12, §3º, do CDC, percebe-se uma diferença fundamental: o inciso II do artigo 43 encontra-se intrinsecamente vinculado ao elemento culpa, diferentemente do que ocorre no CDC, cujos incisos são todos conectados ao elemento nexo de causalidade[84].

Prevê este inciso expressamente que os agentes de tratamento de dados só não serão responsabilizados quando provarem, entre outros fatores, "que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados". Depreende-se que, caso o agente comprove que seguiu todos os deveres impostos pelo legislador e, ainda assim, da sua atividade decorrer um dano, não será responsabilizado por força do artigo 43, inciso II da LGPD.

Neste ponto, resta claro que há uma avaliação de culpa do agente de tratamento de dados, sendo portanto a evidência mais importante que indica o regime da responsabilidade civil na Lei Geral de Proteção de Dados, conforme entendem Tepedino, Terra e Guedes:

> "Nesse inciso II, o legislador afirma, a grosso modo, que, ainda que exista nexo causal entre a conduta do agente e o dano, se ele conseguir provar que cumpriu todos os deveres impostos pela LGPD, tomando as medidas de segurança recomendadas (...), não será responsabilizado. Nessas circunstâncias, o agente terá demonstrado que observou o *standard* esperado e, se o incidente ocorreu, não foi em razão de sua conduta culposa."[85]

---

[81] Art. 927 do CC: "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."

[82] Art. 933 do CC: "As pessoas indicadas nos incisos I a V do artigo antecedente, ainda que não haja culpa de sua parte, responderão pelos atos praticados pelos terceiros ali referidos."

[83] Art. 734 do CC: "O transportador responde pelos danos causados às pessoas transportadas e suas bagagens, salvo motivo de força maior, sendo nula qualquer cláusula excludente da responsabilidade. Parágrafo único. É lícito ao transportador exigir a declaração do valor da bagagem a fim de fixar o limite da indenização."

[84] TERRA, Aline de Miranda. GUEDES, Gisela Sampaio da Cruz. TEPEDINO, Gustavo (Orgs.). **Responsabilidade Civil**. Rio de Janeiro: Forense, 2020. P. 291.

[85] Ibid. P. 292.

A reprovabilidade da conduta do agente de tratamento se vincula à violação do dever de observar os preceitos da LGPD.

Seguindo este raciocínio, o artigo 44, ao tratar dos incidentes de segurança, também se vincula ao elemento culpa em seu parágrafo único, ao prever que o controlador ou o operador que deixar de adotar as medidas de segurança previstas na LGPD responderá pelos danos decorrentes da violação da segurança dos dados. Entende-se, contrariamente, que se adotar as medidas de segurança impostas pelo legislador e, ainda assim, ocorra um dano, ele não responde.

Nesse contexto, há de se ter prudência dada a sensibilidade da objetivação da responsabilidade civil, pois, por mais digno que seja o dever de reparar, protegendo assim os titulares de dados vulneráveis em uma sociedade cada vez mais sujeita a riscos, não se pode fazer do agente que adotou os esforços necessários para a proteção dos dados um ofensor.

Ademais, Guedes ressalta uma comparação entre o artigo 927, do Código Civil brasileiro, cláusula geral de responsabilidade civil objetiva com o artigo 493 do Código Civil português e artigo 2050 do Código Civil italiano, fonte de inspiração do legislador pátrio[86]:

> "Art. 493, "2" do código civil português: "[q]uem causar danos a outrem no exercício de uma atividade perigosa por sua própria natureza ou pela natureza dos meios utilizados, é obrigado a repará-los, exceto se mostrar que empregou todas as providencias exigidas pelas circunstâncias com o fim de as prevenir."
>
> Art. 2050 do código civil italiano: "[q]ualquer um que causa dano a outros no desenvolvimento de uma atividade perigosa, por sua natureza ou pela natureza dos meios utilizados, é obrigado ao ressarcimento se não provar ter adotado todas as medidas idôneas a evitar o dano"."

A doutrina reconhece que em ambos os artigos, caso ocorra um dano e o agente tenha adotado as medidas de segurança estipuladas, não será responsabilizado. Admite-se que não há nestes sistemas uma cláusula geral de responsabilidade objetiva, mas sim um sistema intermediário de presunção de culpa[87], cuja redação e lógica assemelha-se ao adotado na LGPD.

---

[86] GUEDES, Gisela Sampaio da Cruz. *In* **I Simpósio de Responsabilidade Civil e Proteção de Dados**. Evento realizado pelo Instituto Brasileiro de Estudos de Responsabilidade Civil – IBERC. Agosto, 2020. Disponível em < https://www.youtube.com/watch?v=igbbxkbqeKI&t=4213s>. Acesso em 10/04/2021.

[87] TEPEDINO, Gustavo; BARBOSA, Heloisa Helena; MORAES, Maria Cecilia Bodin de. **Código Civil interpretado conforme a Constituição da República - Volume III**. Rio de Janeiro: Renovar, 2006. P. 809.

Diversamente disso, no artigo 927, parágrafo único, do Código Civil brasileiro, não adianta o agente de tratamento alegar que agiu de forma cautelosa, adotando as medidas preventivas em respeito à legislação, porque será responsabilizado objetivamente.

Em uma análise ao histórico de tramitação da LGPD, tanto o seu anteprojeto, quanto a versão inicial do PL. 5.276/2016 adotavam expressamente o regime de responsabilidade civil objetiva. No capítulo sobre a transferência internacional de dados, ao tratar da responsabilidade do cedente e do cessionário, enquanto o primeiro utilizava, em seus artigos 30 e 31, a expressão "independente de culpa"[88], o segundo estabelecia, em seu artigo 35, que ambos responderiam solidária e objetivamente[89].

Percebe-se que a redação final da lei eliminou os termos ventilados, afastando-se completamente da ideia de objetivação.

Por último, conforme pontuam Tepedino, Terra e Guedes, a menção ao Código de Defesa do Consumidor no artigo 45 da LGPD seria inócua, caso o regime de responsabilidade civil adotado fosse o objetivo[90].

A bem da verdade, Caio Mário já previa:

> "O princípio da responsabilidade subjetiva subsistirá no direito brasileiro. O comportamento do agente continuará como fator etiológico da reparação do dano, não obstante a provável aceitação paralela da doutrina do risco. A pessoa do agente estará no centro da responsabilidade civil. O prejuízo será indenizável não como dano em si mesmo, porém na razão de ter sido causado pelo comportamento do ofensor".[91]

Logo, considerando o foco da LGPD na conduta dos agentes de tratamento, a conclusão por um modelo de responsabilização objetiva é contraditório com o próprio espírito da lei, que busca incentivar os agentes de tratamento a adotar boas práticas.

---

[88] Disponível em < http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/ >. Acesso em 24/04/2021.

[89] Disponível em < https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1457459&filename=PL+5276/2016 >. Acesso em 24/04/2021.

[90] TERRA, Aline de Miranda; GUEDES, Gisela Sampaio da Cruz; TEPEDINO, Gustavo (Orgs.). **Responsabilidade Civil**. Rio de Janeiro: Forense, 2020. P. 294.

[91] PEREIRA, Caio Mário da Silva. **Responsabilidade Civil**. Rio de Janeiro: Editora Forense, 9ª ed., 2002. P. 35.

4. O DANO MORAL DECORRENTE DE VAZAMENTO DE DADOS

4.1 A frequência dos vazamentos de dados e a fragilidade das medidas de segurança

O incidente de segurança envolvendo dados pessoais é uma realidade inafastável da sociedade da informação, podendo ser considerado um risco inevitável e inerente ao exercício da atividade de tratamento de dados.

Há de se ter em mente que, mesmo com o estabelecimento de padrões de segurança para a proteção dos dados pessoais, não há como excluir a considerável possibilidade de que ações de terceiros mal-intencionados violem os sistemas de segurança, acarretando no vazamento indevido das informações dos titulares.

As medidas de segurança são criadas de forma reativa com o objetivo de cessar um ataque e fechar brechas para que não aconteça novamente e, por mais que haja um empenho na previsão de um futuro ataque para dificultar a ação dos cibercriminosos, essas tentativas são constantes desconhecidas até o momento em que ocorrem.

Ademais, assim que uma forma de ataque é solucionada, os cibercrimonos já colocaram em prática um novo *modus operandi*, restando clara a fragilidade das medidas de segurança. De acordo com Camila Jimene, não existe segurança absoluta em nenhum cenário e em nenhum mercado, seja analógico ou digital, sendo certo que:

> "Uma organização pode adotar todas as melhores e mais sofisticadas práticas de Segurança da Informação, investir em tecnologia de ponta, estabelecer as melhores políticas e contratos, treinar continuamente todos os seus funcionários, criar o mais completo e adequado Programa de Governança em Privacidade e, ainda assim, ser vítima de um incidente de vazamento de dados, ocasionado por um ataque cibernético, uma falha sistêmica ou, até mesmo, um empregado mal-intencionado."[92]

O próprio artigo 48, caput, da LGPD[93], ao prever o dever de comunicação do agente de tratamento de dados diante de um incidente de segurança, dispõe que esta só deve ocorrer caso o risco ou dano seja relevante aos titulares. Nesse sentido, é fundamental que o controlador e o

---

[92] JIMENE, Camilla do Vale. **Da Importância da Segurança da Informação para Adequação à LGPD**. In: BLUM, Renato Opice (Organizador). Protecao de Dados: Desafios e Solucoes na Adequação à Lei. Rio de Janeiro: Editora Forense, 2020. P. 47.

[93] Art. 48 da LGPD: "O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. [...]"

operador estejam aptos a executar as orientações estipuladas pela LGPD para agirem diante de um vazamento de dados.

Infelizmente, por mais que o agente de tratamento percorra o seu diagrama de fluxo de dados analisando o nível de gravidade e probabilidade de um dano na intenção de mitigar os riscos de acordo com a orientação fornecida pela LGPD, deve-se admitir que grande parte da população já teve seus dados vazados em algum *data breach*.

4.2 O dano moral decorrente de vazamento de dados não deve ser considerado *in re ipsa*

Por óbvio, não se sustenta aqui a necessidade de que haja efetiva comprovação da dor ou sofrimento, até mesmo porque tais sentimentos não configuram elemento hábil à definição ontológica do dano moral, mas, tão somente, eventual consequência de lesão à personalidade.

Em se tratando de pleito indenizatório por danos morais, o que prescinde de comprovação, em realidade, são os efeitos psicológicos ocasionados à parte supostamente lesionada.

Nesse passo, inviável o acolhimento da pretensão indenizatória deduzida, mormente por não configurar o caso hipótese de dano *in re ipsa.*

O dever de reparar não há de ser admitido sem a presença efetiva do dano e do nexo de causalidade entre a atividade e o evento danoso, visto que configuraria uma desnaturalização da finalidade e dos elementos da responsabilidade civil[94].

O seguinte excerto jurisprudencial no qual o entendimento pretoriano foi ao encontro do que ora se aduz. *In verbis*:

> "*INDENIZATÓRIA. DANOS MORAIS. DIVULGAÇÃO INDEVIDA DOS DADOS CADASTRAIS EM GRUPO DE E-MAIL DE ALUNOS. AUSENCIA DE DEMONSTRAÇÃO DE QUALQUER ATO QUE PUDESSE IMPORTAR EM OFENSA AO DIREITO DE PERSONALIDADE DA AUTORA. SENTENÇA DE IMPROCEDÊNCIA MANTIDA.* ***A divulgação dos dados cadastrais da autora e de outros alunos não é negada pela recorrida. Ao contrário, assumiu esta a responsabilidade por eventuais danos que***

[94] TERRA, Aline de Miranda; GUEDES, Gisela Sampaio da Cruz; TEPEDINO, Gustavo (Orgs.). **Responsabilidade Civil.** Rio de Janeiro: Forense, 2020. P. 60.

> ***pudessem ocorrer. Caso em que não se cogita de dano moral na modalidade in re ipsa, havendo necessidade de comprovação, o que inocorre no caso concreto. A divulgação dos dados pessoais da autora, sem conotação pejorativa e por erro de uma funcionária da ré, não tem em sua essência o condão de caracterizar, por si só o dano moral.*** *Ademais, a recorrida tomou todas as medidas cabíveis para minorar as chances de danos aos alunos que tiveram seus dados divulgados indevidamente, ingressando, inclusive com demanda judicial, menos de uma semana após a descoberta da divulgação, para anotar no SPC/SERASA, ao lado do CPF de cada um dos alunos, o vazamento sucedido, a fim de evitar fraudes com a utilização dos dados. Sentença de improcedência confirmada. RECURSO DESPROVIDO.".* (TJRS. Recurso Cível nº 71003906021, Primeira Turma Recursal Cível, Relator Pedro Luiz Pozza, julgado em 13/09/2012 – grifou-se.)

Como de notória sabença, as hipóteses em que o ordenamento jurídico pátrio admite a responsabilização independentemente de se comprovar o dano, sendo *in re ipsa*, são exceções à regra.

Ressalte-se, contudo, que a hipótese ora ventilada não se amolda a uma destas hipóteses excepcionais. A bem da verdade, uma vez consideradas as especificidades do tema em questão, a conclusão a que se chega é apenas uma: o vazamento de informações cadastrais, sem nenhuma repercussão específica, não gera dano moral na medida em que não ofende a dignidade humana.

Far-se-ia necessária, portanto, a prova da lesão efetiva para ocorrência dos danos morais, em que pese seja dispensada a comprovação das consequências da lesão sobre a sensibilidade da vítima.

4.3 Culpa exclusiva de terceiro

O artigo 43 da LGPD trata das excludentes de responsabilidade dos agentes de tratamento, havendo previsão expressa, em seu inciso III, acerca da não responsabilização quando o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.

Comumente, os episódios de vazamento de dados estão atrelados a um ataque sofrido por ação de um terceiro mal-intencionado, o comumente chamado de *hacker*.

No entanto, a despeito da concepção usual de *hacker*, este não necessariamente é um criminoso que atua de forma ilegal na rede mundial de computadores.

Na lição de Liliana Minardi Paesani, muitos *hackers* têm por função atuar na correção de falhas de segurança em sistemas, com vistas a otimizar e melhorar a qualidade dos serviços

prestados. Tal função é fundamental para garantir que apenas as pessoas que legitimamente possuem credenciais de acesso a determinado sistema possam acessar determinadas contas criadas nas plataformas dos provedores de hospedagem[95].

Por outro lado, quando um *hacker* utiliza seus conhecimentos com o objetivo de infringir a lei, alcunha-se o mesmo como *cracker*[96].

Como bem pontuado pelo Juiz Paul Perell, quando do julgamento do caso *Lozanski v. The Home Depot*[97], em um ataque cibernético os "verdadeiros vilões" são os *crackers* que roubaram os dados. Contudo, um dos maiores desafios na tutela dos titulares de dados na internet está em identificar o causador do dano:

> "O ambiente virtual possibilita a criação da identidade pela qual o usuário se apresenta aos demais. A princípio, portanto, abre-se espaço para que o internauta, protegido pelo anonimato, cause danos de difícil reparação, na medida em que o ofendido não possui, *prima facie*, meios para identificar quem lhe causou danos."[98]

Como estes cibercriminosos normalmente não costumam ser encontrados, as demandas judiciais tendem a ser voltadas contra aqueles que tem a custódia dos dados.

Em sendo assim, acaso uma empresa venha a ser alvo de um incidente de segurança que venha a acarretar um vazamento de dados, é necessário que esta, após a descoberta do ataque, não encubra o ocorrido, mas, sim, aja de forma escorreita e de boa-fé, comunicando toda sua base de usuários acerca do ocorrido, atuando de forma transparente e propositiva, reduzindo e mitigando, assim, qualquer responsabilidade.

Ressalte-se, ainda, que a matéria em questão já foi objeto de análise pela jurisprudência pátria, sendo reconhecida a exclusão de responsabilidade do fornecedor de serviços ante a ocorrência de fortuito externo, evidenciando-se a culpa exclusiva de terceiro (*cracker*). *In verbis*:

---

[95] PAESANI, Liliana Minardi. **Direito e Internet: Liberdade de informação, privacidade e responsabilidade civil.** 7. ed. São Paulo: Atlas, 2014. P. 22

[96] Disponível em <https://www.tecmundo.com.br/o-que-e/744-o-que-e-cracker-.htm>. Acesso em 30/08/2020.

[97] Processo 2016 ONSC 5447, para 100. Disponível em <http://www.canadahomedepotdatabreachsettlement.com/media/664229/docs-_15865690-v1-reasons_for_decision_perell_j_-_aug_29_2016.pdf >. Acesso em 19/04/2021.

[98] TERRA, Aline de Miranda; GUEDES, Gisela Sampaio da Cruz; TEPEDINO, Gustavo (Orgs.). *Responsabilidade civil*. Rio de Janeiro: Forense, 2020. P. 268.

> *"RECURSO INOMINADO. AÇÃO INDENIZATÓRIA. RECEBIMENTO DE E-MAIL SPAM E SCAM.* ***FRAUDE. AUSÊNCIA DE RESPONSABILIDADE DO USUÁRIO. CASO DE FORTUITO EXTERNO. CULPA EXCLUSIVA DE TERCEIRO. DANO MORAL NÃO CONFIGURADO****. SENTENÇA MANTIDA. RECURSO CONHECIDO E DESPROVIDO."* (TJPR. Recurso Inominado nº 0035596-68.2017.8.16.0021. 1ª Turma Recursal – Cascavel, Relatora Juíza Vanessa Bassani, julgado em 14/08/2019 – grifou-se.)
>
> * * *
>
> *"RECURSO INOMINADO. CONSUMIDOR. AÇÃO INDENIZATÓRIA POR DANOS MATERIAIS E MORAIS. EMPRÉSTIMO PESSOAL FRAUDULENTO.* ***CASO FORTUITO EXTERNO. CULPA EXCLUSIVA DE TERCEIRO. AUTOR E RÉ QUE RESTARAM VITIMADOS POR GOLPE PERPETRADO POR TERCEIRO FRAUDADOR****. ESTELIONATÁRIO PRATICANDO O EVENTO DANOSO.* ***ROMPIMENTO DO NEXO DE CAUSALIDADE. RESPONSABILIDADE CIVIL NÃO CONFIGURADA. AUSENCIA DE PRESSUPOSTO PROCESSUAL. JULGAMENTO DE IMPROCEDENCIA DA AÇÃO. SENTENÇA MANTIDA****. RECURSO IMPROVIDO."* (TJRS. Recurso Cível nº 71007637622, Primeira Turma Recursal Cível, Relator José Ricardo de Bem Sanhudo, julgado em 29/05/2018 – grifou-se.)

Em linha com o ora exposto, oportuno o ensinamento de Roberto Senise Lisboa, citado por Marcel Leonardi[99], o qual destaca que:

> "Caso se demonstre a culpa exclusiva de terceiro, como se verifica na hipótese do hacker a provedora poderá se beneficiar dessa excludente de responsabilidade, recaindo o dever de indenização por danos morais em desfavor do real violador (artigo, II da Lei nº 8.078/1990)."

Como já exposto acima, o advento da tecnologia trouxe consigo certos infortúnios, dentre os quais os ataques cibernéticos de terceiros mal-intencionados.

Com efeito, não se deve olvidar que os *crackers* estão sempre um passo à frente dos sistemas de segurança da internet, de modo que, ainda que uma empresa tenha um sistema de segurança robusto e preparado, isto não é uma garantia de que a mesma esteja totalmente protegida contra todos os métodos possíveis de invasão em um determinado momento.

E é justamente em razão disso que, no mundo da segurança cibernética, diz-se "quando" e não "se" uma empresa sofrerá um ataque[100]. Nesse sentido, John McAffe, fundador da McAffe, um dos programas antivírus mais utilizados no mundo, declarou[101] que: *"*Eu nem tenho antivírus. Eu acho que o antivírus está morto. É usada uma tecnologia antiga, que não é relevante. Os hackers são dez vezes mais rápidos do que eles, é um sistema sem sentido*"*.

---

[99] LEONARDI, Marcel. **Responsabilidade Civil dos Provedores de Serviços de Internet**. São Paulo: Juarez de Oliveira, 2005. P 70.

[100] Disponível em <https://www.americanbar.org/groups/law_practice/publications/techreport/2017/security/> . Acesso em 30/08/2020.

[101] Disponível em <https://revistapegn.globo.com/Noticias/noticia/2015/09/o-antivirus-de-pc-esta-morto-diz-o-criador-da-empresa-mcafee.html.>. Acesso em 30/08/2020.

Diante de todo o exposto, dúvidas não há quanto à impossibilidade de responsabilização de uma empresa pelo vazamento de dados quando o mesmo ocorre em virtude de ataque cibernético, hipótese na qual resta caracterizada culpa exclusiva de terceiro que reuniu esforços para que o prejuízo ocorresse, restando, portanto, configurada hipótese de fortuito externo.

4.4 Os direitos da personalidade não podem servir como instrumento de mercantilização do instituto do dano moral

Salta aos olhos, aqui, a seguinte indagação: De que modo a divulgação de dados pessoais pode ser considerada uma ofensa aos direitos da personalidade? Afinal de contas, para que pudesse ingressar com uma ação judicial (assim como o seria com qualquer outra), o titular deve divulgar todas estas informações.

O questionamento acima busca apenas ilustrar que a simples divulgação de dados pessoais, por si só, não pode ser considerada apta a autorizar eventual indenização, sendo, portanto, imprescindível uma análise das particularidades do caso concreto para que seja verificada a ocorrência – ou não – de mácula aos direitos da personalidade.

O que se busca, aqui, não é o afastamento da responsabilidade da sociedade empresária pela adoção de medidas de segurança para proteção de dados pessoais. Por outro lado, o que não se pode admitir é que a ocorrência de um incidente de segurança, decorrente de um ataque praticado por terceiros mal-intencionados, gere o dever de indenização sem que haja qualquer prova efetiva de dano.

Tal questão ganha especial relevância quando observada a crescente quantidade de disputas relacionadas à proteção de dados, sobretudo após a edição da LGPD.

Ora, ao admitir que o mero vazamento de dados, por si só, permita ao titular o direito a ser ressarcido por pretensos danos morais, sem qualquer necessidade de comprovação dos prejuízos sofridos, não terá outro condão senão o de fomentar o ajuizamento indiscriminado de demandas indenizatórias, colocando em risco não só a atividade empresarial como, também, a eficiência do Poder Judiciário.

Tendo em mente que a LGPD regula relações cotidianas dos indivíduos e há um aumento da conscientização destes a respeito da importância de protegerem os seus dados pessoais, é patente supor que as discussões a seu respeito passarão a representar expressivo percentual das ações judiciais em trâmite na justiça brasileira.

Conforme ressaltam Martins e Monteiro[102], em seminário ocorrido em setembro de 2019, o Superior Tribunal de Justiça (STJ) previu que "a LGPD, logo em seu primeiro ano de vigência, já poderia vir a ser o objeto de mais de 20 mil processos judiciais".

Analisando a experiência internacional, houve um aumento no número de litígios relacionados à proteção de dados pessoais após a aprovação de leis protetivas semelhantes à LGPD. A título de exemplo, na Irlanda, com base na aplicação do GDPR, entre 1º de janeiro e 31 de dezembro de 2020, a autoridade de proteção de dados irlandesa (*Data Protection Commission – DPC*) recebeu 4.719 reclamações, sendo 4.660 com base no GDPR[103].

Não se desconhece a tendência contemporânea de constitucionalização dos direitos e da aplicação de princípios na solução de contendas, contudo, incumbe ao Judiciário proceder de forma parcimoniosa e casuística, sob pena de incorrer na chamada *"banalização ou mesmo carnavalização do Direito"*[104].

Em sendo assim, o Poder Judiciário não pode albergar pretensão na qual se objetiva a monetização de um instituto ontologicamente existencial.

4.5 A jurisprudência comparada e os danos morais decorrentes da violação de dados pessoais

O exponencial avanço tecnológico é fonte de profícuas discussões na seara do Direito, sendo de grande relevância a discussão acerca da aplicação de seus institutos a situações inimagináveis ao legislador do passado.

---

[102] Disponível em < https://valor.globo.com/legislacao/coluna/protecao-de-dados-pessoais-em-2020.ghtml > Acesso em 04/05/2021.

[103] Disponível em < https://www.dataprotection.ie/sites/default/files/uploads/2021-02/DPC%202020%20Annual%20Report%20%28English%29.pdf > Acesso em 05/05/2021.

[104] KONDER, Carlos Nelson. **Distinções Hermenêuticas da Constitucionalização do Direito Civil: O Intérprete na Doutrina de Pietro Perlingieri**. *In* Revista da Faculdade de Direito – UFPR, Curitiba, vol. 60, n. 1, jan./abr. 2015. P. 205.

Especificamente no que se refere à proteção de dados, a LGPD exsurge com a função de trazer soluções a novas questões, de extrema relevância econômica e social, cuja especificidade não se amoldava ao corpo legislativo existente.

Contudo, há que se pontuar que a referida legislação também não prevê todas as soluções necessárias à solução das mais diversas situações concernentes à matéria.

Nesse sentido, a Lei de Introdução às Normas de Direito Brasileiro, em seu artigo 4º dispõe que: "quando a lei for omissa, o juiz decidirá o caso de acordo com a analogia, os costumes e os princípios gerais de direito".

Deste modo, e uma vez considerada que a nascitura legislação de proteção de dados brasileira possui arrimo na produção legislativa internacional, faz-se salutar a análise de casos similares ao presente no âmbito da jurisprudência alienígena com vistas a melhor compreensão da *quaestio* em análise.

4.5.1 A Experiência Canadense – Dicotomia Da Prova Dos Danos

4.5.1.1 Precedente Li *versus* Equifax

Em setembro de 2017, a empresa Equifax, anunciou que os dados pessoais de 143 milhões de seus usuários foram comprometidos em função de um vazamento de dados em âmbito global.

Em vista de tal fato, um dos usuários afetados ajuizou um pedido de autorização para instituição de ação coletiva perante a Corte Suprema de Quebec[105], alegando que: (i) haveria responsabilidade extracontratual da Equifax em razão de sua falha no armazenamento e guarda de dados pessoais e financeiros de seus clientes; (ii) a violação do direito dos consumidores à privacidade em virtude do vazamento de dados pessoais a terceiros sem que houvesse autorização de seu titular; e (iii) a violação do direito à privacidade e de não divulgação de informações confidenciais dos titulares.

---

[105] Precedente Li c. Equifax inc., 2019 QCCS 4340 (CanLII). Disponível em <https://www.registredesactionscollectives.quebec/en/Fichier/Document?NomFichier=4547.pdf>. Acesso em 08/04/2021.

Com base no alegado, pugnou-se pela condenação da Equifax ao pagamento de indenização pelas despesas, contratempos e inconveniências decorrentes do acesso não autorizado dos dados pessoais.

Ao analisar o caso, a Suprema Corte entendeu que as alegações autorais demonstrariam *prima facie* fundamentos de que o vazamento de dados decorreu de uma falha. No entanto, as alegações do demandante (e aqui se vê o paralelo com a presente demanda) eram insuficientes para demonstrar quaisquer danos sofridos em virtude de tal falha.

Em tal hipótese, a simples falha na prestação do serviço não foi considerada apta a ensejar o prosseguimento da demanda, na medida em que deve haver não apenas a falha, como, também, a existência do dano.

Ademais, restou consignado que a caracterização do sofrimento mental alegado pelo demandante não se caracterizou em nada além de mero aborrecimento, ansiedade e medo comum que as pessoas que vivem em sociedade aceitam rotineiramente (embora às vezes com relutância).

Por fim, restou decidido no julgado em referência que não resta configurado dano indenizável o simples fato de um terceiro estar em posse de dados pessoais sem autorização, e nada mais.

4.5.1.2 Precedente Bourbonnière versus Yahoo!

Em linha com o precedente acima exposto, no caso em tela, a Corte Suprema de Quebec firmou entendimento no sentido de que o fato de um titular de dados pessoais ter sido vítima de um incidente de segurança não dá, por si só, o direito de pleitear indenização por danos morais.

Em 2016, a Yahoo! divulgou o comprometimento de dados pessoais de mais de 500 milhões de dados pessoais, os quais foram roubados por *hackers*.

Diante de tal fato, uma das usuárias afetadas apresentou requerimento solicitando autorização para ajuizamento de uma ação coletiva em nome de todos os cidadãos de Quebec que foram vítimas de tal vazamento de dados.

Em suas razões, foi descrita a ocorrência de danos de ordem psicológica e emocional, além de potencial prejuízo financeiro.

Ao analisar tal requerimento, a Corte Suprema entendeu que a falha atribuída ao Yahoo! foi sua negligência no que se refere à proteção das informações pessoais e financeiras de seus usuários. Contudo, tal falta não dá ensejo à condenação da empresa ao pagamento de indenização de forma automática, de forma que qualquer dano indenizável subsequente deve ser demonstrado, o que não foi feito no caso e é justamente o que se alega na presente hipótese.

Deste modo, restou decidido que o dano alegado consistia apenas em inconveniências ordinárias e transitórias, as quais seriam insuficientes para constituir "dano compensável".

4.5.2 A Jurisprudência Norte-Americana – Sem Prova do Dano, não há Processo

No precedente Pisciotta *versus* Old National Bancorp[106], o Tribunal de Apelações dos Estados Unidos para o Sétimo Circuito firmou entendimento no sentido de que se os únicos danos alegados após um incidente de segurança de dados são os gastos com o monitoramento de crédito, o demandante não tem direito ao recebimento de qualquer tipo de indenização.

Na hipótese em questão, a empresa demandada, Old National Bancorp, coletava informações de clientes relativos a aplicativos de contas, empréstimos e outros serviços bancários.

Essas informações incluíam nomes, endereços, números do seguro social, números de carteira de motorista, datas de nascimento e outras informações financeiras dos clientes.

Em 2005, o site da empresa foi hackeado, comprometendo as informações pessoais que esta mantinha sobre seus clientes.

---

[106] Precedente F.3d -, 2007 WL 2389770. Disponível em <https://jenner.com/system/assets/assets/3681/original/Pisciotta_v_Old_National.pdf?1319643351>. Acesso em 08/04/2021.

Em vista de tais fatos, os demandantes Luciano Pisciotta e Daniel Mills ingressaram com uma ação coletiva no Tribunal Distrital dos Estados Unidos para o Distrito Sul de Indiana, reivindicando indenização sob o fundamento de que houve: (i) negligência da empresa demandada quanto à guarda e proteção de dados pessoais; (ii) inadimplemento contratual com a empresa demandada e inadimplemento implícito do contrato havido entre esta e seu parceiro de hospedagem do site.

Os demandantes alegaram que houve negligência da empresa em proteger seus dados pessoais, o que fez com que cada membro da classe sofresse danos econômicos substanciais e sofrimento emocional, além da preocupação havida com a possibilidade de terceiros usarem indevidamente suas informações pessoais.

No entanto, os demandantes não demonstraram a existência de quaisquer perdas financeiras ou que qualquer membro da classe já tivesse sofrido algum dano efetivo em decorrência do vazamento de seus dados pessoais.

Ao analisar o pleito dos demandantes, em primeira instância, o Tribunal Distrital dos Estados Unidos para o Distrito Sul de Indiana entendeu que os demandantes não fizeram prova de que a conduta da empresa demandada havia lhes causado qualquer dano cognoscível.

Restou consignado, ainda, que o custo havido pelos demandantes com monitoramento de crédito não é resultado de qualquer lesão presente, mas sim a antecipação de lesão futura que ainda não se materializou.

Em face de tal decisão, os demandantes interpuseram recurso ao Tribunal de Apelações dos Estados Unidos para o Sétimo Circuito, que, ao julgar o mesmo, entendeu que sem mais do que alegações de aumento do risco de roubo de identidade futuro, os demandantes não sofreram um dano que a lei esteja preparada para remediar.

4.5.3 A Experiência Europeia – *General Data Protection Regulation*

De acordo com o artigo 82 do Regulamento Geral sobre a Proteção de Dados (GDPR, em inglês), qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação

do regulamento tem direito a receber uma indenização do agente responsável pelo tratamento ou do subcontratante pelos danos sofridos.

Apesar de garantir o direito de indenização dos titulares de dados, o RGPD não prescreve um mecanismo específico para se fazer valer esse direito, deixando o julgamento a cargo dos países individualmente, de acordo com o sistema de responsabilidade civil de cada um.

Na Áustria, no precedente *Wirthensohn* versus *Österreichische* Post, restou firmado, em sede de apelação, que deverá ser demonstrado um grau mínimo de dano pessoal para ensejar a responsabilização com consequente indenização, não sendo suficiente o sentimento de mágoa por parte do titular de dados afetado.

A *Österreichische* Post, empresa responsável pelo serviço postal no país, utilizou indevidamente os dados pessoais de seus clientes traçando análises estatísticas acerca de sua afinidade política. Um dos titulares de dados, ao fazer uma solicitação de acesso aos seus dados, recebeu uma cópia de suas supostas afiliações partidárias.

Ao processar o serviço postal, o demandante argumentou apenas que se sentiu incomodado por ter sido descrito desta forma, sem ser notificado ou dar o seu consentimento.

Em Novembro de 2019, o Tribunal Regional de Feldkirch (*Landgericht* Feldkirch)[107], na Áustria, em 1ª instância, condenou a empresa ao pagamento de indenização ao requerente em decorrência de dano pelo tratamento ilegal de seus dados pessoais, sob o entendimento de que o mero distúrbio caracterizado como um dano emocional, não material, provocado por tal tratamento seria suficiente para ensejar a indenização.[108]

Entretanto, em fevereiro de 2020, o Tribunal Federal de Innsbruck (*Oberlandesgericht* Innsbruck)[109] reformou em sede de 2ª instância a decisão anterior, com base na legislação

---

[107] Processo 57Cg30/19b, decidido em 07/08/2019. Disponível em <https://gdprhub.eu/index.php?_title=LG_Feldkirch_-_57_Cg_30/19b_-_15>. Acesso em 07/04/2021.

[108] FRITZ, Gernot; KLIMPFINGER, Boris. *Can I claim damages for hurt feelings under GDPR? An Austrian court says 'yes'*. Fresh-fields Bruckhaus Deringer blog, novembro de 2019. Disponível em < https://digital.freshfields.com/post/102fth1/can-i-claim-damages-for-hurt-feelings-under-gdpr-an-austrian-court-says-yes > Acesso em 06/05/2021.

[109] Processo 1 R 182/19b, decidido em 13/02/2020. Disponível em: <https://gdprhub.eu/index.php?title=OLG_Innsbruck_-_1_R_182/19b>. Acesso em 09/04/2021.

austríaca de responsabilidade civil, firmando o entendimento de que o demandante deve comprovar ter sofrido lesão considerável, que resulte em danos pessoais, decorrente da violação ao GDPR[110]. O simples fato de a empresa ter utilizado indevidamente os dados não enseja a verificação de dano.

No mesmo sentido, na Alemanha, dois julgamentos decidiram pela limitação da compensação pelo dano, considerando que um dano imaterial trivial não ensejaria uma compensação.

Em novembro de 2018, o Tribunal Local de Diez (*Amtsgericht* Diez)[111] decidiu, em um caso no qual o titular de dados recebeu um e-mail spam, que um dano mínimo não implica automaticamente um pedido de indenização por dano moral.

Assim, o Tribunal considerou que a violação do GDPR sem danos como consequência não dará origem a uma reclamação por danos e que "danos mínimos" não dão origem a danos nos termos do artigo 82 do GDPR. Faz-se necessária uma desvantagem perceptível na esfera do titular de dados.

Em junho de 2019, o Tribunal Federal de Dresden (*Oberlandesgericht* Dresden)[112] confirmou amplamente o mesmo entendimento. O autor entrou com uma ação de indenização contra o Facebook por danos materiais e morais, de acordo com o Artigo 82 do GDPR, para a exclusão de uma postagem e o por conta do bloqueio temporário de sua conta de usuário.

O Tribunal Federal de Dresden indeferiu a pretensão do autor, não considerando que houve violação às disposições do GDPR e danos materiais ou morais, tendo em vista que não houve prejuízo relevante à sua imagem ou reputação.

---

[110] FRITZ, Gernot; SCHEITEL, Julian. *Damages for hurt feelings under GDPR? Austrian court tightens up requirements*. Fresh-fields Bruckhaus Deringer blog, março de 2020. Disponível em < https://digital.freshfields.com/post/102g1c4/damages-for-hurt--feelings-under-gdpr-austrian-court-tightens-up-requirements > Acesso em 06/05/2021.

[111] Processo 8 C 130/28, decidido em 07/11/2018. Disponível em <https://gdprhub.eu/index.php?title=AG_Diez_8_C_130/18_7.11.2018>. Acesso em 08/04/2021.

[112] Processo 4 U 760/19, decidido em 11/06/2019. Disponível em: <https://gdprhub.eu/index.php?title=OLG_Dresden_-_4_U_760/19>. Acesso em 08/04/2021.

Assim, na opinião do Tribunal, danos morais triviais não caracterizam a responsabilidade civil do agente de tratamento de dados. Caso contrário, haveria um risco substancial de abuso por parte dos demandantes.

5. CONCLUSÃO

É premissa básica da Lei Geral de Proteção de Dados regulamentar e dispor de normas com o objetivo de assegurar o regular tratamento de dados pessoais, sendo fundamental o tema da responsabilização para que esse conjunto de medidas seja realmente efetivo, tendo em vista que são inúmeros os direitos dos titulares de dados, as formas de violá-lós, bem como os sujeitos que podem violá-los.

Conforme elucidado ao longo da pesquisa, os inúmeros episódios de incidentes de segurança gerando o vazamento de dados pessoais deixa evidente que um dos aspectos centrais do novo marco legal é, não só a regulamentação acerca da coleta e tratamento, mas, principalmente, a responsabilidade civil das entidades que não conseguirem garantir a integridade do direito fundamental em voga.

A despeito da essencialidade do tema, o legislador não estabeleceu um claro regime de responsabilidade civil a ser aplicável aos agentes de tratamento de dados. Diante da omissão legislativa, cabe à doutrina cumprir a sua função interpretadora da lei.

Sendo assim, a presente monografia buscou realizar um estudo acerca da natureza jurídica da responsabilidade civil na referida lei, partindo da análise das normas gerais do instituto dispostas no Código Civil e a evolução histórica do tema no tocante a proteção de dados para, então, desaguar nos argumentos das duas correntes formadas.

Esse cotejamento se faz necessário para demonstrar as circunstâncias que levam a crer que o legislador deixou pistas para a adoção do regime subjetivo e da culpa como fundamento, pelo menos, como regra geral.

Verificou-se que a adoção do regime de responsabilidade civil objetiva acarretará uma potencial avalanche de litígios e disputas judiciais entre titulares de dados e os entes que realizam o tratamento desses dados, sejam eles controladores ou operadores.

É concebível que o titular possa sofrer danos devido ao processamento irregular de dados pessoais, mas se for permitido que quantias substanciais de violações sejam reivindicadas simplesmente estabelecendo que o processamento é desagradável, em vez de se exigir que o autor prove o dano real sofrido, resultará em um congestionamento ainda maior nos Tribunais pátrios.

Ainda, tal responsabilização ensejaria verdadeiro desincentivo à observância dos deveres de proteção, prevenção e segurança impostos aos agentes de tratamento, desmerecendo a intenção de um ambiente virtual de livre fluxo informacional como resposta para uma economia global baseada em dados.

Nesse diapasão, é de suma importância que o instituto da responsabilidade civil seja estrategicamente pensado.

Por tudo exposto, percebe-se claramente que a intenção do legislador, ao pautar a Lei Geral de Proteção de Dados na criação de deveres aos agentes de tratamento de dados estabelecendo um standard de conduta, é a de adoção da responsabilidade subjetiva.

No que toca à responsabilidade dos agentes de tratamento em virtude de vazamento de dados decorrentes de ataques cibernéticos, dada a sua frequência, depreende-se que não havendo repercussão específica na esfera do titular, não deve implicar na imediata responsabilização e dever de indenizar, pois não gera dano moral na medida em que não ofende a dignidade humana.

Ora, para que não ocorra a mercantilização do instituto do dano moral, o dano moral decorrente de vazamento de dados não deve ser considerado *in re ipsa*, sendo necessária a prova efetiva da lesão sofrida pelo titular dos dados pessoais envolvidos no incidente de segurança.

Em breve, a Lei Geral de Proteção de Dados Pessoais estará em pleno vigor, logo caberá aos operadores do direito a produção de respostas eficazes para tal lacuna. O ideal seria a clareza do legislador para evitar insegurança e ativismo judicial. No entanto, perante a dubiedade, será necessário um olhar atento quanto a futuro posicionamento dos Tribunais Superiores.

6. REFERÊNCIAS

ALECRIM, Emerson. **Google confirma novo smart speaker Nest após vazamento**. Disponível em <https://tecnoblog.net/351638/google-nest-speaker-alto-falante-inteligente-confirmado/>. Acesso em 26/08/2020.

Anteprojeto de Lei para a Proteção de Dados Pessoais. Disponível em <http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/ >. Acesso em 24/04/2021.

BANISAR, David. **National Comprehensive Data Protection/Privacy Laws and Bills 2020**. Disponível em < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416>. Acesso em 12/04/2021.

BELTOV, Martin. **O AdGuard Ad Blocker foi hackeado, Redefinir suas senhas!** Disponível em <https://sensorstechforum.com/pt/adguard-ad-blocker-hacked-reset-passwords/>. Acesso em 26/08/2020.

BRASIL. Câmara dos Deputados. **Projeto de Lei 5.276/2016**. Disponível em <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=62B6CCB8D15F03BD169F7421D3CDB6EE.proposicoesWeb1?codteor=1457971&filename=Avulso+-PL+5276/2016 >. Acesso em 24/04/2021.

BRASIL. **Constituição da República Federativa do Brasil**. Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm>. Acesso em 20/02/2021.

BRASIL. **Lei nº 8.078/ 1990**. Código de Proteção e Defesa do Consumidor. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em 10/03/2021.

BRASIL. **Lei nº 10.406/ 2002**. Código Civil. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406.htm.>. Acesso em 05/04/2021.

BRASIL. **Lei nº 12.414/2011**. Disciplina o cadastro positivo. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. Acesso em 10/04/2021.

BRASIL. **Lei nº 12.527/2011**. Regula o acesso a informações públicas. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em 11/04/2021.

BRASIL. **Lei nº 12.737/2012**. Dispõe sobre a tipificação criminal de delitos informáticos. Disponível em < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em 10/04/2021.

BRASIL. **Lei nº 12.965/2014**. Marco Civil da Internet. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/_Ato2011- 2014/2014/Lei/L12965.htm.>. Acesso em 05/04/2021.

BRASIL. **Lei nº 13.709/2018**. Lei Geral de Proteção de Dados Pessoais. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em 05/04/2021.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Recurso Especial 1.402.104/RJ**. Rel. Ministro Raul Araújo. Quarta Turma. Julgado em 27/05/2014.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial 1.193.764/SP**. Rel. Ministra Nancy Andrighi. Terceira Turma. Julgado em 08/08/2011.

CASCAES, Amanda Celli, BRESEGHELLO, Fabíola Meira de Almeida, TUTIKIAN, Priscila David Sansone (Coord.). **Comentários à Lei Geral de Proteção de Dados à luz do Código de Defesa do Consumidor**. São Paulo: Ed. Singular, 1ª edição, 2019.

CASTRONOVO, Carlo. ***La nuova responsabilità civile***. Milano: Giuffrè, 2006.

CAVALIERI FILHO, Sergio**. Programa de Responsabilidade Civil**. 10. ed. rev. e ampl. São Paulo: Atlas, 2012.

COUTO E SILVA, Clóvis Veríssimo do. **O conceito de dano no direito brasileiro e comparado**. In: Revista dos Tribunais, v. 667, São Paulo: RT, maio/1991.

Dados: o novo petróleo do mundo e combustível para o futuro. Disponível em < https://bakertillybr.com.br/dados-novo-petroleo/ > Acesso em 12/04/2021.

FLUMIGNAN, Wévertton Gabriel Gomes. **Responsabilidade civil dos provedores no Marco Civil da Internet (Lei 12.965/14)**. Dissertação de Mestrado Faculdade de Direito, Universidade de São Paulo, 2018.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais, 2019.

FRITZ, Gernot; KLIMPFINGER, Boris. **Can I claim damages for hurt feelings under GDPR? An Austrian court says 'yes'**. Fresh-fields Bruckhaus Deringer blog, novembro de 2019. Disponível em < https://digital .freshfields.com/post/102fth1/can-i-claim-damages-for-hurt-feelings-under-gdpr-an-austrian-court-says-yes >. Acesso em 06/05/2021.

FRITZ, Gernot; SCHEITEL, Julian. **Damages for hurt feelings under GDPR? Austrian court tightens up requirements**. Fresh-fields Bruckhaus Deringer blog, março de 2020. Disponível em < https://digital .freshfields.com/post/102g1c4/damages-for-hurt--feelings-under-gdpr-austrian-court-tightens-up-requirements >. Acesso em 06/05/2021.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo Curso de Direito Civil: Responsabilidade Civil**. 15. ed. São Paulo: Saraiva, 2017.

GOMES, Orlando. **Obrigações**. 8ª edição. Rio de Janeiro: Forense, 1992.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro: Responsabilidade Civil**. 15. ed. São Paulo: Saraiva, 2020. v. 4.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Venceslau. Término do Tratamento de Dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro**. São Paulo: Revista dos Tribunais, 2019.

HARARI, Yuval Noah. **21 Lições para o Século 21**. Trad. Paulo Geiger. São Paulo: Companhia das Letras, 2018.

HART, Herbert. L. A. **O conceito de Direito**. Pós-escrito editado por Penélope A. Bulloch e Joseph Raz. Tradução de A. Ribeiro Mendes. 2.ed. São Paulo: Martins Fontes, 2012.

HSU, Tiffany. **Cibercriminosos fazem planos de fidelização perderem US$ 1 bilhão por ano nos EUA**. Disponível em <https://oglobo.globo.com/economia/cibercriminosos-fazem-planos-de-fidelizacao-perderem-us-1-bilhao-por-ano-nos-eua-23662569>. Acesso em 26/08/2020.

JIMENE, Camilla do Vale. **Da Importância da Segurança da Informação para Adequação à LGPD**. In: BLUM, Renato Opice (Organizador). **Proteção de Dados: Desafios e Soluções na Adequação à Lei**. Rio de Janeiro: Editora Forense, 2020.

KONDER, Carlos Nelson. Distinções Hermenêuticas da Constitucionalização do Direito Civil: O Intérprete na Doutrina de Pietro Perlingieri. In Revista da Faculdade de Direito – UFPR, Curitiba, vol. 60, n. 1, jan./abr. 2015.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas, 2003.

LEONARDI, Marcel. **Responsabilidade Civil dos Provedores de Serviços de Internet**. São Paulo: Editora Juarez de Oliveira, 2005.

LIMA, Cintia Rosa Pereira de. In **I Simpósio de Responsabilidade Civil e Proteção de Dados**. Evento realizado pelo Instituto Brasileiro de Estudos de Responsabilidade Civil – IBERC. Agosto, 2020. Disponível em < https://www.youtube.com/watch?v=igbbxkbqeKI&t=4213s>. Acesso em 03/04/2021.

MARTINS, Elaine. **O que é cracker?** Disponível em <https://www.tecmundo.com.br/o-que-e/744-o-que-e-cracker-.htm>. Acesso em 30/08/2020.

MCKEAY, Martin. **The Building Wave of Internet Traffic**. Disponível em < https://blogs.akamai.com/sitr/2020/04/the-building-wave-of-internet-traffic.html >. Acesso em 12/04/2021.

MENDES, Laura Schertel; DONEDA, Danilo. **Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018), o novo paradigma da proteção de dados no Brasil**. REVISTA DE DIREITO DO CONSUMIDOR, v. 120, 2018.

MENDES, Laura Schertel. **A vulnerabilidade do consumidor quanto ao tratamento de dados pessoais**. In: MARQUES, Claudia Lima; GSELL, Beate. **Novas tendências do direito do consumidor: rede Alemanha-Brasil de pesquisas em direito do consumidor**. São Paulo: Ed. RT, 2015.

MIRAGEM, Bruno. **Direito Civil: Responsabilidade Civil**. São Paulo: Saraiva, 2015.

MONTEIRO, Renato Leite. **Lei Geral de Proteção de Dados do Brasil: análise contextual detalhada**. Jota, 14 de julho de 2018. Disponível em < https://www.jota.info/opiniao-e-

analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada-14072018 > Acesso em 13/04/2021.

MORAES, Maria Celina Bodin de. **Danos à pessoa humana - uma leitura civil-constitucional dos danos morais**. Rio de Janeiro: Renovar, 2003.

MORAES, Maria Celina Bodin de. **Risco, solidariedade e responsabilidade objetiva**. Revista dos Tribunais, São Paulo, Ed. Rt, V. 854, dez. 2006.

MULHOLLAND, Caitlin. **A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco?** 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 21/03/2021.

O antivírus de PC está morto, diz o criador da empresa McAfee. Disponível em <https://revistapegn.globo.com/Noticias/noticia/2015/09/o-antivirus-de-pc-esta-morto-diz-o-criador-da-empresa-mcafee.html>. Acesso em 30/08/2020.

PAESANI, Liliana Minardi. **Direito e Internet: Liberdade de informação, privacidade e responsabilidade civil**. 7. ed. São Paulo: Atlas, 2014.

PAYÃO, Felipe. **Reddit assume invasão e vazamento de dados**. Disponível em <https://www.tecmundo.com.br/seguranca/132813-reddit-assume-invasao-vazamento-dados.htm>. Acesso em 26/08/2020.

PEREIRA, Caio Mário da Silva. **Responsabilidade Civil**. 9. ed. rev. Rio de Janeiro: Forense, 1999.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais: Comentários à Lei no 13.709/2018**. 1. ed. São Paulo: Saraiva Educação, 2018.

Precedente Li c. Equifax inc., 2019 QCCS 4340 (CanLII). Disponível em <https://www.registredesactionscollectives.quebec/en/Fichier/Document?NomFichier =4547 .pdf>. Acesso em 08/04/2021.

Processo 1 R 182/19b, decidido em 13/02/2020. Disponível em: <https://gdprhub.eu/index.php?title=OLG_Innsbruck_-_1_R_182/19b>. Acesso em 09/04/2021.

Processo 4 U 760/19, decidido em 11/06/2019. Disponível em: <https://gdprhub.eu/ index.php?title =OLG_Dresden_-_4_U_760/19>. Acesso em 08/04/2021.

Processo 8 C 130/28, decidido em 07/11/2018. Disponível em <https://gdprhub.eu/ index.php?title=AG_Diez_8_C_130/18_7.11.2018>. Acesso em 08/04/2021.

Processo 2016 ONSC 5447, para 100. Disponível em <http://www.canadahomedepotdatabreach settlement.com/media/664229/docs-_15865690-v1-reasons_for_decision_perell_j_-_aug_29_2016.pdf >. Acesso em 19/04/2021.

Processo 57Cg30/19b, decidido em 07/08/2019. Disponível em <https://gdprhub.eu/index.php? title=LG _Feldkirch_-_57_Cg_30/19b_-_15>. Acesso em 07/04/2021.

Proteção de dados pessoais em 2020. Disponível em <https://valor.globo.com/legislacao/ coluna/protecao-de-dados-pessoais-em-2020.ghtml > Acesso em 04/05/2021.

REINALDO, Demócrito. **Direito da Informática: Temas Polêmicos**. Bauru/SP: EDIPRO, 2002.

RIES, David G. **2017 Security**. Disponível em <https://www.americanbar.org/groups/ law_practice/publications/techreport/2017/security/>. Acesso em 26/08/2020.

RHOR, Altieres. **Dados de milhões de usuários do site Dailymotion vazam na web**. Disponível em <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/dados-de-milhoes-de-usuarios-do-site-dailymotion-vazam-na-web.html>. Acesso em 26/08/2020.

RHOR, Altieres. **Megavazamentos de dados expõem informações de 223 milhões de números de CPF**. Disponível em < https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2021/01/25/vazamentos-de-dados-expoem-informacoes-de-223-milhoes-de-numeros-de-cpf.ghtml > Acesso em 12/04/2021.

RODRIGUES, Sílvio. **Direito Civil: Responsabilidade Civil**. 19ª ed. São Paulo: Saraiva, 2002, v. 4.

SRNICEK, Nick. **Platform capitalism**. Cambridge: Polity Press, 2018.

State of the Internet/Security - Volume 5, Issue 2: Retail Attacks and API Traffic. Disponível em <https://www.akamai.com/us/en/multimedia/documents/state-of-the-

internet/state-of-the-internet-security-retail-attacks-and-api-traffic-report-2019.pdf>. Acesso em 26/08/2020.

TEPEDINO, Gustavo; BARBOSA, Heloisa Helena; MORAES, Maria Cecilia Bodin de. **Código Civil interpretado conforme a Constituição da República - Volume III**. Rio de Janeiro: Renovar, 2006.

TERRA, Aline de Miranda. GUEDES, Gisela Sampaio da Cruz. TEPEDINO, Gustavo (Orgs.). **Responsabilidade Civil**. Rio de Janeiro: Forense, 2020.

TIC Domicílios. Publicado pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação. Disponível em <https://www.cetic.br/media/docs/publicacoes/2/12225320191028-tic_dom_2018_livro_eletronico.pdf >. Acesso em 03/04/2021.

TROVÃO, Antonio Lucas M.C.; PIETZSCH, Ingo Dieter. **Lei Geral de Proteção de Dados e o Direito na Era Digital**. Disponível em <https://www.radloff.com.br/lei-geral-de-protecao-de-dados-e-o-direito-na-era-digital/>. Acesso em 20/04/2021.

UNIÃO EUROPÉIA. **General data protection regulation EU** (2016/679). Disponível em: < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 > Acesso em 05/05/2021.