
**UNIVERSIDADE FEDERAL DO RIO DE JANEIRO**

**CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS**

**FACULDADE DE DIREITO**

# A PROTEÇÃO DE DADOS PESSOAIS NO BRASIL: UMA ANÁLISE DA TUTELA JURISDICIONAL SOB OS FUNDAMENTOS DA LEI 13.709/2018

**GABRIEL ARAUJO SPOLIDORO MATTOS**

**Rio de Janeiro**

**2022**


**GABRIEL ARAUJO SPOLIDORO MATTOS**

# A PROTEÇÃO DE DADOS PESSOAIS NO BRASIL: UMA ANÁLISE DA TUTELA JURISDICIONAL SOB OS FUNDAMENTOS DA LEI 13.709/2018

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. Marilson Santana dos Santos

Rio de Janeiro

2022

CIP - Catalogação na Publicação

M444p

Mattos, Gabriel Araujo Spolidoro
A PROTEÇÃO DE DADOS PESSOAIS NO BRASIL: UMA ANÁLISE DA TUTELA JURISDICIONAL SOB OS FUNDAMENTOS DA LEI 13.709/2018 / Gabriel Araujo Spolidoro Mattos. -- Rio de Janeiro, 2020.
71 f.

Orientador: Marilson Santana.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade Nacional de Direito, Bacharel em Direito, 2020.

1. Lei Geral de Proteção de Dados. 2. Tutela. 3. Jurisdicional. 4. LGPD. I. Santana, Marilson, orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.


**GABRIEL ARAUJO SPOLIDORO MATTOS**

# A PROTEÇÃO DE DADOS PESSOAIS NO BRASIL: UMA ANÁLISE DA TUTELA JURISDICIONAL SOB OS FUNDAMENTOS DA LEI 13.709/2018

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. Marilson Santana.

Data da Aprovação: ___/___/___

Banca Examinadora:

_____

Orientador

_____

Membro da Banca

_____

Membro da Banca

**Rio de Janeiro**

**2022**

## AGRADECIMENTOS

Gostaria de agradecer em primeiro lugar aos meus pais, Marcos e Teresa, pelo suporte e dedicação imensuráveis na minha formação, pelos ensinamentos e lições sem os quais eu não teria chegado até aqui.

Agradeço às minhas irmãs, Naiara e Tabata, pelo apoio e auxílio durante todo esse tempo, e por me darem a certeza de que sempre as teria ao meu lado.

Agradeço a Yasmim, pelo amor, carinho, companheirismo e, principalmente, por sempre ter acreditado em mim, mesmo quando tive dúvida.

Por fim, gostaria de agradecer a todos os meus amigos que me acompanharam nesse processo, em especial ao Vinicius e Brenda, pelos momentos de descontração, leveza e irmandade que muitas vezes serviram de válvula de escape nos momentos mais difíceis. E nos fazem pensar nas ocasiões em que a vida merecer ser aproveitada a cada segundo.

## RESUMO

Os dados pessoais estão inseridos na realidade atual como um elemento extremamente valioso na esfera privada de seus titulares, tendo em vista a necessária inserção e manejo desses para quase todas as interações e relações interpessoais ou jurídicas modernas. A vista disso, o presente trabalho objetiva estudar a tutela dos dados pessoais no brasil, primeiro sob um viés histórico-normativo, perpassando pelas legislações que regulavam o instituo de maneira esparsa até a edição da lei 13.709/2018 de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados. E como objetivo específico proceder com a análise da tutela jurisdicional deste direito fundamental, sob o escopo de proteção normativa da LGPD, a fim de abordar e elucidar o entendimento que tem sido formado na aplicação e interpretação concreta destes dispositivos. Destacando se possível, dentro desse cenário, a possível tendência que está se formando para a construção de uma cultura jurídica e social de valorização e proteção de dados pessoais privados.



**Palavras-Chave:** LGPD; Tutela Jurisdicional; Dados Pessoais; Jurisprudência; Privacidade

**ABSTRACT**

Personal data are inserted in the current reality as an extremely valuable element in the private sphere of their holders, in view of the necessary insertion and handling of these for almost all modern interpersonal or legal interactions and relationships. In view of this, the present work aims to study the protection of personal data in Brazil, first under a historical-normative perspective, passing through the legislation that regulated the institute in a sparse way until the enactment of law 13.709/2018 of August 14, 2018, known as the General Data Protection Act. And as a specific objective to proceed with the analysis of the judicial protection of this fundamental right, under the scope of normative protection of the LGPD, in order to address and elucidate the understanding that has been formed in the application and concrete interpretation of these provisions. Highlighting if possible, within this scenario, the possible trend that is forming for the construction of a legal and social culture of appreciation and protection of private personal data.

**Key words:** LGPD; Jurisdictional Guardianship; Personal data; Jurisprudence; Privacy.

**Sumário**

# INTRODUÇÃO

Os dados pessoais hoje revelam-se como um bem jurídico fundamental à personalidade do indivíduo. Sobretudo nas relações e modelo econômico da sociedade atual, pautados na busca constante pela inovação tecnológica e no trato cada vez mais eficiente com a informação.

Nesse sentido, o direito desempenha um papel fundamental na busca e elaboração de ferramentas jurídicas capazes de acompanhar essa evolução, a fim de suprir as lacunas e novas demandas que surgem cotidianamente. Neste cenário, foi promulgada a lei 13.709/2018, com o condão de criar um sistema legal de proteção de dados pessoais no Brasil.

Ante o exposto, nesse trabalho será realizado um estudo sobre os dados pessoais, enquanto um direito fundamental constitucional, e a sua regulação no ordenamento jurídico brasileiro. Será subdividido em três partes principais, na tentativa de alcançar o objetivo específico, consistente na análise da tutela jurisdicional dos dados pessoais sob os fundamentos da lei 13.709/18, e observar a tendência criada pelos Tribunais brasileiros.

Assim, no primeiro capítulo será abordado não só os conceitos inerentes ao entendimento deste instituto, mas também os marcos legais promulgados no país, que visavam regular e proteger esse bem jurídico. De modo a demonstrar a importância das leis esparsas e o seu campo de aplicabilidade, até a entrada em vigor da LGPD.

Na segunda etapa será realizada uma análise da Responsabilidade Civil aplicada à lei geral de proteção de dados. E como esse instituto se relaciona e é abordado pelas normas da referida lei. Tendo em vista que esta trouxe diversas inovações jurídicas sobre esse ponto, prevendo inclusive a hipótese de sanções administrativas através da aplicação de multa.

Na terceira parte, portanto, será almejada a resposta ao objetivo específico deste estudo. Que será feita através da análise da aplicação prática da LGPD nos tribunais, de modo a observar o entendimento adotado pelos julgadores na solução desses litígios. E com isso, entender se existe um padrão de aplicação nas demandas de natureza similar, além de verificar a complexidade com que esses casos concretos vêm chegando ao judiciário.

# 1. ANTECEDENTES LEGAIS DA PROTEÇÃO DE DADOS NO BRASIL

## 1.1 Conceito e Importância dos Dados Pessoais na Era da Informação

A tecnologia no mundo informatizado faz parte da nossa realidade social de maneira inequívoca e enraizada. Seja nas relações jurídicas, econômicas ou interpessoais, a internet das coisas e as tecnologias da informação estão presentes. Ao longo do tempo a humanidade passou por diferentes modelos econômicos, desde sistemas agrários até o auge da industrialização, ao passo que a presente quadra histórica pertence à chamada 'era da informação'. Através das novas tecnologias, o conhecimento torna-se um meio de adquirir mais conhecimento, transformando uma economia baseada no processamento eficiente da informação no contexto do consumo e circulação de bens e serviços em escala global.

Por meio de um clique, e em poucos instantes, somos capazes de fazer compras, realizar transações bancárias antes consideradas complexas e captar informações de qualquer lugar, por conta dessas ferramentas. Contudo, neste cenário de constante troca, os dados privados assumem hoje uma posição de extremo valor nas relações econômico-sociais, entre particulares ou não. Ao passo que informações pessoais são frequentemente utilizadas para outros fins além daquele pretendido na relação jurídica inicial, e muitas vezes, sem o próprio consentimento de seu titular.

Nesse cenário de exposição, o próprio direito constitucional à privacidade se apresenta cada vez mais difuso, levando em consideração que a ideia deste bem jurídico e da vida privada em si, se alargam frente as novas interações vividas na rede. Com base em informações privilegiadas captadas online, diferentes setores da economia se beneficiam para, em poucos segundos, traçar um perfil detalhado de seus clientes e potenciais consumidores, tais como bancos, planos de saúde, comércio varejista, marketing digital, redes sociais, dentre outros exemplos. Através desse perfil, as empresas podem estabelecer seu público-alvo para oferecer individualmente produtos e serviços a um número irrestrito de indivíduos.

Essa capacidade de obter e armazenar dados acerca de milhões de pessoas ocorre graças chamados ‘bancos de dados’. Cujo conceito pode ser definido como uma coleção de dados inter-relacionados, representando informações sobre um domínio específico. Ou seja, sempre que for possível agrupar informações que se relacionam e tratam de um mesmo assunto, pode-se dizer que existe a configuração de um banco de dados.

Atualmente, diante de um mercado completamente globalizado, o material contido em qualquer desses bancos pode se conectar, e complementar com as de outros, numa verdadeira rede de dados sensíveis, num conglomerado de bancos de dados. O que leva ao necessário debate acerca da segurança, responsabilização e diretrizes as quais as empresas que captam e armazenam dados privados devem se submeter.

A valorização desse bem jurídico (dados pessoais) o coloca numa posição de privilégio, na medida em que diversos serviços online sequer são pagos em dinheiro, mas com o fornecimento de destes. Vide como exemplo as próprias redes sociais, tais como Facebook, Instagram, YouTube, companhias que movimentam bilhões de dólares anuais[1] graças ao alcance que possuem através de seus usuários, cujos dados servem como uma verdadeira de moeda de troca.

Nesse sentido, a tutela da identidade e privacidade revela-se essencial na busca da efetivação desses direitos fundamentais. Diante do contexto tecnológico atual, a primeira tarefa do ordenamento é a de encaixar esses institutos passíveis de proteção, dentro do atual ramo jurídico ‘Direito Digital’, que nasce como consequência dos avanços técnicos e científicos, e cuida de alinhar esse fenômeno ao avanço do próprio direito.

Dito isso, o direito digital, pode ser compreendido, no entendimento de Marcelo Camilo de Tavares Alves, como aquele que:

[1] A Alphabet, dona do Google, registrou lucro líquido de US$ 41,22 bilhões em 2020, um crescimento de 20,43% sobre o ano anterior.
https://g1.globo.com/economia/tecnologia/noticia/2021/02/03/lucro-da-dona-do-google-cresce-20percent-em-2020.ghtml

> (...) possui um objeto delimitado, qual seja a própria tecnologia, dividido em duas partes, sendo a primeira o objeto mediato, ou seja, a informação, e o segundo o objeto imediato, ou a tecnologia; a existência de uma metodologia própria, a qual visa possibilitar uma melhor compreensão dos problemas derivados da constante utilização das novas tecnologias da informação (informática) e da comunicação (telemática); tal tarefa se realiza mediante o uso de um conjunto de conceitos e normas que possibilitam a resolução dos problemas emanados da aplicação das novas tecnologias às atividades humanas; a existência de fontes próprias, ou seja, fontes legislativas, jurisprudenciais e doutrinárias; não havendo como negar a existência dessas fontes no âmbito do Direito Digital; foi justamente a existência de ditas fontes que possibilitaram, em um grande número de 8 países, principalmente os mais desenvolvidos, a criação da disciplina do Direito Digital nos meios acadêmicos[2]

Esta ramificação do direito cuida, portanto, da apropriação dos avanços digitais e suas ferramentas, em sentido amplo, na aplicação teórica e prática do direito. Além de almejar a regulação da mencionada expansão das tecnologias da informação aos princípios, regras e normas constitucionais.

Logo, o debate acerca da responsabilização de empresas e instituições que atuam no tratamento dos dados de pessoas naturais em larga escala vem ganhando força e visibilidade na última década, ao passo que garantir a proteção contra eventual uso indevido é uma tarefa de extrema relevância, na qual foi assumida, no Brasil, pela Lei 13.709 de 2018, a Lei Geral de Proteção de Dados (LGPD).

Com a edição da presente lei, procurou-se oferecer uma resposta à lacuna existente no tocante a fiscalização, e responsabilização, no tratamento de dados pessoais, assim como a observância de protocolos específicos para sua coleta e utilização em si. Após sua promulgação, o Brasil se juntou a outras dezenas de países que já detém legislação sobre o tema, e cuja finalidade é zelar pela segurança das informações privadas de pessoas

[2] ALVES, Marcelo de Camilo Tavares. Direito Digital. Goiânia, 2009. p, 9-10. Disponível em http://aldeia3.computacao.net/greenstone/collect/trabalho/import/Direito%20Digital.pdf Acesso em 10.06.2022.

naturais, através da atribuição de diversas regras, direitos e deveres específicos a serem seguidos por qualquer empresa, pessoa ou órgão que atue com o tratamento destes.

O maior exemplo legal desta matéria no cenário internacional é a GDPR (General Data Protection Regulation), que trata da regulação e proteção de dados em vigor na União Europeia, cujo trâmite no parlamento europeu começou em 2012, e passou a produzir efeitos em 2018. Essa lei foi uma forte influência na formulação LGPD, e é perceptível os pontos de congruência entre ambas, como por exemplo a valoração do consentimento como elemento subjetivo essencial para a captação dos dados do titular, assim como a indicação e responsabilidade dos agentes encarregados pela operacionalidade dos dados, cuja positivação culminou numa nova espécie de responsabilidade civil no direito brasileiro.

Ao avaliar as inovações advindas desta lei, deve-se ressaltar um ponto importante da LGPD (a ser mais bem trabalhado nos capítulos posteriores), que diz respeito à necessidade de adequação, por parte do coletor dos dados, às ‘Bases Legais’ estabelecidas no seu texto. Em suma, o manejo dos dados pessoais, em especial os dados sensíveis, só serão possíveis caso ocorra sob consentimento específico e destacado pelo titular, e na ausência do primeiro, quando encontrar respaldo em uma ou mais bases legais elencadas no artigo 11° da referida norma. A saber, quando for indispensável para: (I) cumprimento de obrigação legal ou regulatória pelo controlador; (II) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; (III) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; (IV) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral. (V) proteção da vida ou da incolumidade física do titular ou de terceiro; (VI) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (VII) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Tendo em vista as referidas bases, qualquer atuação que não esteja respaldada expressamente numa das hipóteses citadas configura-se num tratamento de dados ilegal. Essa é uma ferramenta valiosa na proteção de direitos individuais, ao passo que o manejo de dados sensíveis ilegalmente enseja em diversas sanções de responsabilização face ao controlador de dados, que na LGPD, é classificado como qualquer pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais[3].

Além do direito à indenização, em consonância com o instituto da responsabilidade civil, estão previstas no código diferentes sanções administrativas. Como por exemplo a aplicação de multa por infração, assim como a suspensão parcial do funcionamento do banco de dados pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador.

Esses são apenas exemplos que visam coibir o uso e disseminação de dados pessoais de maneira desenfreada, a fim de assegurar a inviolabilidade da intimidade, da honra e da imagem, o respeito à privacidade, e todas os direitos fundamentais garantidos na constituição. Haja vista a relativização constante de direitos na seara virtual, e a atual necessidade de adequação do ordenamento jurídico na garantia destes.

Nesse sentido, a abordagem quanto a tutela que efetivamente é prestada no âmbito judicial e administrativo é o ponto essencial a ser estudado no presente trabalho. Por conseguinte, foi instituída através da Medida Provisória n° 869/18, a ANPD – Autoridade Nacional de Proteção de Dados, órgão com atribuição de fiscalizar e sancionar as empresas que atuem no tratamento de dados pessoais em caso de transgressão, ou não adequação às regras ementadas. Assim, dada a natureza jurídica e a subordinação do presente órgão, dúvidas surgem quanto à sua capacidade de atuação efetiva, de modo que:

---

3 Artigo 5°, Inciso VI, LGPD - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

> a MP 869/18 fundou a ANPD como órgão da administração pública federal, integrante da presidência da República e com autonomia técnica. Com isso, os especialistas temem que, do modo como foi arquitetada, a ANPD não goze 38 Cf. Art. 52 da Lei n° 13.709/2018 39 de suficiente autonomia para que se tenha um ambiente de efetiva segurança jurídica, com capacidade de fomentar atividades econômicas baseadas em dados ao mesmo tempo em que assegura proteção aos titulares desses dados, especialmente quando se fala em tratamento de dados pessoais pelo Poder Público. (Tupinambá, 2019, p. 38/39).

Nesse diapasão, a tarefa investigativa a que se limita o presente estudo, versa sobre a evolução do microssistema legal brasileiro em relação à proteção de dados pessoais, e quais são os impactos trazidos pela Lei 13.709/2018 nos tribunais brasileiros, um ano após esta produzir eficácia plena.

Apesar do debate levantado pela LGPD, na qual passou a ter **plena** eficácia em setembro de 2020, a discussão que cerceia o tema de proteção de dados e sua inserção no âmbito digital não é recente. Em verdade, tão logo com o próprio surgimento da internet o direito pátrio se ocupou de tentar preencher essa lacuna, tanto no campo teórico, quanto no ponto de vista legal.

Assim, em que pese a Edição da lei 13.709/2018, é necessário resgatar a trajetória legal enfrentada pelo campo da segurança da informação no Brasil, de modo a analisar as diversas fontes do direito nacional e estrangeiro, que exerceram influência na própria criação da LGPD. Portanto, qualquer tentativa de traçar esse roteiro, para os fins deste trabalho, passa pela necessidade de elucidar alguns conceitos fundamentais do Direito digital.

Em pouco mais de vinte anos de uso comercial, a internet foi capaz de modificar inúmeros aspectos da convivência humana. Sendo a ampliação do conhecimento e do acesso à cultura o seu impacto mais relevante. Baseando-se nas décadas anteriores à abertura da internet, as informações difundiam-se pelos livros impressos. As pesquisas acadêmicas eram realizadas em enciclopédias disponíveis, respectivamente, em bibliotecas e bancas de jornais. Com a internet, esses materiais perderam espaço

rapidamente para as *homepages* com seus reduzidíssimos custos de divulgação das informações.

Pela facilidade do acesso em qualquer hora e lugar, a velocidade da transmissão do conhecimento aumentou exponencialmente. De modo que este fenômeno tecnológico e social continua se reinventando em todos os setores tradicionais da economia, além dos novos que foram criados pela própria evolução da internet. Exemplos disso podem ser observados através do avanço do mercado de criptomoedas, a criação dos NFT's (tokens não fungíveis) e o desenvolvimento do 'metaverso', realidade virtual onde é possível ter qualquer tipo de interação social, seja comercial, profissional ou recreativa.

Todas essas atividades e múltiplas interações ocorrem simultaneamente no chamado 'ciberespaço'[4], que na definição de Rabaça e Barbosa[5] é um espaço cibernético, um universo virtual formado pelas informações que circulam e/ou estão armazenadas em todos os computadores ligados em rede, especialmente a Internet; uma dimensão virtual da realidade, onde os indivíduos interagem através de computadores interligados. Ao falarmos em ciberespaço é comum pensar em algo que não é palpável, algo imaterializado, um lugar distante de nossa realidade, onde relações sociais, culturais, econômicas ao se estabelecerem se fazem no imaginário, um ambiente futurístico. Numa concepção um pouco mais ampla, tem-se que o ciberespaço pode ser compreendido como um universo virtual, plástico, fluido. O ciberespaço, enfim, é uma grande máquina abstrata, porque semiótica, mas também social, onde se realizam não somente trocas simbólicas, mas transações econômicas, comerciais, novas práticas comunicacionais, relações sociais, afetivas e, sobretudo, novos agenciamentos cognitivos.

Dessa forma, diante dos infinitos negócios que tomam forma e se desenvolvem dentro do ciberespaço, ficou reservado ao direito a missão de criar uma proteção legal capaz de prover segurança e previsibilidade às partes envolvidas. Assim, as primeiras normas que visam tutelar esse direito de alguma forma, podem ser observadas

[4] SILVA, Taziane Mara; TEIXEIRA, Talita de Oliveira; Ciberespaço: uma nova configuração do ser no mundo. Psicol. rev. (Belo Horizonte) vol.21 no.1 Belo Horizonte jan. 2015. Disponível em http://dx.doi.org/DOI-10.5752/P.1678-9523.2015V21N1P176 Acesso em 03.06.2022.
[5] RABAÇA, Carlos; BARBOSA, Gustavo G. Dicionário de comunicação. 2.ed. rev. e atual. Rio de Janeiro: Campus, 2001, p.123.

genericamente na própria constituição de 1988, e na Lei Nº 9.296, De 24 De Julho De 1996, na qual regulamenta o inciso XII, parte final, do art. 5° da carta magna. Além da constituição federal, existem alguns marcos legais que merecem destaque especial, como o Código de Defesa do Consumidor, a Lei do Cadastro Positivo e principalmente o Marco Civil da Internet, sendo este último a maior referência legislativa nacional na proteção de dados até a edição da Lei 13.709/2018. Por fim, no âmbito internacional a maior fonte de influência para LGPD é a GDPR (General Data Protection Regulation), em vigor na União Europeia.

## 1.2 Proteção de Dados na Constituição Federal de 1988.

Tendo como uma de suas características elementares o fato de ser uma constituição analítica[6], a CF/88 tratou de garantir e estabelecer um extenso rol de direitos e garantidas fundamentais. No art. 5°, o constituinte ampliou de maneira histórica estas garantias ao instituir, por exemplo, a livre manifestação do pensamento[7], liberdade religiosa [8], liberdade de locomoção[9] e liberdade de associação[10]. Prerrogativas inerentes a um estado democrático de direito contemporâneo, principalmente num cenário de pós ditadura[11].

De tal modo, ao inserir o direito à privacidade numa classificação constitucionalista, tem-se a inclusão desta no rol de 'direitos da personalidade'. Nos quais são classificados por Carlos Alberto Bittar [12] como

---

[6] 4 SILVA, José Afonso da. Curso de Direito Constitucional Positivo. 37 ed. São Paulo: Malheiros, 2014, p. 40. Disponível em https://www.migalhas.com.br/coluna/din%C3%A2mica-constitucional/353997/33-anos-da-constituicao-federal-o-carater-analitico-do-texto Acesso em 16.05.2022

[7] Brasil, Constituição Federal de 1988, Art.5°, Inciso IV: *"é livre a manifestação do pensamento, sendo vedado o anonimato";*

[8] Brasil, Constituição Federal de 1988, Art.5°, Inciso VI: *"é inviolável a liberdade de consciência e de crença, sendo assegurado o livre exercício dos cultos religiosos e garantida, na forma da lei, a proteção aos locais de culto e a suas liturgias;"*

[9] Brasil, Constituição Federal de 1988, Art.5°, Inciso XV: é livre a locomoção no território nacional em tempo de paz, podendo qualquer pessoa, nos termos da lei, nele entrar, permanecer ou dele sair com seus bens

[10] Brasil, Constituição Federal de 1988, Art.5°, Inciso XVII: é plena a liberdade de associação para fins lícitos, vedada a de caráter paramilitar

[11] BONAVIDES, Paulo. Curso de Direito Constitucional. 10. ed. São Paulo: Malheiros, 2000. p. 539-540

[12] BITTAR, Carlos Alberto. Os direitos da personalidade. 6. ed. Rio de Janeiro: Forense Universitária, 2003.

> os direitos reconhecidos à pessoa humana tomada em si mesma e em suas projeções na sociedade, previstos no ordenamento jurídico exatamente para a defesa de valores inatos no homem, como a vida, a higidez física, a intimidade, a honra, a intelectualidade e outros tantos.

Assim, o conceito de privacidade enquanto princípio constitucional serviu para nortear as futuras legislações que estariam por vir. Diante disso, através de uma interpretação extensiva, a proteção de dados pessoais foi instituída de maneira genérica, sob o escopo do direito à privacidade e inviolabilidade da vida privada, descrito no inciso X, do referido artigo 5° da CF/88 assim transcrito: “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”. Com base nessa norma, em complemento com a regra do inciso XII[1] e os princípios e garantias fundamentais, tem-se a base legal onde se desenvolverá a proteção legislativa dessa garantia.

Nesse sentido, a Lei Nº 9.296/96, atuando na esfera do direito penal, regulamentou o disposto no inciso XII, ao caracterizar como crime o ato de realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei. Com o avanço tecnológico, e diante de um cenário completamente novo em relação àquele existente na promulgação da constituição, o Senado tratou de solidificar a proteção dos dados pessoais no rol do artigo 5° desses direitos através de uma nova emenda constitucional.

Conforme o exposto, a leitura constitucional aborda o tema de através de normas genéricas, e amparadas em princípios jurídicos de condão universal. De modo que em 2019, o Plenário do Senado Federal aprovou a Proposta de Emenda à Constituição (PEC) 17/2019, que acrescentou o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão, e fixar a competência privativa da União para legislar sobre a matéria. Por acordo entre as lideranças, foram votados os dois turnos na mesma sessão. Aprovada de forma unânime, a PEC recebeu 64 votos no primeiro turno e 76 no segundo, superando o mínimo de 49. Fato que indica a crescente preocupação geral em regular o

tratamento dessa espécie de dados, como corrobora o parecer (SF) nº 45, de 2019, elaborado pela Comissão de Constituição, Justiça e Cidadania, de relatoria da Senadora Simone Tebet, no qual afirma que:

> (...) é importante ressaltar que a proteção de dados pessoais se tornou um grande desafio aos legisladores de todo o mundo, em especial nesses tempos de mudanças das relações sociais e de avanços tecnológicos, cuja velocidade seria inimaginável em outros tempos. Daí ser natural que a legislação tenha de se adequar a essa realidade em constante mutação, sob pena de atingir direitos da população, pelo fato de que determinadas informações são, na sua essência, pessoais. A partir dessa nova realidade, para muitos especialistas no assunto, a resistência do Direito não pode permanecer constante e inerte a esse novo paradigma.

Assim, a atuação do poder constituinte derivado foi exercida para adequar a tutela dos direitos individuais à atual realidade digital, que se encontra em constante mutação. Apesar de sua regulação ocorrer em lei específica, a inclusão do inciso XII-A é uma medida jurídica essencial para garantir que a segurança de dados privados, sobretudo no ciberespaço, capaz de incluir o Brasil no rol de Países com regulamentação avançada sobre o tema, conferindo, portanto, mais credibilidade no cenário internacional.

### 1.3 Proteção de Dados no Código de Defesa do Consumidor

O Código de Defesa do consumidor possui uma relação estreita com a tutela e proteção de dados pessoais. Haja vista que as relações de consumo, tais quais se observam hoje, evoluíram para uma lógica de mercado onde o ‘dado’ por si só é o bem mais valioso na relação entre indivíduo e corporações, no meio digital. Através de informações sensíveis dos usuários, as empresas varejistas, bancos e prestadores de serviço são capazes de moldar o perfil socioeconômico de cada cliente e/ou potencial consumidor.

Dito isso, a monetarização dos dados pessoais apresenta-se como uma tendência amplamente antecipada, por conta inclusive, da atual pandemia de coronavírus, na qual forçou o isolamento social para contenção do contágio em massa, e consequentemente impulsionou o comércio e os negócios online. Assim, esse fenômeno que hoje é vital para

uma parcela bastante representativa de novos serviços e produtos foi bem exemplificado por uma declaração que se tornou bastante popular da Comissária europeia do consumo, Meglena Kuneva. Em sua fala afirmou que "os dados pessoais são o novo óleo da Internet e a nova moeda do mundo digital[13]", tornando evidente o advento de um novo terreno adentrado pelas relações de consumo, onde o consumidor passa a ser, em si, a fonte de um ativo que são as suas informações pessoais, suscitando a necessidade de adequação das normas que regulam o consumo para que levem em conta esta nova situação.

Nesse sentido, destaca-se o artigo 43 do CDC, no qual além de instituir os bancos de dados e cadastros de consumidores, também determina que seja garantido amplo acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre cada indivíduo, bem como sobre as suas respectivas fontes. A norma assegura que o consumidor tenha autonomia para controlar quais informações pessoais o fornecedor possui em seu banco de dados, além de lhe ser facultada a possibilidade de exclusão dos respectivos arquivos.

Vale ressaltar que historicamente o principal ponto de debate entre 'Relações de Consumo x Dados pessoais' se estabeleceu no entorno das Informações Creditícias. Num cenário onde as informações pessoais eram capazes de determinar, e muitas vezes restringir, o acesso a crédito junto a diferentes instituições financeiras. No entanto, o legislador procurou ir além na redação do aludido art. 43, conforme ensina Bruno Bioni[14]:

> Note-se a amplitude do dispositivo em questão, que alcança todo e qualquer dado pessoal do consumidor, indo muito além, portanto, dos bancos de dados de informações negativas para fins de concessão de crédito. A racional do legislador foi alcançar todo e qualquer banco de dados que atinja o livre desenvolvimento da personalidade do consumidor.
>
> A começar pela exigência de que o consumidor deve ser notificado da abertura de um banco de dados pessoais por ele não solicitado (art. 43, § 2º, do CDC). Esse dever de comunicação prévia permite que o consumidor acompanhe o fluxo de seus dados pessoais, já que tal atividade deve ser a ele comunicada e,

[13] Disponível em https://www.legiscompliance.com.br/artigos-e-noticias/3111-a-lgpd-e-o-consumidor-4-0 Acesso em 03.06.2022.
[14] BIONI, Bruno Ricardo. *Proteção de dados pessoais:* a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 282.

> em última análise, ser transparente. Por meio de uma interpretação extensiva de tal dispositivo, como propõe Antônio Herman Benjamin, o termo abertura cingir-se-ia a toda e qualquer movimentação dos dados pessoais, possibilitando ao consumidor acompanhar de forma dinâmica a circulação de suas informações pessoais.

A fim de complementar o CDC, foi publicado o Decreto Federal nº 7.962/2013 (Lei do E-commerce), que regulamenta o Código de Defesa do Consumidor em relação ao comércio eletrônico. Isso significa que, além do CDC, a Lei do E-commerce regulamentará de forma específica as transações realizadas entre loja virtual e cliente. Note-se que mesmo antes da LGPD entrar em debate no congresso, a proteção de dados na internet sempre foi um tema em debate no Legislativo brasileiro, ganhando especial atenção diante do fenômeno da monetização dos dados pessoais, e do constante avanço dos negócios e transações realizadas online.

Contudo, apesar de sua importância normativa aplicada à um setor com histórico de baixa regulamentação, o referido decreto trata de ratificar, em síntese, alguns princípios, garantias e dispositivos já estabelecidos pelo CDC. Como por exemplo o 'direito de arrependimento', a exposição ampla, detalhada e acessível acerca das informações do produto, assim como o atendimento facilitado ao consumidor[15].

Vale destacar, no entanto, a determinação do artigo 4° inciso VI, que diz:

> Art. 4º Para garantir o atendimento facilitado ao consumidor no comércio eletrônico, o fornecedor deverá:
>
> VII - utilizar mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor.

[15] BRASIL. Decreto n° 7.962/2013: Art. 1º Este Decreto regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico, abrangendo os seguintes aspectos: I - informações claras a respeito do produto, serviço e do fornecedor; II - atendimento facilitado ao consumidor; e III - respeito ao direito de arrependimento.

A relevância deste artigo consiste na criação de uma obrigação legal para o fornecedor, no tocante ao tratamento seguro dos dados pessoais do consumidor. Assim como a necessidade de se criar um espaço digital protegido para a realização de pagamentos e armazenamento de informações sensíveis do comprador. Tais determinações futuramente seriam mais bem delineadas e amplamente regularizadas pela Lei n°12.965, de 23 de Abril De 2014 (Marco Civil da Internet), e especialmente pela Lei 13.709/2018 a LGPD.

### 1.4 Lei do Cadastro Positivo

A Lei nº 12.414/2011, conhecida como lei do cadastro positivo, disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Com isso, a situação econômica do postulante ao crédito não é mais analisada a partir de dados relativos a dívidas não pagas, apenas. Mas também passa pelo crivo de outras informações que possam exprimir dados positivos sobre a sua capacidade financeira e o seu histórico de adimplemento. Daí por que tal legislação ficou conhecida como Lei do "Cadastro Positivo", haja vista que a avaliação do crédito passa a ter uma amplitude maior do que apenas o exame de informações a respeito de dívidas não pagas, cuja conotação seria negativa.

Dessa forma, temos como cadastro negativo o conglomerado de informações que contém dados de inadimplência, ou seja, compromissos financeiros que não foram pagos no tempo e modo acordados. O Cadastro Positivo, por sua vez, apresenta o histórico de pagamentos, operações de crédito que você já pagou ou ainda está pagando. Nesse sentido, vale ressaltar que o cadastro positivo não é controlado/ regulado pelo governo federal, mas pelas empresas responsáveis pela gestão da base de dados. Nas quais são empresas privadas, homologadas pelo Banco Central do Brasil e autorizadas por ele a operar o banco de dados do Cadastro Positivo. Essas empresas são também conhecidas como Gestores de Banco de Dados ou GBDs, como o SPC Brasil.

Assim, é possível afirmar que esta lei permitiu fluxos de informações em conformidade com a proteção de dados, de uma forma que sustente a evolução do conceito de autodeterminação da informação em nosso ordenamento jurídico. Portanto, a LCP, assim como o CDC, fixou-se sobre a autodeterminação informacional, conforme complementa o ensinamento de Bioni[16]:

> Essa nova peça legislativa setorial acabou por trazer, de uma forma original e mais sistematizada, a orientação de que o titular dos dados pessoais deve ter o direito de gerenciá-los. Nesse sentido, requer-se mais do que a simples comunicação da abertura do banco de dados, tal como fez a legislação consumerista. Exige-se o consentimento do titular dos dados pessoais que deve ser, por seu turno, informado e externado por meio de assinatura em um instrumento específico ou em cláusula apartada. Essa esfera de controle deve se prolongar, inclusive, para os casos de compartilhamento da base de dados com terceiros, hipótese na qual deverá haver um consentimento específico para tanto

Tal como ocorre no MCI, e no CDC, a Lei do Cadastro Positivo se baseia no referencial principiológico da autodeterminação informacional, onde o indivíduo detém a prerrogativa de controlar e gerir os próprios dados. Dessa forma, a fim de garantir que o postulante ao crédito possa gerir as próprias informações, a norma estabelece, por exemplo, que o gestor dos bancos de dados deverá encerrar ou reabrir o cadastro do solicitante[17], assim como deve proceder automaticamente ao cancelamento de pessoa natural ou jurídica que tenha manifestado previamente, por meio telefônico, físico ou eletrônico, a vontade de não ter aberto seu cadastro.[18]

## 1.5 Marco Civil da Internet

O Marco Civil da Internet (MCI), incorporado pela Lei n° 12 965/2014, ocupou pioneiramente o papel de regular o uso da Internet no Brasil. Por meio da previsão de princípios, garantias, direitos e deveres para quem usa a rede, bem como da determinação de diretrizes para a atuação do Estado, num cenário anterior a edição da LGPD.

---

[16] BIONI, Bruno Ricardo. Proteção de Dados Pessoais - A Função e os Limites do Consentimento. 1. ed. Rio de Janeiro: Editora Forense Ltda., 2018. p. 182.
[17] BRASIL. Lei Nº 12.414, de 9 De junho De 2011 - Art. 5°, Parágrafo 6°.
[18] BRASIL. Lei Nº 12.414, de 9 De junho De 2011 - Art. 5°, Parágrafo 7°

Dentre os direitos previstos, encontra-se a proteção da privacidade[19]e dos dados pessoais. Tidos como um dos pilares do MCI, ao lado da neutralidade de rede e da liberdade de expressão, a sua proeminência consolidou-se com o episódio do escândalo de espionagem revelado pelo ex-analista Edward Snowden, da Agência Nacional de Segurança dos Estados Unidos[20]. Tais revelações repercutiram no MCI, que adotou mudanças substanciais em seu texto a fim de "endurecer" a proteção ao direito à privacidade e aos dados pessoais, bem como na própria aceleração de seu trâmite legislativo que, com a adoção do regimento de urgência, culminou em sua aprovação no Congresso brasileiro em 2014.

As referidas alterações puderam ser observadas, por exemplo, através da inclusão dos incisos VI, VII, VIII e IX ao artigo 7°, todos destinados especificamente a proteção de dados pessoais, leia-se:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> VI - Informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
>
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
>
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
>
> a) justifiquem sua coleta;
>
> b) não sejam vedadas pela legislação; e
>
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

[19] BRASIL. Lei n° 12.965/2014: Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei.
[20] Disponível em https://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html

> IX - Consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

Através deste artigo o MCI estabeleceu garantias e princípios importantes, no tocante ao controle dos usuários sobre seus dados pessoais. Isso porque uso, armazenamento e tratamento, seria condicionado a finalidade que justifique sua coleta, que não for vedada pela legislação, ou estejam especificadas nos contratos de prestação de serviços. Além disso, buscou qualificar o consentimento como devendo ser livre, expresso e informado.

Nesse sentido, o MCI dedicou mais quatro dispositivos pelos quais se procurou estabelecer uma orientação do que venha a ser um consentimento expresso e informado. Aquele que exerce tal atividade de tratamento de dados pessoais deve prestar informações claras e completas, utilizando-se de cláusulas contratuais destacadas e dando publicidade às suas políticas de uso para o preenchimento dos adjetivos em questão.

Em complemento ao MCI, foi publicado o Decreto n° 8.771, que ocupa a missão de regulamentar a citada lei, de maneira que indica procedimentos para a guarda e proteção de dados de usuários por provedores de conexão e aplicação, além de apontar medidas de transparência na requisição de dados cadastrais pela administração pública. O Decreto trata ainda do papel do Comitê Gestor da Internet, que estabelecerá diretrizes para preservação da neutralidade.

## 1.6 Proteção De Dados Na União Europeia - GDPR

Conforme o exposto, o controle, fiscalização e diretrizes acerca da proteção de dados no Brasil sempre foi feito através de leis isoladas nas quais, atuando dentro de seu nicho, complementavam-se dentro de um microssistema legal de proteção de dados pessoais. No entanto, a ausência de um referencial legal forte e completo sobre o tema

deixou o país fora de um grupo de dezenas de nações que já contam com um escopo de proteção legal específico.

Essa deficiência normativa impacta negativamente diferentes setores da economia, haja vista o momento tecnológico e os modelos econômicos que foram formados em escala global. A ausência de segurança jurídica no tratamento de dados implica necessariamente em desconfiança de investidores que atuam nesse setor e consequentemente na escolha, por parte destes, em migrar para regiões com um debate e regulação avançada. De modo que a edição da Lei n° Lei nº 13.709, de 2018 surge num momento de necessidade, conforme pode-se extrair do parecer elaborado pela Comissão de Assuntos Econômicos do Senado, de relatoria do Senador Ricardo Ferraço[21]:

> "No mérito, já pudemos discorrer acerca da oportunidade e da urgência de aprovação do presente marco legal de proteção de dados. Não se trata de uma opção legislativa, mas uma necessidade inafastável. Reconhecemos, pois, a importância ímpar da proposição.
>
> A despeito do contexto de crise econômica, **é seguro afirmar que o País tem perdido oportunidades valiosas de investimento financeiro internacional em razão do isolamento jurídico em que se encontra por não dispor de uma lei geral e nacional de proteção de dados pessoais (LGPD)."** (*grifos aditados*).

Diante desse contexto de necessidade, e sentimento de urgência em aprovar um projeto de Lei nacional de proteção de dados pessoais, a LGPD nasceu com grande inspiração da regulação europeia, por reconhecimento expressivo de sua relevância para o mundo. Essa relevância pode ser observada, principalmente, pela sua abrangência. Tendo em vista que a GDPR está em vigor em toda a UE, atingindo diretamente mais de 20 países de maneira harmônica e eficiente, e indiretamente todas as empresas situadas fora do bloco econômico, mas que de alguma forma atuam dentro deste.

[21] Disponível em Senado Federal https://legis.senado.leg.br/sdleg-getter/documento?dm=7751566&ts=1571776637073&disposition=inline#:~:text=No%20m%C3%A9rito%2C%20j%C3%A1%20pudemos%20discorrer,a%20import%C3%A2ncia%20%C3%ADmpar%20da%20proposi%C3%A7%C3%A3o.

### 1.6.1 Princípios Norteadores da GDPR adotados pela LGPD

Assim, deve-se destacar num primeiro momento, os princípios norteadores da GDPR, nos quais foram replicados quase em unanimidade pela Lei brasileira. A saber: i) licitude, ii) lealdade, iii) transparência, iv) limitação de finalidade, v) minimização dos dados, vi) limitação de armazenamento, vii) exatidão, viii) integridade e ix) confidencialidade.

A reprodução destes princípios, e o seu respectivo significado, podem ser observados da seguinte forma:

**Ilicitude:** Preceitua que os dados pessoais somente podem ser tratados se houver permissão ou fundamentação legal para tal finalidade, devendo seguir os parâmetros descritos no artigo 6º, item 1, letras 'a' a 'f', 23 do GDPR.24.

**Lealdade:** Este princípio pode ser traduzido no direito brasileiro como uma espécie da 'Boa- Fé', de modo que tal instituto deve ser observado pelo responsável pelo tratamento dos dados. Nesse sentido, o princípio da Lealdade significa dizer que o manuseio dos dados pessoais pelo 'controlador' deve ocorrer de maneira a não desrespeitar a expectativa razoável de seu titular. Tampouco que os dados sejam utilizados de modo a criar efeitos adversos e injustificados sobre o indivíduo[22].

**Transparência:** O princípio da transparência impõe concisão, facilidade de acesso e compreensão das informações atinentes ao tratamento de dados pessoais, além de exigir uma linguagem clara e simples com a devida identificação do responsável pelo tratamento e a finalidade a que o tratamento se destina. Além disso, esse princípio determina que o controlador de dados deverá atuar de forma clara, aberta e honesta, impondo que este publicize a maneira forma e os motivos pelos quais estes serão coletados e utilizados.

Nesse sentido, vale ressaltar que os princípios norteadores da GDPR (e como veremos a frente também da LGPD), se complementam numa verdadeira cadeia principiológica. De

[22] EU General Data Protection Regulation (GDPR) An Implementation and Compliance Guide. 3. ed. Cambridgeshire: It Governance Privacy Team, 2018. P.19: *"In general, fairness means that you should only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them. You need to stop and think not just about how you can use personal data, but also about whether you should".*

modo que o conceito de transparência está necessariamente relacionado com a própria ideia de 'lealdade'[23].

**Limitação da Finalidade:** Este princípio, conforme sugere a sua nomenclatura, preleciona que a coleta e respectivo tratamento dos dados deverá ocorrer de forma a delimitar, objetiva e limitada ao fim a que se propõe. Isto é, a atividade será realizada apenas se estiver alicerçada nas bases jurídicas, que impõem os requisitos necessários para a legalidade da atividade fim[24].

**Minimização dos Dados:** Este princípio surge como um derivado da "Limitação da Finalidade", e afirma que os dados devem ser adequados, pertinentes e limitados ao que é necessário para atingir às finalidades para as quais são tratados. Este entendimento é endossado pela obra "EU General Data Protection Regulation (GDPR)", ao afirmar que: '*This means that you should hold no more data beyond what is strictly required'*[25].

**Limitação do Armazenamento/ Exatidão:** O primeiro estatui que a guarda das informações pessoais deve ser exercida de modo que, a identificação de seus titulares seja possível apenas durante o período necessário para o seu tratamento. Enquanto o segundo busca garantir aos titulares dos dados a exatidão, a clareza, a relevância e a atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento[26]

**Integridade e Confidencialidade:** Por fim, sob o risco de soar repetitivo, deve-se destacar mais esse princípio elencado na GDPR. A integralidade, complementada pela confidencialidade, podem ser entendidos como a necessidade de que os dados pessoais

---

[23] EU General Data Protection Regulation (GDPR) An Implementation and Compliance Guide. 3. ed. Cambridgeshire: It Governance Privacy Team, 2018. P.20: "*Transparency is fundamentally linked to fairness. Transparent processing is about being clear, open and honest with people from the start about who you are, and how and why you use their personal data. Transparency is always important, but especially in situations where individuals have a choice about w hether they wish to enter into a relationship with you. If individuals know at the outset what you will use their information for, they will be able to make an informed decision about whether to enter into a relationship, or perhaps to try to renegotiate the terms of that relationship".*

[24] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. Comentários ao GDPR. 2. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 52-53.

[25] EU General Data Protection Regulation (GDPR) An Implementation and Compliance Guide. 3. ed. Cambridgeshire: It Governance Privacy Team, 2019 - tradução livre: Isso significa que não se deve armazenar mais dados além do que é estritamente necessário.

[26] https://www.trf3.jus.br/lei-geral-de-protecao-de-dados-pessoais-lgpd/principios#:~:text=Este%20princ%C3%ADpio%20busca%20garantir%20aos,da%20finalidade%20de%20seu%20tratamento.

sejam tratados de forma a garantir sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental[27].

Tendo em vista a base principiológica da GDPR, vale destacar que suas raízes advém de um debate maduro e contínuo acerca da proteção de dados pessoais. Conforme pode-se observar, por exemplo, da Diretiva 95/46/CE do Parlamento Europeu (norma revogada pela GDPR), que já visava harmonizar a defesa dos direitos e das liberdades fundamentais das pessoas singulares, em relação às atividades de tratamento de dados e assegurar a livre circulação de dados pessoais entre os Estados-Membros[28][29]. Assim como o Regulamento (CE) n.o 45/2001 do Parlamento Europeu e do Conselho, que foi aplicado ao tratamento de dados pessoais pelas instituições, órgãos, organismos ou agências da União. O Regulamento (CE) n° 45/2001, bem como outros atos jurídicos da União aplicáveis ao tratamento de dados pessoais, que foram adaptados aos princípios e regras estabelecidos pela GDPR.

Nesse mesmo sentido, vale dizer que a regulação jurídica desses direitos, naquele continente, ocorre desde a década de 70, através das resoluções n°22 e 29 publicadas pelo Conselho da Europa. De modo que a maturidade e densidade do arcabouço jurídico sobre a proteção de dados pessoais na UE, foi um fator de influencia inevitável para o Congresso Nacional, conforme indicado pelo citado parecer da Comissão de Assuntos Econômicos do Senado, de relatoria do Senador Ricardo Ferraço de 2018:

> “ Tais normas, além de limitadas ao seu respectivo escopo de aplicabilidade, não regem a questão sob a ótica dos mais modernos regimes internacionais de proteção de dados. A título de ilustração, o Conselho da Europa já disciplina juridicamente o tratamento de dados pessoais desde 1973, através da Resolução nº 22 e, no ano seguinte, da Resolução nº 29, ambas versando sobre princípios para proteção de informações pessoais em bancos de dados automatizados, tanto no setor público, como privado.

[27] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. Comentários ao GDPR. 2. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 63

[28] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO L 281 de 23.11.1995, p. 31).

[29] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO L 281 de 23.11.1995, p. 31).

> Essas Resoluções deram margem à consolidação da Convenção para a Proteção de Indivíduos com Relação ao Processamento Automático de Dados Pessoais – Convenção nº 108, do Conselho da Europa, de 1981 – considerado o primeiro instrumento internacional disciplinando especificamente o assunto com força legal, aberta inclusive a países não membros da Comunidade Europeia. Alguns anos mais tarde, em 1995, foi editada a Diretiva nº 46, recentemente sucedida pelo Regulamento Geral de Proteção de Dados (RGDP), que entrou em vigor no último dia 25 de maio".

Tal entendimento é reforçado pela nota técnica SCI/PGR 06/2016, de autoria do Ministério Público Federal, no tocante à importância da Legislação européia no papel de nortear a redação da Lei 13.709/2018.

> (...) não se deve menoscabar que para um país em desenvolvimento adotar nas suas linhas gerais um modelo bem sucedido de uma nação desenvolvida significa buscar replicar uma experiência institucional que é desejada para a sua sociedade. Além do menor custo de não criar uma nova estrutura a partir do nada, se espelhar em profícuas legislações alheias permite acreditar no que se implementou independentemente de eventuais desconfortos iniciais, e garante interlocutores externos que possam dialogar sobre possíveis ajustes necessários a cada realidade[30].

Como se observa, são inegáveis os avanços implementados indiretamente pela GDPR, na semântica de proteção de dados pessoais no Brasil. Além do alicerce principiológico *per si*, a construção de conceitos fundamentais no tratamento de dados como um todo é outro ponto que merece atenção nesta lei, com ênfase para o instituto do consentimento[31].

### 1.6.2 Absorção do Instituto do Consentimento Europeu pela LGPD

A ideia de consentimento aqui pode se definir como a obrigatoriedade do controlador em oferecer aos indivíduos escolha e controle reais sobre a gestão de seus dados. De modo que o consentimento genuíno deve colocar os indivíduos no controle, a fim de que se construa uma relação de confiança e engajamento mútuo.

---

[30] Nota Técnica SCI/PGR 06/2016 do Ministério Público Federal – Disponível em https://static.poder360.com.br/2018/05/relatorio-ricardoferraco-usodedados.pdf

[31] L.119/1 (GDPR), Jornal da União Europeia, Publicado em 04.05.2016: «Consentimento» do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento;

Assim, o consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrônico, ou uma declaração oral. Percebe-se, portanto, que a gestão do consentimento passa pela autodeterminação do indivíduo em autorizar expressamente a coleta e tratamento destes, num cenário onde a obrigação maior é do responsável pelo tratamento[32].

Tendo em vista que este último necessariamente precisa disponibilizar essa opção para o usuário, de maneira que seja possível viabilizar o consentimento expresso, objetivo, e em respeito aos princípios e bases legais que justifiquem a sua coleta para uma finalidade específica.

Nesse sentido, reafirma Bruno Bioni [33]

> (...) a diretiva europeia irá adjetivar o consentimento na tentativa de operacionalizá-lo. A sua qualificação como devendo ser livre, informado, inequívoco, explícito e/ou específico é uma das características marcantes do progresso geracional das leis de proteção de dados pessoais, na medida em que procura resolver a problemática em torno de um controle ilusório ou pouco efetivo das informações pessoais por parte do seu titular (vide subcapítulo 3.2 supra). Nesse sentido, aliás, a diretiva irá impor não só o direito de o titular dos dados pessoais controlá-los, mas, simetricamente, deveres aos data controllers – quem processa os dados pessoais – para aperfeiçoar tal estratégia regulatória.
>
> Trata-se, enfim, de uma abordagem regulatória que se centra nesses dois atores – o titular das informações pessoais e quem as processa – para, por meio de direitos e obrigações simétricas, ser garantido o prometido controle dos dados pessoais.
>
> Acumulam-se, ainda, proposições bem específicas, indicando-se os meios pelos quais seria operacionalizado tal controle. Propõe-se a utilização de "caixas de diálogo", a serem exibidas pelo website, para que o usuário as assinale como uma forma de externar o seu consentimento; ou outros métodos capazes de informar o usuário para que ele exerça, de forma "amistosa", o controle sobre seus dados pessoais ; e, ainda, listando, de forma não exaustiva, quais seriam as ferramentas de coleta de dados pessoais, como cookies, web bugs e spywares.

---

[32] Regulamento (Ue) 2016/679 Do Parlamento Europeu e do Conselho, 27.04.2016: «Responsável pelo tratamento», a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro

[33] Proteção de dados pessoais: a função e os limites do consentimento / Bruno Ricardo Bioni. – Rio de Janeiro: Forense, 2019, p.182

Diante do exposto, ficam estabelecidos os principais pontos tanto no campo principiológico quanto conceitual, através da ideia do consentimento, que formaram a base de influência exercida pela GDPR. De modo que torna necessário proceder com a análise das inovações da Lei Geral de Proteção de Dados propriamente dita, a fim de elucidar o seu impacto na tutela de direitos individuais no Brasil.

# 2 RESPONSABILIDADE CIVIL NA LGPD

## 2.1 Responsabilidade *Lato Sensu*

O instituto da responsabilidade civil é, possivelmente, um dos conceitos que mais evoluiu e se desenvolveu no direito privado brasileiro. Genericamente, o artigo 927 do Código Civil, estabelece: *"aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo".* Dispondo, portanto, da máxima onde aquele que causa danos ilicitamente a terceiro tem o dever de reparar.

A remissão feita pelo próprio código aos artigos 186 e 187 vai indicar 'quem' age ilicitamente sendo o agente que por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral[34]. Abarca-se também 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[35].

No entanto, em que pese a vinculação do dano ao ato ilícito propriamente dito, temos que na evolução do referido instituto a responsabilidade civil, este se subdivide em duas espécies gerais, a objetiva e subjetiva. Como não é o objeto deste trabalho dissertar acerca dos seus aspectos e variantes encontradas no direito, podemos classificar, de acordo com Maria Helena Diniz [36], que responsabilidade civil, de maneira geral:

> é a aplicação de medidas que obriguem alguém a reparar dano moral ou patrimonial causado a terceiros em razão de ato do próprio imputado, de pessoa por quem ele responde, ou de fato de coisa ou animal sob sua guarda (responsabilidade subjetiva), ou, ainda, de simples imposição legal (responsabilidade objetiva).

Assim, em tese será subjetiva aquela vinculada necessariamente à conduta do agente, partindo da análise do dolo ou culpa. Ao passo que será objetiva, aquela decorrente de lei, e quando basta, para fins de reparação, seja constatado nexo causal e

---

[34] Artigo 186 do Código Civil.

[35] Artigo 187 do Código Civil

[36] DINIZ, Maria Helena. Curso de direito civil brasileiro: responsabilidade civil. Vol. 7. 27ªed. São Paulo: Saraiva, 2013.p.84

respectivo dano. Como ocorre nas relações de consumo, por exemplo, no tocante ao fornecedor[37].

Ante o exposto, é fundamental ao abordar a responsabilidade civil, seja observado o instituto do dano. Tendo em vista que a responsabilização pressupõe, necessariamente a ocorrência deste, seja moral ou patrimonial. Conforme preleciona Carlos Alberto Gonçalves[38], ao dispor que

> Sem a prova do dano, ninguém pode ser responsabilizado civilmente. O dano pode ser material ou simplesmente moral, ou seja, sem repercussão na órbita financeira do ofendido. O Código Civil consigna um capítulo sobre a liquidação do dano, ou seja, sobre o modo de se apurarem os prejuízos e a indenização cabível. A inexistência de dano é óbice à pretensão de uma reparação, aliás, sem objeto.

Levando em consideração a existência do dano como pressuposto fático da responsabilidade, deve-se resgatar o entendimento da professora Maria Helena Diniz[39], ao elencar os requisitos para a aplicação do instituo no caso concreto:

> (...) (a) existência de uma ação (comissiva ou omissiva), qualificada juridicamente, isto é, que se apresenta como um ato ilícito ou lícito, pois ao lado da culpa, temos o risco; (b) ocorrência de um dano moral e/ou patrimonial causando à vítima por ato comissivo ou omissivo do agente ou de terceiro por quem o imputado responde, ou por um fato de animal ou coisa a ele vinculado. Não pode haver responsabilidade civil sem o dano que deve ser certo, a um bem ou interesse jurídico, sendo necessária a prova real e concreta dessa lesão. E, além disso, o dano moral é cumulável com o patrimonial (STJ, Súmula n. 37); (c) nexo de causalidade entre dano e ação (fato gerador da responsabilidade) pois a responsabilidade civil não poderá existir sem o vínculo entre a ação e o dano.

Por esse ângulo, serão abordados os fundamentos gerais inerentes ao instituto da responsabilidade civil, aplicados ao caso da Lei 13.709/2018. Tendo em vista que a Lei Geral de Proteção de Dados foi responsável por inaugurar uma nova espécie legal sobre

---

[37] Artigos 12 e 13 do Código de Defesa do Consumidor

[38] Gonçalves, Carlos Roberto Direito civil esquematizado® v. 3 / Carlos Roberto Gonçalves; coordenador Pedro Lenza. – São Paulo: Saraiva, 2014. p72

[39] DINIZ, Maria Helena. Proteção jurídica da existencialidade. São Paulo, Revista Eletrônica Direito e Sociedade, Canoas, v. 8, n. 2, p. 181-191, ago. 2020.

o tema, de modo que a análise de sua parte teórica será realizada de acordo com as normas específicas.

Assim, uma vez realizada essa análise da teórica, o objetivo será observar o comportamento dos tribunais na aplicação prática desses conceitos. Especialmente no que tange ao manejo e aplicação das normas dispostas na lei específica.

## 2.2 Responsabilidade Civil aplicada a Lei Geral de Proteção de Dados.

Na LGPD, além dos princípios de direito dispostos no subcapítulo acima, destaca-se o da responsabilização e prestação de contas, descrito no artigo 6°, inciso X. Através deste, determina-se que as atividades de tratamento de dados pessoais e os respectivos agentes deverão demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Nesse sentido, a responsabilidade civil no âmbito da Lei 13.709/18 decorre do descumprimento das normas estabelecidas no código, e variam de acordo com a natureza, extensão e condições em que ocorreu o evento danoso. O artigo indica que 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.

A fim de garantir o pagamento de indenização, portanto, o artigo também possibilita a equiparação entre operador (pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador) e controlador. Que ocorrerá quando o primeiro descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador. Hipótese que a responsabilidade será solidária entre ambos.

Além dos aspectos técnicos inerentes à atividade de tratamento, coleta e gestão de bancos de dados, a implementação de medidas eficazes (citadas no princípio responsabilização e prestação de contas) perpassa, necessariamente, pela observância das regras e princípios da Lei 13.709/2018. Nesse sentido, a coleta dos dados pessoais deverá

respeitar os princípios da finalidade[40], adequação[41], segurança [42]e necessidade[43], assim como os requisitos elencados nos artigos 7° e 11°, transcritos a seguir:

| | |
|---|---|
| Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:<br><br>I - Mediante o fornecimento de consentimento pelo titular; II - Para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV - Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; VII - para a proteção da vida ou da incolumidade física do titular ou de terceiros; VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; IX - Quando necessário para atender aos interesses legítimos do controlador ou | Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:<br>I - Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;<br>II - Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:<br>a) cumprimento de obrigação legal ou regulatória pelo controlador;<br>b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;<br>c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;<br>d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;<br>e) proteção da vida ou da incolumidade física do titular ou de terceiro;<br>f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou<br>f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, |

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

[41] Art. 6°, II da LGPD - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

[42] Art. 6°, VII da LGPD - 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;

[43] Art. 6°, III da LGPD - 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;

| | |
|---|---|
| de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. | serviços de saúde ou autoridade sanitária;<br>g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. |

Vale destacar o papel do 'consentimento', enquanto instituto jurídico essencial para a coleta e tratamento de dados pessoais. O legislador procurou valorizar a autodeterminação informativa[44] do indivíduo, a fim de que este fosse o ator mais relevante no processo, capaz de decidir e gerir as suas informações.

O tratamento, portanto, só estará em conformidade com a lei se a coleta tiver respaldo nas respectivas bases legais. De modo que, as informações obtidas sem apoio nos princípios e requisitos citados deverão ser descartadas. Assim, o primeiro fundamento da responsabilização decorre justamente da obtenção, pelo controlador, de dados particulares sem a devida justificativa/finalidade.

A obrigação pela prestação de contas também surge com o condão de fiscalizar a atuação do controlador dos dados. Conforme o entendimento extraído de seu art. 38, a autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

À vista disso, a Lei prevê que o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem[45], não só porque a ANPD poderá requisitar informações, a qualquer momento, das operações de tratamento de dados pessoais, mas também em razão da possibilidade de inversão do ônus da prova a

[44] Artigo 2°, inciso II da LGPD.
[45] Artigo 37° da LGPD.

favor do titular dos dados. Quando for verossímil a alegação e houver hipossuficiência para fins de produção de prova, ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa[46].

### 2.2.1 Autoridade Nacional de Proteção de Dados

A criação da ANPD, representa um passo essencial para a efetiva garantia à proteção dos dados pessoais. Este órgão surge vinculado ao Poder Executivo, com o caráter de Agência reguladora, cujo alcance amplo pode atingir basicamente qualquer setor da economia, inclusive as atividades estatais de políticas públicas e serviços públicos. Portanto, a ANPD é o órgão da administração pública federal responsável por zelar pela proteção de dados pessoais e por implementar e fiscalizar o cumprimento da LGPD no Brasil.

Dentre as atribuições mais relevantes desse órgão, destaca-se justamente a capacidade de fiscalizar e aplicar sanções contra os operadores e controladores, quando o tratamento de dados seja realizado em desacordo com a legislação. Cujo procedimento deverá ocorrer mediante a instauração de processo administrativo que assegure o contraditório e ampla defesa, inclusive assegurado o direito de recurso, conforme o devido processo legal estabelecido na constituição federal.

Nesse sentido, a via administrativa é um perfeito exemplo de aplicação da responsabilidade civil objetiva no âmbito da LGPD. Isso porque a motivação jurídica para instauração de processo administrativo decorre tão somente do descumprimento legal pelo ente controlador, isto é, independe da apuração de dolo, culpa ou omissão na conduta do agente.

As sanções administrativas, reguladas no capítulo VIII da LGPD, dispõem de um grande leque de punições cabíveis no caso de descumprimento legal. Que variam desde advertência, com a indicação de prazo para adoção de medidas corretivas[47], até a aplicação de multa (limitada ao valor de cinquenta milhões de reais). Além de dispor

[46] Art. 42, § 2°, da LGPD
[47] Art. 52, inciso I, Lei 13709/2018.

também da possibilidade de suspensão do exercício da atividade de tratamento dos dados pessoais, e até mesmo a proibição do exercício dessa atividade, a depender do grau da infração.

Contudo, além da natureza sancionadora e fiscalizadora, a Agência Nacional de Proteção de Dados tem um dever pedagógico para a promoção de boas práticas de governança voltada às empresas, no tratamento e coleta de dados. Assim como o dever de promover e informar à sociedade civil sobre o tema, tendo em vista a relevância da matéria.

Nesse sentido, sustenta Andriei Gutierrez:

> A fiscalização e possibilidade de aplicação de sanções é parte essencial da institucionalização da proteção dos dados pessoais materializada pela criação da ANPD.
>
> Mas é necessário que se construa um arcabouço de estímulo às boas práticas por parte das organizações de modo a reduzir ao máximo a necessidade de se recorrer ao expediente da punição. Nesse campo, a publicação de diversos guias, orientações e estudos por parte da ANPD pode trazer uma baliza importante para que controladores e operadores possam adequar suas práticas e processos internos da maneira mais eficiente possível de modo a evitar que sejam alvo de processos administrativos e, eventualmente, de sanções.[48]

Dessa forma, em que pese a capacidade sancionadora do órgão, repisa-se que o Brasil não é um país com uma cultura jurídica elaborada, no tocante a proteção e tutela de dados pessoais. Fato que engrandece outra atribuição essencial da ANPD, consistente na obrigação de promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança[49].

Nesse diapasão, a autoridade também teria papel central na transformação cultural das organizações. Além da atribuição punitiva, portanto, a atuação no sentido de promover políticas públicas, campanhas e iniciativas focadas, sobretudo, nas pequenas e médias empresas e organizações que não terão tantos recursos quanto as grandes para buscar assessorias externas (seja de matrizes ou de empresas especializadas).

---

[48] LGPD: Lei Geral de Proteção de Dados comentada [livro eletrônico] / coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. – 2. ed. rev., atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2020

[49] Art. 55-J, VI da LGPD.

# 3. ATUAÇÃO JURISDICIONAL E TUTELA DE DADOS PESSOAIS NOS TRIBUNAIS BRASILEIROS

Como citado no presente trabalho, a LGPD entrou plenamente em vigor em agosto de 2020, e desde então vem sendo aplicada recorrentemente nos Tribunais Brasileiros. Diante disso, para alcançar o objetivo desta dissertação, será feita uma análise aprofundada da jurisprudência já produzida, a fim de termos uma noção mais vívida acerca dos debates produzidos no âmbito jurisdicional.

É necessário repisar que o brasil não é um país com uma cultura jurídica madura sobre o tema, de modo que o olhar crítico acerca das decisões proferidas nessa fase recém-chegada da legislação é de grande valia, e pode revelar a tendencia dos próximos anos sobre o assunto. Assim, deve-se fazer um apanhado geral da atual situação jurisprudencial da LGPD, antes de olharmos para os respectivos casos concretos e soluções adotadas.

Para auxiliar nessa tarefa, será utilizado como base o estudo elaborado pelo Centro de Direito, Internet e Sociedade (CEDIS-IDP) do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP) e o Jusbrasil. No qual apresenta o 'Painel LGPD nos Tribunais'[50], que consiste em uma seleção das mais importantes decisões judiciais que envolvem a Lei Geral de Proteção de Dados (Lei nº 13.709/18), analisadas em uma série de artigos durante o seu primeiro ano de vigência.

Entre setembro de 2020 e outubro de 2021 foram levantadas 584 decisões que, de alguma maneira, citavam a LGPD. Nessa amostragem, foram encontradas um total de 274 decisões que aplicavam efetivamente os dispositivos da nova lei. Deve-se destacar ainda, que dentro do grupo menor, foi observado que as disposições preliminares, constantes do capítulo I, e o capítulo II, que fala do Tratamento dos dados pessoais, representavam em conjunto objeto central de 61,8% das decisões proferidas nos tribunais brasileiros (36,4% referente ao capítulo I e 25,4% sobre o capítulo II).

[50] https://www.jusbrasil.com.br/static/pages/lgpd-nos-tribunais.html

Tal dado estatístico revela que o judiciário passa, verdadeiramente, por um período de adaptação e construção basilar sobre o assunto. Tendo em vista que as decisões abordam, majoritariamente, dispositivos gerais, que versam justamente sobre os conceitos, princípios e requisitos legais que envolvem o tratamento de dados pessoais.

O estudo revelou também, que à época de sua conclusão a justiça estadual e trabalhista foram responsáveis, respectivamente, por 47,1% e 41,2% das decisões analisadas. Restando aos tribunais superiores a parcela de 8%, e nas esferas da justiça federal e eleitoral o caráter residual das decisões proferidas. Algo esperado, pelo menos no ponto de vista da justiça estadual, por ser responsável pela massa contenciosa dos litígios trazidos ao poder judiciário.

A vista disso, poderia ser esperado também que a aplicação da LGPD aos casos concretos, nesse primeiro momento, fosse mais restrita às relações de consumo, numa lógica de responsabilização por perdas e danos decorrente da falha na prestação de um serviço, ou oriunda do tratamento de dados pessoais irregular. Isso porque, como visto anteriormente, a responsabilidade civil dos controladores é, em tese, objetiva, o que facilita a sua aplicação prática, tal como ocorre em face dos fornecedores[51], no âmbito consumerista.

No entanto, o que foi observado através da análise dessas decisões revelou uma outra tendência. No sentido de que os debates travados nos tribunais foram muito além, cujas decisões puderam abordar tanto a questão do dano moral/patrimonial inerente da responsabilidade civil *per si*, quanto tópicos mais complexos e elaborados. Como a

[51] Art. 12 do 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 do 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."

aplicação dos princípios norteadores da lei, do papel da Autoridade Nacional de Proteção de Dados - ANPD, da limitação no tratamento de dados pessoais pelo Poder Público, e até mesmo a questão do limite jurisdicional para deferir a produção de provas, capazes de infringir banco de dados privado.

Dessa forma, nos subcapítulos a seguir serão abordados os cinco principais temas em destaque nos tribunais. A fim de que possamos analisar as respectivas soluções adotadas na seara jurisdicional, no tocante a fundamentação e aplicação técnica das normas dispostas na LGPD aos casos concretos.

### 3.1 Danos Morais Decorrentes do Vazamento de Dados

Conforme o exposto no capítulo específico, o entendimento extraído através do estudo da lei seca é de que a responsabilidade do controlador [52] de dados pessoais é, em tese, objetiva. E decorre da norma disposta no artigo 42 da Lei 13.709/2018, na qual deixa de considerar o elemento 'culpa' na conduta do agente, para determinar a reparação de danos. No entanto, cumpre salientar que a responsabilidade objetiva não necessariamente será aplicada de forma automática, e pode variar a depender do caso concreto. A variação aqui descrita depende principalmente da natureza jurídica desta relação.

Nas relações de consumo, por sua vez, é natural que a modalidade objetiva seja utilizada em face do controlador, tendo em vista que pelo princípio da especialidade das normas, o CDC será a legislação cabível, concomitantemente, na solução do litígio. Para Cezar Roberto Bitencourt[53], este princípio determina que haverá a prevalência da norma especial sobre a geral, evitando o *bis in idem*, e pode ser estabelecido *in abstracto*,

[52] Art. 5°, VI da LGPD: VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
[53] BITENCOURT, Cezar Roberto. Tratado de direito penal: parte geral. 17. ed. São Paulo: Saraiva, 2012.p 231.

enquanto os outros princípios exigem o confronto in concreto das leis que definem o mesmo fato. Nesse sentido entende Marcos Gomes da Silva Bruno[54]:

> "Quando se trata de incidente que gera danos a consumidores, a possibilidade de responsabilização objetiva, independentemente de culpa, se torna mais evidente, na medida em que aplicável o Código de Proteção e Defesa do Consumidor (Lei 8.078/90).
>
> Portanto, no caso de incidentes envolvendo dados pessoais que causem danos a consumidores, é provável a aplicação da responsabilidade objetiva, e também da inversão do ônus da prova para afastar o nexo causal, e consequentemente a indenização, motivo pelo qual os registros e controles das operações envolvendo dados pessoais devem ser rigorosos e estritos, a fim de viabilizar a defesa da empresa".

A vista disso, já é possível observar diversas decisões que aplicam a responsabilidade na esfera da proteção de dados pessoais, de modo a encontrar até mesmo divergência no que diz respeito aos termos em que o dano moral pode ser concebido no caso concreto. Nesse sentido, destacam-se duas decisões conflitantes, uma do Tribunal de Justiça do Estado do Rio de janeiro, e a segunda proferida no Tribunal de Justiça de São Paulo, que ilustram com clareza duas correntes divergentes.

No entanto, antes de colacionar as respectivas ementas, é necessário contextualizar o ambiente em que foram proferidas. Ambos os processos tratam da hipótese em que os titulares pleitearam danos morais em razão de vazamento de dados pessoais, que ocorreu em decorrência de violações de segurança sofridas pelas empresas, nos seus bancos de dados. Acontecimento que por si só não indica a existência de culpa derivada de uma ação ou omissão dolosa dos controladores e operadores, cuja responsabilização, na espécie, ocorreria, portanto, de forma objetiva.

Nesse sentido entendeu o E. Tribunal de Justiça do Rio de Janeiro, através do acórdão proferido pela 26° Câmara Cível, no voto da Desembargadora Natacha de Oliveira, cuja ementa e breve resumo transcritos a seguir:

---

[54] BRUNO, Marcos Gomes da Silva, LGPD: Lei Geral de Proteção de Dados comentada [livro eletrônico] / coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. – 2. ed. rev., atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2020

> APELAÇÃO. VAZAMENTO DE DADOS PESSOAIS. RELAÇÃO DE CONSUMO. RISCO DO EMPREENDIMENTO. LEI GERAL DE PROTEÇÃO DE DADOS. DANOS MORAIS.
>
> A sentença condenou a ré a pagar R$ 10.000,00 de indenização por danos morais. Apelo do réu. Falha do serviço comprovada. Dever de proteção dos dados pessoais. Lei 13.709/18. Ataque de hacker que se insere no risco do empreendimento. Dano moral configurado. Verba que não comporta redução. Acesso aos dados que não poderão ser revertidos. Dados pessoais não anonimizados. Sumula 343 desta Corte.
>
> Recurso desprovido. (TJRJ – 26° Câmara Cível – Apelação n° 0045559-71.2020.8.19.0002 – publicado em 04.02.2022).

Diante desse caso concreto, percebe-se a aplicação simples e direta do instituto da responsabilidade civil objetiva, pela falha na prestação do serviço, tendo em vista se tratar de uma relação de consumo. Merece destaque também, a observância da relatora acerca da teoria do risco do empreendimento, segundo a qual todo aquele que se disponha a exercer alguma atividade no mercado de consumo tem o dever de responder pelos eventuais vícios ou defeitos dos bens e serviços fornecidos, independentemente da culpa[55].

No caso em tela o vazamento dos dados pessoais da autora ocorreu em virtude de um ataque hacker sofrido por um dos parceiros internacionais da empresa ré, que ocasionou na exposição de informações de alguns dos seus usuários. Esse ataque, nos termos do acórdão citado, não se revela suficiente para afastar o dever de indenizar, mesmo inexistindo culpa da empresa controladora. Na qual detém o ônus de, nos termos do artigo 6°, VII, observar o dever se segurança, através da 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.

Nesse caso, a relatora entendeu que a mera publicidade desses dados, sem o consentimento de seu titular, enseja na aplicação de danos morais. Ainda que estes não

[55] FILHO, Sergio Cavalieri. Programa de Responsabilidade Civil. 8 ed. Revista e ampliada. São Paulo: Editora Atlas, 2009. p. 244.

tenham sido efetivamente utilizados por terceiros, porque isso, em tese, não implicaria na inexistência de potencial utilização dos dados da autora pelos que tiveram acesso aos mesmos.

Assim, em relação à natureza da responsabilidade, a jurisprudência não deixa qualquer margem para dúvidas sobre a aplicação de sua espécie objetiva nas relações de consumo, ante a própria necessidade de aplicação do CDC nesses casos. Contudo, as decisões não encontraram uma solução pacífica no que tange ao cabimento dos danos morais decorrente do vazamento.

Isso porque, uma segunda corrente entende que o dano moral que advém do vazamento de dados pessoais não pode ser presumido. Isto significa que, o mero vazamento, ou brecha na segurança interna não necessariamente implica na existência efetiva de dano sofrido pelo consumidor. Sendo imperioso, portanto, que essa consequência negativa esteja comprovada nos autos, como fruto da falha de segurança e respectiva exposição indevida das informações do titular.

Nesse sentido, confira-se a ementa do acórdão proferido pela 19° Câmara de Direito Privado do estado de São Paulo, de relatoria do Desembargador Renato Camilo Costa:

> RESPONSABILIDADE CIVIL. Ação de obrigação de fazer e indenização por danos morais. Alegação da autora de que teve seus dados pessoais vazados pela empresa ré. Consideração de que inexiste prova cabal das consequências danosas do vazamento de seus dados. Hipótese em que a falta de comprovação cabal da verificação concreta de consequências danosas, em virtude do vazamento de dados pessoais, importa na conclusão de que a postulação deduzida pela autora está lastreada em meros danos hipotéticos, ou seja, à possibilidade da ocorrência de fatos lesivos, à expectativa de prejuízo potencial, em decorrência de suposto receio de uso futuro e incerto dos seus dados em eventuais fraudes no comércio, o que só poderia mesmo ter resultado no decreto de improcedência do pedido inicial. Postulação deduzida pela autora baseada em mera possibilidade da ocorrência de dano. Danos morais não caracterizados. Pedido inicial julgado improcedente. Sentença mantida (RI,252). Recurso improvido.

> Dispositivo: negaram provimento ao recurso (TJSP – 19° Câmara de Direito Privado – Apelação n° 1025226-41.2020.8.26.0405 – publicado em 16.09.2022).

No entendimento dessa corrente, em que pese a incidência da responsabilidade objetiva nas relações de consumo, a aplicação do dano moral depende necessariamente do nexo de causalidade. Assim dizendo, dependerá da relação de consequência entre uma ação ou omissão, e fruto dela, a observância de um dano a personalidade de seu titular. Como bem ensina Maria Helena Diniz[56], não pode haver responsabilidade civil sem o dano que deve ser certo, a um bem ou interesse jurídico, sendo necessária a prova real e concreta dessa lesão.

A fim de solidificar esse entendimento, deve-se repisar os fundamentos do referido julgado, no qual argumenta pela inaplicabilidade dos danos morais, nos seguintes termos [57]

> (...) não se nega que constitui obrigação da ré proteger os dados pessoais de seus clientes e que, por falha em seu sistema de segurança, possibilitou que terceiros tivessem acesso a esses dados, **tanto é que lhe incumbia adotar medidas de preservação e guarda segura de questionados dados, de molde a evitar fraudes, em consonância com o que preconiza a Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - artigos 42 e 46), mas não há se olvidar que, para que a concessionária de energia elétrica pudesse ser responsabilizada pelo fato que lhe é imputado na demanda, imprescindível seria a prova da efetiva verificação do dano moral, situação que não se materializou no caso em apreço**, mesmo porque, conquanto assevere a autora que passou a receber mensagens indesejadas via celular e e-mail, ligações de telemarketing, além de ter sido obrigada a agir com mais cautela para não adimplir eventuais boletos fraudulentos, não produziu prova eficaz de tais alegações. (*grifos aditados*)

Assim, fica claro que a falha na prestação do serviço é reconhecida pelo Tribunal, tendo em vista o descumprimento comprovado dos artigos 6 e 46 da LGPD[58]. O ponto

---

[56] DINIZ, Maria Helena. Proteção jurídica da existencialidade. São Paulo, Revista Eletrônica Direito e Sociedade, Canoas, v. 8, n. 2, p. 181-191, ago. 2020.

[57] (TJSP – 19° Câmara de Direito Privado – Apelação n° 1025226-41.2020.8.26.0405 – publicado em 16.09.2022).

[58] Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

controvertido para aplicação dos danos reside, portanto, nas seguintes teses: (i) Emprego da teoria do 'risco do empreendimento' de forma absoluta, por se tratar de relação de consumo; ou (ii) Avaliar, no caso concreto, se a exposição foi capaz de acarretar, efetivamente, algum dano real ao titular dos dados, sob pena de não restar configurado o dano moral na espécie.

Particularmente, soa desmedida a solução adotada pela primeira linha de pensamento, tendo em vista que um dos elementos primordiais do 'dano', reside justamente na existência de um prejuízo efetivo suportado pela vítima. Destaca-se também a natureza da reparação aos danos, tendo em vista se tratar de uma obrigação muito mais compensatória que punitiva[59], como acreditam alguns julgadores.

> Mas a finalidade precípua da indenização não é punir o responsável, mas recompor o patrimônio do lesado, no caso do dano material, e servir de compensação, na hipótese de dano moral. (...) Não se justifica, pois, como pretendem alguns, que o julgador, depois de arbitrar o montante suficiente para compensar o dano moral sofrido pela vítima (e que, indireta e automaticamente, atuará como fator de desestímulo ao ofensor), adicione-lhe um plus a título de pena civil, inspirando-se nas punitive damages do direito norte-americano"

### 3.1.2 Desvio de Finalidade no Tratamento de Dados.

Na hipótese em comento, diferente do que ocorre no vazamento dos dados privados, não existe uma falha de segurança no banco de dados do controlador. Mas sim o uso indevido dessas informações. Assim, é importante relembrar que a coleta e uso, legal, dos dados pessoais deve observar dois requisitos principais, a finalidade e o consentimento do titular[60].

O primeiro reside na ideia de que a coleta dos dados deve se pautar na realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

---

[59] GONÇALVES, Carlos Roberto. Responsabilidade civil. 8° ed. São Paulo; Saraiva, 2003 cit., p. 573.
[60] Art. 7° da Lei 13.709/2018

Enquanto o consentimento, nos termos da LGPD, pode ser entendido como a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Tendo em vista a aplicabilidade prática desses conceitos, é necessário colacionar as decisões produzidas acerca do tema. Na ementa transcrita a seguir, o Tribunal de Justiça de São Paulo entendeu pela ilegalidade no ato praticado pela empresa ré, na qualidade de fornecedora da relação ou do Serviço de consumo, em incluir os dados da autora no cadastro do Serasa por dívida prescrita há mais de 05 anos. Sob o fundamento de violação dos artigos 6° e 7° da LGPD, no sentido de que tal prática fere o princípio da não discriminação, e incorre na quebra do requisito de tratamento dos dados, que consiste na proteção de crédito.

> INDENIZATÓRIA. Serasa "Limpa Nome". Incidência do CDC. Mantidos os benefícios da justiça gratuita à autora. Preliminar de falta de fundamentação da sentença. Afastada. Divulgação de informações de dados do consumidor amparada em dívidas prescritas. Possibilidade para cobrança na esfera extrajudicial, desde que não seja abusiva ou vexatória. Comprovado o acesso de terceiros às informações registradas nos cadastros de serviços de proteção ao crédito. Inteligência do art. 43, § 5º, do CDC. Inscrição que influencia de forma negativa a pontuação do score do consumidor. Plataforma de proteção do crédito que visa alertar os fornecedores sobre eventuais maus pagadores. Prática que viola os artigos 6º, IX e 7º, X, da Lei nº 13.853/2019 – Lei Geral de Proteção de Dados Pessoais (LGDP). Infringência ao disposto no art. 882 do Código Civil. Dano moral. Caracterizado. Precedentes desta C. Câmara. Valor indenizatório que deve atender aos critérios de razoabilidade e proporcionalidade. Sentença reformada. RECURSO PROVIDO.
>
> (TJ-SP - AC: 10242630720218260564 SP 1024263-07.2021.8.26.0564, Relator: Anna Paula Dias da Costa, Data de Julgamento: 26/04/2022, 38ª Câmara de Direito Privado, Data de Publicação: 27/04/2022)

Em atenção a referida ementa, percebe-se que mesmo quando os dados foram obtidos de forma legal, com o consentimento do titular, o uso dessas informações deve respeitar os limites encontrados na própria legislação. Ainda que seja legal, em regra, a inscrição do devedor no cadastro Serasa, fazê-lo por conta de uma dívida prescrita viola um dos requisitos legais expressos da LGPD, que é a proteção ao crédito.

O mesmo ocorre com a realização de propaganda abusiva, a exemplo da sentença proferida pela 7° Vara Cível de Ribeirão Preto[61]. Nos autos da ação indenizatória ajuizada sob o resumido fundamento de que o polo passivo indevidamente armazena os dados pessoais do autor e dispensa tratamento abusivo por meio do envio semanal de mensagens (SMS) com propaganda de telemarketing em seu telefone pessoal. E recusando-se a fornecer ou excluir seus dados pessoais do banco de dados, violando preceitos da LGPD.

Na fundamentação do *decisum*, o magistrado reconheceu acertadamente a violação, nos seguintes termos:

> A qualificação do encarregado da gestão de dados não consta do site do polo passivo (controlador) e não foi fornecida mesmo após devida solicitação administrativa, em expressa violação ao art. 41[62], §1º, da LGPD, pois impossibilita o recebimento de reclamações e tomada de providências pelo titular da informação indevidamente tratada, sendo disponibilizada somente na peça defensiva dos autos (fls. 51)
>
> (...) Noutro giro, conforme esclareceu a defesa, o telefone do polo ativo pertencia anteriormente à empresa que era sua cliente, sendo obtido de forma lícita; todavia, ciente da alteração da titularidade da linha, incorreu o polo passivo em violação a preceitos do CDC e da LGPD ao negar acesso aos pedidos de fornecimento e exclusão de dados da parte contrária, ora acatados, conforme expressa tutela legal, repelindo-se a tese de legítimo interesse do controlador (art. 10[63], LGPD):

Cumpre salientar, portanto, que a negativa de fornecimento de informações ao titular incorre em clara violação do seu direito disposto no artigo 18 desta lei. Cuja

---

[61] 7° Vara Cível da Comarca de Ribeirão Preto, Processo n° 1007913-21.2021.8.26.0506, Juiz Thomaz Carvalhaes Ferreira – Data de Publicação: 27.01.2022

[62] Art. 41. 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.

[63] Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
I - apoio e promoção de atividades do controlador; e
II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.
§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.
§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial..

determinação estabelece que este o controlador, deverá fornecer ao titular a qualquer tempo, mediante requisição, informações relativas à existência, correção, anonimização, bloqueio ou eliminação de dados desnecessários ou excessivos.

Além disso o titular dispõe da capacidade de revogar o consentimento anteriormente fornecido, a qualquer tempo, tendo em vista o objetivo do legislador em prezar pela autodeterminação do titular em dispor sobre as próprias informações.

### 3.2 Pedido de Provas Judiciais e LGPD

Um dos pontos de destaque trazidos pela jurisprudência nesses primeiros anos de vigência da Lei Geral de Proteção de Dados, reside no pedido de produção de provas judiciais que decorra da análise ou exposição de um banco de dados privado. Como se sabe, o código de processo civil estabelece que as partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, para provar a verdade dos fatos em que se funda o pedido ou a defesa, para influir eficazmente na convicção do juiz.

Nesse sentido, em que pese o ônus da prova recair sobre quem alega o fato constitutivo de direito, o CPC também dispõe que diante de peculiaridades da causa, relacionadas à impossibilidade ou à excessiva dificuldade de cumprir este encargo, poderá o juiz atribuir o ônus da prova de modo diverso. Desde que o faça por decisão fundamentada, e dê à parte a oportunidade de se desincumbir do ônus que lhe foi atribuído. Soma-se a isso, o dever atribuído pela sistemática processual de que ninguém se exime de colaborar com o Poder Judiciário para o descobrimento da verdade.

Assim, no âmbito de aplicação da LGPD, o acesso ao banco de dados, ou informações sigilosas pela via judicial é formalmente possível. Seja pela capacidade de coerção e auto exequibilidade conferida às decisões do Poder Judiciário, seja pela inteligência das normas dispostas na lei 13.709/2018. Tendo em vista que uma das hipóteses para o tratamento de dados é o exercício regular de direitos em processo

judicial, administrativo ou arbitral[64]. O que vale igualmente para os dados pessoais sensíveis cujo tratamento poderá ocorrer, inclusive, sem o consentimento do titular, quando for indispensável para o exercício regular de direitos, inclusive em contrato e em processo judicial[65].

Contudo, o ponto controvertido nesse subcapítulo paira sobre os limites na produção de provas. Até que ponto o deferimento de um pedido de provas pode ser enquadrado como algo indispensável para o exercício regular do direito, e em que momento a sua produção pode acarretar, justamente, na violação de um bem jurídico protegido pela lei 13.709/2018.

### 3.2.1 Acesso ao Algoritmo de Plataformas Digitais

A vista disso, deve-se observar a decisão do Tribunal Superior do Trabalho, no Julgamento da Correição Parcial interposta pela 'Uber Do Brasil Tecnologia Ltda' contra decisão proferida nos autos do mandado de segurança n° 0010250-20.2022.5.03.0000, em tramite no TRT 03. A fim de contextualizar a lide, deve-se observar o seguinte trecho do relatório do *decisum*[66];

> Trata-se de Correição Parcial, com pedido de liminar, apresentada pela UBER DO BRASIL TECNOLOGIA LTDA, em face da decisão proferida pela Desembargadora Sabrina de Faria Froes Leão, do TRIBUNAL REGIONAL DO TRABALHO DA 3ª REGIÃO que, nos autos do mandado de segurança nº MSCiv 0010250-20.2022.5.03.0000, indeferiu a liminar postulada pela ora Requerente, mantendo, por conseguinte, a decisão interlocutória proferida nos autos da ação principal (processo nº 0010056-72.2022.5.03.0112 ROT), **na qual determinou-se a realização de perícia no algoritmo do aplicativo utilizado pela Requerente, para fazer prova**

[64] Art. 7º da LGPD -- O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307.

[65] Art. 11 da LGPD -- O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

[66] TST - CorPar: 10002121320225000000, Relator: Guilherme Augusto Caputo Bastos, Corregedoria-Geral da Justiça do Trabalho, Data de Publicação: 01/04/2022

> **quanto ao vínculo de emprego postulado pelo ora terceiro interessado**, tendo sido determinado o trâmite processual em segredo de justiça. (*grifos aditados*)

O objetivo do recurso era o de reformar a decisão que determinou a produção de prova pericial no algoritmo utilizado para o funcionamento do aplicativo da empresa. O objetivo da perícia no caso concreto era estabelecer eventual comprovação de relação de emprego entre a plataforma e colaborador. Ressalta-se que o pedido deferido no processo de origem foi mantido, num primeiro momento, nas instâncias superiores, inclusive no julgamento liminar do mandado de segurança. O que chama atenção para o entendimento primário dos magistrados, no que se refere a possibilidade jurídica de se produzir a prova sobre este objeto.

Isso porque, como sustentou a empresa o Relator Guilherme Augusto Caputo Bastos, a realização da perícia incorreria em prejuízos imensuráveis para a companhia. Justamente por violar o sigilo que protege esse ativo intelectual, na medida em irá revelar diversas informações que integram o segredo do negócio, e que poderia ser utilizado pela concorrência direta.

Na espécie, em que pese o direito do titular em ter acesso as próprias informações, mesmo que seja para fins de comprovar alegação de direito, essa disposição encontra limites na própria LGPD. Na qual tratou de restringir a prerrogativa de acesso relativa aos segredos comercial e industrial, conforme as normas dispostas nos arts. 6º, VI; 9º, II; 19, § 3º; e 20 § 1º.

Essa decisão é um exemplo que retrata a importância de uma interpretação sistemática da norma. Isto é, a necessidade do aplicador do direito em observar a lei em todos os seus aspectos, a fim de evitar contradição no julgamento do caso concreto. O deferimento e produção de provas judiciais, portanto, não pode ser adotado sob princípios e critérios jurídicos genéricos, sem que sejam avaliados os potenciais danos práticos, capazes de violar a própria LGPD, e os bens jurídicos defendidos por esta, como o segredo comercial e industrial.

Ressalta-se que a discussão sobre esse exato mesmo ponto já foi objeto de outros processos oriundos da justiça do trabalho, onde foram proferidas decisões suspendendo a realização de perícia no algoritmo do aplicativo de plataformas digitais. Tais como nos processos de Correição Parcial: 1001522-88.2021.5.00.0000; 1000822-15.2021.5.00.0000; 1000215-02.2021.5.00.0000; 1001652-15.2020.5.00.0000 e 1000175-83.2022.5.00.0000. Todos propostos por empresas de transporte por aplicativo, visando a reforma de decisões que determinavam a realização de perícia em seus respectivos algoritmos, no amito do Tribunal Superior do Trabalho.

### 3.2.2 Acesso ao Banco de dados de Redes Sociais

Para falar deste ponto, foi selecionado acórdão do Tribunal de Justiça do Rio de janeiro, no qual além da LGPD, fundamentou-se no Marco Civil da Internet para dar provimento parcial ao Agravo de Instrumento n° 0050391-22.2021.8.19.0000. O caso em questão trata, na origem, de ação que visa a tutela da honra póstuma da vereadora Marielle Franco, vítima de um homicídio bárbaro e de amplo conhecimento no país, dadas as proporções midiáticas do fato.

A ação foi interposta pelos familiares da vítima em face do Facebook e do Twitter, tendo em vista postagens lamentáveis e vexatórias que violavam a honra da família e vítima. O conteúdo dos ‘*posts’* revelava, nos termos do magistrado de piso, verdadeiro escarnecimento com o assassinato de um ser humano e constituem agressão à dor da família, em ato de bullying virtual.

A inicial foi instruída com pedido de tutela antecipada que visava: (i) a retirada das publicações da plataforma dos réus; (ii) a guarda dos registros de acesso referentes as publicações mencionadas; (iii) a identificação dos IPs dos usuários responsáveis por cada publicação; (iv) informações relativas a eventual impulsionamento/ financiamento das publicações, formas de pagamento e respectivos financiadores; e (v) os usuários logados que tiveram acesso a essa publicação, e os dados que a empresa tem disponíveis sobre os usuários não logados (IP e outros metadados da classificação de segmentação de público

alvo - sexo, idade, cor/raça, faixa de renda), a fim de viabilizar eventual direito de resposta.

A tutela foi integralmente deferida no pedido principal, o que motivou a interposição do referido agravo contra o item ‘v’. Adianta-se que o recurso foi provido para reforma do item destacado acima, tendo em vista o entendimento da Relatora Maria Helena Machado no tocante a disponibilização/guarda dos dados relativos aos usuários que tiveram acesso a publicação. Haja vista que o deferimento deste pedido incorreria, consequentemente, na violação da LGPD e do MCI, nos termos da ementa transcrita a seguir[67].

> AGRAVO DE INSTRUMENTO. DIREITO CIVIL. OBRIGAÇÃO DE FAZER. TWITTER BRASIL. PUBLICAÇÕES OFENSIVAS. TUTELA DE URGÊNCIA EM CARÁTER ANTECIPADO. CONCESSÃO. PRESERVAÇÃO DE DADOS PESSOAIS DE TODOS OS USUÁRIOS QUE ACESSARAM A PUBLICAÇÃO. TERCEIROS ESTRANHOS À LIDE. DIREITO À PRIVACIDADE. REFORMA PARCIAL DO DECISUM COM FULCRO NO VERBETE Nº 59 DA SÚMULA DO TJRJ.
>
> - Agravante que se insurge contra a parte da decisão agravada que determinou a preservação de dados de todos os usuários que acessaram publicações ofensivas à memória de vereadora assassinada, alegando que não há fundamento legal ou jurídico para quebra do sigilo dos dados de usuários que apenas tiveram acesso às publicações combatidas, de forma genérica e inespecífica.
>
> - A Lei nº 12.965/2014 prevê como princípios que regulam o uso da internet no Brasil, em seu artigo 3º, a proteção da privacidade e dos dados pessoais, assegurando, como direitos e garantias dos usuários de internet, no artigo 7º, a inviolabilidade e o sigilo do fluxo de suas comunicações privadas armazenadas, salvo por ordem judicial.
>
> - Segurança de dados que é um ponto de extrema relevância para empresas prestadoras de serviços de internet, posto que elas são responsáveis por guardar e criar mecanismos que protejam tais informações.
>
> - In casu, a determinação do juízo a quo para que o agravante armazene os dados dos usuários logados que tiveram acesso à publicação apontada na petição inicial do processo originário e dos usuários não logados (IP e outros metadados da classificação de segmentação de público-alvo - sexo, idade, cor/raça, faixa de renda), a fim de viabilizar eventual direito de resposta, **vai**

[67] (0050391-22.2021.8.19.0000 - AGRAVO DE INSTRUMENTO. Des(a). MARIA HELENA PINTO MACHADO - Julgamento: 29/03/2022 - QUARTA CÂMARA CÍVEL)

> **de encontro, a princípio, aos preceitos fundamentais e norteadores do Marco Civil da Internet (Lei nº 12.965/2014).**
>
> - **A Lei Geral de Proteção de Dados Pessoais (LGPD), qual seja, nº 13.709/2019 assegura a todo cidadão a titularidade de seus dados pessoais e a garantia dos direitos fundamentais de liberdade, de intimidade e de privacidade, razão pela qual uma determinação de forma generalizada importa a decretação da quebra de sigilo e a violação à intimidade de terceiros que não compõem a relação jurídica objeto dos autos**.
>
> - Assim, por não pertencer à relação processual, não podem os efeitos da decisão que deferiu a tutela se estender até a esfera de atuação jurídica do terceiro que não compõe a lide.
>
> - Decisão concessiva da tutela de urgência pelo Juízo a quo que se afigura parcialmente contrária à Lei e à prova dos autos e deve ser reformada em parte, à luz do verbete nº 59 da Súmula deste Tribunal de Justiça.
>
> PROVIMENTO DO RECURSO. (*grifos aditados*).

Ante o exposto, como já sustentado anteriormente, é possível o acesso ao banco de dados por determinação judicial, a fim de instruir e produzir a dilação probatória nos autos. No entanto, em que pese a relevância e sensibilidade do caso, o levantamento de informações relativas a todos os usuários que tiveram acesso a publicação fere direitos e garantias previstas tanto no MCI quanto na LGPD.

Isso porque, na espécie, o artigo 17 da LGPD garante que toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade. A tutela da privacidade, portanto, também é regulada pelo MCI, através do art. 3°, II e III, que elege como princípios a proteção da privacidade e dos dados pessoais, na forma da lei. Logo, o ato de deferir a guarda e acesso dos dados privados de todo e qualquer usuário que teve acesso às publicações, revela-se como uma medida descabida pelo judiciário, ainda que seja para produção de provas na demanda.

Nesse sentido, o debate trazido pelo caso concreto revela a importância de outros pontos que pairam o estudo dos dados pessoais. Sendo eles o ‘consentimento’ e a limitação do poder público no acesso e tratamento de dados privados. Nesse debate, o primeiro é o objeto basilar na positivação da lei 13.709/2018.

Como já citado neste trabalho, o legislador prezou pelo protagonismo do titular, que detém a capacidade de autodeterminação de seus dados. De modo que o acesso em processo judicial, mesmo que sigiloso, de informações pertinentes a indivíduos que não possuem relação direta com a demanda, passa por cima dos objetivos precípuos da legislação. Acerca da relevância do 'consentimento', enquanto elemento fundamental da autodeterminação pretendida pelo legislador, entende o autor Bruno Bioni[68]:

> O titular dos dados pessoais alçou papel de protagonista a partir da segunda geração de leis de proteção de dados pessoais. Naquele momento, optou-se por uma estratégia regulatória que nele depositava a responsabilidade de autoproteger as suas informações pessoais. Essa diretriz normativa foi fundada a partir do direito de o indivíduo controlar os seus dados pessoais, socorrendo-se, por isso, à técnica legislativa de exigir o consentimento do titular dos dados pessoais para que eles fossem coletados, utilizados, compartilhados, enfim, para toda e qualquer etapa de tratamento de tais informações.
>
> A própria intelecção da proteção de dados pessoais foi forjada sob a alcunha de autodeterminação informacional. Da decisão da Corte Constitucional alemã ao referencial teórico de Alan Westin consolidou-se a crença reducionista de que autodeterminação informacional corresponderia ao elemento volitivo – autonomia da vontade – do titular do dado. Com ela, o consentimento atingiu umstatus canônico, cujo reverência se fez sentir ao longo de todo o percurso geracional das leis de proteção de dados pessoais.

Diante disso, apesar das hipóteses legais de dispensa do consentimento do titular, tal escusa não pode atingir terceiros estranhos a lide (no âmbito judicial). E tampouco tem a prerrogativa de passar por cima da autonomia da vontade nas hipóteses onde a finalidade da coleta e tratamento se dá sob fundamentos genéricos ou desproporcionais ao fim pretendido. Até porque, o acesso a uma publicação numa rede social não necessariamente pressupõe concordância ou anuência com o conteúdo ali previsto, e muito menos qualquer contribuição para sua produção.

---

[68] Bioni, Bruno Ricardo Proteção de dados pessoais: a função e os limites do consentimento / Bruno Ricardo Bioni. – Rio de Janeiro: Forense, 2019. p. 327.

### 3.3 Tutela Coletiva de Dados Pessoais sob a LGPD

Em que pese eventual controvérsia doutrinária acerca da classificação de direitos difusos e coletivos, seu conceito legal pode ser encontrado no artigo 81, incisos I e II do CDC respectivamente. Assim, para a legislação consumerista o primeiro pode ser entendido como os transindividuais, de natureza indivisível, de que sejam titulares pessoas indeterminadas e ligadas por circunstâncias de fato. Já o segundo, seriam *os* transindividuais, de natureza indivisível de que seja titular grupo, categoria ou classe de pessoas ligadas entre si ou com a parte contrária por uma relação jurídica base.

Logo, ambos são equivalentes no que diz respeito à indivisibilidade dos bens jurídicos (ou seja, seu objeto). Isso significa que é impossível satisfazer apenas um dos titulares de um interesse seja ele difuso ou coletivo. A satisfação de uma pessoa, portanto, significa necessariamente a satisfação de todos os cotitulares. A diferença entre ambas as espécies reside, em síntese, no fato de um deter como titular um grupo de pessoas indeterminado, e ligado por uma circunstância factual (interesse difuso), como o direito ao meio ambiente por exemplo. Enquanto os titulares de direitos/interesses coletivos estão delimitados por um grupo de indivíduos específico, integrantes de uma categoria ou classe, tal como ocorre nos sindicatos.

De toda maneira, as suas distinções teóricas possuem pouca relevância prática para os objetivos deste trabalho, tendo em vista que ambos dispõem das mesmas ferramentas processuais para buscar a tutela jurisdicional. Além de possuírem fim semelhante, ao passo que a 'tutela coletiva', por si, procura resguardar interesse de cunho social, e que pode ser aproveitado por um grupo de pessoas como um todo. Nesse sentido, confira-se o entendimento da doutrina em relação a sua distinção processual[69][70]:

[69] NERY JR., Nelson; NERY, Rosa Maria Andrade. Código de Processo Civil comentado: e legislação processual civil extravagante em vigor. 4. ed. São Paulo: Revista dos Tribunais, 1999. p.1864

[70] WATANABE, Kazuo. Disposições gerais. In: _____ et al. Código brasileiro de defesa do consumidor: comentado pelos autores do anteprojeto. 7. ed. Rio de Janeiro: Forense Universitária, 2001. tít. III, cap. 1, p. 722-784.

> Cumpre ressaltar que, processualmente, o que qualifica o direito como difuso, coletivo ou individual homogêneo é o conjunto formado pela causa de pedir e pelo pedido deduzido em juízo. O tipo de pretensão e seu fundamento, ou seja, o objeto litigioso trazido pelo autor da demanda, é que caracterizam a natureza do direito para fins de tutela jurisdicional.

Dessa forma, o ponto principal é esclarecer que, além da jurisprudência contenciosa, consistente na aplicação da Lei 13.709/18 para a solução dos litígios entre particulares, é necessário chamar a atenção também para os casos que versam sobre a sua relevância na proteção de direitos e interesses difusos. Cuja persecução se dá através de ferramentas processuais específicas, como a Ação Civil Pública, e pela atuação de entidades especializadas, principalmente na representação do Ministério Público. Ressalta-se que o uso da ACP para tutela de dados pessoais coletivos é um fenômeno até anterior à edição da LGPD, quando o código de defesa do consumidor, Marco Civil da Internet e outras leis esparsas eram aplicadas.

Isso pôde ser observado com mais frequência a partir de 2015, quando, por exemplo, o Ministério Público Federal do Piauí abriu uma ACP contra a Google Brasil. Oportunidade em que desenvolveu tese sobre abusividade na leitura automática de mensagens do Gmail, dada a falta de consentimento informado, o que incorreria numa prática abusiva. Nesse caso, o julgamento em primeira instancia entendeu pelo desprovimento da ACP em 2018, sob o fundamento de que a leitura automatizada para fins publicitários faz parte do modelo de negócios, de modo a possibilitar a oferta do serviço sem custos aos usuários. Isso não impediu, contudo, que a Secretaria de Estado Consumidores (Senacon) intervisse posteriormente via processo administrativo no final de 2019, numa clara atuação pelos direitos coletivos dos consumidores, exercida também na seara administrativa. Além dessa, outras ações civis foram abertas nesse ínterim, antes da promulgação efetiva da LGPD no segundo semestre de 2018.

A vista disso, após a publicação da Lei 13.709/2018 é possível observar que, apesar de transparecer como principal característica um forte viés de proteção focado nos

direitos individuais, a LGPD também abarca direitos e interesses coletivos em diversos dispositivos. Senão vejamos o entendimento elucidado por Rafael A. F. Zanatta [71]:

> Como herdeira dessa tradição de abertura aos direitos difusos – que define as características do direito civil e processual brasileiro na segunda metade do século XX –, a Lei Geral de Proteção de Dados Pessoais possui um caráter propositalmente ambíguo. A legislação assume um forte caráter de afirmação de direitos individuais, porém mantém, em sua estrutura, dispositivos que garantem claramente instrumentos de proteção de direitos coletivos e difusos. Nesse sentido, é uma lei ambígua. Ela é claramente orientada aos direitos individuais, porém, também é uma legislação de proteção de direitos difusos
>
> Ao mesmo tempo, a LGPD adota uma série de elementos típicos da defesa ambiental e da defesa do consumidor, em especial a mobilização de ideias relacionadas a "direitos difusos" e tutela coletiva. A legislação é clara ao afirmar que o direito de peticionamento pode ser exercido "perante os organismos de defesa do consumidor" (art. 18, § 8o), reforçando a estrutura das centenas de Procons criados desde a década de 1970 no país. Mas não só. Essa norma atrai para o polo de aplicação desses direitos toda a estrutura dos Procons, Defensorias Públicas, ONGs e Ministérios Públicos (o que é chamado de "Sistema Nacional de Defesa do Consumidor"), na medida em que a LGPD também afirma que "a defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente", "acerca dos instrumentos de tutela individual e coletiva" (art. 22).
>
> (...) De modo muito claro, a LGPD estabelece que o judiciário poderá ser instado pelos legitimados, a defender os interesses e os direitos dos titulares de dados, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva (art. 22). Mais detalhadamente, poderá o judiciário ser instado a determinar a responsabilidade dos controladores e operadores pelo ressarcimento de danos individuais e/ou coletivos que tenham causado no exercício de atividade de tratamento de dados pessoais, quando houver violação da legislação de proteção de dados (art. 42, caput e § 3º, da LGPD).

O legislador foi feliz em positivar tais dispositivos, que conferem ao ordenamento brasileiro o embasamento teórico necessário para tutelar esse direito fundamental, sob as ferramentas processuais adequadas. Dito isso, o ajuizamento de ações civis públicas que visam a tutela de dados pessoais passa a ganhar uma nova roupagem após a lei 13.709/2018, haja vista as inovações em seu conteúdo, que apresenta inclusive uma nova espécie de responsabilidade civil.

[71] ZANATTA, Rafael A. F.; SOUZA, Michel R. O. A tutela coletiva na proteção de dados pessoais: tendências e desafios, in: DE LUCCA, Newton; ROSA, Cíntia. Direito & Internet IV: Proteção de Dados Pessoais. São Paulo: Quartier Latin, 2019. p.11.

### 3.3.1 ACP Metro de São Paulo: Caso das Portas Interativas

O caso em comento teve início no ano de 2018, através da proposição da ACP n° 1090663-42.2018.8.26.0100 pelo IDEC em face da Concessionaria da Linha 4 do Metro de São Paulo S.A. (Via Quatro), por conta de uma ação que deveria ocorrer em suas respectivas plataformas. O processo foi julgado procedente em maio de 2021, e atualmente tramita em segunda instancia, na fase de Apelação. Para melhor esclarecimento da controvérsia, leia-se o relatório da sentença:

> Trata-se de ação civil pública proposta pelo Instituto Brasileiro de Defesa do Consumidor (IDEC) em face da empresa Concessionária Da Linha 4 Do Metrô De São Paulo S.A. (Via Quatro). Requer a proibição de coleta e tratamento de imagens e dados biométricos tomados, sem prévio consentimento, de usuários das linhas de metrô operadas pela ré, implementados em sete estações da Linha 4-Amarela: Luz, República, Paulista, Fradique Coutinho, Faria Lima, Pinheiros e Butantã. Requereu o autor a concessão de tutela de urgência para que cesse a coleta de dados das portas interativas digitais, comprovando-se o desligamento das câmeras já instaladas, sob pena de multa diária de R$50.000,00 (cinquenta mil reais). Ao final, requer a condenação da ré (i) a não utilizar dados biométricos ou qualquer outro tipo de identificação dos consumidores e usuários do transporte público, (ii) ao pagamento de indenização pela utilização indevida da imagem dos consumidores e (iii) indenização por danos coletivos em valor não inferior a R$100.000.000,00. Juntou documentos.

A coleta de dados aqui descrita ocorreria através da leitura biométrica da face dos passageiros, por meio das câmeras instaladas nas ‘Portas Digitais’. Vale ressaltar, que o rosto humano é considerado um dado pessoal sensível desde a lei nº 14.414/2011 (Lei do Cadastro Positivo). A leitura biométrica teria como objetivo a captação de emoções, faixa etária e sexo dos passageiros com o objetivo de utilizá-los para fins comerciais e estatísticos.

Ademais, por se tratar, na espécie, de um dado pessoal sensível[72], o bem jurídico coletivo a ser tutelado nos autos detém um escopo de proteção ainda maior pela LGPD.

[72] Art. 5º Para os fins desta Lei, considera-se:

Isso porque os dados sensíveis são uma espécie de dados pessoais que compreendem uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade: discriminação[73].

A principal tese de defesa da concessionária consistia em dizer que a coleta biométrica não incorreria em reconhecimento facial dos passageiros, mas tão somente a **detecção** do rosto e expressões. Em síntese, a diferença é que o segundo não seria capaz de associar o dado coletado a algum indivíduo em específico. Além de informar também que os dados obtidos seriam automaticamente transformados num código binário, de modo que não seriam armazenadas qualquer imagem, vídeo ou áudio em banco de dados. No entanto, a requerida não foi capaz de produzir qualquer prova no processo capaz de corroborar com essa afirmação.

Logo, não restaram dúvidas acerca das violações dos dados e privacidade dos usuários do metrô. O que merece atenção neste caso é a riqueza de conceitos e institutos jurídicos manejados sob a aplicação da Lei Geral de Proteção de Dados, que se amoldam num exemplo prático extremamente didático. No qual também passa a integrar e enriquecer a jurisprudência sobre o tema.

Acerca das violações observadas, a principal consiste justamente na ausência de consentimento pelos titulares, aqui representados pela coletividade. Ressuscitando a importância desse instituto na construção da normatização dos dados pessoais. Conforme estabelece o artigo 11, I, para o tratamento dos dados pessoais sensíveis, é imprescindível que o seu titular ou representante legal dê o consentimento de forma específica e destacada, para finalidades delimitadas.

---

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

[73] Bioni, Bruno Ricardo Proteção de dados pessoais: a função e os limites do consentimento / Bruno Ricardo Bioni. – Rio de Janeiro: Forense, 2019.p.119.

Além da exigência do consentimento *lato sensu*, ressalta-se que este não pode ser obtido/fornecido de qualquer maneira. Isto é, a lei impõe a obrigação de que este ocorra de maneira específica e destacada, de modo a não correr risco da existência de vício na obtenção dos dados sensíveis. Senão vejamos:

> O consentimento será entendido como específico, desde que ele seja manifestado em relação a propósitos claramente determinados pelo controlador, anteriormente ao procedimento de coleta dos dados pessoais. Permanecem as obrigações de granularidade (dispostas em relação ao consentimento livre, o que exige a existência de opt-in para cada finalidade em específico), sendo adicionada também a determinação de que o consentimento seja manifestado de modo destacado das eventuais outras previsões contidas no documento (o que faz referência ao consentimento destacado, conforme explanado a seguir).
>
> Para que o consentimento seja entendido como destacado, é importante que o titular dos dados tenha, de fato, pleno e efetivo acesso ao documento que esclarecerá todos os fatos relevantes sobre o tratamento dos seus dados pessoais. Nesse sentido, especialmente nas situações em que o consentimento for manifestado dentro de contexto geral e mais amplo, deve ser destacado o trecho relativo ao tratamento dos dados (isso pode se dar, a partir do uso de caixa alta, fontes em negrito, sublinhado, itálico, entre outros), garantindo ao titular o efetivo acesso ao referido conteúdo. (LIMA, 2020). [74]

Ademais, no caso desta ACP existe ainda um fator agravante na conduta da concessionária, que reside na coleta potencial de dados referentes a crianças e adolescentes. Tendo em vista que o titular nesse caso é a coletividade, figurada pelos usuários e potenciais usuários do serviço de transporte público, isso também faz incidir as normas protetivas o Estatuto da Criança e do Adolescente. Já que a imagem desse público goza de maior proteção, conforme indica o artigo 17 do ECA.

Além do debate envolvendo o prisma do consentimento por mais uma vez, no âmbito processual foi manejada a ferramenta das ações coletivas para fazer cessar violação dos interesses difusos. Em que pese a histórica atuação do MP, quase que exclusiva nessa espécie de ação, esta foi proposta por uma entidade particular, igualmente legítima nos termos do artigo 5°, inciso V da Lei 7.347/85.

---

[74] LIMA, Caio César Carvalho: LGPD: Lei Geral de Proteção de Dados comentada [livro eletrônico] / coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. – 2. ed. rev., atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2020, pg. 221-222.

A tutela coletiva prática, nos termos da LGPD, evidenciou que a aplicação da responsabilidade objetiva face aos controladores também pode ocorrer sob a roupagem de danos morais coletivos. Tendo em vista a comprovação da prática ilícita e abusiva, cuja extensão danosa se deu para um número imensurável de indivíduos. Acerca de sua possibilidade jurídica, entende a lição de Carlos Alberto Bittar Filho [75]sobre o dano moral coletivo:

> "(...) a injusta lesão da esfera moral de uma dada comunidade, ou seja, é a violação antijurídicade um determinado círculo de valores coletivos" e "Quando se fala em dano moral coletivo, está se fazendo menção ao fato de que o patrimônio valorativo de uma certa comunidade (maior ou menor), idealmente considerado, foi agredido de maneira absolutamente injustificável do ponto de vista jurídico; quer isso dizer, em última instância, que se feriu a própria cultura, em seu aspecto imaterial".

Conclui-se que a nova sistemática legal de proteção dos dados pessoais, enquanto direito fundamental, dispõe de um grande leque de ferramentas jurídicas para a efetivação. Seja na apuração do litígio entre particulares, de modo contencioso, seja pelos procedimentos que atuam pela proteção e garantia de interesses difusos e coletivos.

[75] in Do Dano Moral Coletivo no Atual Contexto Jurídico Brasileiro, Revista de Direito do Consumidor, v. 12, p. 55

# 4 CONCLUSÃO

Ante o exposto, o presente estudo pretendeu instruir uma trajetória completa acerca dos marcos legais de proteção de dados no Brasil, de modo a demonstrar o crescente engajamento da comunidade jurídica sobre o tema. O fenômeno dos dados pessoais enquanto verdadeira moeda de troca, nessa era da sociedade da informação, colocou em voga o quão relevante é esse direito fundamental, e a respectiva urgência pela sua regulação protetiva.

Em que pesem os debates sobre o tema que ocorrem nas últimas décadas, e a edição de leis setoriais, é inegável que a LGPD surge com grande entusiasmo e com o condão de suprir lacunas. Uma legislação nesse sentido, conforme exposto ao longo do texto, é responsável por garantir maior segurança jurídica não só para os titulares, mas também para potenciais investidores e empresas que atuam de alguma forma no Brasil. Colocando o país num rol de nações que há tempos perceberam a necessidade de tutelar os dados privados, diante dos modelos de negócios e avanços tecnológicos avassaladores do século XXI.

Dessa forma, os institutos e ferramentas processuais trazidas pela LGPD estão sendo capazes de influir na garantia efetiva dos dados pessoais privados, em caso de violação ou irregularidade no tratamento. Sobretudo ao elencar o consentimento como elemento imprescindível para a sua coleta e utilização. De modo que a autodeterminação informacional procura empoderar o titular dos dados privados, no qual detém o poder de decidir e dispor sobre estes, nos termos da lei.

Assim, essa prerrogativa ganha forma através dos diversos dispositivos que a regulam. Como por exemplo o direito do titular de revogar, a qualquer tempo, o consentimento dado, nos termos do artigo 17, IX. Além de, nos termos do mesmo artigo, requerer que o controlador forneça informações das entidades públicas e privadas com as quais o controlador uso compartilhado de dados; a exclusão de todas as suas informações do banco de dados deste; a anonimização dentre outras garantias positivadas na norma.

O ponto é a garantia do titular de dispor, gerir e controlar quais e como os seus dados são tratados pelo controlador. Pautando-se, portanto, no consentimento e na autodeterminação informacional garantida pela Lei 13.709/2018. A vista disso, a preocupação objeto deste trabalho foi o de observar se a tutela efetiva, exercida na atuação jurisdicional, seria capaz de proteger os objetivos positivados pelo Legislador.

Nesse sentido, através da inauguração inclusive de uma nova espécie de responsabilidade civil através do artigo 42, a expectativa seria que a jurisprudência nesses primeiros anos ficasse limitada a debates gerais e principiológicos. Restritos na aplicação eventual de danos morais nas relações de consumo. No entanto, o resultado da análise surpreendeu positivamente pela multiplicidade de casos concretos, hipóteses específicas e tópicos distintos trazidos para apreciação do julgador. O embate de teses revelou, na verdade, o amadurecimento dos juristas acerca da tutela de dados pessoais, enquanto um fenômeno contínuo, que iniciou muito antes da lei 13.709/2018.

Pode-se concluir, nesse sentido, que a tutela jurisdicional revela uma tendencia de amadurecimento na cultura jurídica de proteção de dados pessoais no Brasil. Cultura essa que passa tanto pela intenção legislativa, doutrinária e acadêmica, mas também pelo entendimento prático do judiciário. No qual, ao aplicar a norma ao litígio, acaba por balizar com mais clareza como devem se pautar os limites para extensão do dano, a responsabilização, o respeito aos requisitos de tratamento, coleta. E de que modo as empresas responsáveis por tratamento de dados adotam corretamente as medidas legais de proteção, anonimização, segurança dos dados pessoais incluídos em seus bancos de dados.

Por fim, é essencial repisar que a contribuição da tutela jurisdicional na construção de uma cultura de valorização dos dados, ocorre de maneira mitigada, após a provocação do poder judiciário. Sendo igualmente importante, portanto, chamar a atenção para o necessário esforço a ser desprendido em conjunto, pela sociedade, associações, empresas, estudiosos, e a própria ANPD na edificação gradativa desse entendimento. Seja através

da adequação coorporativa às normas replicadas na lei 13.709/18, seja pela educação, publicidade e debates públicos. A fim de instruir também os titulares, figurados aqui pela sociedade civil enquanto coletividade, cujo interesse difuso na matéria pode ser inclusive, pleiteado pelas ferramentas processuais próprias.

# BIBLIOGRAFIA

ALVES, Marcelo de Camilo Tavares. Direito Digital. Goiânia, 2009, p. 27.

GONÇALVES, Carlos Roberto. Responsabilidade civil, cit., p. 573.

FILHO, Sergio Cavalieri. Programa de Responsabilidade Civil. 8 ed. Revista e ampliada.São Paulo: Editora Atlas, 2009

ZANATTA, Rafael A. F.; SOUZA, Michel R. O. A tutela coletiva na proteção de dados pessoais: tendências e desafios, in: DE LUCCA, Newton; ROSA, Cíntia. Direito & Internet IV: Proteção de Dados Pessoais. São Paulo: Quartier Latin, 2019. ISBN: 9788574538389.

in Do Dano Moral Coletivo no Atual Contexto Jurídico Brasileiro, Revista de Direito do Consumidor, v. 12, p. 55

Gouveia, Luís Manuel Borges (2004), "Notas de contribuição para uma definição operacional". Página consultada a 22 de Dezembro de 2008.

Tribunal de Justiça do Estado de São Paulo. 37ª Vara Cível. Decisão de antecipação de tutela. Ação civil pública nº 1090663-42.2018.8.26.0100. São Paulo, 14 set. 2018.

DONEDA, Danilo. A PROTEÇÃO DOS DADOS PESSOAIS COMO UM DIREITO FUNDAMENTAL. **Espaço Jurídico**, Joaçaba, v. 12, n. 2, p. 91-108, dez. 2011.

MONTEIRO, Renato Leite. **Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?** 2018

BITENCOURT, Cezar Roberto. Tratado de direito penal: parte geral. 17. ed. São Paulo: Saraiva, 2012.

BODIN DE MORAES, Maria Celina. LGPD: um novo regime de responsabilização civil dito “proativo”. Editorial à Civilistica.com. Rio de Janeiro: a. 8, n. 3, 2019. Disponível em: . Data de acesso

SANTOS, Marianny Costa. O JUDICIÁRIO BRASILEIRO E A PERSPECTIVA EM ATRIBUIR SUA FUNÇÃO DECISÓRIA AS MÁQUINAS INTELIGENTES. **Enpejud**, [*s. l*], v. 5, p. 400-415, jun. 2020.

ROQUE, André. A TUTELA COLETIVA DOS DADOS PESSOAIS NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD). **Revista Eletrônica de Direito Processual**: REDP, Rio de Janeiro, v. 20, n. 2, p. 01-19, ago. 2019. Quadrimestral. Disponível em: https://www.e-publicacoes.uerj.br/index.php/redp/index. Acesso em: 27 maio 2021.

DUARTE, Júlia Tupynambá. **A APLICAÇÃO DA TUTELA DA PROTEÇÃO DE DADOS PESSOAIS NO CASO DAS PORTAS INTERATIVAS DIGITAIS DO METRÔ DE SÃO PAULO**. 2019. 66 f. TCC (Graduação) - Curso de Direito, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2019.

SARTORI, Ellen Carina Mattias. Privacidade e dados pessoais: a proteção contratual da personalidade do consumidor na internet. Revista de Direito Civil Contemporâneo. vol. 9. ano 3. p. 49-104. São Paulo: Ed. RT, out.-dez. 2016.

GROSSI, Bernardo Menicucci (Org.) Lei Geral de Proteção de Dados: Uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial [recurso eletrônico] / Bernardo Menicucci Grossi (Org.) -- Porto Alegre, RS: Editora Fi, 2020. 455p. ISBN -978-65-87340-21-0 Disponível em: http://www.editorafi.org

Veronese, Alexandre; Melo, Noemy. O Projeto de Lei 5.276/2016 em contraste com o novo Regulamento Europeu (2016/679 UE). Revista de Direito Civil Contemporâneo. vol. 14. ano 5. p. 71-99. São Paulo: Ed. RT, jan.-mar. 2018

LGPD: Lei Geral de Proteção de Dados comentada [livro eletrônico] / coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. – 2. ed. rev., atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2020.

BITTAR, Carlos Alberto. Os Direitos da Personalidade. 7ª ed. São Paulo: Forense, 2006. GONÇALVES, Carlos Roberto. Direito Civil brasileiro, Responsabilidade. 7ª ed. São Paulo. Saraiva, 2011. V.7. p. 24

https://www.bbc.com/portuguese/brasil-37677421

https://g1.globo.com/economia/tecnologia/noticia/2021/02/03/lucro-da-dona-do-google-cresce-20percent-em-2020.ghtml

BRASIL, LEI N° 10.406, DE 10 DE JANEIRO DE 2002, Código Civil. Disponível em http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm

DINIZ, Maria Helena. Proteção jurídica da existencialidade. São Paulo, Revista Eletrônica Direito e Sociedade, Canoas, v. 8, n. 2, p. 181-191, ago. 2020.

BRASIL, LEI Nº 13.709, DE 14 DE AGOSTO DE 2018, Lei Geral de Proteção de Dados, Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

DINIZ, Maria Helena. Curso de direito civil brasileiro: responsabilidade civil. Vol. 7. 27ªed. São Paulo: Saraiva, 2013.

Bioni, Bruno Ricardo Proteção de dados pessoais: a função e os limites do consentimento / Bruno Ricardo Bioni. – Rio de Janeiro: Forense, 2019.

(0050391-22.2021.8.19.0000 - AGRAVO DE INSTRUMENTO. Des(a). MARIA

HELENA PINTO MACHADO - Julgamento: 29/03/2022 - QUARTA CÂMARA CÍVEL)

TST - CorPar: 10002121320225000000, Relator: Guilherme Augusto Caputo Bastos, Corregedoria-Geral da Justiça do Trabalho, Data de Publicação: 01/04/2022.

7° Vara Cível da Comarca de Ribeirão Preto, Processo n° 1007913-21.2021.8.26.0506, Juiz Thomaz Carvalhaes Ferreira – Data de Publicação: 27.01.2022.

MENDES, Laura Schertel. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. Revista de Direito do Consumidor, n. 106, jul./ago., [s. l.], 2016.

NERY JR., Nelson; NERY, Rosa Maria Andrade. Código de Processo Civil comentado: e legislação processual civil extravagante em vigor. 4. ed. São Paulo: Revista dos Tribunais, 1999.

WATANABE, Kazuo. Disposições gerais. In: _____ et al. Código brasileiro de defesa do consumidor: comentado pelos autores do anteprojeto. 7. ed. Rio de Janeiro: Forense Universitária, 2001. tít. III, cap. 1, p. 722-784.