

UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS JURÍDICAS
DEPARTAMENTO DE DIREITO
CURSO DE GRADUAÇÃO EM DIREITO

Carolina Pelegrino de Marcantonio

**O NOVO REGIME DE RESPONSABILIDADE CIVIL INAUGURADO PELA LEI
GERAL DE PROTEÇÃO DE DADOS PESSOAIS**

Florianópolis

2022

Carolina Pelegrino de Marcantonio

**O NOVO REGIME DE RESPONSABILIDADE CIVIL INAUGURADO PELA LEI
GERAL DE PROTEÇÃO DE DADOS PESSOAIS**

Trabalho de Conclusão do Curso de Graduação
em Direito do Centro de Ciências Jurídicas da
Universidade Federal de Santa Catarina como
requisito para a obtenção do título de Bacharel
em Direito.

Orientadora: Profa. Dra. Carolina Medeiros
Bahia.

Coorientador: Caio Eduardo Dias

Florianópolis

2022

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Marcantonio, Carolina Pelegrino de
O NOVO REGIME DE RESPONSABILIDADE CIVIL INAUGURADO
PELA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS /
Carolina
Pelegrino de Marcantonio ; orientador, Carolina Medeiros
Bahia, coorientador, Caio Eduardo Dias, 2022.
93 p.

Trabalho de Conclusão de Curso (graduação) -
Universidade Federal de Santa Catarina, Centro de Ciências
Jurídicas, Graduação em Direito, Florianópolis, 2022.

Inclui referências.

1. Direito. 2. Lei Geral de Proteção de Dados Pessoais .
3. Responsabilidade Civil. I. Medeiros Bahia, Carolina .
II. Dias, Caio Eduardo . III. Universidade Federal de
Santa Catarina. Graduação em Direito. IV. Título.

UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS JURÍDICAS
COLEGIADO DO CURSO DE GRADUAÇÃO EM DIREITO

TERMO DE APROVAÇÃO

O presente Trabalho de Conclusão de Curso, intitulado “O novo regime de responsabilidade civil inaugurado pela Lei Geral de Proteção de Dados Pessoais”, elaborado pela acadêmica **Carolina Pelegrino de Marcantonio**, defendido em **22/07/2022** e aprovado pela Banca Examinadora composta pelos membros abaixo assinados, obteve aprovação com nota 10,0 (Dez), cumprindo o requisito legal previsto no art. 10 da Resolução nº 09/2004/CES/CNE, regulamentado pela Universidade Federal de Santa Catarina, através da Resolução nº 01/CCGD/CCJ/2014.

Florianópolis, **22 de julho de 2022**

Carolina M. Bahia

Profa. Dra. Carolina Medeiros Bahia
Professora Orientadora

Carlos M. S. Cunha

Carlos Mendes da Silveira Cunha
Membro de Banca

Paulo Vitor Petris Tambosi

Paulo Vitor Petris Tambosi
Membro de Banca



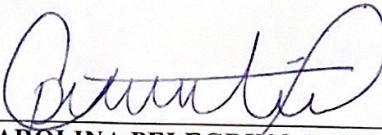
Universidade Federal de Santa Catarina
Centro de Ciências Jurídicas
COORDENADORIA DO CURSO DE DIREITO

TERMO DE RESPONSABILIDADE PELO INEDITISMO DO TCC E
ORIENTAÇÃO IDEOLÓGICA

Aluna: Carolina Pelegrino de Marcantonio
Matrícula: 1720474-7
Título do TCC: O novo regime de responsabilidade civil inaugurado pela Lei
Geral de Proteção de Dados Pessoais
Orientadora: Profa. Dra. Carolina Medeiros Bahia

Eu, Carolina Pelegrino de Marcantonio, acima qualificada; venho, pelo presente termo, assumir integral responsabilidade pela originalidade e conteúdo ideológico apresentado no TCC de minha autoria, acima referido

Florianópolis, 22 de julho de 2022.



CAROLINA PELEGRINO DE MARCANTONIO

AGRADECIMENTOS

De início, gostaria de agradecer aos meus pais, que me ensinaram a importância do estudo e fizeram o possível e o impossível para que ele não me faltasse. Graças à sua confiança e apoio, fui e sou capaz de conquistar os meus anseios, dentre eles estudar Direito na Universidade Federal de Santa Catarina. Agradeço todo amor e por sempre estarem presentes em minha vida.

Ao Léo, a pessoa que mais esteve presente na elaboração deste trabalho, por todo carinho, paciência, comidas e mimos que me deram força a continuar e tornaram os meus dias mais leves. Agradeço o companheirismo de sempre e por acreditar em mim e me ajudar a conquistar os meus sonhos e objetivos, independentemente da dificuldade que enfrentaremos.

Aos meus primos, Milena e André, que sempre foram um exemplo e admiração de profissionais dedicados, esforçados e merecedores de todo estudo e trabalho realizado. Sou grata por todas as orientações, conselhos e conversas, que me ajudam a levar a vida de uma forma mais tranquila e feliz.

À minha família, Patrícia, Fábio, Eduardo, Mi, André, Mônica, Keli, Ed, Vó Jô, Marie e Cloe, que aceitaram o meu caminho e sempre se fizeram presentes, apesar da distância. Agradeço aos vídeos, às fotos, às ligações, aos mimos e por toda torcida. Não é fácil viver longe, mas eles sempre fizeram ser o mais fácil possível.

À minha “dupla” da faculdade, Ana, Clara, Gabi, Júlia, Luiza, Manu, Paola, Paula e Vitória, por serem as melhores amigas que alguém poderia ter. Graças a nossa força e união conquistamos e iremos conquistar grandiosidades nessa vida, unidas desde a primeira fase e juntas até o fim (da vida!).

Ao meu amigo Caio, que esteve presente todos os dias nessa reta final do curso e que me ajudou a acreditar e que me deu forças, tornando os dias mais leves e as caronas cheias de música e risadas, e, também, à Gi, por terem me acolhido em sua casa para me fazer jantares gostosas nos dias mais difíceis.

Aos meus colegas de trabalho, Amanda, Júlia, Vini, Caio, João, Anderson, Ricardo, Luiz, Gustavo e Maria Emília, por terem feito os dias mais felizes e me aconselharem por esse caminho da vida. Agradeço à Amanda, Vini, Júlia e Caio por entenderem essa fase de tensão e sempre conversarem comigo para me acalmar e fazer acreditar; ao Anderson por todas as dicas

de temas e de como elaborar um TCC; e ao Luiz, que me ensinou tanto sobre português, escrita e sempre me incentivou a estudar e acreditar no meu potencial.

Ao Martin, que está ao meu lado desde os dois anos de idade e que ficou em casa neste último mês, por tornar os dias mais leves e engraçados e por sempre insistir para que jantássemos como uma família feliz.

Um especial agradecimento à minha orientadora, Professora Carolina Bahia. Não só pela orientação neste trabalho, mas pela orientação que vem me dando desde a segunda fase de minha graduação. Aos nossos tempos de Revista Avant, como editora-membro, coordenadora de grupo, subeditora e editora-chefe e bolsista de extensão, de Revista Sequência, como Professora de Direito Civil e, agora, orientadora de TCC. Obrigada por me ajudar a ser uma pessoa, uma estudante e uma profissional melhor e por ter sempre me dito que ia ficar tudo bem e me fazer acreditar em meu potencial.

Ao Caio Eduardo Dias, que, desde o momento em que falei meu tema a ele, acreditou na minha capacidade de realizar a presente pesquisa, sempre com palavras de empolgação e encorajamento, que me deram energia para chegar até aqui.

Gostaria de agradecer também aos presentes na Banca de Defesa deste trabalho, Professora Carolina Bahia, Carlos Mendes da Silveira Cunha e Paulo Vitor Petris Tambosi, por terem se interessado na pesquisa e por se disporem a me auxiliar na sua correção e melhora.

Por fim, um especial muito obrigada à Universidade Federal de Santa Catarina, que me acolheu e que foi um lar por esses cinco anos de graduação, onde me desenvolvi de tantas maneiras, no encontro de pessoas e Professores tão admiráveis, grupos de estudo e de pesquisa engrandecedores e aulas de diversos centros que moldaram a pessoa que sou hoje e que só aumentou o meu amor pelo estudo e a vontade de conquistar o meu mundo.

Eu termino este agradecimento com muito amor no coração, por cada pessoa que me transformou de alguma maneira e que me ajudou de tantas formas diferentes, sempre com muito amor e crença na minha pessoa. Sou eternamente grata por cada um de vocês.

RESUMO

A Lei Geral de Proteção de Dados Pessoais deixou de englobar alguns pontos importantes para sua integral compreensão, sendo uma legislação que abrange um tema ainda muito recente no ordenamento jurídico brasileiro. Diante disso, a doutrina e a jurisprudência não possuem um entendimento consolidado acerca de qual teria sido o regime de responsabilidade civil adotado pela Lei. Este, portanto, é o problema que o presente estudo busca analisar: determinar qual o regime adotado pela legislação, a partir da análise de seus artigos e princípios, bem como diante do enfrentamento das teorias apresentadas pelos defensores do regime da responsabilidade civil subjetiva e objetiva. Para a obtenção do resultado almejado, utilizou-se o método indutivo e a pesquisa bibliográfica e legislativa, a fim de demonstrar a inovação da Lei ao instaurar o regime de responsabilidade proativa perante o tratamento irregular dos dados pessoais de seus titulares. Conclui-se, desse modo, que para haver a implementação desse novo regime, os agentes de tratamento deverão apresentar uma postura proativa, com medidas e instrumentos aptos à garantia dos direitos dos titulares dos dados, haver orientação por parte da Autoridade Nacional de Proteção de Dados Pessoais e a uniformização jurisprudencial. Por fim, demonstrou-se que sua implementação, diferentemente do que alguns opositores apontam, não será capaz de prejudicar o desenvolvimento econômico e tecnológico e nem a celeridade processual do Poder Judiciário.

Palavras-chave: Lei Geral de Proteção de Dados Pessoais; Responsabilidade Civil; Regime Proativo.

ABSTRACT

The Personal Data Protection Law promoted a very important change in the Brazilian legal system. However, some key points for a full understanding of this law are still missing and can handicap its comprehension. This can lead to a lack of understanding of the doctrine and the jurisprudence regarding the elected civil liability regime by the law. This study aims to analyze the definition of the regime adopted by the legislation, from the parsing of your articles and principles to the confrontation of theories presented by the subjective and objective civil liability's defenders. In order to do so, bibliographic and legislative research was conducted to make evident the law's innovation by introducing the proactive liability regime towards the holders' personal data irregular treatment. In conclusion, the data protection agents must take a proactive attitude with measures and devices able to guarantee the personal data holders' rights, by means of a Personal Data's Protection National Authorities orientation and jurisprudential uniformity. Ultimately, this study shines a light on the discussion weather the new regime's implementation will harm the economic and technological development and the Judiciary's procedural celerity, making clear that actions are needed to mitigate the dangers regarding the law.

Keywords: Personal Data Protection Law; civil liability; proactive regime.

LISTA DE ABREVIATURAS E SIGLAS

ANPD: Autoridade Nacional de Proteção de Dados Pessoais

CDC: Código de Defesa do Consumidor

CFOAB: Conselho Federal da Ordem dos Advogados do Brasil

GDPR: Regulamento Geral de Proteção de Dados Pessoais Europeu

HC: *Habeas Corpus*

IBGE: Instituto Brasileiro de Geografia e Estatística

ICO: *Information Commissioner Officer*

LGPD: Lei Geral de Proteção de Dados Pessoais

MCI: Marco Civil da Internet

MP: Medida Provisória

OCDE: Organização para a Cooperação e o Desenvolvimento Econômico

PEC: Projeto de Emenda Constitucional

PL: Projeto de Lei

RE: Recurso Extraordinário

RIPD: Relatório de Impacto à Proteção dos Dados Pessoais

STF: Supremo Tribunal Federal

UE: União Europeia

SUMÁRIO

1 INTRODUÇÃO	11
2 O DIREITO À PROTEÇÃO DOS DADOS PESSOAIS.....	14
2.1 O ADVENTO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)	16
2.1.1 A influência internacional.....	18
2.1.2 O cenário brasileiro	21
2.2 A PROTEÇÃO DOS DADOS PESSOAIS COMO UM DIREITO FUNDAMENTAL ...	24
2.3 OS FUNDAMENTOS DA DISCIPLINA DA PROTEÇÃO DE DADOS PESSOAIS	27
3 OS PRINCIPAIS SUJEITOS ENVOLVIDOS NO TRATAMENTO DOS DADOS PESSOAIS.....	30
3.1 O DIREITO DO TITULAR DE DADOS	31
3.2 AGENTES DE TRATAMENTO DOS DADOS PESSOAIS.....	36
3.2.1 A boa-fé e os princípios norteadores.....	38
3.2.2 Requisitos para o tratamento dos dados	43
3.2.3 O término do tratamento	48
4 RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO DOS DADOS PESSOAIS.....	51
4.1 A CORRENTE SUBJETIVISTA DA RESPONSABILIDADE CIVIL NA LGPD.....	55
4.2 A CORRENTE OBJETIVISTA DA RESPONSABILIDADE CIVIL NA LGPD	57
4.3 A RESPONSABILIDADE PROATIVA.....	61
5. IMPLEMENTAÇÃO DA RESPONSABILIDADE PROATIVA.....	65
5.1 BOAS PRÁTICAS E GOVERNANÇA.....	67
5.2 A ATUAÇÃO DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS E A UNIFORMIZAÇÃO JURISPRUDENCIAL.....	71
5.3 RELATÓRIO DE IMPACTOS PELOS AGENTES DE TRATAMENTO DE DADOS .	75
5.4 IMPACTOS NO DESENVOLVIMENTO ECONÔMICO E DE NOVAS TECNOLOGIAS	78
6 CONCLUSÃO.....	82
REFERÊNCIAS BIBLIOGRÁFICAS	85

1 INTRODUÇÃO

A coleta e o tratamento de dados pessoais não é algo novo, mas vem crescendo de forma significativa na medida em que há a evolução tecnológica e a intensificação do uso da *internet*. Dessa forma, hoje são atribuídas aplicações que não eram conhecidas no passado e a própria compreensão da personalidade dos indivíduos vem sofrendo mutações.

Os dados pessoais têm o condão de apresentar projeções das personalidades individuais e o seu tratamento, em virtude disso, possui um risco inerente, diante das possíveis falhas de segurança que podem levar à ofensa aos direitos e garantias de seus titulares. Assim, ao mesmo tempo que facilitam o seu tratamento, os meios digitais também aumentam o risco aos titulares dos dados pessoais.

Além da violação da privacidade e do acesso não autorizado a dados pessoais, os titulares de dados ficam sujeitos a danos patrimoniais e morais. Em virtude disso, a Lei não só estabelece medidas de segurança técnicas e administrativas a serem adotadas pelos agentes de tratamento, como dispõe sobre sanções administrativas e responsabilização civil nas hipóteses em que se verificar o tratamento dos dados em desconformidade com a Lei.

Diante desse cenário, a presente pesquisa busca estudar o regime de responsabilidade civil adotado pela Lei Geral de Proteção dos Dados Pessoais (LGPD), no intuito de entender se a Lei instaurou um novo regime, ao impor aos agentes de tratamento de dados a adoção de medidas aptas e capazes de demonstrar o cumprimento da legislação, diante dos riscos inerentes ao tratamento e dos possíveis danos que podem ocorrer em desfavor dos titulares dos dados.

Desse modo, em um primeiro momento será feita uma pesquisa bibliográfica demonstrando o cenário da implementação do direito à proteção dos dados pessoais, analisando a importância da existência de uma legislação específica à sua proteção. Para isso, será explorada a influência internacional e o cenário brasileiro de elaboração das legislações referentes ao tema, bem como o caminho legislativo até o direito à proteção dos dados pessoais alcançar o patamar de direito fundamental no ordenamento jurídico brasileiro.

Continuamente, estudar-se-á os fundamentos da disciplina da proteção dos dados pessoais prevista na Lei Geral de Proteção de Dados Pessoais, para que seja possível compreender o intuito e a abrangência da legislação.

Em seguida, serão observados os principais sujeitos envolvidos no tratamento dos dados pessoais, para que se entenda quem serão os responsáveis em caso de tratamento irregular, bem como quais as figuras indispensáveis à correta observância da legislação.

Para tanto, será examinado quais os direitos dos titulares dos dados previstos na Lei; quem são os agentes de tratamento de dados que irão realizar a atividade de processamento dos dados – com a menção da figura do encarregado de dados e da Autoridade Nacional de Proteção de Dados Pessoais -; e, ao final, para que seja compreendida a abrangência da atividade de tratamento de dados, serão analisadas a boa-fé e os princípios norteadores da sua execução, os seus requisitos e como deverá ocorrer o término do tratamento.

Dessa forma, passar-se-á à análise das discussões doutrinárias existentes acerca do regime de responsabilidade civil escolhido pela Lei Geral de Proteção de Dados Pessoais. Observar-se-á que parte da doutrina entende que impera na Lei o regime da responsabilidade subjetiva e outra parte entende que seria o da responsabilidade objetiva. Entretanto, o presente estudo, por meio da pesquisa bibliográfica e análise dos artigos e princípios previstos na legislação específica, irá averiguar se houve a inauguração de um novo regime de responsabilidade civil.

Serão examinados os artigos 42 a 46 da Lei, os princípios da segurança, da prevenção e, sobretudo, da responsabilização e prestação de contas e a necessidade de constatação, ou não, de culpa do agente de tratamento ou, ainda, se a Lei inaugurou um novo regime de responsabilidade civil diante de incidentes envolvendo os dados pessoais dos titulares.

Por fim, será analisado, a partir da pesquisa bibliográfica e do estudo das disposições legais e da história da responsabilidade civil, a viabilidade do regime de responsabilidade civil adotado pela Lei Geral de Proteção de Dados Pessoais.

Examinar-se-á, portanto, as boas práticas e a governança na atividade de tratamento dos dados; a importância da Autoridade Nacional de Proteção de Dados Pessoais (ANPD), para orientar a sociedade e solucionar lacunas da legislação; a necessidade da uniformização jurisprudencial, para trazer segurança jurídica na solução dos conflitos envolvendo a responsabilidade civil e o direito à proteção dos dados pessoais; e a imprescindibilidade da elaboração do Relatório de Impacto pelos agentes de tratamento de dados como forma de mitigação de riscos e redução das sanções e indenizações em virtude do tratamento irregular ou do descumprimento legal.

Ao final, será realizada uma análise comparativa, para demonstrar que, apesar do que alguns opositores alegam, a aplicação a responsabilidade civil prevista na Lei Geral de Proteção de Dados não inibirá o desenvolvimento econômico e tecnológico e não terá o condão de obstruir o judiciário, mas haverá a garantia do direito à proteção dos dados pessoais dos titulares de dados, que não deve ser visto com um *status* inferior ao desenvolvimento econômico e tecnológico.

Dessa forma, o presente estudo foi realizado pelo método de abordagem indutiva, por meio de pesquisa qualitativa, exploratória, bibliográfica e legislativa visto que foram analisadas as teorias de responsabilidade civil existentes e defendidas por parte da doutrina e os artigos e os princípios previstos na legislação da proteção dados para chegar a uma conclusão sobre a necessidade do abandono da análise binária do regime jurídico de responsabilidade civil e a implementação de um novo regime instaurado pela Lei Geral de Proteção de Dados.

2 O DIREITO À PROTEÇÃO DOS DADOS PESSOAIS

O direito à proteção dos dados pessoais tem ocupado cada vez mais o debate público, à medida que as tecnologias da informação se desenvolvem e se tornam mais complexas, com um significativo aumento no volume dos dados pessoais que circulam o meio digital (CZYMMECK, 2019, p. 8). A coleta dos dados pessoais não é algo novo, a humanidade sempre coletou, registrou e manipulou dados, contudo, hoje em dia essas atividades ocorrem de maneira muito mais eficiente, veloz e volumosa, permitindo que a eles sejam atribuídas aplicações não antes imagináveis, que, sem uma legislação específica, vinham sendo realizadas sem limites (FRAZÃO, 2019, p. 10).

A Revista *The Economist*, em 6 de maio de 2017¹, apontou os dados pessoais como os principais recursos econômicos da época, por serem insumos essenciais a praticamente todas as atividades econômicas, além de representarem a esfera individual dos cidadãos e a reestruturarem relações sociais e políticas (FRAZÃO, 2019, p. 10). A própria compreensão da personalidade humana sofreu grandes mutações diante do conjunto de dados que formam projeções das personalidades individuais no plano virtual (BASAN; FALEIROS JÚNIOR, 2020, p. 136). Dessa forma, as instituições utilizam o processamento dos dados pessoais de forma a criar um perfil comportamental dos indivíduos, controlar e decodificar comportamentos (NOGAROLI; PAVAN, 2021, pp. 130-131).

Os dados pessoais, ao serem manipulados, alcançam o limiar da cognição e passam a ser uma extensão do titular a que se referem, ultrapassando a seara da privacidade e chegando a atingir outros direitos da personalidade e a própria democracia (GONDIM, 2021, p. 3). A sociedade contemporânea encara um novo estágio de desenvolvimento econômico e tecnológico, marcado pela propulsão de uma nova indústria de geração de valor, cuja matéria prima essencial advém do tratamento dos dados pessoais, disseminada em escala mundial por meio da *internet* (BARRETO JÚNIOR; NASPOLINI, 2019, p. 139).

A história é marcada por inúmeras experiências e avanços para obtenção, coleta, registro e acesso a dados (FRAZÃO, 2019, p. 10), o cenário legal pátrio desde 2014 já contava com uma importante moldura da tutela dos direitos humanos, do desenvolvimento da privacidade e do exercício da cidadania, por meio do Marco Civil da Internet (MCI), Lei 12.

¹ *THE ECONOMIST* (Londres). ***The world's most valuable resource is no longer oil, but data: the data economy demands a new approach to antitrust rules. The data economy demands a new approach to antitrust rules.*** 2017. Disponível em: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em: 12 jun. 2022.

965 (PERILLI, 2020, p. 192). Entretanto, as definições tradicionais jurídico-institucionais que dizem respeito à privacidade e à intimidade passaram a ser inadequadas diante dos atuais desafios de processamento de dados pessoais (MORAES; QUEIROZ, 2019, p. 119).

Com o amadurecimento do conceito da privacidade, esta passou a ser compreendida em um contexto mais alargado (MALDONADO, 2020, p. 242) e girar em torno de questões relacionadas aos dados pessoais, pelo fato de uma considerável parcela das liberdades individuais hoje serem exercidas por novos métodos, algoritmos e técnicas (DONEDA, 2019, p. 266). A proteção dos dados pessoais, desse modo, propõe o tema da privacidade, mas modifica os seus elementos, uma vez que aprofunda os seus postulados (DONEDA, 2019, p. 280).

O que se vislumbrou é que as garantias pensadas a partir do tradicional perspectiva do direito à privacidade são insuficientes no atual cenário da sociedade da informação, sendo necessário prover novas garantias, com especificidades e princípios próprios (MULHOLLAND; FRAJHOF, 2020, p. 11). O tratamento dos dados pessoais trouxe consigo uma série de falhas de segurança que permite que terceiros colem e usem tais dados para as mais distintas finalidades, atingindo um número crescente de indivíduos (SOUZA *et al.*, 2020, p. 44).

Tais incidentes envolvendo dados pessoais, como o vazamento e o compartilhamento de dados, não são incomuns (SANTOS *et al.*, 2021, p. 3), eles ocorrem quando um terceiro não autorizado obtém acesso a sistemas e bancos de dados de uma instituição, que pode ensejar danos a seus titulares (ARAÚJO; FIQUEIREDO, 2020, p. 340), como perda de controle dos dados, limitação a direitos, discriminação, roubo ou fraude de identidade, perda financeira, perda de sigilo, dentre tantas outras desvantagens (UNIÃO EUROPEIA, 2016). Observa-se que, ao mesmo tempo em que os meios digitais facilitaram a comunicação e o intercâmbio dos dados pessoais, também levaram a um aumento no risco aos seus titulares (KLEE; PEREIRA NETO, 2019, p. 15).

Isto é, a ampliação dos horizontes e das possibilidades que se vislumbram a partir do desenvolvimento das novas tecnologias trouxe consigo novos ricos, complexidades e desafios à regulação jurídica desses fenômenos (MENDES *et al.*, 2020, p. 23). Nesse contexto, passa-se a falar do impacto e da mudança na forma de interagir nas relações sociais, profissionais e comerciais, de maneira a identificar o impacto que o tratamento de dados pessoais possui na sociedade atual (SLEIMAN, 2021, p. 16).

Assim, tornou-se necessária a reflexão sobre como se adaptar a esse novo cenário sem, em contrapartida, obstruir o avanço econômico e tecnológico, desde a criação de novos modelos

de negócios até o aperfeiçoamento de políticas públicas ou sua utilização para fins humanitários (MENDES *et al.*, 2020, p. 23). Nesse cenário, a disciplina da proteção de dados pessoais adentrou vigorosamente a agenda nacional e internacional; o desenvolvimento de novos paradigmas econômicos e sociais centrados no uso massivo de dados pessoais demonstra a necessidade e a urgência de equilibrar o seu potencial disruptivo e inovador com os direitos e as legítimas expectativas dos cidadãos quanto ao controle, à adequação e à segurança do fluxo de suas informações pessoais (BIONI, 2021, p. 23).

Desse modo, é imprescindível que o ordenamento jurídico ofereça instrumentos que assegurem a fruição das novas vantagens proporcionadas pelas tecnologias de forma proporcional à manutenção da expectativa dos titulares referente a segurança de seus dados pessoais (DONEDA, 2009, p. 87). Ao analisar-se as relações contratuais na sociedade atual, há a necessidade de se partir da premissa de que há uma reinvenção da proteção de dados pessoais, uma vez que se trata de uma ferramenta essencial para o livre desenvolvimento da personalidade humana (NOGAROLI; PAVAN, 2021, p. 135).

Os avanços tecnológicos forçam o sistema jurídico a encontrar novas estruturas normativas para lidar com os riscos e com as oportunidades oferecidas por tais inovações (LEONARDI, 2011, p. 27). Desse modo, a *internet*, ao contrário de outras tecnologias, desafia de modo único a capacidade de controle por parte dos Estados (LEONARDI, 2011, p. 32). A principal dificuldade, portanto, é oferecer soluções eficientes para os problemas que se apresentam (LEONARDI, 2011, p. 39) e as respostas jurídicas poderão ser a responsabilização administrativa, civil ou penal do agente de tratamento dos dados (GONDIM, 2021, p. 2).

2.1 O ADVENTO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Em agosto de 2018 foi sancionada no Brasil a Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, o novo marco legal brasileiro que trata da proteção dos dados pessoais; é uma legislação extremamente técnica, que traz princípios, direitos e obrigações relacionadas ao uso dos dados pessoais, um dos ativos mais valiosos da sociedade digital (PINHEIRO, 2021, p. 19).

Em suma, a Lei determina os fundamentos da disciplina da proteção dos dados pessoais; delimita importantes conceitos necessários à sua compreensão; os princípios a serem observados; e possui capítulos sobre o tratamento dos dados pessoais; os direitos dos titulares de dados; o tratamento pelo Poder Público; a transferência internacional de dados; os agentes

de tratamento; segurança e boas práticas; fiscalização das atividades que envolvem o processamento dos dados; e a respeito da Autoridade Nacional de Proteção de Dados Pessoais e do Conselho Nacional de Proteção de Dados Pessoais, que serão analisados mais profundamente no decorrer do presente estudo.

A Lei aplica-se a qualquer operação de tratamento de dados realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou de onde estejam localizados os dados, desde que a operação de tratamento seja realizada em território nacional; que a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou que os dados pessoais objetos do tratamento tenham sido coletados em território nacional (art. 3º, I a III, LGPD), ou seja, os dados pessoais do titular que se encontre no país no momento da coleta (KLEE; PEREIRA NETO, 2019, p. 18).

Em contrapartida, a Lei não se aplica ao tratamento de dados pessoais realizados por pessoa natural para fins exclusivamente particulares e não econômicos e realizados para fins exclusivamente jornalístico e artísticos; ou acadêmicos; para fins exclusivos de segurança pública; defesa nacional; segurança do Estado; atividades de investigação e repressão de infrações penais; ou provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na LGPD (art. 4º, I a IV, LGPD).

A aplicação da Lei, como se vê, dá-se inclusive quando os dados estão localizados em território diverso do brasileiro, fora de sua atuação direta como Estado soberano, todavia, a sua aplicação legal não é incondicionada, mas deve obedecer aos requisitos de seu art. 3º, incisos I a III (BRANCO, 2020, p. 19). É possível observar que nas três hipóteses o tratamento ou foi realizado no Brasil, ou os indivíduos cujos dados são tratados estão no Brasil, ou os dados foram coletados no mesmo país, isto é, há uma conexão com a ideia do território brasileiro, porém, existe uma expansão da aplicação da Lei para além das fronteiras do Estado, independentemente da nacionalidade dos envolvidos (BRANCO, 2020, p. 19).

A legislação proporciona aos titulares garantias em relação ao uso de seus dados por meio de princípios, direitos e mecanismos de tutela idealizados tanto para a proteção do cidadão quanto para que o mercado e o setor público possam tratar as informações pessoais dentro dos parâmetros e dos limites de sua utilização (MENDES; DONEDA, 2018, p. 566). A necessidade de uma lei específica sobre a proteção de dados pessoais decorre da forma em que vem sendo

sustentado o modelo atual de negócios na sociedade digital, na qual os dados passaram a ser a principal moeda de troca dos usuários para ter acesso a determinados bens, serviços e conveniências (PINHEIRO, 2021, p. 48).

Trata-se de uma legislação principiológica, com uma forma mais objetiva de se tratar um tema que necessita de uma aplicação procedimental dentro dos modelos de negócios das estruturas empresariais, que dependem da orientação da Autoridade Nacional de Proteção de Dados, órgão da administração pública federal, criada com a função de executar as adequações necessárias para garantir a aderência da legislação (PINHEIRO, 2021, p. 57).

O advento da LGPD é um marco no Brasil por consolidar, em uma legislação única e harmônica, uma matéria que vinha sendo tratada de forma fragmentada e assistemática; a Lei tem como uma de suas principais contribuições introduzir no ordenamento um nível mais elevado de segurança jurídica, ao estabelecer balizas e regras mais claras sobre o tema (BIONI, 2021, p. 24). Para compreendê-la, é imprescindível analisar o contexto histórico e cronológico da sua regulamentação tanto no Brasil quanto em virtude das influências internacionais que a moldaram.

A Lei foi promulgada pelo presidente Michel Temer, originária do Projeto de Lei Complementar nº 53/2018, e dialoga com as demais fontes normativas do ordenamento jurídico brasileiro, quais sejam, o Código Civil, o Código de Defesa do Consumidor, o Marco Civil da Internet, a Lei do Cadastro Positivo e a Lei do Acesso à Informação, uma vez que todas asseguram direitos relacionados à proteção de dados e à privacidade, e vem para modernizar o tratamento de tais informações no Brasil (KLEE; PEREIRA NETO, 2019, p. 14). Entretanto, a disciplina jurídica da proteção de dados pessoais vem sendo construída há, pelo menos, cinco décadas (DONEDA, 2021, pp. 36).

2.1.1 A influência internacional

O primeiro diploma normativo que tratou especificamente dessa matéria foi a Lei de Proteção de Dados do Estado de Hesse, na Alemanha, que entrou em vigor em 1970 (DONEDA, 2021, pp. 36). Nessa época, houve a formação de blocos econômicos regionais, que estimularam o compartilhamento dos dados pessoais, o que fez crescer a preocupação com a proteção da privacidade dos indivíduos, e a legislação veio para preservar esse fluxo de dados pessoais capaz de sustentar o livre comércio internacional (VAINZOF, 2049, pp. 24-25).

Com o passar do tempo, os contornos do que passou a se entender por proteção de dados pessoais tornaram-se muito mais concretos do que costumavam ser, não obstante, os seus principais institutos e ferramentas ainda fazem parte da maioria das legislações de proteção de dados mundiais, proporcionando-lhes uma gramática e estruturas assemelhadas, estabelecendo mecanismos que procuram mitigar os riscos decorrentes de seu tratamento (DONEDA, 2021, p. 36).

O aumento exponencial no volume, intensidade e complexidade no tratamento dos dados pessoais faz com que a sua disciplina venha incorporando novos elementos, com o objetivo de garantir a tutela jurídica integral do titular dos dados, por meio do fortalecimento dos instrumentos de garantias individuais e coletivas (DONEDA, 2021, p. 37). O desenvolvimento econômico e tecnológico, principalmente ocorrido na Europa e nos Estados Unidos, proporcionou condições para que fossem estabelecidos instrumentos regulatórios e jurídicos acerca da disciplina da proteção dos dados pessoais (DONEDA, 2021, p. 39), que passou a influenciar os demais países que buscavam se relacionar com esses Estados.

Com efeito, a partir da legislação de Hesse, outras nasceram na Europa na década de 1970, como a pioneira Lei sueca de proteção de dados, *Datalagen*, de 1973, e a lei francesa de proteção de dados pessoais de 1978, *Informatique et Libertés* (DONEDA, 2021, p. 44). Tais leis propunham-se a regular um cenário no qual centros de tratamento de dados de grande porte concentravam a coleta e a gestão dos dados pessoais e tratavam sobre a concessão de autorizações para a criação de bancos de dados e de seu controle *a posteriori* pelos órgãos públicos (SAMPAIO, 1997, p. 490).

Porém, essas legislações não demoraram muito para se tornarem ultrapassadas diante da multiplicação dos centros de processamento de dados, que dificultou o controle baseado em um regime rígido de autorizações e que demandava um minucioso acompanhamento. (DONEDA, 2019, pp. 175-176). A partir da década de 1980, buscou-se sofisticar a tutela dos dados pessoais, com a preocupação não só perante a liberdade de fornecer ou não os seus dados pessoais, mas em garantir a sua efetividade; procurava-se, portanto, fazer com que o titular dos dados participasse consciente e ativamente das fases sucessivas do processo de tratamento (DONEDA, 2019, p. 178).

No entanto, percebeu-se que não seria a maioria das pessoas que estaria disposta a exercitar essas prerrogativas de autodeterminação informativa, uma vez que os custos envolvidos, fossem eles econômicos ou sociais, geralmente as compeliavam a aquiescer com situações que não eram as ideais (DONEDA, 2019, p. 178). Já a partir da década seguinte, as leis passaram a buscar suprir as desvantagens do enfoque individual existente até então e houve

a criação de instrumentos que buscavam elevar o padrão coletivo de proteção, voltado para a busca de resultados concretos, procurando fortalecer a posição do titular em relação às entidades que tratavam os seus dados, reconhecendo o desequilíbrio inerente à relação (DONEDA, 2019, p. 179).

A partir dos anos 1990, com o desenvolvimento do modelo de negócios da economia digital, que possui uma dependência muito maior dos fluxos internacionais das bases de dados, viabilizados pelos avanços tecnológicos e pela globalização, inspirou-se o surgimento de regulamentações de proteção de dados pessoais de forma mais consistente (PINHEIRO, 2021, p. 23).

Esse debate teve início na União Europeia (UE) e consolidou-se com a promulgação do Regulamento Geral de Proteção de Dados Pessoais Europeu nº 679 (GDPR), aprovado em 27 de abril de 2016, que passou a exigir que os demais países e empresas que buscassem manter relações comerciais com esses países deveriam ter uma legislação de mesmo nível (PINHEIRO, 2021, p. 24).

Em 1995, na União Europeia, foi adotada a Diretiva 95/46/CE, relativa à proteção das pessoas no que diz respeito ao tratamento dos dados pessoais e à sua livre circulação, que veio a ser substituída pelo Regulamento Geral de Proteção de Dados Europeu em 2016, contemplada pelo pressuposto de que o mercado de dados possui a facilidade de superar fronteiras e o encadeamento de atividades concernentes à exploração desse novo ativo econômico (OLIVEIRA, 2019, p. 13).

Nessa toada, o Estado que não possuísse uma legislação de mesmo nível poderia passar a sofrer dificuldades econômicas e impasses na consolidação de negócios com esses países, além de ser um dos requisitos para o ingresso na Organização para a Cooperação e o Desenvolvimento Econômico (OCDE), o que poderia vir a afetar econômica e significativamente o Brasil (PINHEIRO, 2019, p. 318).

O GDPR é considerado um marco em diversos países que o utilizaram como base para a elaboração de suas próprias legislações (BACHA, 2021, p. 58). O seu maior propósito foi a aplicação coerente e homogênea da proteção dos dados pessoais no âmbito da União Europeia, evitando-se, assim, que as diferentes legislações freassem a circulação dos dados entre os países-membros, ao mesmo tempo que garantissem segurança jurídica e transparência aos agentes de tratamento e aos titulares de dados (BACHA, 2021, p. 59).

O processo de revisão, compilação, uniformização e atualização das normativas dos estados-membros até então vigentes iniciou-se em 2012, decorrendo-se quatro anos até chegar ao texto consolidado em 2016, e entrou em vigor em 25 de maio de 2018 (LINKE, 2019, p.

126). A consequência disso é que não apenas os cidadãos residentes na União Europeia que são protegidos pelas disposições previstas no Regulamento, mas qualquer sujeito, independentemente de sua nacionalidade ou território, sendo vedada a transferência internacional de dados a países que não se adequam aos parâmetros mínimos de proteção exigidos pela norma (LINKE, 2019, p. 130).

A importância do GDPR decorre da garantia de que os cidadãos possam exercer o controle sobre os seus próprios dados, representando um significativo avanço no âmbito do direito à proteção dos dados pessoais e da própria personalidade de seus titulares, além de apresentar a proteção dos dados pessoais como um direito fundamental (BACHA, 2021, p. 60).

O GDPR, portanto, demonstra a necessidade dos agentes de tratamento adotarem medidas em conformidade com a Lei, transparecendo a natureza, o contexto e as finalidades do tratamento, os riscos aos titulares, que deverão ser avaliados de maneira a determinar o grau de risco das operações, a probabilidade da ocorrência e as medidas aplicáveis à sua mitigação; além disso, o tratamento somente será considerado legítimo quando realizado de acordo com os fundamentos previstos na legislação (BACHA, 2021, p. 60). Diante desse cenário, foi elaborada a regulamentação da proteção de dados no Brasil, que não somente foi acelerada pela entrada em vigor do GDPR em 2018, como o utilizou de base à sua estruturação.

2.1.2 O cenário brasileiro

O primeiro movimento legislativo brasileiro que fez referência direta às legislações sobre proteção de dados pessoais foi o Projeto de Lei nº 2.796 de 1980, de autoria da Deputada Cristina Tavares, que assegurou aos cidadãos acesso às suas informações constantes em bancos de dados, que acabou sendo arquivado sem publicação (DONEDA, 2021, p 48). Com a intensificação da demanda por direitos à proteção de dados, as legislações dos Estados de São Paulo e Rio de Janeiro, no final da década de 1980, adquiriram normas sobre o direito de acesso e retificação dos dados pessoais, com a previsão dos princípios da finalidade e do consentimento informado (DONEDA, 2021, p 48).

Em 1988, alcançou-se a presença do *habeas data* na Constituição da República Federativa do Brasil, desenvolvido ainda na fase do processo constituinte, sendo a Constituição Federal pioneira na sua contemplação (BIONI, 2021, p. 23):

Art. 5º, LXXII - conceder-se-á *habeas data*:

- a) para assegurar o conhecimento de **informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados** de entidades governamentais ou de caráter público;
- b) para a **retificação de dados**, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo (BRASIL, 1998) (Grifo nosso).

O referido instrumento processual tem a finalidade de garantir que a pessoa física ou jurídica tenha acesso ou promova a retificação de suas informações registradas em bancos de dados de órgãos públicos ou instituições similares. Nos termos do voto do Ministro Gilmar Mendes no julgamento do Recurso Extraordinário nº 673.707:

Parece-me, digna de nota, desde logo, a ideia de que, no plano processual, nós temos o *habeas data* com o propósito, o intento de tutelar aquilo que entendemos ser uma **proteção da autonomia privada nesse âmbito da autodeterminação sobre os dados, que ganha cada vez mais importância, na medida em que temos toda essa ampla evolução tecnológica**. (BRASIL, 2015, p. 35) (Grifo nosso).

Assim, o tema da proteção dos dados pessoais foi se fazendo presente no debate político. O Código de Defesa do Consumidor (CDC), Lei nº 8.078 de 1990, acabou concentrado um volume considerável de demandas relacionadas aos dados pessoais (DONEDA, 2021, p. 50). O seu artigo 43, por exemplo, que se aplica aos bancos de dados de proteção ao crédito, é largamente utilizado de forma a consolidar o direito do consumidor sobre seus dados pessoais, que acabou fomentando o debate acerca do registro de dados sobre operações financeiras do consumidor, que canalizou à elaboração legislativa da Lei do Cadastro Positivo, Lei nº 12.414 de 2011, com a presença de conceitos como dados sensíveis e dos princípios da finalidade, transparência, minimização e segurança (DONEDA, 2021, p. 51).

Ademais, a Lei 12.527 de 2011, Lei de Acesso à Informação, por sua vez, definiu o que é a informação pessoal e regulamentou o princípio da transparência (DONEDA, 2021, p. 52). Em 2014, o Marco Civil da Internet (MCI), Lei nº 12.965, implementou direitos e procedimentos relacionados ao uso de dados pessoais dos usuários da *internet*, que passou a elencar em seu rol o princípio da proteção dos dados pessoais (DONEDA, 2021, p. 52).

A proposta do MCI foi estabelecer linhas gerais ao uso da *internet* no Brasil, deixando alguns temas a serem desenvolvidos posteriormente, com o objetivo de não ser uma legislação sensível aos avanços tecnológicos, o que poderia levar à sua defasagem (BRANDÃO, 2019, p. 37). Algumas matérias acabaram sendo reguladas pelo Decreto nº 8.771 de 2016, como obrigações e responsabilidades acerca da segurança da informação, além de haver inaugurado previsões sobre a proteção dos dados pessoais (BRANDÃO, 2019, p. 44).

No Brasil, portanto, já haviam estipulações sobre a proteção dos dados pessoais, mas a questão ainda estava sendo vista de maneira difusa (PINHEIRO, 2021, p. 25). O debate legislativo em torno desse assunto, no intuito de criar uma norma que reunisse a matéria em um

único texto, teve início em 2010, com a propositura pelo Ministério da Justiça de um texto-base do Anteprojeto de Lei sobre proteção de dados, texto este que, após sucessivas modificações e seu respectivo *iter* legislativo, veio a se tornar a LGPD (BIONI, 2021, p. 25).

A matéria começou a ganhar escala e, em 2016, a Presidência da República enviou o Anteprojeto, com aprimorações, ao Congresso Nacional; em agosto de 2018 a Lei foi sancionada, mas passou por algumas dilações em sua *vacatio legis*: alguns dispositivos da Lei entraram em vigor em 28 de dezembro de 2018, já outros, com o advento da MP nº 869/2018, que veio a se converter na Lei 13.853/2019, tiveram sua vigência alterada para 14 de agosto de 2020 (BIONI, 2021, p. 25).

Explica-se, quando da publicação da Lei nº 13.709/2018, a Presidência da República vetou os dispositivos que dispunham sobre a criação da ANPD e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; com a conversão da MP nº 869/2018 na Lei 13.853/2019, houve a inclusão dos artigos 55-A a 55-L, 58-A e 58-B, para dispor sobre a criação da Autoridade Nacional e a composição de seu Conselho (KLEE; PEREIRA NETO, 2019, p. 13).

O prazo inicial que havia sido estabelecido para a adaptação à Lei foi de 18 meses e a MP nº 869/2018 ampliou-o em mais seis, totalizando em 24 meses (PINHEIRO, 2021, pp. 19). Entretanto, devido à pandemia da covid-19, a Lei entrou em vigor somente em setembro de 2020, com a aprovação da Medida Provisória nº 959 em 29 de abril de 2020, que deixou de produzir efeitos com a publicação da Lei nº 14.058 de 2020 e, posteriormente, com a aprovação do PL nº 1.179 de 2020, que foi convertido na Lei nº 14.010 de 2020, prorrogou a aplicação das multas previstas para 1º de agosto de 2021, por meio da alteração de seu artigo 65 (PINHEIRO, 2021, p. 20).

Recentemente, em 14 de junho de 2022, foi publicada no Diário Oficial da União a Medida Provisória nº 1.124, que transformou a Autoridade Nacional de Proteção de Dados em uma autarquia de natureza especial, deixando de ser um órgão da Administração Pública e Federal integrante da Presidência da República, e criou um cargo comissionado de diretor-presidente, sem aumento de despesas (BRASIL, 2022).

Tal mudança estava prevista no artigo 55-A da Lei, que foi vetado em virtude da MP, passando a caracterizá-la como uma “autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal” (BRASIL, 2022), contudo, sua estrutura organizacional e competências continuaram as mesmas (PINCER, 2022). A MP já entrou em vigor, mas, para continuar assim, precisa do aval dos plenários da Câmara dos Deputados e do Senado Federal (PINCER, 2022), sendo que o prazo para

deliberação se encerra em 25 de agosto de 2022, podendo ser prorrogada por mais sessenta dias (BRASIL, 2022).

Dessa forma, a legislação foi dividida em 65 artigos, 10 capítulos e é mais enxuta que o GDPR, sendo que, em alguns aspectos, deixou margem para uma interpretação mais ampla e trouxe alguns pontos de insegurança jurídica, por permitir espaço à subjetividade (PINHEIRO, 2021, p. 27). Por certo, há a possibilidade de fiscalização por meio dos agentes legitimados, como o Ministério Público, mas a centralização do diálogo em um único órgão fiscalizador facilitará os avanços na implementação das novas exigências e garantirá o cumprimento e o melhor proveito da regulamentação (PINHEIRO, 2021, pp. 28-29).

2.2 A PROTEÇÃO DOS DADOS PESSOAIS COMO UM DIREITO FUNDAMENTAL

Com a entrada em vigor da LGPD, a proteção dos dados pessoais alcançou uma posição inédita no âmbito da sociedade tecnológica, contudo, para que houvesse o reconhecimento mundial de um direito humano e fundamental à proteção de dados pessoais, transcorreu-se certo tempo, iniciando-se, em especial, a partir da década de 1980 (SARLET, 2020, p. 2).

Em 1981, na Convenção de Estrasburgo nº 108, a respeito da proteção dos indivíduos no processamento automatizado dos dados pessoais, e no ano de 2000, na Carta de Direitos Fundamentais da União Europeia, o direito à proteção de dados alçou à condição de direito fundamental, de natureza autônoma, entrando em vigor com o Tratado de Lisboa em 2009 aos estados integrantes (SARLET, 2020, p. 5).

No dia 7 de maio de 2020, o Supremo Tribunal Federal (STF) proferiu uma decisão histórica com relação à proteção dos dados pessoais, por meio de uma maioria de 10 votos favoráveis, em que o Plenário referendou medida cautelar concedida pela relatora da Ação Direta de Inconstitucionalidade nº 6.387, Ministra Rosa Weber, proposta pelo Conselho Federal da Ordem dos Advogados do Brasil (CFOAB), para suspender a eficácia da MP nº 954 de 2020 que, em seu art. 2º, *caput*, estipulava que as empresas de telecomunicações deveriam compartilhar dados de seus consumidores com o Instituto Brasileiro de Geografia e Estatística (IBGE) (MENDES *et al.*, 2021, p. 141).

A decisão abrangeu o argumento de que tal medida representaria uma restrição constitucionalmente ilegítima dos direitos à privacidade, intimidade e sigilo dos dados pessoais; em antecipação ao voto, o Ministro Luiz Fux pronunciou-se nos seguintes termos:

De sorte que eu lavro uma ementa concordando inteiramente com o brilhante voto da Ministra Rosa Weber, que foi cirúrgica num momento tão complexo para fazer esse cotejo entre essa liberdade de informação que municia a estatística e, de outro lado, a privacidade pessoal, para, concordando com Sua Excelência, reitero, a Ministra Rosa Weber, assentar, em primeiro lugar, que **a proteção de dados pessoais e autodeterminação informativa são direitos fundamentais autônomos extraídos da garantia da inviolabilidade da intimidade e da vida privada e, conseqüentemente, do princípio da dignidade da pessoa humana** [...], porque essa Lei define princípios e procedimentos para o tratamento dos dados e também critérios de responsabilização dos agentes por eventuais danos ocorridos em virtude desse tratamento, muito embora, sincera e honestamente, essa responsabilidade *ex post facto* não vai afastar a ameaça de lesão, risco que também foi muito bem assentado pelo Ministro Luís Roberto Barroso. **Nós temos ilícitos de lesão, que vão ocorrer quando esses dados forem compartilhados, mas há o ilícito de perigo. E o ilícito de perigo se coíbe com uma tutela inibitória, proibindo-se que haja uma atitude que possa levar à consumação de um dano.** [...] Reitero aqui, a partir da liminar da Ministra Rosa Weber, que as leis que tratam da coleta e processamento de dados devem atender a propósitos legítimos, específicos, explícitos e informados, limitar a coleta ao mínimo necessário para a realização de suas finalidades normativas – o que não ocorre com essa medida provisória -, **prever medidas técnicas e administrativas de segurança aptas a proteger os dados pessoais e prevenir a ocorrência de danos.** [...] Exatamente por isso tudo, no meu modo de ver, **a Medida Provisória nº 954/2020 ultrapassa todos os limites fixados pelos direitos fundamentais à proteção de dados, à autodeterminação informativa e à privacidade**, inobservando ainda o postulado da proporcionalidade, mormente porque não delimita o objeto e incorre em excesso ao determinar o compartilhamento de dados de milhões de brasileiros, quando as pesquisas amostrais realizadas pelo IBGE, em geral, envolvem apenas 70 mil pessoas. Então, é absolutamente um tratamento imoderado, irrazoável e que não merece a chancela da Suprema Corte. (BRASIL, 2020) (Grifo nosso).

A decisão trouxe o reconhecimento de um direito fundamental à proteção de dados como um direito autônomo e representou uma evolução em relação à jurisprudência anterior da Suprema Corte, expressa em julgados como o RE nº 418.416-8/SC de 2006 e o HC nº 91.867/PA de 2012 (MENDES *et al.*, 2021, p. 142). O julgado permite identificar que o STF é sensível ao reconhecimento de normas de direito fundamental fora do catálogo específico, a partir do exame da existência de um vínculo, que pode ser evidenciado por considerações de ordem histórica, do bem jurídico protegido com alguns dos valores essenciais ao resguardado da dignidade humana (MENDES, 2019, p. 208).

Pela primeira vez, encontrou-se consenso em torno do conceito de dado pessoal e sobre a sua necessária tutela constitucional, que levou à tramitação do Projeto de Emenda Constitucional (PEC) nº 17 de 2019, de modo a inserir a proteção de dados pessoais no rol dos direitos e garantias fundamentais (MENDES *et al.*, 2021, pp. 152-154). A PEC, de autoria do senador Eduardo Gomes (MDB-TO) e relatada pela Senadora Simone Tebet (MDB-MS), foi aprovada no Senado Federal em julho 2019 e encaminhada à Câmara dos Deputados, que aprovou o texto com mudanças, em 31 de agosto de 2019, e estabeleceu a proteção de dados pessoais como direito individual de forma específica (SENADO FEDERAL, 2021).

Então, a matéria voltou para a análise do Senado, em que foi aprovada pelo Plenário em 20 de outubro de 2021, tornando a proteção dos dados pessoais um direito fundamental, e a PEC foi aprovada de forma unânime, com 64 votos no primeiro turno e 76 no segundo (SENADO FEDERAL, 2021). A Emenda Constitucional nº 115 foi promulgada no dia 10 de fevereiro de 2022, pelo presidente do Congresso Nacional, senador Rodrigo Pacheco (PSD-MG), que incluiu a proteção de dados pessoais entre os direitos e garantias fundamentais na Constituição Federal de 1988:

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
LXXIX - **é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.** (BRASIL, 1988) (Grifo nosso).

A proteção de dados pessoais é fruto da evolução histórica da sociedade e cada vez mais representa riscos às liberdades e garantias individuais dos cidadãos (BRASIL, 2019, p. 4). O avanço da tecnologia oportuniza, por um lado, a racionalização de negócios e da atividade econômica, por outro lado, pode causar prejuízos incomensuráveis aos cidadãos e à própria sociedade, dando margem, inclusive, à concentração de mercados (BRASIL, 2019, p. 5).

O avanço que o direito fundamental apresenta hoje é resultado da afirmação dos direitos fundamentais como núcleo da proteção da dignidade da pessoa humana e da visão de que a Constituição é o local adequado para positivar as normas asseguradoras dessas pretensões (MENDES; BRANCO, 2018, p. 197). Com o avanço tecnológico em uma sociedade cada vez mais conectada, com uma intensa troca de dados, emerge-se a necessidade de adaptação legislativa, para viabilizar a resposta adequada aos desafios da atualidade (MENDES *et al.*, 2021, p. 154).

Com efeito, é fundamental que se reconstruam e se reinterpretem direitos e garantias fundamentais, uma vez que a vitalidade e continuidade das normatizações, em especial, da Constituição Federal, depende da sua capacidade adaptativa às transformações sociais e históricas, protegendo os direitos e as liberdades dos cidadãos (MENDES *et al.*, 2021, p. 155). De acordo com Norberto Bobbio (2004, p. 19), os direitos são produtos históricos que nascem das necessidades da civilização humana e, por isso, são mutáveis e suscetíveis a transformações e ampliações.

A sedimentação dos direitos fundamentais como normas obrigatórias é resultado de maturação histórica, o que permite compreender que os direitos não são sempre os mesmos em todas as épocas e não correspondem a imperativos de coerência lógica (MENDES; BRANCO, 2018, p.198). A visão dos direitos fundamentais em termos de gerações indica o caráter

cumulativo de sua evolução, como frutos de momentos históricos diferentes, e a sua diversidade aponta para a busca de uma base absoluta e válida em todos os tempos (MENDES; BRANCO, 2018, p. 202).

No mundo da inovação disruptiva, as soluções para aumentar a eficácia do direito fundamental à proteção de dados deverão ser criativas, as garantias deverão possuir uma regulamentação técnico-computacional mais rigorosa e as decisões perante os casos concretos precisarão ser explicadas, em linguagem natural, de forma a viabilizar o entendimento e, inclusive, a contestação (CAMARGO, 2021, p. 225). Para isso, os direitos de explicação e revisão deverão estabelecer exigências técnicas quanto à capacidade das próprias aplicações detalharem os motivos que levaram a uma determinada conclusão, sob pena de não cumprimento das obrigações legais, com a necessidade de avanços consistentes no campo normativo (CAMARGO, 2021, p. 226).

A tutela jurídica do direito fundamental à proteção de dados pessoais impõe-se na exata medida em que a informação se tornou a substância essencial da composição de uma nova morfologia estruturante da sociedade (NOGAROLI; PAVAN, 2021, p. 136). Dessa forma, o catálogo dos direitos fundamentais vem-se avolumando conforme as exigências específicas de cada momento histórico, sendo pretensões que se descobrem a partir da perspectiva do valor da dignidade humana (MENDES; BRANCO, 2018, pp. 204-206). Com efeito, a previsão constitucional dos direitos fundamentais influenciará as decisões judiciais que envolvam a temática da proteção de dados daqui em diante, atribuindo também um maior peso à responsabilidade civil dos agentes de tratamento dos dados (TEIXEIRA, 2021, p. 49).

2.3 OS FUNDAMENTOS DA DISCIPLINA DA PROTEÇÃO DE DADOS PESSOAIS

A Lei Geral de Proteção de Dados Pessoais, nos incisos de seu art. 2º, estipulou um rol cumulativo dos fundamentos que devem nortear a aplicação da Lei:

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I - o respeito à privacidade;
II - a autodeterminação informativa;
III - a liberdade de expressão, de informação, de comunicação e de opinião;
IV - a inviolabilidade da intimidade, da honra e da imagem;
V - o desenvolvimento econômico e tecnológico e a inovação;
VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (BRASIL, 2018).

Ao analisar o referido artigo, é possível evidenciar que a Lei se relaciona com o texto constitucional brasileiro, no que concerne ao seu conteúdo, e com o GDPR, uma vez que visa proteger e garantir a privacidade, a liberdade, a segurança, a justiça, a promoção do progresso econômico e social e a garantia da segurança jurídica (PINHEIRO, 2021, pp. 95-96). Dessa forma, além de inovar o ordenamento jurídico brasileiro, a LGPD trouxe os fundamentos legais a explicitar a importância da proteção dos dados pessoais e tecer uma melhor interpretação dos seus dispositivos acerca da realidade multidisciplinar da norma (TEIXEIRA, 2021, p. 16).

Um dos objetivos da Lei, portanto, é a proteção do direito fundamental à privacidade (inciso I), elencando-a como seu primeiro fundamento (SOUZA *et al.*, 2020, p. 47). A necessidade da proteção dos dados pessoais como forma de proteção da privacidade se mostra cada vez mais presente, já que quando são organizados, ordenados e associados são capazes de estabelecer parâmetros fidedignos a identificar e traçar perfis consistentes dos indivíduos (VAINZOF, 2020, p. 28). Com efeito, o intuito da Lei foi preservar a vida privada no cenário do desenvolvimento tecnológico atual, por meio de uma tutela adequada aos titulares dos dados pessoais (SOUZA *et al.*, 2020, p. 49).

Os modelos de negócios atuais são pautados e rentabilizados no tratamento desses dados, não sendo possível que os seus titulares tenham controle sobre todas as entidades que o realizam, justamente por isso que a autodeterminação informativa se apresenta como fundamento da LGPD (inciso II) (VAINZOF, 2020, p. 29). Assim, tendo em vista que os dados se referem à vida do seu titular, este deve saber como serão coletados, com que intuito e quem terá acesso, podendo decidir se permitirá ou não a sua ocorrência (OLIVEIRA, 2019, p. 15). A autodeterminação informativa, portanto, é o controle pessoal sobre o trânsito de dados relativo ao próprio titular e uma extensão das liberdades do indivíduo, que vai além do nível da esfera íntima e atinge emanções de natureza pública dos titulares (VAINZOF, 2020, p. 29).

O inciso III dispõe sobre a liberdade de expressão, de informação, de comunicação e de opinião, uma vez que o uso irregular dos dados pessoais poderá levar à violação desses direitos. Sem comunicação livre, não se pode falar em sociedade livre ou soberania popular, além disso, não somente as manifestações puras de pensamento precisarão estar protegidas, mas também a externalização de gostos, interesses e características do titular, realizadas por algoritmos, mediante o processamento dos dados (VAINZOF, 2020, p. 32).

O que se observa nesse primeiro bloco de fundamentos é a preocupação com a proteção do indivíduo, já os incisos V e VI, demonstram uma preocupação com o livre desenvolvimento do indivíduo na esfera da economia, fazendo referência à livre iniciativa e o fomento econômico do país e devendo ser reconhecida a importância dos avanços tecnológicos para o

desenvolvimento humano e social, ligados aos princípios de ordem econômica presentes na Constituição Federal (OLIVEIRA, 2019, p. 15). Assim, embora seja uma lei reguladora, a LGPD não deverá servir como impeditivo à evolução econômica (TEIXEIRA, 2021, p. 17), em razão da possibilidade de as informações poderem ser absorvidas e tratadas, gerando conhecimento para qualquer pessoa ou entidade aplicar o que considerarem pertinente, por meio de novos modelos de negócios (VAINZOF, 2020, p. 37).

De acordo com a Constituição, a ordem econômica, fundada na valorização do trabalho humano e na livre-iniciativa, tem por fim assegurar a todos a existência digna, motivo pelo qual o tratamento jurídico equilibrado para as atividades desempenhadas no mercado é condição para se evitar a retração da economia pautada em dados (VAINZOF, 2020, pp. 40-41). A lei visa proteger os cidadãos de possíveis abusos do Estado ou de outros cidadãos, em diferentes níveis econômicos, mas também visa proteger os cidadãos no exercício de seu trabalho e no direito de empreender, sob regras, sem sofrer abusos (OLIVEIRA, 2019, p. 15).

O fundamento que resume os anteriores está augurado no último inciso (VII), do artigo 2º, e, por sua vez, estabelece relação direta com os fundamentos da República e introduz os direitos humanos; o desenvolvimento da personalidade; a dignidade; e o exercício da cidadania (OLIVEIRA, 2019, p. 16). Por derradeiro, se a proteção de dados está em voga em todo o mundo, evidente que tais direitos irão fundamentar a legislação, eis que a República Federativa do Brasil ratifica a Declaração Universal dos Direitos Humanos (TEIXEIRA, 2021, pp. 17-18).

Com efeito, a proteção da pessoa humana deve ser entendida como valor máximo do ordenamento jurídico, ao passo que não levar em consideração os novos problemas oriundos da evolução tecnológica de uma sociedade – que influencia na sua experiência científica, política e cultural – significaria abater o direito ao seu próprio tempo, tornando-o obsoleto e incapaz de garantir os preceitos da pessoa com a velocidade característica da evolução tecnológica, o que é fundamental (VAINZOF, 2020, p. 47). Os dados pessoais são informações de cunho íntimo e pessoal, cuja associação à personalidade dos indivíduos pode não apenas o identificar, mas revelar muito a seu respeito, a ponto de poder impactar no seu próprio exercício da cidadania (VAINZOF, 2020, p. 49).

3 OS PRINCIPAIS SUJEITOS EVOLVIDOS NO TRATAMENTO DOS DADOS PESSOAIS

A Lei Geral de Proteção de Dados Pessoais dispõe sobre o tratamento dos dados pessoais por pessoa natural ou jurídica, de direito público ou privado (art. 1º), e aplica-se a qualquer operação de tratamento realizada por pessoa natural ou jurídica, de direito público ou privado (art. 3º). A lei determina que os agentes responsáveis pelo tratamento dos dados pessoais são o controlador e o operador de dados (art. 5º, IX), que irão processar os dados pessoais dos titulares.

Não obstante, é importante mencionar a Autoridade Nacional de Proteção de Dados, órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD (art. 5º, XIX), e o encarregado de dados, que será indicado pelo controlador, como forma de canal de comunicação entre os agentes de tratamento, os titulares de dados e a ANPD (art. 5º, VIII).

O presente estudo irá esmiuçar os direitos dos titulares de dados e a atividade e responsabilização civil dos agentes de tratamento, quais sejam do controlador e do operador. De todo modo, irá mencionar sobre a essencialidade da figura do encarregado de dados e, ao final do estudo, demonstrará a importância da Autoridade Nacional de Proteção de Dados na orientação e implementação da Lei Geral de Proteção de Dados, na busca pela segurança jurídica no ordenamento brasileiro, pela garantia dos direitos dos titulares de dados e pelo desenvolvimento econômico e tecnológico da sociedade.

Com efeito, os agentes de tratamento são o controlador e o operador e o destinatário da Lei é o titular de dados pessoais, entretanto, existem outros partícipes importantes quando da aplicação da legislação, quais sejam o encarregado e a ANPD (BOMFIM; PINHEIRO, 2021, p. 229). O impacto da LGPD, portanto, traz direitos aos titulares e deveres e responsabilidades aos agentes de tratamento, sendo que todos os sujeitos terão que se adaptar a uma nova cultura de tutela dos dados pessoais, cabendo à doutrina, ao judiciário e à Autoridade Nacional de Proteção de Dados harmonizarem a interpretação e aplicação da Lei (TEPEDINO; TEFFÉ, 2019, pp. 166-167).

3.1 O DIREITO DO TITULAR DE DADOS

O direito do titular de dados consiste em um ponto de extrema importância no contexto da proteção dos dados pessoais, uma vez que posiciona o indivíduo a que se referem os dados pessoais objeto do tratamento no centro da tutela jurídica (SANTOS, 2020, p. 52). A Lei Geral de Proteção de Dados surgiu com o objetivo de garantir direitos fundamentais e apresenta uma série de direitos específicos, sendo que o direito à proteção dos dados pessoais é irrenunciável e não pode ser cedido ou transmitido (SANTOS, 2020, p. 53).

Emerge, portanto, a imprescindibilidade da agenda de proteção de dados pessoais para a proteção de diversos direitos e, em específico, o significativo papel que a sistemática dos direitos dos titulares de dados pode representar nesse campo (KORKMAZ; SACRAMENTO, 2021, p. 3). É nessa direção que a LGPD sistematiza, sobretudo em seu capítulo III, as disposições referentes aos “Direitos do titular”, que elencou, de forma expressa, os direitos que são assegurados aos titulares de dados pessoais e que por eles serão exercidos.

De acordo com o artigo 17 da Lei, toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais à liberdade, à intimidade e à privacidade. O titular dos dados pessoais, à vista disso, tem o direito de obter, a qualquer momento e mediante requisição (art. 18):

- I - Confirmação da existência de tratamento;
- II - Acesso aos dados;
- III - Correção de dados incompletos, inexatos ou desatualizados;
- IV - Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
- V - Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
- VI - Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
- VII - Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- VIII - Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- IX - Revogação do consentimento, nos termos do § 5º do art. 8º desta Lei. (BRASIL, 2018).

O artigo 18 elenca os específicos direitos que poderão ser exercidos pelo titular dos dados pessoais. Em linhas gerais, a lei determina que deve ser garantida ao titular a confirmação da existência de tratamento de seus dados pessoais (inciso I) e concedido o acesso facilitado às informações sobre esse tratamento (inciso II), bem como a possibilidade de exigir do agente de tratamento desses dados, a qualquer momento e mediante requisição, os direitos estipulados (SANTOS, 2020, p. 53).

O direito à confirmação da existência do tratamento de dados se apresenta como um primeiro passo para que diversas prerrogativas do titular sejam efetivamente exercidas, sob essa acepção e sem que se exija justificativa, todo e qualquer titular possui o direito de confirmar a existência de tratamento de seus dados pessoais (KORKMAZ; SACRAMENTO, 2021, p. 5).

O direito de acesso, por sua vez, abrange as informações para além do acesso aos dados pessoais propriamente ditos, as informações que circundam o tratamento também deverão ser disponibilizadas ao titular, entre as quais as finalidades, as categorias, os destinatários, os prazos de conservação, a origem dos dados, dentre outras (MALDONADO, 2020, p. 250).

A confirmação da existência de tratamento ou o acesso aos dados pessoais deverão ser providenciados imediatamente e em formato simplificado, porém, se demandada no intuito de obter declaração clara e completa das informações, poderá ser concedido um prazo de até 15 dias a partir do requerimento (art. 19, I e II, LGPD).

O direito à correção dos dados incompletos, inexatos ou desatualizados, previsto no inciso III, por sua vez, objetiva garantir a precisão dos dados dos titulares a fim de evitar riscos, com o propósito de inibir fraudes (SANTOS, 2020, p. 54). Tal prerrogativa justifica-se, enquanto representação da personalidade do titular de dados, pela intrínseca associação entre a pessoa humana e os dados pessoais que lhe dizem respeito (KORKMAZ; SACRAMENTO, 2021, p. 8).

Com efeito, o responsável pelo tratamento dos dados deve guardar um registro do histórico das modificações e das atualizações realizadas pelo titular e informar aos demais agentes com os quais tenha compartilhado aqueles dados sobre o ato de correção (KORKMAZ; SACRAMENTO, 2021, p. 9). O escopo principal do direito aqui alinhado guarda consonância com a cotidiana identificação de pessoas dentro do próprio território nacional, em que os dados deverão ser atualizados em decorrência de alteração de nome, endereço, estado civil, gênero, entre outros (MALDONADO, 2020, p. 252).

A LGPD, ainda, garante ao titular anonimizar, bloquear ou eliminar os dados pessoais que lhe digam respeito e que se enquadrem como desnecessários, excessivos ou tratados em desconformidade com a Lei (inciso IV). A anonimização, consiste na exclusão da possibilidade de associação, direta ou indireta, de um dado a um indivíduo, a partir de meios técnicos razoáveis e disponíveis no momento do tratamento (PINHEIRO, 2021, p. 42),

A anonimização deve garantir um determinado grau de confiança perante a sua irreversibilidade, sem a qual a técnica perderia por completo sua finalidade de proteção (KORKMAZ; SACRAMENTO, 2021, p. 10). A própria nomenclatura “anonimizado” indica

que a informação era um dado pessoal que passou por um procedimento para que os vínculos com o seu titular fossem apagados (KORKMAZ; SACRAMENTO, 2021, p. 10).

O exercício ao direito à anonimização, entretanto, não se dá de forma ilimitada, uma vez que a falta de execução da anonimização poderá não ser considerada como um descumprimento por parte do agente de tratamento, a depender da situação fática apresentada (SANTOS, 2020, p. 54). O legislador reconhece o elevado grau de dificuldades técnicas e operacionais para o processo, de modo que, a depender do quadro que se apresente, poderá ser escusada a não adoção de medidas para esses fins, isto é, não será exigível do agente de tratamento que adote o referido processo se este mostrar-se impossível (MALDONADO, 2020, p. 253).

O bloqueio dos dados pessoais, por sua vez, consiste na suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados (art. 5º, XIII, da LGPD). Já a eliminação concerne à exclusão dos dados armazenados em bancos de dados, de forma definitiva (art. 5º, XIV).

Um dos direitos com maior margem de discussão em termo de executividade do rol de direitos do artigo 18 é a portabilidade dos dados pessoais (inciso V), que consiste no direito de transferir os dados pessoais de um agente de tratamento para outro, isto é, refere-se à possibilidade de, junto ao agente de tratamento, obter dados pessoais, de modo a serem transmitidos a outro agente, de maneira fácil e estruturada (MALDONADO, 2020, p. 260).

A Lei deixou claro que há um limite determinado pelo segredo industrial e comercial, sendo necessário realizar a diferenciação entre o que são dados pessoais do titular (fornecidos por ele) e o que é o aprendizado oriundo da relação de clientela, que compõe o fundo de comércio das empresas e é, portanto, um ativo empresarial (PINHEIRO, 2021, p. 125). Embora a portabilidade dos dados possa ter implicações em outras esferas do direito, como no âmbito concorrencial, a finalidade central do instituto é apontada como a de fortalecer a autodeterminação informativa (KORKMAZ; SACRAMENTO, 2021, p. 13).

Com efeito, evidencia-se o objetivo de mitigar o aprisionamento tecnológico do titular dos dados a um determinado agente de tratamento, perante a existência de outros que possam vir a oferecer uma prestação mais vantajosa (KORKMAZ; SACRAMENTO, 2021, p. 13). O intuito da regra, portanto, é possibilitar ao titular que, na posse de seus dados e de seu histórico, obtenha similar contratação em concorrente, exercendo, assim, sua livre opção (MALDONADO, 2020, p. 261).

Além da possibilidade de eliminação dos dados desnecessários, excessivos ou tratados em desconformidade com a LGPD, o titular tem direito à eliminação dos dados pessoais que

tiverem sido tratados por intermédio da base legal do consentimento² (inciso VI), salvo nas hipóteses em que a manutenção dos dados pelo controlador for permitida por lei³ (KORKMAZ; SACRAMENTO, 2021, p. 17). Por evidente, o titular que fornece o consentimento poderá, igualmente, retirá-lo, sendo acerca desse aspecto de que trata o inciso: o titular, quando assim lhe aprouver, poderá postular a eliminação de seus dados se já não existir mais o seu consentimento perante o tratamento (MALDONADO, 2020, p. 261).

Os agentes de tratamento de dados que efetuarem a coleta e o tratamento dos dados pessoais poderão compartilhá-las com entidades públicas e privadas (inciso VII), desde que mediante fundamento normativo e expressamente informado ao titular de dados, com o intuito de manter o titular em pleno controle de seus dados pessoais, de forma a que conheça todas as entidades que realizam o tratamento por força do compartilhamento (MALDONADO, 2020, p. 262).

Com efeito, deve ser garantido ao titular que, mediante requerimento, tenha acesso às suas informações que foram repassadas, para que, se for o caso, possa exercer as demais prerrogativas, como a eliminação ou correção dessas informações quando impertinentes, e os agentes deverão comunicar as entidades sempre que houver quaisquer eliminações ou correções dos dados, mantendo as bases das entidades igualmente atualizadas (KORKMAZ; SACRAMENTO, 2021, p. 18).

Ao titular também é garantido o direito de obter informações sobre a possibilidade de não fornecer o seu consentimento e sobre quais serão as consequências dessa negativa (inciso VIII). O consentimento é definido pela Lei como uma manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (art. 5º, XII). Nessa direção, é razoável que as informações sobre quais serão as consequências diante de eventual recusa do fornecimento, para que o titular possa realizar um juízo sobre a conveniência do ato (KORKMAZ; SACRAMENTO, 2021, p. 19).

² O artigo 7º da Lei Geral de Proteção de Dados traz as bases legais que autorizam o tratamento dos dados pessoais e a primeira delas diz respeito ao tratamento dos dados pessoais mediante o fornecimento de consentimento pelo titular. O consentimento, por sua vez, consiste em manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (art. 5º, XII, LGPD). Na sistemática da lei, o consentimento ocupa lugar de destaque, tendo sido mencionado inúmeras vezes pelo legislador; deve ser destacado, todavia, que, a despeito dessa atenção especial, o consentimento não se encontra em posição hierarquicamente superior perante as demais bases legais (MALDONADO, 2020, p. 263).

³ Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
I - cumprimento de obrigação legal ou regulatória pelo controlador;
II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Com efeito, os agentes de tratamento possuem os deveres de transparência e de informação, remanescendo ao titular o direito de instar o controlador a prestar o esclarecimento de forma clara, expressa e inequívoca, devendo explicitar as consequências decorrentes do não consentimento (MALDONADO, 2020, p. 263).

O titular também poderá revogar, a qualquer tempo e por procedimento gratuito e facilitado, o consentimento que tenha fornecido anteriormente (inciso IX). Essa revogação produz seus efeitos somente a partir do momento em que for efetivada, não incidindo sobre o tratamento já efetuado a partir do consentimento até então existente (SANTOS, 2020, p. 57). Nessa conformidade, poderá operar-se no instante seguinte ao do fornecimento, sendo certo que, em tal ocorrência, o tratamento dos dados deverá cessar, salvo se existir outra base legal que se cumule a ela e permita a manutenção do tratamento (MALDONADO, 2020, p. 263).

Os parágrafos 1º e 8º do artigo 18, ainda, tratam do direito do titular em formalizar, quando e se lhe convier, reclamações contra os agentes de tratamento de dados perante a Autoridade Nacional de Proteção de Dados Pessoais, aos organismos de defesa do consumidor ou recorrer ao poder judiciário em ações individuais ou coletivas para defender seus direitos e interesses (BRASIL, 2018).

Os demais artigos do Capítulo III da Lei demonstram que a confirmação da existência ou o acesso aos dados pessoais deverão ser providenciados pelos agentes de tratamento de forma simplificada e imediata, por meio de declaração clara e completa (art. 19). Além disso, o titular poderá solicitar a revisão das decisões tomadas unicamente com base em tratamento automatizado de dados (art. 20), não podendo ser utilizados em seu prejuízo os dados referentes ao exercício regular do seu direito (art. 21).

Com efeito, a utilização indevida dos dados revela conduta abusiva e eivada de má-fé por parte dos agentes de tratamento, de modo a expor o controlador ou terceiro a consequências, materiais ou morais, decorrentes da violação da legislação (MALDONADO, 2020, pp. 272-273). A preocupação do legislador é garantir que o titular possa assegurar que seus dados sejam tratados de forma segura, verídica e no cumprimento de sua finalidade (PINHEIRO, 2021, pp. 124-125).

Evidencia-se, portanto, que o titular de dados pessoais ganha protagonismo em um cenário em que suas informações pessoais estão, progressiva e constantemente, sendo coletadas e utilizadas por agentes públicos e privados (KORKMAZ; SACRAMENTO, 2021, p. 25). Deveras, emerge-se perante os agentes de tratamento dos dados o imperativo de assegurar o controle sobre tais informações, coordenando as perspectivas individual e coletiva (KORKMAZ; SACRAMENTO, 2021, p. 25).

Os titulares de dados, dessa forma, possuem a prerrogativa de invocar esses direitos, devendo, para tanto, formalizar as suas solicitações perante os agentes de tratamento, competindo a estes observar o prazo da lei e manter uma clara comunicação com o titular, seja na hipótese de acolhimento de pedido, ou não (MALDONADO, 2020, p. 273). Assim, para a validação de tais direitos, é inafastável que os agentes de tratamento, a par de conhecerem de forma profunda a Lei, estabeleçam os paradigmas práticos de conformidade, para que seja viabilizado o exercício do titular de dados de forma ampla, precisa e completa (MALDONADO, 2020, p. 274).

3.2 AGENTES DE TRATAMENTO DOS DADOS PESSOAIS

Os agentes de tratamento de dados são os responsáveis pelo exercício de tratamento dos dados pessoais, que consiste em um amplo conjunto de operações e possui diversas etapas de manuseio (BRASIL, 2018, art. 5º, IX e X). O tratamento é o elemento central da proteção dos dados pessoais, de modo que sua definição é bastante ampla (BRANCO, 2020, p. 37): é toda operação que tenha sido realizada por meio de algum tipo de manipulação dos dados pessoais (PINHEIRO, 2021, p. 41).

A LGPD, portanto, estabeleceu em seu inciso X do artigo 5º um rol exemplificativo das atividades que se enquadram no conceito de tratamento dos dados pessoais (COTS; OLIVEIRA, 2019, p. 11):

Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. (BRASIL, 2018).

A Lei classifica os agentes de tratamento de dados em duas categorias: o controlador e o operador (art. 5º, IX). Aquele é uma pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais (inciso VI). O operador, por sua vez, é uma pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (inciso VII).

Nas palavras de Marcel Leonardi (2019, p. 73), o controlador determina as finalidades e o caminho a serem adotados no tratamento dos dados pessoais, isto é, controla as razões e o método que serão empregados na atividade de tratamento; enquanto o operador realiza o tratamento conforme as instruções recebidas do controlador.

De acordo com Patrícia Peck Pinheiro (2021, p. 43), o controlador é a pessoa natural ou jurídica que recebe os dados pessoais por meio do consentimento ou por hipóteses de exceção; já o operador realiza o tratamento dos dados motivado por um contrato ou obrigação legal.

Ambos possuem um papel institucional, por meio da tomada de decisões (controlador) e da realização de atividades sob um comando (operador), de forma que não poderá ser apontado a um funcionário específico da empresa a capacidade de decisão e realização das atividades, mas à instituição (PINHEIRO, 2021, p. 43). O controlador, portanto, controla a finalidade e os meios gerais sobre os quais os dados serão utilizados e, por ser o principal tomador de decisão, detém a responsabilidade primária de garantir que as atividades estejam em conformidade com a Lei (KREMER, 2020, p. 291).

Com efeito, ele possui o poder de decisão perante questões como o motivo sobre a coleta dos dados; a forma que se dará a coleta; sobre quem ocorrerá; qual será o conteúdo a ser coletado; a finalidade para que os dados serão coletados; para quem serão divulgados, compartilhados ou transferidos; e por quanto tempo ficarão retidos. (KREMER, 2020, pp. 291-292). A todo caso que a LGPD for aplicável, a figura do controlador se fará necessária, uma vez que é o interessado direto na obtenção e no processamento dos dados e, a partir dos métodos e estratégias de tratamento por ele adotados, conferir-lhes-á finalidade econômica (KREMER, 2020, p. 295).

Dessa forma, o controlador é necessário para fins de governança, prestação de contas e, sobretudo, responsabilidade jurídica. Distintivamente, o operador irá desempenhar as atividades de tratamento de dados pessoais em nome do controlador (KREMER, 2020, p. 306), com a função de decidir sobre o método que será utilizado para a coleta e o tratamento dos dados; a forma em que serão armazenados; como serão assegurados; e quais serão os meios de portabilidade, recuperação e retenção dos dados tratados (KREMER, 2020, p. 306).

Cabe ressaltar, ainda, uma outra figura estabelecida pela Lei Geral de Proteção de Dados, que não se trata de um agente de tratamento, mas que deverá atuar em conjunto com eles, efetuando um papel intermediário: o encarregado (FEIO, 2019, p. 53). Este se trata da pessoa natural ou jurídica, contratada internamente ou terceirizada e indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares de dados e a Autoridade Nacional de Proteção de Dados, sendo o responsável dentro da instituição pela supervisão do cumprimento das regras previstas na Lei e orientação dos funcionários e dos contratados a respeito das práticas a serem adotadas (FEIO, 2019, p. 53).

A imputação da necessidade de um encarregado para o tratamento dos dados pessoais tem o objetivo de garantir que as informações fiquem centralizadas e que o controlador se certifique de que a aplicação das normas receberá efetiva validação (PINHEIRO, 2021, p. 144).

Os agentes de tratamento de dados são fundamentais para que haja a eficácia da LGPD e para a promoção de uma cultura de proteção de dados pessoais dentro das instituições, bem como são os responsáveis por propor políticas e conscientizar os agentes internos, gerenciando e fiscalizando o processamento dos dados (MELLO; MIRAMONTES, 2021, p. 74).

Essa modalidade de negócio, no entanto, responsável por transformar o cotidiano em estratégia de comercialização de dados pessoais (KREMER, 2020, p. 294), por meio do poder de decisão que os agentes detêm sobre a forma com que serão tratados, possui consequências significativas no que tangem aos danos decorrentes em desfavor de seus titulares (KREMER, 2020, p. 291).

A atividade do controlador, ainda que não antes regulamentada, sempre existiu no exercício de processamento dos dados pessoais e, conseqüentemente, no desenvolvimento de diversas atividades comerciais que disso dependem (OLIVEIRA, 2021, p. 32). O operador, como uma extensão da figura do controlador, tem a função de atribuir ao tratamento desses dados fins econômicos, por meio de uma estrutura tecnológica que permite o seu armazenamento e processamento (OLIVEIRA, 2021, p. 32).

Com efeito, pode-se dizer que os agentes de tratamento dos dados pessoais figuram como novos atores nesse cenário de proteção de dados, uma vez que adquiriram uma série de deveres a serem cumpridos, sob pena de serem responsabilizados pela irregularidade do tratamento (SCALETSCKY; VAZ, 2020, p. 26).

3.2.1 A boa-fé e os princípios norteadores

Considerando que a LGPD é uma legislação principiológica, a atividade dos agentes de tratamento de dados sempre deverá ser orientada pelos princípios presentes no artigo 6º da Lei. Este, por sua vez, dispõe que o tratamento dos dados pessoais deverá observar a boa-fé e dez princípios cardiais, quais sejam i) finalidade; ii) adequação; iii) necessidade; iv) livre acesso; v) qualidade dos dados; vi) transparência; vii) segurança; viii) prevenção; ix) não discriminação; x) responsabilização e prestação de contas.

A boa-fé prevista no *caput* do enunciado concerne à boa-fé objetiva que, a partir de sua função integrativa, estabelece deveres implícitos a todas as relações jurídicas, anexos ao dever jurídico principal, como os deveres de lealdade, probidade, garantia, respeito e informação (FARIAS; ROSENVALD, 2018, *apud* LINKE, 2019, p. 155).

O princípio da finalidade (i) estipula que a coleta dos dados pessoais deverá ter um propósito específico, previamente definido e informado ao titular, sendo vedada a sua utilização para uma finalidade diversa, posteriormente à sua coleta (MORAES; QUEIROZ, 2019, p. 14). Isto é, o princípio exige que seja respeitada a correlação entre o tratamento dos dados e a finalidade informada (OLIVEIRA; LOPES, 2019, p. 28) e os dados somente poderão ser utilizados para fins legítimos, específicos e explícitos (SOUZA *et al.*, 2020, p. 53).

Esse princípio conta com grande relevância prática, já que garante ao titular a delimitação dos propósitos do tratamento e dos terceiros que poderão acessá-los (VAINZOF, 2020, p. 128), visando mitigar o risco intrínseco à atividade. Dessa forma, é de crucial relevância que os controladores avaliem, desde a coleta dos dados, os propósitos específicos que almejam obter, uma vez que estes servirão como fronteira de legalidade (VAINZOF, 2020, p. 130).

De acordo com o princípio da adequação (ii), os dados coletados somente poderão ser utilizados na medida que forem necessários para atingir os objetivos anteriormente informados, de acordo com o contexto do tratamento (SOUZA *et al.*, 2020, p. 54). O princípio, como se vê, está vinculado ao da finalidade, uma vez que o tratamento de dados pessoais somente poderá ser realizado mediante a verificação de compatibilidade com as finalidades informadas ao titular, de acordo com o contexto do tratamento (VAINZOF, 2020, pp. 132-133). Desse modo, havendo solicitação de um dado desnecessário ao tratamento, o agente terá desrespeitado o princípio aqui analisado, ante a incompatibilidade entre o dado coletado e a atividade desempenhada (TEIXEIRA, 2021, p. 21).

Ademais, apenas os dados indispensáveis para atingir a finalidade poderão ser coletados, como indica o princípio da necessidade (iii). Dessa forma, a sua coleta será restringida ao estritamente necessário para o cumprimento da finalidade informada e a eliminação dos dados deverá ocorrer sempre que houver requisição do titular ou com o fim de seu tratamento (OLIVEIRA; LOPES, 2019, p. 29).

Nota-se que, da mesma forma, o referido princípio guarda relação direta com os princípios da finalidade e da adequação, visto que enfatiza a delimitação da licitude do tratamento de acordo com a finalidade e a proporcionalidade (VAINZOF, 2020, p. 134). Somente o mínimo necessário poderá ser coletado, porque um grande conjunto de dados tende

a gerar incentivos, por exemplo, à ataques *hackers* dentro e fora das instituições, sendo necessário que haja medidas regulatórias para desestimular o uso desproporcional (SOUZA *et al.*, 2020, pp. 54-55). Nessa toada, da mesma forma que há uma evolução tecnológica a propiciar o tratamento dos dados em larga escala, deve-se construir, em paralelo, modelos especializados à sua proteção (VAINZOF, 2020, p. 137).

O princípio do livre acesso (iv), por sua vez, assegura o acesso dos titulares aos próprios dados pessoais, quando assim desejarem. Isto é, para que o titular possa controlar o uso de seus dados pessoais, além de lhe dever ser informado sobre o propósito do tratamento, é necessário que lhe seja garantido o livre acesso (VAINZOF, 2020, p. 137).

Com efeito, o titular tem o direito de obter do controlador, sem custo, a confirmação da existência de tratamento; o acesso aos dados; a correção dos dados incompletos, inexatos ou desatualizados; a anonimização, o bloqueio ou a eliminação dos dados desnecessários, excessivos ou tratados em desconformidade com a Lei; a portabilidade dos dados; a eliminação dos dados tratados com o consentimento do titular; a explicitação das entidades com as quais o controlador realizou o compartilhamento dos dados; informações sobre a possibilidade de não fornecer consentimento e as consequências da negativa; e a revogação do consentimento (art. 18, I a IX, LGPD).

Em suma, o princípio viabiliza que o titular acompanhe a utilização de seus dados, de forma a controlar o fluxo informacional que lhe diga respeito (VAINZOF, 2020, p. 138), bem como solicitar eventual revisão de decisões em procedimentos exclusivamente automatizados com base nesses dados (OLIVEIRA; LOPES, 2019, p. 29).

Já o princípio da qualidade dos dados (v), estipula que os dados deverão ser fiéis à realidade, completos, relevantes e com atualizações periódicas, conforme a necessidade (DONEDA, 2010, p. 46). Os mais variados dados pessoais, se isoladamente analisados, dificilmente afetariam o titular, contudo, quando processados em conjunto, resultam em um compilado da personalidade de cada um dos titulares (VAINZOF, 2020, p. 138).

Dessa forma, os controladores precisam adotar medidas, desde o momento da coleta, que garantam a precisão e a atualização dos dados (VAINZOF, 2020, p. 139). Esse princípio se relaciona, em grande escala, com os princípios da transparência e do livre acesso, na medida em que asseguram o conhecimento e os meios de correção de informações equivocadas (OLIVEIRA; LOPES, 2019, p. 29).

O princípio da transparência (vi), por sua vez, indica que informações sobre a finalidade, tratamento e agentes de tratamento deverão ser claras e acessíveis aos titulares, conferindo-lhe autodeterminação (SOUZA *et al.*, 2020, 57). Para fins de mitigação de riscos, é

importante que os controladores considerem os titulares sempre como vulneráveis quanto ao conhecimento das possibilidades de tratamento, existindo a necessidade de transmitirem informações claras, completas e ostensivas (VAINZOF, 2020, p. 140).

Com efeito, os controladores deverão apresentar informações sobre o tratamento de dados de maneira eficaz e sucinta, a fim de evitar a fadiga informacional e garantir a confiança nos procedimentos, permitindo a compreensão dos titulares que, se necessário, poderão desafiá-los e exercer seus direitos (VAINZOF, 2020, p. 142).

Pelo princípio da segurança (vii), “as medidas técnicas e administrativas devem ser sempre atualizadas e hábeis a proteger os dados de acessos não autorizados, de acidentes e de situações ilícitas” (SOUZA *et al.*, 2020, p. 57). Essa medida se justifica pelos riscos inerentes ao tratamento dos dados, em virtude de acessos não autorizados a bases de dados; usos indevidos de informações pessoais; ataques a sistemas; destruição; perda; alteração; comunicação; ou difusão de dados pessoais, que colocam em risco os direitos dos titulares e os agentes ficam expostos às possíveis sanções administrativas e responsabilizações civis (VAINZOF, 2020, p. 142).

Diante dessas circunstâncias, os agentes deverão utilizar medidas aptas a proteger os dados de eventuais violações, já que não envolvem somente eventos dolosos, mas também acidentais (VAINZOF, 2020, p. 143). O princípio, portanto, impõe a adoção de medidas ligadas à prevenção do ilícito (OLIVEIRA; LOPES, 2019, p. 29).

Na abrangência do princípio da prevenção, medidas técnicas cabíveis deverão ser adotadas pelos agentes para evitar danos decorrentes de tratamento irregular dos dados pessoais (viii) (SOUZA *et al.*, 2020, p. 57). A LGPD é uma norma que visa modificar a cultura do tratamento dos dados pessoais, prevendo que deverão formular regras de boas práticas e de governança, as quais estimularão a adoção de padrões técnicos que facilitem o controle dos titulares sobre os seus dados pessoais (VAINZOF, 2020, p. 147).

Dentro desse aspecto de governança, a figura do encarregado e o relatório de impacto à proteção de dados pessoais – como será adiante demonstrado – são peças fundamentais, uma vez que a ANPD poderá considerar como parâmetro, entre outros, a adoção reiterada de tais mecanismos, para uma possível amenização de seus efeitos (BRASIL, 2018, art. 52, § 1º, VIII e IX).

O princípio da não discriminação (ix), por sua vez, implica a impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos. Em outras palavras, os dados colhidos não poderão ser manuseados de forma discriminatória ou direcionados a fins discriminatórios (SOUZA *et al.*, 2020, p. 58). Aqui, encontra-se respaldo no princípio da

transparência, uma vez que deverá haver clareza no tratamento aplicado, na medida em que qualquer diversidade de tratamento deverá ser plenamente justificada, não discriminatória e ter como principal parâmetro a boa-fé objetiva (VAINZOF, 2020, p. 151).

O dispositivo parece revelar que o legislador admitiu o tratamento distintivo dos dados pessoais, desde que não abusivo e lícito, por exemplo, é possível que uma instituição financeira precifique o crédito com base em dados pessoais, como o nível de inadimplência do titular, em atenção aos princípios gerais de direito previstos na lei e à boa-fé objetiva; em contrapartida, a circulação desautorizada de listas entre empregadores, com informações pessoais de seus empregados⁴, encontrar-se-ia no uso discriminatório dos dados pessoais (MORAES; QUEIROZ, 2019, p. 14).

Por fim, pelo princípio da responsabilização e prestação de contas (x), requer-se do agente de tratamento a capacidade de demonstração da eficácia das medidas adotadas para o cumprimento das normas de proteção dos dados pessoais (SOUZA *et al.*, 2020, p. 60). A intenção da Lei foi em alertar os agentes de tratamento que eles são os responsáveis pelo fiel cumprimento de todas as exigências legais.

Contudo, não basta somente pretender cumprir a Lei, sendo necessário que as medidas adotadas sejam comprovadamente eficazes. A exigência de prestação de contas por parte dos agentes, demonstra que estes deverão manter os registros das operações de tratamento que realizarem (art. 37), não só porque a ANPD poderá solicitar informações, mas também em razão da possibilidade de inversão do ônus da prova em favor dos titulares de dados no judiciário.

Percebe-se que a LGPD tem o relevante papel de consolidar os preceitos que já existiam de modo não exclusivo em outras leis. Assim, o rol de princípios do art. 6º lhe confere um nível de coerência e organização, uma vez que tais princípios representam a cristalização de avanços que foram alcançados por legislações anteriores e fortalecem a unidade desse sistema (OLIVEIRA; LOPES, 2019, p. 29). A principiologia da LGPD é de extrema relevância no contexto de inovação tecnológica atual, por cumprir o papel de guiar o intérprete diante de uma nova forma de lidar com os dados pessoais e para modificar os hábitos dos agentes de tratamento e dos titulares de dados, no que tange ao compartilhamento de suas informações pessoais (SOUZA *et al.*, 2020, pp. 61-62).

⁴ A título de exemplo, os dados sensíveis possuem informações que podem levar facilmente à discriminação do titular, como origem étnica, religião, orientação sexual e posição política (OLIVEIRA; LOPES, 2019, p. 29).

3.2.2 Requisitos para o tratamento dos dados

Além de os agentes de tratamento deverem observar os princípios previstos na legislação, deverão adotar ao menos uma das dez bases legais para o tratamento dos dados pessoais, previstas no art. 7º da Lei Geral de Proteção de Dados, isto é, o tratamento não poderá ser realizado senão dentro de uma das hipóteses taxativas previstas em seus incisos (OLIVEIRA, 2020, p. 48):

Art. 7º **O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:**

- 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 terceiro;
- 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 de terceiro, 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. (BRASIL, 2018) (Grifo nosso).

A Lei Geral de Proteção de Dados exige que, caso a base de dados escolhida pelo agente de tratamento seja o fornecimento, pelo titular, de seu consentimento (inciso I), este deverá ser livre e informado, por escrito e através de uma cláusula destacada das demais, que não seja genérica, ou por outro meio que demonstre a manifestação inequívoca de vontade (OLIVEIRA, 2020, p. 48).

Para que o consentimento seja válido e legítimo deverá ser livre; informado; inequívoco; e destinado a uma finalidade determinada (FRAJHOF; MANGETH, 2020, p. 69), caso contrário, será nulo, nos termos da Lei (art. 9º, §1º⁵). Para que seja livre, os titulares deverão ter a escolha sobre quais os tipos de dados que serão tratados em cada operação e qual

⁵ Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: [...]

§ 1º Na hipótese em que o **consentimento** é requerido, esse **será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.** (BRASIL, 2018).

a finalidade específica que o tratamento utilizará; deverão ser amplamente informados acerca do tratamento; e, para que seja inequívoco, o controlador deverá demonstrar tal autorização (LIMA, 2020, pp. 203-204).

O consentimento, ainda, poderá ser revogado a qualquer momento, mediante manifestação expressa do titular, por um procedimento facilitado e gratuito; diante disso, quando o agente de tratamento utilizar essa base legal para a coleta e tratamento dos dados pessoais, será necessário dispor de uma plataforma que seja capaz de gerir todos os consentimentos que foram concedidos, cronologicamente ordenados, e efetuar a exclusão dos dados pessoais diante de eventual requisição do titular (OLIVEIRA, 2020, pp. 49-50).

Essa preocupação já se encontrava presente em algumas legislações setoriais, é o caso do Código de Defesa do Consumidor, que confere ao indivíduo (art. 43) o direito de exigir a correção imediata de quaisquer dados que considerar inexatos; da Lei do Cadastro Positivo, que previu a necessidade de autorização prévia e consentimento informado do consumidor para que seja feita a abertura de seu cadastro; e do Marco Civil da Internet, que instituiu (art. 7º, VII) como direito e garantia do usuário que seus dados pessoais não sejam fornecidos a terceiros sem que antes haja seu consentimento livre, expresso e informado (FRAJHOF; MANGETH, 2020, p. 68).

Apesar disso, os dados pessoais poderão ser tratados sem a necessidade de concessão do consentimento do titular, quando a relação jurídica em questão exigir que o controlador cumpra determinada obrigação legal ou regulatória (inciso II), nesses casos, o titular não poderá se opor ao tratamento (FRAJHOF; MANGETH, 2020, p. 72). A LGPD visa garantir que a Lei não entre em conflito com outras legislações vigentes no país, prestando-se a evitar antinomias (OLIVEIRA, 2020, p. 50).

O tratamento dos dados pessoais, portanto, poderá ser necessário a atender o interesse público, que justifique a obrigação legal ou regulatória. Importante salientar que obrigações contratualmente assumidas não se encontram acobertadas pelo presente inciso, não podendo relações privadas ser utilizadas como fundamento para o tratamento dos dados pessoais (LIMA, 2020, p. 205).

A previsão da possibilidade de tratamento e uso compartilhado dos dados pessoais necessários à execução de políticas públicas, previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, pela administração pública, no inciso III, demonstra que esses órgãos deverão se adequar, nos termos da Lei, ao tratar e compartilhar dados pessoais.

A Administração Pública, portanto, deverá fornecer ao titular informações claras e inequívocas sobre a base legal para o tratamento dos dados, a finalidade e quais os procedimentos que serão utilizados ao longo do ciclo de vida do dado dentro dos sistemas da Administração Pública (OLIVEIRA, 2020, p. 52). Esta somente não estará obrigada a cumprir com as exigências da lei caso o tratamento seja feito exclusivamente para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação ou de repressão de infrações penais (art. 4º, III).

O inciso III do art. 7º da Lei deverá ser analisado em conjunto com o regramento próprio das hipóteses de tratamento de dados pessoais realizados pelo Poder Público, previsto no capítulo IV da Lei. Com efeito, apesar de o titular de dados estar dispensado de fornecer seu consentimento, o art. 23, I, da Lei impõe que ele seja informado sobre a realização do tratamento, por meio de informações claras e atualizadas, em veículos de fácil acesso, devendo estar disponíveis informações sobre previsão legal que autorize o tratamento; a existência de compartilhamento de dados; a finalidade para a qual se destina; e a forma como o tratamento será realizado (BRASIL, 2018). Tal previsão assegura a obrigatoriedade de que haja a mais ampla divulgação dos atos administrativos, para garantir o controle da legitimidade e legalidade da conduta pública (FRAJHOF; MANGETH, 2020, p. 74).

O tratamento também poderá ser desempenhado para a realização de estudos por órgão de pesquisa⁶, garantida, sempre que possível, a anonimização⁷ dos dados pessoais (inciso IV). A partir dessa base legal, sempre que possível e em observância à utilização de técnicas razoáveis na ocasião do tratamento, os dados deverão ser anonimizados, a fim de mitigar possíveis danos decorrentes de eventuais vazamentos ou acessos não autorizados às bases de dados que possam vir a ocorrer (OLIVEIRA, 2020, p. 53). Os dados, portanto, deixarão de ser associados aos titulares de dados e, caso haja qualquer violação, mitigar-se-á o risco de

⁶ Art. 5º [...] XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; (BRASIL, 2018).

⁷ A antítese do conceito de dado pessoal seria um dado anônimo, isto é, aquele que é incapaz de revelar a identidade de uma pessoa (BIONI; 2019; p. 22). Essa inaptidão pode ser fruto de um processo pelo qual é quebrado o vínculo entre os dados e seus respectivos titulares, o que é chamado de anonimização, processo que poderá se valer de diferentes técnicas para eliminar os elementos identificadores de uma base de dados (DONEDA, 2006, p. 44). De acordo com a Lei, a anonimização é definida como a utilização de meios técnicos razoáveis que estão disponíveis no momento do tratamento, que permitem que determinado dado perca a possibilidade de associação, direta ou indireta, a um sujeito (art. 5º, XI). Embora a lei tenha optado em permitir a discricionariedade do controlador em anonimizar os dados pessoais – “sempre que possível” – no inciso IV do art. 7º da LGPD, a sua dispensa em assim não fazer deverá ser justificada, em atenção ao que determinam os princípios da segurança, da prevenção e da responsabilização e prestação de contas (art. 5º, VII, VIII e X) (FRAJHOF; MANGETH, 2020, p. 75).

ocorrência de danos e eventuais sanções administrativas ou condenação dos agentes de tratamento ao pagamento de indenizações.

Quando o tratamento for necessário para a execução de contrato ou de procedimentos preliminares relacionados a um negócio jurídico do qual faça parte o titular (inciso V), se dará a pedido do próprio titular dos dados. Esta hipótese se assemelha com o tratamento de dados por meio da base legal do consentimento; porém, no caso do inciso V, o titular não poderá revogar o seu fornecimento, uma vez que a outra parte estará resguardada pela Lei para a manutenção da posse durante a vigência do contrato e, se necessário, por um prazo posterior ao seu término (OLIVEIRA, 2020, p. 54).

Para a sua aplicação, será necessário haver a ponderação entre os princípios da necessidade – limitação do tratamento ao mínimo necessário –, da finalidade – por meio de propósitos legítimos e específicos - e da adequação – que impede que haja sua alteração para um fim incompatível com o previamente informado ao titular (FRAJHOF; MANGETH, 2020, p. 77).

No caso do tratamento para o exercício regular de direitos em processo judicial, administrativo ou arbitral (inciso VI), o controlador de dados não precisará do fornecimento de consentimento pelo titular de dados para coletar, processar e armazenar seus dados, desde que esteja no exercício regular de seus direitos (FRAJHOF; MANGETH, 2020, p. 78). Assim, nas situações em que os dados pessoais servirem como elemento ao exercício de direitos em demandas em geral (judiciais, administrativas ou arbitrais), eles poderão ser armazenados, exclusivamente para essa finalidade, enquanto subsistir tal necessidade (LIMA, 2020, p. 207).

O tratamento poderá ocorrer, ainda, para a proteção da vida ou da incolumidade física do titular ou de terceiro (inciso VII), com o objetivo de garantir a proteção de bens de elevado interesse público, desde que devidamente comprovada essa necessidade e exposta a finalidade (OLIVEIRA, 2020, p. 56).

Esse critério, contudo, é restritivo e somente terá lugar nas poucas situações em que for constatado, como exemplo, é possível mencionar a obtenção de dados de geolocalização de dispositivos de telefone celular para tentar localizar eventuais vítimas que estejam perdidas em virtude de determinado incidente (LIMA, 2020, p. 207). Observa-se que a hipótese somente poderá ser aplicada em situações excepcionais e de forma pontual, não sendo possível para justificar ações genéricas (VIOLA; TEFFÉ, 2021, p. 252).

O inciso VIII prevê o tratamento dos dados para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

O tratamento dos dados pessoais de saúde pelos agentes de tratamento deverá ser feito sempre em benefício dos pacientes e titulares dos dados (FRAJHOF; MANGETH, 2020, p. 79).

O artigo 11, II, *f*, da LGPD, por exemplo, estabelece que os dados pessoais sensíveis⁸ poderão ser tratados sem o fornecimento de consentimento do titular, se forem indispensáveis à tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (OLIVEIRA, 2020, p. 57).

Outra base legal que ampara o tratamento dos dados é para atender aos interesses legítimos do controlador ou de terceiro, exceto nos casos que prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (inciso IX). Trata-se de uma base legal que, na realidade, permite o tratamento dos dados pessoais para uma finalidade diferente daquela inicialmente informada ao titular e consentida por ele (FRAJHOF; MANGETH, 2020, p. 80).

Apesar de o legítimo interesse parecer uma salvaguarda demasiadamente ampla, a lei busca estabelecer a sustentabilidade das dinâmicas comerciais atuais, muito pautadas na coleta, tratamento e compartilhamento de dados pessoais, evitando que a LGPD se torne um óbice à inovação; devendo-se avaliar se o interesse do controlador é manifestamente importante e justificável a ponto de dispensar a anuência do titular de dados (FRAJHOF; MANGETH, 2020, pp. 80-81). Dessa forma, o legítimo interesse somente poderá fundamentar o tratamento dos dados pessoais para finalidades legítimas, nos seguintes termos:

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. (BRASIL, 2018).

Os parágrafos 1º a 3º do referido artigo, ainda, determinam que somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados e que o controlador deverá adotar medidas para garantir a transparência do tratamento. Além disso, a ANPD poderá solicitar ao controlador um relatório de impacto, como será demonstrado adiante, quando o tratamento utilizar a aludida base legal, observados os segredos comercial e industrial (OLIVEIRA, 2020, p. 60).

⁸ Estatuiu a LGPD que dado sensível é todo dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (art. 5º, II). Os dados pessoais sensíveis, em linhas gerais, são dados pessoais que poderão implicar riscos e vulnerabilidades potencialmente mais graves aos direitos e liberdades fundamentais dos titulares (VAINZOF, 2020, p. 85).

Por fim, o inciso X prevê a possibilidade de tratamento dos dados pessoais para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. O objetivo do legislador foi evitar que titulares de dados pessoais tentem se esquivar de cobranças por dívidas legítimas (OLIVEIRA, 2020, p. 61). Informações sobre adimplência e inadimplência de determinado titular poderão ser utilizadas, a fim de se tomar decisão acerca da concessão ou não de crédito. Nesse ponto, a Lei do Cadastro Positivo e o Código de Defesa do Consumidor também são pertinentes e deverão ser observados quando houver o uso da referida base legal para fundamentar o tratamento dos dados (LIMA, 2020, p. 209).

É extremamente importante destacar que não existe hierarquia entre bases legais previstas no artigo 7º, são igualmente importantes e nenhuma delas deverá prevalecer em relação às demais. Cada controlador terá a função de escolher qual será a base legal mais apropriada em cada caso concreto, a depender de qual se enquadrar melhor diante das finalidades do tratamento (LEONARDI, 2019, p. 74). A aplicação de algumas dessas bases legais ainda pode gerar certo receio, em virtude da ausência de orientação, contudo, principalmente por meio das vindouras diretrizes da ANPD e da aplicação prática do tema, será possível atingir uma estabilidade normativa nesse sentido (OLIVEIRA, 2020, p. 62).

3.2.3 O término do tratamento

O tratamento dos dados pessoais tem natureza variável e depende de certas circunstâncias para sua continuidade; nessa seara, exsurge a questão sobre quais serão os limites para a utilização dos dados pessoais e quando deverá ocorrer o término do seu tratamento (GUEDES; MEIRELES, 2019, p. 118). O Marco Civil da Internet já previa a exclusão dos dados pessoais fornecidos a determinada aplicação de *internet*, a requerimento do usuário, quando ocorrer o término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros (art. 7º, inciso X). A finalidade de tal dispositivo é permitir ao usuário da *internet* que possa controlar as suas informações, conferindo-lhe o direito de solicitar a exclusão definitiva de seus dados ao final da relação (BITELLI, 2014, p. 11).

A Lei Geral de Proteção de Dados, por sua vez, determina que o término do tratamento dos dados deverá ocorrer nas hipóteses em que haja (art. 15):

- I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
- II - fim do período de tratamento;

- III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou
- IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei. (BRASIL, 2018).

Na ocorrência de alguma dessas situações, sem a necessidade de haver um pedido expresso por parte do titular, deverá ocorrer o término do tratamento dos dados pessoais, com a eliminação destes. O inciso I prevê que o término do tratamento e a consequente exclusão dos dados deverá ocorrer quando for verificado que finalidade almejada foi alcançada ou que os dados pessoais deixaram de ser necessários ou pertinentes ao tratamento. Ainda, nos casos em que houver a especificação do período de guarda dos dados pessoais e este for alcançado (inciso II), os dados não mais poderão ser tratados.

Outrossim, nas situações em que houver expressa solicitação do titular para a exclusão de seus dados (inciso III), o atendimento do pedido será mandatório (LIMA, 2020, p. 236). E, por fim, a ANPD poderá determinar ao agente que elimine os dados em relação aos quais não for possível comprovar a licitude do tratamento (inciso IV). Desse modo, quando identificada quaisquer dessas situações, os dados pessoais deverão ser eliminados, salvo nos seguintes casos:

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, **autorizada a conservação para as seguintes finalidades:**

- I - cumprimento de obrigação legal ou regulatória pelo controlador;
- II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
- IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados. (BRASIL, 2018) (Grifo nosso).

Os dados pessoais, portanto, apesar do disposto no artigo 15, poderão ser conservados caso haja uma determinação legal ou regulatória que demande a sua manutenção (inciso I). Órgãos de pesquisa poderão manter suas bases de dados por prazo indeterminado, recomendando-se a realização do processo de anonimização sempre que pertinente (inciso II). Em específicas situações, em que subsistir motivação para a retenção dos dados pessoais, será possível a transferência a terceiro, desde que respeitadas os requisitos para o tratamento dos dados pessoais (inciso III). E, por fim, ocorrendo o término do tratamento, o controlador poderá, após realizar o processo de anonimização, mantê-los restritamente a seu uso (inciso IV), sendo vedado o acesso de terceiros (LIMA, 2020, p. 238).

O artigo prevê situações em que poderá ser preservada a manutenção das bases de dados pessoais, contudo, não determinou o prazo para tal conservação. O Marco Civil da

Internet, determina que a guarda dos registros de acesso a aplicações de *internet*, sob sigilo, em ambiente controlado e seguro, subsistam pelo prazo de seis meses ou de acordo com regulamento específico (art. 15). Entretanto, caberá à ANPD estipular o prazo que será utilização pela Lei de proteção dos dados pessoais.

Em suma, a LGPD determina que deverá haver a eliminação dos dados pessoais quando encerrado o seu tratamento, com a intenção de diminuir os riscos do uso não autorizado ou indevido (GUEDES; MEIRELES, 2019, p. 120). Entretanto, será possível a manutenção do tratamento quando este se enquadrar em uma das situações previstas no art. 16 da Lei. Por ser regra de exceção, a interpretação deverá ser restritiva, sem admitir outras hipóteses (GUEDES; MEIRELES, 2019, p. 120).

4 RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO DOS DADOS PESSOAIS

A Lei Geral de Proteção de Dados estabeleceu, pela primeira vez no ordenamento jurídico brasileiro, um conjunto de normas vocacionadas a regular o tratamento de dados pessoais em todas as atividades do cotidiano e setores da economia (BIONI; DIAS, 2020, p. 2). Por meio do processamento desses dados pessoais, extrai-se a possibilidade de conhecer seus titulares e, diante dos riscos que esse cenário representa aos indivíduos, o objetivo da lei foi delimitar as obrigações dos agentes de tratamento e fixar um regime jurídico próprio de responsabilização civil (MENDES; DONEDA, 2018, p. 9).

O surgimento da era digital tem suscitado a necessidade de repensar importantes aspectos de organização social, democracia, tecnologia, privacidade e liberdade, sendo que muitos enfoques não apresentam a sofisticação teórica que determinados problemas requerem (LÉVY, 2000, p. 833). A proteção de dados pessoais consiste em um dos mais sensíveis desafios que o direito contemporâneo vem enfrentando em virtude do avanço tecnológico verificado nas últimas décadas (SCHREIBER, 2020, p. 577).

A partir da vigência da LGPD, o tema deixou de ser tangenciado pelas leis esparsas, ao passo que trouxe uma maior segurança jurídica; não obstante, a Lei não foi direta ao determinar o regime de responsabilidade civil a ser adotado em caso de tratamento irregular de dados, inexistindo entendimento consolidado, uma vez que os tribunais e a doutrina vêm apresentando entendimentos divergentes.

As novidades tecnológicas instigam a formulação de novas regras e soluções, no intuito de viabilizar respostas que se repute apropriadas aos novos desafios da atualidade (TEPEDINO; SILVA, 2019, p. 70). É necessário interpretar a legislação em consonância com o momento histórico a que está inserida, de modo que os cidadãos não sejam prejudicados pela ausência de adequação teórica.

Passa-se, portanto, ao estudo do regime de responsabilidade civil adotado pela LGPD, em face dos danos decorrentes da violação da legislação e das normas técnicas voltadas à segurança dos dados pessoais, que se revela a principal novidade trazida pela Lei. Dessa forma, este capítulo tratar-se-á sobre os agentes de tratamento de dados, a atividade que desempenham e qual será o regime de responsabilidade civil a ser aplicado como regra geral nos casos envolvendo a proteção dos dados pessoais.

A Lei Geral de Proteção de Dados estabeleceu um conjunto de regras e princípios vocacionados a regular o tratamento dos dados pessoais em todas as atividades do cidadão e

dos setores da economia. Diante dos riscos que o titular de dados experencia em virtude desse tratamento, a Lei empregou um regime de responsabilidade civil próprio, em seu Capítulo IV, Seção III, sobre responsabilidade e ressarcimento de danos, da LGPD, que demonstra que os efeitos resultantes dessa realidade deverão ser compensados e, preferivelmente, mitigados (COSTA, 2012).

Contudo, a doutrina brasileira vem desafiando um exercício difícil de dogmática jurídica: definir qual o regime geral de responsabilidade civil dos agentes de tratamento de dados previsto na legislação (BIONI; DIAS, 2020, p. 2), uma vez que a Lei não foi explícita acerca de qual o regime de responsabilidade civil a ser aplicado diante do tratamento que causar danos aos titulares de dados, em decorrência da inobservância das disposições legais (SANTOS *et al.*, 2021, p. 4).

Verifica-se que existem duas situações que ensejam a responsabilização civil na lei em estudo: as que decorrem da violação da LGPD propriamente dita e as que violam normas técnicas voltadas à segurança e à proteção dos dados pessoais (art. 42, § 1º, LGPD). No entanto, mister salientar que, em que pese tais disposições, a Lei não especificou qual a espécie de responsabilidade civil adotada, por isso se faz necessário um aprofundamento nos estudos acerca da matéria.

Em linhas gerais, nas hipóteses em que houver o descumprimento da Lei pelos agentes de tratamento, estes poderão estar sujeitos a ações indenizatórias individuais; ações indenizatórias coletivas; sanções administrativas por parte de órgãos de proteção ao consumidor; ou sanções administrativas aplicadas pela ANPD – importante destacar, contudo, que o tratamento irregular dos dados pessoais pelos agentes de tratamento poderá ensejar em sua responsabilização tanto no âmbito civil quanto nos campos do direito penal e administrativo (SANTOS *et al.*, 2021, p. 5).

Com efeito, o agente que, no exercício do tratamento dos dados, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à Lei, será obrigado a repará-lo (KLEE; PEREIRA NETO, 2019, p. 25). O art. 22 da Lei, prevê que a defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo por meio de tutela individual ou coletiva. Em síntese, a tutela judicial do titular dos dados abarca medidas preventivas e providências processuais que buscam evitar, reparar e compensar os direitos violados (BESSA; NUNES, 2021, p. 1.172).

A partir do momento que o ordenamento jurídico institui direitos, o faz para disciplinar a relação entre as partes e mitigar as suas violações; estas, por sua vez, são atos ilícitos que acarretam o dever de indenizar (OLIVEIRA, 2019, p. 36). A responsabilidade civil dos agentes,

portanto, ocorrerá a partir do ato ilícito e terá como objetivo tornar indene o prejudicado e reestabelecer a situação em que ele estaria caso não tivesse sofrido o dano (ARAÚJO; FIGUEREDO, 2020, p. 343).

Tal responsabilidade, aliás, não será somente do controlador, mas também do operador; este se submete aos comandos daquele, entretanto, também possui o dever de desempenhar suas atividades sob a égide da legislação e aplicar as medidas necessárias e adequadas para a segurança dos dados pessoais (OLIVEIRA, 2019, p. 39). Nessa toada, a Lei instituiu que haverá responsabilidade solidária entre o controlador e o operador, nas seguintes situações:

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

§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I - o **operador** responde **solidariamente** pelos danos causados pelo tratamento **quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;**

II - os **controladores** que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem **solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.** [...] (BRASIL, 2018). (Grifo nosso).

Tal previsão busca garantir a efetiva indenização ao titular de dados (OLIVEIRA, 2019, p. 40). A primeira delas é a solidariedade entre o controlador e o operador, nas hipóteses em que este descumprir com as obrigações da legislação de proteção de dados ou quando não estiver seguindo as instruções lícitas do controlador; a segunda previsão, por sua vez, será verificada quando dois ou mais controladores estiverem diretamente envolvidos no tratamento dos dados pessoais.

Observa-se que o operador somente será condenado a ressarcir o titular caso a atividade de tratamento não seja realizada em conformidade com as obrigações estipuladas previamente pelo controlador ou caso viole um dispositivo da Lei. Sua obrigação, portanto, será a de fornecer garantias de implementação de medidas técnicas e organizacionais adequadas ao propósito do tratamento, de forma a cumprir com os requisitos legais de segurança determinados pela legislação (KREMER, 2020, p. 306). O controlador, no entanto, incumbir-se-á de responder por todos os danos e incidentes causados ao titular de dados em virtude do tratamento, salvo nos seguintes casos:

Art. 43. Os agentes de tratamento só **não** serão responsabilizados quando provarem:

I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;

II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou

III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro. (BRASIL, 2018) (Grifo nosso).

O dispositivo, portanto, determina as situações em que o dano sofrido pelo titular não terá relação com a conduta dos agentes. A reparação do dano, como se vê, somente poderá ser exigida de quem tenha realizado o tratamento dos dados de alguma forma (inciso I), caso contrário, não haverá nexo de causalidade entre o dano e o suposto ato ilícito. Ademais, quando, apesar do dano, o agente demonstrar que não descumpriu nenhuma norma de segurança, será afastado o seu dever de indenizar a vítima (inciso II).

Por fim, será inexistente a obrigação de reparar o dano quando o agente comprovar que o prejuízo foi causado por culpa exclusiva do titular ou de terceiro (inciso III). Percebe-se que tais excludentes irão depender de um robusto conjunto probatório por parte dos agentes de tratamento de dados, acabando por se tratar de um processo complexo e extenso (OLIVEIRA, 2019, p. 42).

Os artigos 42 a 45 tratam de seção específica da LGPD, que dispõe sobre responsabilidade e ressarcimento dos danos causados pelos agentes de tratamento. A seção embarca a solidariedade; inversão do ônus da prova; danos coletivos; direito de regresso; excludentes de responsabilidade; tratamento irregular de dados; e aplicação legal diante das relações de consumo. Em contrapartida, há uma lacuna a respeito do regime de responsabilidade civil a ser aplicado aos agentes de tratamento de dado e a doutrina e a jurisprudência estão distantes de apresentarem uma solução unânime para essa problemática ainda muito recente na comunidade jurídica (KREMER, 2020, p. 312).

Uma parte da doutrina entende que impera na Lei a responsabilidade civil subjetiva e, outra, que seria a responsabilidade objetiva (TEIXEIRA, 2021, p. 13). Não obstante, como será demonstrado, a questão não deve ser pautada em uma premissa de falsa dualidade de regimes jurídicos de responsabilidade civil – se objetiva ou subjetiva (BIONI; DIAS, 2020, p. 2) -, ao passo que a Lei instituiu um regime de responsabilidade civil próprio para situações envolvendo os danos decorrentes do tratamento dos dados pessoais (NOVAKOSKI; NASPOLINI, 2020, p. 2). A LGPD possui uma redação baseada em princípios gerais, o que permite que haja interpretações adequadas perante a realidade a que está inserida, garantindo, concomitantemente, o desenvolvimento das atividades empresariais e a efetiva proteção do cidadão (LEONARDI, 2019, p. 85).

4.1 A CORRENTE SUBJETIVISTA DA RESPONSABILIDADE CIVIL NA LGPD

Para que haja incidência de responsabilidade civil, deverá haver uma ação ou omissão por parte de um agente; restar configurado dano a outrem; existir nexos causal entre o ato e o prejuízo experienciado pela vítima; e, salvo determinadas situações, será necessária a demonstração da culpa do agente. O Código Civil adota como regra geral a teoria subjetiva da responsabilidade civil, impondo a necessidade da demonstração da culpa do agente; porém, também adota a teoria do risco, afastando tal necessidade em casos específicos, qual seja nas hipóteses de responsabilidade civil objetiva (TEIXEIRA, 2021, p. 32). A LGPD, por sua vez, determina que os operadores e os controladores que falharem na proteção dos dados pessoais estarão sujeitos às sanções administrativas e à responsabilização civil e, ocorrendo quaisquer incidentes de segurança, deverão comunicar ao titular e à ANPD.

Ambas as correntes possuem uma premissa comum, qual seja o argumento de que a Lei padece de grave inexatidão terminológica (TASSO, 2020, p. 104), uma vez que o enunciado de seu artigo 42 não foi suficientemente claro quanto ao regime de responsabilidade civil adotado (CAPANEMA, 2020, p. 166). Sem embargo, essas duas facetas da responsabilidade divergem quanto aos fundamentos que ensejam a incidência do dever de indenizar; de um lado, a responsabilidade subjetiva exige a demonstração de culpa do agente, enquanto, de outro, a responsabilidade civil objetiva fundamenta-se no risco inerente à atividade praticada que, mesmo sem a constatação de culpa, poderá ensejar no dever de indenizar (SCALETSCKY; VAZ, 2020, p. 16).

De acordo com a corrente subjetivista, o silêncio do legislador na previsão direta da responsabilidade civil objetiva, inseriria como regra geral a responsabilidade subjetiva; isto é, para afastar o pressuposto da culpa, a conduta deveria estar prevista em lei ou importar em atividade de risco, nos termos do art. 927 do Código Civil⁹ (GONDIM, 2021, p. 25). Desse modo, pelo fato de a responsabilidade objetiva ser uma exceção à regra, ela deveria ter sido indicada expressamente no corpo da Lei, caso fosse a opção do legislador (OLIVEIRA, 2019, p. 41).

O artigo 42, em contrapartida, não emprega a expressão “independentemente da existência de culpa”, como fizeram o Código Civil (artigos 927, parágrafo único, e 931) e o

⁹ Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. Parágrafo único. **Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.** (BRASIL, 2002) (Grifo nosso).

Código de Defesa do Consumidor (artigos 12 e 14), o que poderia ensejar na preferência pela responsabilidade subjetiva (SCHREIBER, 2020, p. 584), como se vê:

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, **em violação à legislação de proteção de dados pessoais**, é obrigado a repará-lo. (BRASIL, 2018) (Grifo nosso).

A corrente aponta para a parte final do art. 42, que alude ao dano causado “em violação à legislação de proteção de dados pessoais”, expressão que sugeriria uma responsabilidade fundada na violação de deveres jurídicos (culpa normativa) (SCHREIBER, 2020, p. 584). Nesse sentido, se a culpa traduz a violação a um dever jurídico, a referência do aludido artigo a uma responsabilidade pela violação da legislação demonstraria a consagração da responsabilidade subjetiva pela LGPD (SCHREIBER, 2020, p. 585). Além disso, o artigo 43 da Lei estipula que os agentes de tratamento somente não serão responsabilizados em situações determinadas:

Art. 43. **Os agentes de tratamento só não serão responsabilizados quando provarem:**

- I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
 - II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
 - III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.
- (BRASIL, 2018) (Grifo nosso).

A estipulação dos deveres a serem cumpridos pelos agentes de tratamento de dados é outro fundamento levantado pela corrente no intuito de demonstrar que a opção do legislador foi o regime subjetivo de responsabilidade civil, uma vez que não seria lógico a existência de tais deveres, se não fosse para a avaliação do pressuposto da culpa (GONDIM, 2021, p. 7); de modo que responsabilizar os agentes, independentemente da configuração de culpa, não seria compatível com o ordenamento jurídico em questão (SANTOS *et al.*, 2021, p. 13). Entretanto, como será adiante demonstrado, a atividade de tratamento deverá observar parâmetros estipulados na Lei que vão além da simples leitura do art. 43, para que seja possível compreender quando deverá ocorrer a responsabilização e quando não.

Para mais, lembram seus defensores que, em versões anteriores do Projeto de Lei que deu origem à LGPD, foram incluídas disposições que conceituavam, expressamente, a atividade de tratamento de dados como atividade de risco e que independiam da existência de culpa dos agentes para ensejar em sua responsabilização; no entanto, tais previsões foram retiradas no decorrer do processo legislativo (BRUNO, 2019, p. 366).

Contudo, o fato de o legislador haver optado em retirar tais disposições do texto da Lei, apenas indica que sua escolha não foi o regime de responsabilidade civil objetiva como regra geral; porém, isso não quer dizer que o regime escolhido foi o da responsabilidade

subjetiva, uma vez que, como já visto, não se deve limitar a interpretação da Lei à suposta dualidade de regimes, sendo possível ir além dessa distinção.

Diante do exposto, seria possível um observador menos atento crer que o legislador teria optado pelo regime da responsabilidade civil subjetiva (MORAES; QUEIROZ, 2019, pp. 126-127). Tal regime, entretanto, atribuiria um ônus desproporcional ao titular de dados (KREMER, 2020, p. 312), uma vez que as condições para a produção probatória são extremamente mais acessíveis aos próprios agentes de tratamento do que aos titulares dos dados, visto que aqueles possuem capacidade técnica e contextual muito mais favorável do que os titulares (OLIVEIRA, 2019, p. 44). Passa-se, portanto, à análise dos argumentos apresentados pela corrente objetivista sobre o regime de responsabilidade civil adotado pela Lei Geral de Proteção de Dados.

4.2 A CORRENTE OBJETIVISTA DA RESPONSABILIDADE CIVIL NA LGPD

A responsabilidade civil objetiva desloca-se da noção da culpa para a ideia do risco, ora encarado como “risco-proveito”, em que será reparável o dano causado a outrem em consequência de uma atividade realizada em benefício do responsável; ora como “risco-criado”, a que se subordina todo aquele que, sem indagação de culpa, expuser alguém a suportar um perigo (GONÇALVES, 2021, p. 19).

Nesse sentido, a corrente objetivista entende que a LGPD possui como um de seus principais fundamentos a mitigação do risco, ligado de forma intrínseca ao tratamento dos dados, vinculando a obrigação de reparação do dano ao exercício da atividade dos agentes de tratamento de dados (MENDES; DONEDA, 2018, p. 477). Essa atividade possui uma potencialidade danosa considerável, que poderá prejudicar o titular diante de incidentes de segurança, como vazamentos não intencionais e invasão de sistemas ou bases de dados por terceiros não autorizados (MULHOLLAND, 2020).

Nessa toada, a interpretação do art. 42 da LGPD deveria ser realizada em atenção ao risco inerente à atividade de tratamento de dados, eliminando a situação na qual a vítima seria forçada a suportar um dano em razão da dificuldade, prática, financeira ou probatória, de comprovar a culpa do agente (NOVAKOSKI; NASPOLINI, 2020, p. 11). Nessa linha de raciocínio, não faria sentido a LGPD ter criado um sistema de proteção de dados que, em sua

concretização, propiciasse uma situação de perpetuação desse estado de lesão (BARRETO JÚNIOR *et al.*, 2018, p. 253).

Desse modo, para caracterizar a responsabilidade dos agentes quanto ao tratamento irregular dos dados, não se deveria perquirir se a falha se deu por culpa ou dolo, mas bastaria a constatação da sua ocorrência (MIRAGEM, 2019, p. 26). Enfim, a evidência do nexo causal entre a conduta do agente e o dano sofrido pelo titular, somada ao risco intrínseco à atividade de tratamento de dados, importaria na responsabilização objetiva dos agentes, independentemente da existência de culpa (TEIXEIRA, 2021, p. 59).

Conforme já mencionado no subcapítulo anterior, tanto na primeira versão do Projeto de Lei da Proteção dos Dados pessoais quanto na proposta legislativa feita pelo Senado Federal, houve a expressa adoção de um regime de responsabilidade civil objetiva: a primeira preceituava que o tratamento dos dados seria uma atividade de risco e a segunda que os agentes de tratamento responderiam independentemente da existência de culpa, pela reparação dos danos (BIONI; DIAS, 2020, p. 5).

Tal constatação é realizada pela corrente objetivista para asseverar que o legislador teria optado por um regime de responsabilidade civil objetiva. Entretanto, como demonstrado, a corrente subjetivista refuta tal fundamentação devido ao fato de que tais disposições foram excluídas do texto final da Lei, o que poderia significar que o legislador, afinal, teria optado pela não aplicação do regime da responsabilidade objetiva na Lei.

Outro ponto levantado pelos defensores da corrente objetivista é o fato de que o artigo 44 da LGPD teria exprimido uma versão adaptada da noção de defeito do serviço, constante do artigo 14, § 1º, do Código de Defesa do Consumidor, conforme se vê diante da seguinte comparação:

Art. 44, Lei Geral de Proteção de Dados	Art. 14, § 1º, Código de Defesa do Consumidor
<p>Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:</p> <p>I - o modo pelo qual é realizado;</p> <p>II - o resultado e os riscos que razoavelmente dele se esperam;</p> <p>III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.</p> <p>Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano. (BRASIL, 2018) (Grifo nosso)</p>	<p>Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.</p> <p>§ 1º O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais:</p> <p>I - o modo de seu fornecimento;</p> <p>II - o resultado e os riscos que razoavelmente dele se esperam;</p> <p>III - a época em que foi fornecido. (BRASIL, 1990) (Grifo nosso)</p>

A LGPD, portanto, teria empregado uma construção análoga à matéria empregada na legislação consumerista, que se ocupa da responsabilidade do fornecedor de produtos ou serviços, cuja configuração prescinde da verificação de culpa do causador do dano, isto é, da responsabilidade objetiva (SCHREIBER, 2020, pp. 587-588). Entretanto, observa-se que no caput do art. 14 do CDC consta expressamente que o fornecedor de serviços irá responder pelos danos causados aos consumidores “independentemente da existência de culpa” e, o art. 44 da LGPD, em contrapartida, não apresenta tal disposição manifestamente.

Ademais, a corrente alega que, a partir do Tema Repetitivo nº 710 do Superior Tribunal de Justiça, haveria uma tendência do Tribunal em apontar a responsabilidade objetiva do responsável pelo banco de dados pessoais, o que indicaria que o reconhecimento da responsabilidade civil dos agentes de tratamento de dados poderia seguir o mesmo caminho (TEIXEIRA, 2021, p. 62):

O desrespeito aos limites legais na utilização do sistema "*credit scoring*", configurando abuso no exercício desse direito (art. 187 do CC), **pode** ensejar a responsabilidade objetiva e solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente (art. 16 da Lei n. 12.414/2011) pela ocorrência de danos morais **nas hipóteses de utilização de informações excessivas ou sensíveis (art. 3º, § 3º, I e II, da Lei n. 12.414/2011), bem como nos casos de comprovada recusa indevida de crédito pelo uso de dados incorretos ou desatualizados.** (BRASIL, 2014).

Como se vê, o Tema Repetitivo é bastante específico em sua normatização, sendo que somente poderá - isto é, a depender da análise do caso concreto - ensejar na responsabilidade objetiva do responsável pelo banco de dados a indenizar, somente o dano moral, especificamente nos casos de utilização de informações excessivas ou sensíveis ou quando comprovada recusa indevida de crédito pelo uso de dados incorretos ou desatualizados dos titulares. Desse modo, o fundamento da corrente objetivista não evidencia qual o regime geral de responsabilidade civil adotado pela LGPD, mas somente demonstra uma das exceções à regra.

À vista disso, a Lei também prevê que, extraordinariamente, deverá ocorrer a incidência da responsabilidade objetiva no âmbito das relações de consumo (art. 45, LGPD) e, em atenção ao art. 37, § 6º, da Constituição Federal, no tratamento dos dados pessoais pelas pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos.

Importante salientar que, apesar de a regra geral não ser a responsabilidade objetiva, o titular não terá o dever de comprovar a culpa do agente, caso seja verossímil sua alegação; haja a constatação de hipossuficiência para fins de produção de prova; ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa, por meio da previsão na legislação da possibilidade de inversão do ônus probatório em favor do titular de dados:

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

§ 2º **O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados** quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa. [...] (BRASIL, 2018) (Grifo nosso).

Como se vê, o ônus da prova não é estático, podendo ser invertido nas situações previstas no § 2º, no intuito de auxiliar a resolução do mérito, de forma mais ágil e acurada. Desse modo, a vítima terá que comprovar a realização de algum tratamento de dados, o dano sofrido e o nexo causal entre o tratamento e o dano, restando aos agentes o dever de comprovar a não ocorrência de algum dos elementos que caracterizam a sua responsabilidade (de acordo com o art. 43 da Lei), se for o caso (BIONI; DIAS, 2020, p. 18). Tal medida se dá pelo fato de os agentes de proteção de dados possuírem todas as informações acerca da atividade e terem o dever de manter os registros da atividade de tratamento pelo tempo previsto na legislação¹⁰ (OLIVEIRA, 2019, p. 43).

Diante disso, “a LGPD se alinha com toda a legislação vigente, de modo coerente e seguro, na busca pela reparação efetiva e justa, guardando as especificidades de cada contexto” (OLIVEIRA, 2019, p. 45). A controvérsia da natureza jurídica do regime de responsabilidade adotado pela Lei, portanto, fica restrita às situações em que não existirem uma relação de consumo entre o titular e o agente de tratamento ou uma relação que envolva o titular e o Poder Público.

O regime da LGPD, assim, apresenta um papel residual, sendo aplicável, por exemplo, nas relações entre associações e associados ou empregadores e empregados (SANTOS *et al.*, 2021, p. 9). Com efeito, o que fez a Lei foi indicar que o regime de responsabilidade civil adotado não foi o da responsabilidade civil objetiva (SANTOS *et al.*, 2021, p. 17).

Diante do exposto, detém-se que a corrente objetivista entende que, em virtude do risco intrínseco à atividade de tratamento desempenhada pelos agentes, a ocorrência do dano, por si só, deveria ter o condão de ensejar na responsabilização dos agentes. Entretanto, essa alternativa enfraqueceria a intencionalidade da Lei em construir e fomentar um sistema de gerenciamento de riscos nas instituições (KREMER, 2020, p. 312).

¹⁰Art. 37. **O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem**, especialmente quando baseado no legítimo interesse. (BRASIL, 2018) (Grifo nosso).
Art. 40. **A autoridade nacional poderá dispor** sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como **sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência**. (BRASIL, 2018) (Grifo nosso).

É necessário sopesar o desenvolvimento empresarial e tecnológico e a proteção do direito do titular de dados, ao passo que, caso fosse aplicada a responsabilidade objetiva como regra geral, poderia haver o seu prejuízo de tal desenvolvimento e, caso fosse o regime da responsabilidade subjetiva, os titulares restariam prejudicados diante da necessidade de constatação de culpa do agente de tratamento. Com efeito, é imprescindível que a discussão vá além da análise binária do regime jurídico de responsabilidade civil (BIONI; DIAS, 2020, p. 21), a fim de determinar a regra geral prevista na Lei.

4.3 A RESPONSABILIDADE PROATIVA

Foi observado nos últimos subcapítulos que os defensores das correntes da responsabilidade objetiva e subjetiva, em síntese, debatem acerca da necessidade de demonstração, ou não, da culpa do agente de tratamento em casos de violação à LGPD. O art. 42 da Lei exprime que haverá responsabilização do agente em casos de violação, contudo, tal previsão é extremamente abrangente e deve ser analisada em consonância com os demais artigos e princípios da legislação, para que se entenda, de fato, quando será enquadrada a violação legal.

O art. 43, por sua vez, prevê os casos em que não haverá responsabilização dos agentes: quando não realizarem o tratamento; quando não houver violação da Lei; ou quando a culpa for do titular ou de terceiro. Isto é, quando os agentes realizarem o tratamento e houver violação que ocasione um dano ao titular, sem culpa deste ou de terceiro, deverá haver a sua responsabilização. Entretanto, é necessário compreender quando será caracterizada tal violação e, nesse sentido, o artigo 44 da Lei prevê o seguinte:

Art. 44. **O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:**

I - o modo pelo qual é realizado;

II - o resultado e os riscos que razoavelmente dele se esperam;

III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Parágrafo único. **Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.** (BRASIL 2018) (Grifo nosso).

Depreende-se que quando ocorrer violação da Lei ou quando não for fornecida a segurança que o titular puder esperar do tratamento, este será caracterizado como irregular. Quando ocorrer violação, portanto, haverá o dever de indenizar (art. 42), porém, o parágrafo

único do art. 44 prevê que também ocorrerá tal dever nas hipóteses em que advirem danos em virtude da violação da segurança.

Com efeito, a responsabilização não ocorrerá somente em caso de violação à LGPD, é impreterível que se interprete o art. 42 em conjunto com o parágrafo único do art. 44, que institui uma hipótese adicional de responsabilidade civil, qual seja a ausência de adoção das medidas protetivas indicadas no art. 46. Desse modo, havendo tratamento irregular – inobservância à Lei ou ausência de segurança que o titular poderia esperar -, haverá o dever de indenizar, consideradas as circunstâncias relevantes, previstas nos incisos I a III do art. 44 e no art. 46, que, por sua vez, assim dispõe:

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

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. (BRASIL, 2018) (Grifo nosso).

A ilicitude da atividade desempenhada pelos agentes de tratamento, portanto, será determinada pelo descumprimento da legislação ou pela frustração da expectativa do titular sobre o procedimento, tendo em vista que se trata de uma relação contratual, que preza pela transparência e boa-fé (OLIVEIRA, 2019, p. 44).

Apesar de a expectativa do titular ser um critério subjetivo, os incisos I a III do art. 44, no intuito de mitigar a insegurança jurídica, esmiuçou quais serão as circunstâncias que deverão ser analisadas para que haja a caracterização do tratamento como irregular, quais sejam o modo pelo qual é realizado; o resultado e os riscos que razoavelmente dele se esperam; e as técnicas disponíveis à época do tratamento (OLIVEIRA, 2019, p. 44). Não se trata, contudo, de qualquer expectativa de segurança, mas de expectativas juridicamente legítimas (BIONI; DIAS, 2020, p. 13).

Os agentes de tratamento, portanto, deverão ajustar os parâmetros de segurança a serem aplicados, na medida em que correspondam à probabilidade e à gravidade que eventuais violações possam assumir em face do impacto aos direitos dos titulares, isto é, deverão estimar os riscos e aplicar as medidas de segurança correspondentes (BIONI; DIAS, 2020, p. 16).

A Lei dispõe, entretanto, que deverão ser consideradas somente as técnicas disponíveis à época do tratamento - o que é diferente de “existentes”; isto é, imagine, por exemplo, que em um país esteja sendo testado um sistema de segurança extremamente eficiente, mas que ainda não esteja sendo comercializado fora daquele país, tal sistema existe, porém ainda não estaria disponível aos demais; ou, ainda, caso o produto viesse a ser comercializado em outros países,

porém, com um valor exorbitantemente alto, nesse caso, dever-se-ia ser analisada a possibilidade de o controlador ter acesso ao determinado sistema, a depender de seu padrão econômico (COTS; OLIVEIRA, 2019, p. 186).

Nesse sentido, os profissionais que se encarregarem do tratamento dos dados pessoais, em atenção ao princípio da segurança (art. 6º, VII), deverão mantê-los preservados em um ambiente seguro, observadas as técnicas, procedimentos e tecnologias que garantam a sua proteção, para que haja a mitigação de eventuais acessos não autorizados, vazamentos, perda, alteração ou destruição dos dados (TEIXEIRA, 2021, p. 24).

Em uma sociedade em que as operações realizadas com dados pessoais crescem e se tornam mais necessárias a cada dia, é fundamental que a atividade de tratamento seja regulamentada com requisitos de segurança adequados a serem observados pelos agentes, para evitar vazamentos de dados e danos aos titulares (MENKE; GOULART, 2021, p. 616). O que se busca, em linhas gerais, é que os agentes de tratamento conheçam a sua base de dados e estejam preparados para gerir riscos de segurança, seguindo as normas e organizando sua atividade por meio de políticas, bem como que estejam preparados para agir em caso de incidentes (MENKE; GOULART, 2021, p. 628).

Como uma extensão a esse princípio, o princípio da prevenção (art. 6º, VIII) determina que haja a adoção de medidas prévias para evitar fortuitos na atividade de tratamento, por meios de mitigação de riscos. Aqui ganha importância a figura do encarregado de dados, que fará a intermediação entre os agentes, a ANPD e os titulares de dados, bem como irá orientar os funcionários para que atuem em conformidade com a Lei (GOMES, 2020, p. 77).

Por fim, o princípio da responsabilização e prestação de contas (art. 6º, X), determina que os agentes deverão tomar todas as medidas cabíveis a cumprir com as exigências legais de forma comprovadamente eficaz, mantendo as evidências das medidas e demonstrando sua probidade e boa-fé (LIMA, 2020, *apud* TEIXEIRA, 2021, p. 26). Ao prever tal princípio, a intenção da Lei foi de alertar os agentes de tratamento de que eles são responsáveis pelo fiel cumprimento das exigências legais, não bastando somente cumprir a legislação, mas adotando medidas aptas a mitigar os riscos inerentes à atividade (VAINZOF, 2019, p. 153).

A união da responsabilização dos agentes ao conceito de prestação de contas demonstra um novo sistema de responsabilidade previsto pela LGPD. Com efeito, tal sistema, previsto nos artigos 42 a 46 da Lei, mostra-se especialíssimo, uma vez que prevê a necessidade de demonstração, pelo agente de tratamento, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados, bem como a eficácia dessas medidas (MORAES; QUEIROZ, 2019, p. 126).

O legislador, dessa forma, busca prevenir e evitar a ocorrência de tais danos, determinando às empresas que ajam proativamente na sua prevenção, por meio da identificação dos riscos e da escolha das medidas apropriadas para sua mitigação (MORAES, 2019, p. 5). Não se trata mais, portanto, da aplicação das regras da responsabilidade subjetiva ou objetiva, mas da responsabilidade proativa, hipóteses em que não é suficiente que os agentes de dados cumpram os artigos da lei, mas que também seja demonstrada a adoção de medidas eficazes.

As características peculiares da hipótese de responsabilidade civil em questão possibilitam garantir a efetividade do recurso da compensação, adaptando-o às especificidades da atividade de processamento de dados e aos requisitos de proteção que ele apresenta; desse modo, tem-se um modelo mais maduro de responsabilização civil (MORAES; QUEIROZ, pp. 133-134). Diante disso, deverá existir um juízo de valor em torno da atividade, para que haja, ou deixe de haver, a responsabilização dos agentes (BIONI; DIAS, 2020, p. 8).

5. IMPLEMENTAÇÃO DA RESPONSABILIDADE PROATIVA

Foi visto no capítulo anterior que a LGPD previu a responsabilidade proativa em caso de tratamento irregular pelos agentes de tratamento de dados e não das responsabilidades subjetiva ou objetiva, com a análise da necessidade de comprovação, ou não, de culpa. Dessa forma, buscou-se equilibrar a proteção ao direito dos titulares de dados e o avanço tecnológico, por meio de aplicação de medidas de segurança aptas à proteção dos dados dos titulares.

Ao interpretar a Lei, depreende-se que não bastará ao agente a simples comprovação de que não violou dever jurídico, mas que aplicou as melhores medidas de segurança possíveis à época do tratamento. Assim, caso demonstrem a aplicação de métodos técnicos e administrativos que deles seria possível esperar, mas que, mesmo assim, ocorreu um incidente, poderão se escusar do dever de indenizar, ou, ao menos, reduzirem a sua condenação.

Essas situações deverão ser ponderadas a partir da análise dos artigos 42 a 46 da Lei, bem como de seus princípios. Em suma, o art. 42 determina que deverá haver a responsabilização civil dos agentes de tratamento em caso de violação à legislação. O art. 44, por sua vez, apresenta uma segunda alternativa de responsabilização dos agentes: quando não houver a aplicação da segurança que puder ser esperada pelo titular.

Essa expectativa do titular será delimitada pelo art. 46, que determina que as medidas de segurança técnicas e administrativas deverão ser aptas a proteger as bases de dados, e pelos incisos I a III do art. 44, com o confronto do modo pelo qual o tratamento foi realizado, o resultado e os riscos que razoavelmente dele poder-se-iam esperar e as técnicas disponíveis à época. Por fim, será necessário avaliar também os princípios da segurança, da prevenção e da responsabilização e prestação de contas, que exigirão dos agentes a manutenção de um ambiente seguro, adoção de medidas prévias e a demonstração de sua eficácia.

Essas medidas deverão ser observadas de forma a atender os requisitos de segurança, os padrões de boas práticas e de governança e os princípios gerais previstos na legislação, inclusive após o término do tratamento dos dados (VAINZOF, 2019, p. 143). Pressupõe-se que os agentes possuam a *expertise* necessária para garantir a integridade dos dados e a preservação dos direitos dos titulares, sendo que o risco da atividade está intrinsecamente ligado ao dever de segurança que lhes é imputável (TEIXEIRA, 2021, p. 58).

Exigir-se-á, em síntese, atitudes conscientes, diligentes e proativas em relação à utilização dos dados pessoais (MORAES; QUEIROZ, 2019, p. 130), percebendo as novas demandas e oferecendo uma resposta à altura (OLIVEIRA, 2019, p. 13). Entretanto, além da

proteção dos dados pessoais, é preciso reconhecer a importância dos avanços tecnológicos e da livre iniciativa para o desenvolvimento humano e social (OLIVEIRA, 2019, p. 15).

O mercado de dados, em virtude do incremento tecnológico, possui influência direta na possibilidade de ocorrência de dano, proporcionalmente à sua importância econômica e abrangência (OLIVEIRA, 2019, p. 38). A LGPD, desse modo, aparece como um marco essencial para que as empresas e órgãos possam se adequar à nova realidade da proteção dos dados pessoais (OLIVEIRA, 2019, p. 38), instituindo mecanismos para impedir a causação do dano, que incidirá antecipadamente, com uma natureza multidisciplinar e transversal (LOPES, 2010, p. 1.230).

Para isso, o direito não poderá ser uma barreira à utilização de novas técnicas, devendo prevalecer um clima de cooperação dominado pela ética (WALD, 2001, p. 15). O jurista deve reconhecer tais mudanças e adotar medidas capazes de acompanhar a evolução tecnológica, deixando de buscar em paradigmas do passado as bases para as soluções das controvérsias atuais (TEPEDINO, 2008, pp. 23-24).

A LGPD, desse modo, estabelece obrigações a serem observadas no tratamento dos dados pessoais, prevendo uma série de procedimentos para estabelecer uma sistemática própria à aplicação de medidas preventivas e reparatórias (SCALETSCKY; VAZ, 2020, p. 15). Desse modo, os agentes precisam adotar parâmetros que sejam capazes de assegurar que aqueles que irão acessar os dados pessoais, tratá-los-ão em observância às instruções do controlador (VAINZOF, 2020, p. 144).

As inovações tecnológicas trazem a possibilidade de novos modelos de negócios, com novos desafios sobre a maneira que o referencial legal deverá ser repensado para manter o equilíbrio entre o estímulo da inovação e as formas de proteger as garantias e as liberdades individuais e coletivas (CARVALHO *et al.*, 2020, p. 7). Assim, tanto o controlador quanto o operador têm o dever de pensar regras e técnicas de proteção aos dados que possam efetivar a legislação nas atividades de tratamento (KREMER, 2020, p. 307).

5.1 BOAS PRÁTICAS E GOVERNANÇA

Em seu Capítulo VII, “da segurança e das boas práticas”, a LGPD prevê as Seções “da segurança e do sigilo dos dados” e “das boas práticas e da governança¹¹”, onde visa orientar sobre as medidas a serem tomadas no desempenho da atividade de tratamento dos dados (TEIXEIRA, 2021, p. 24). A primeira seção determina que os sistemas utilizados para o tratamento deverão atender aos requisitos de segurança, aos padrões de boas práticas e de governança, aos princípios gerais previstos na Lei e às demais normas regulamentares (art. 49).

A seção destinada às boas práticas e à governança, por sua vez, prevê que os agentes de tratamento de dados poderão formular regras e boas práticas que estabeleçam condições de organização; regime de funcionamento; procedimentos; normas de segurança; padrões técnicos; obrigações específicas aos envolvidos no tratamento; ações educativas; mecanismos internos de supervisão e mitigação de riscos; e outros aspectos relacionados ao tratamento (art. 50).

O aludido artigo determina que a aptidão dessas medidas deverá ser ajustada de acordo com as características da atividade de tratamento em questão (BIONI; DIAS, 2020, p. 20), levando em consideração a natureza do tratamento, o seu escopo, a finalidade, a probabilidade e a gravidade dos riscos e dos benefícios decorrentes do tratamento (art. 50, § 1º).

O § 2º, por sua vez, estipula que, na aplicação dos princípios da segurança e da prevenção, deverão ser observadas a estrutura, a escala e o volume das operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares de dados, podendo:

- I - implementar programa de governança em privacidade** que, no mínimo:
- a) demonstre o comprometimento do controlador em adotar **processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;**
 - b) seja aplicável **a todo o conjunto de dados pessoais** que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
 - c) seja **adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;**
 - d) estabeleça **políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;**
 - e) tenha o objetivo de estabelecer **relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;**
 - f) esteja **integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;**
 - g) conte com **planos de resposta a incidentes e remediação;** e
 - h) seja **atualizado constantemente** com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

¹¹De acordo com o Instituto Brasileiro de Governança Corporativa (IBGC), governança corporativa é o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas (IBGC, 2022).

II - **demonstrar a efetividade de seu programa de governança** em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei. (BRASIL, 2018) (Grifo nosso).

O art. 50 e seus parágrafos primeiro e segundo, portanto, são um possível caminho para dar densidade normativa aos incisos do art. 44 (BIONI; DIAS, 2020, p. 15), isto é, o modo pelo qual o tratamento é realizado (inciso I) e o resultado e os riscos que razoavelmente dele se esperam (inciso II) são calibrados pelas supramencionadas variações (art. 50, §§ 1º e 2º). A estrutura normativa da LGPD, portanto, parte do pressuposto de que haverá uma alta variação do potencial lesivo entre as diferentes atividades de tratamento de dados, sendo determinante a avaliação das maneiras pelas quais serão executadas e os riscos que delas derivam (BIONI; DIAS, 2020, p. 15).

A título de elucidação, imagine uma empresa nova de tecnologia, com poucos colaboradores, que forneça soluções de inteligência artificial para automatizar diagnósticos e prognósticos na área da oncologia; para isso, será necessário um grande volume de dados sensíveis dos pacientes de inúmeros hospitais e laboratórios, que será muito mais arriscado do que a atividade de tratamento de dados de consumidores desempenhada por uma grande rede de supermercados, com mais de quinhentos colaboradores, por exemplo (BIONI; DIAS, 2020, p. 16). Percebe-se a necessidade de ajustar as medidas de segurança ao ponto que correspondam à probabilidade e à gravidade que as violações possam vir a assumir, por meio da estimação dos riscos inerentes ao tratamento (BIONI; DIAS, 2020, p. 16).

Com a informatização quase total das atividades que visam o tratamento dos dados pessoais, praticamente todos os dados serão mantidos em sistemas que possam vir a apresentar uma vulnerabilidade capaz de ocasionar vazamentos ou destruição; em virtude disso, são necessárias práticas de segurança da informação, que busquem proteger a confidencialidade, integridade e disponibilidade dos sistemas e dos dados pessoais, protegendo-os contra acessos, usos e modificações não autorizados e garantindo que as informações estejam disponíveis sempre que necessárias (MENKE; GOULART, 2021, p. 622).

Ademais, um atributo importante, presente no Regulamento Europeu (GDPR, 2016), é o da resiliência, que se baseia na disposição à adaptação, isto é, no tratamento de dados irão ocorrer erros ou incidentes, mas é essencial que, diante disso, os sistemas e processos sejam recompostos e tenham as funcionalidades reestabelecidas, sem que tudo volte a ser como antes, mas que passe a funcionar com melhorias (MENKE; GOULART, 2021, p. 622). Com efeito, é necessário levar em consideração as vulnerabilidades, ameaças, incidentes e controle dos

processos¹², para que sejam atribuídas medidas técnicas e administrativas¹³ por meio de um programa de segurança da informação (MENKE; GOULART, 2021, p. 623).

Essas medidas estão em consonância com o art. 46 da Lei, uma vez que visam não só a proteção contra acessos não autorizados, mas também situações de perda, alteração ou qualquer tratamento inadequado ou ilícito (MENKE; GOULART, 2021, p. 624). Evidencia-se que para estar em conformidade com os ditames legais, os agentes deverão implementar soluções de natureza multidisciplinar, uma vez que os modelos de governança deverão adotar um conjunto de processos internos; controles tecnológicos; políticas corporativas; regulamentos; contratos; dentre outros – o que se vê é a sinergia entre direito e tecnologia, sendo que essa abordagem faz todo sentido diante da cultura digital que representa a atualidade (BRUNO, 2019, p. 373).

A economia do compartilhamento é uma realidade visível, que transforma mercados e estruturas sociais - como as formas de organização de trabalho, por exemplo; é a partir da compreensão desse contexto que devem ser pensadas formas de regulação capazes de proteger os direitos dos titulares de dados (CAMARGO, 2021, p. 31). Em uma realidade onde os métodos tradicionais não são capazes de salvaguardar os direitos e as liberdades individuais no tratamento de dados, novas formas de proteção são necessárias, conjuntamente com padrões regulatórios e métodos computacionais que garantam o fluxo de dados dentro dos padrões estabelecidos pela regulação (CAMARGO, 2021, p. 44).

A regulação da segurança em ambientes cibernéticos não é novidade no ordenamento brasileiro, a Lei do Cadastro Positivo menciona a necessidade de observância de aspectos técnico-operacionais, a utilização de certificações de adequação de segurança dos sistemas e políticas de segurança da informação; o Marco Civil da Internet também estabelece medidas de segurança como o estabelecimento de controle estrito sobre o acesso aos dados, previsão de

¹²Uma **vulnerabilidade** é uma fraqueza que atinge sistemas, ambientes, processos, protocolos, dentre outros; a **ameaça** é uma situação que pode atingir uma vulnerabilidade; o **incidente**, por sua vez, é um caso que envolve a afetação de uma vulnerabilidade a partir da ameaça; e os **controles** são as medidas utilizadas para impedir que um incidente ocorra ou para diminuir a probabilidade de sua ocorrência. Um exemplo de incidente pode ser uma situação em que um sistema possui uma falha técnica (vulnerabilidade), que viabilize a exploração por um agente não autorizado, ou, ainda, a publicação inadvertida de informações sigilosas (MENKE; GOULART, 2021, p. 623) (Grifo nosso). São muito recorrentes os acessos não autorizados, por meio de violações de mecanismos de segurança, que acarretem o vazamento de dados pessoais, em virtude da exploração das vulnerabilidades de um servidor.

¹³As **medidas administrativas** são aquelas que visam não somente a promoção da conformidade das ações com toda a LGPD, mas também aquelas que visam a organização da segurança da informação na instituição, por exemplo, políticas de segurança; *standards*; guias de procedimentos para controlar o comportamento dos agentes e prover um nível de proteção aos recursos computacionais e aos dados; minimização; anonimização; e transparência no tratamento. Já as **medidas técnicas** envolvem o uso de recursos, como *firewalls*; *antimalwares* e antivírus; controles de acesso nos sistemas operacionais; tokens; criptografia, dentre outros (MENKE; GOULART, 2021, p. 623).

mecanismos de autenticação, criação de inventário detalhado dos acessos aos registros e uso de solução de gestão dos registros (art. 13) (MENKE; GOULART, 2021, p. 624).

Os programas de boas práticas e governança previstos na Seção II do Capítulo VII da LGPD, por sua vez, deverão levar em consideração as medidas técnicas e administrativas; demonstrar o comprometimento por meio de políticas internas; a sua aplicação em todos os dados coletados; a realização de revisão e avaliação sistemáticas de impactos e riscos; o uso de plano de resposta a incidentes; e a realização de avaliações periódicas (MENKE; GOULART, 2021, p. 625). O controle do risco, como visto, é fundamental à segurança dos dados, em que o processo de sua gestão deverá passar pela análise de risco, com o objetivo de apurar quais as ameaças a que o ambiente está exposto e quais as medidas necessárias para seu controle (MENKE; GOULART, 2021, p. 627).

Além de todas as medidas profiláticas a serem aplicadas, em caso de incidente de segurança envolvendo dados pessoais, o controlador será o responsável por analisar se o evento poderá acarretar riscos ou danos aos titulares, para que seja, quando necessário, comunicado à ANPD e ao titular, dentro do prazo estipulado pela legislação, sendo ele o responsável por avaliar o cenário e adotar as medidas que entender serem pertinentes (VAINZOF, 2020, p. 156).

Em resumo, o que se busca é compreender as vulnerabilidades dos sistemas e projetar quais as medidas de correção necessárias, levando em conta a probabilidade da ocorrência do dano, sendo que o programa de governança deverá ser adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados (MENKE; GOULART, 2021, p. 627).

Importa observar que a indicação para a elaboração de códigos de conduta e programas de governança é facultativa na LGPD, contudo, as organizações são estimuladas a observar a regulação, diante da eventual necessidade de comprovação da correta aplicação da Lei (PALMEIRA, 2020, p. 336). Os códigos de conduta são, ao lado dos relatórios de impacto e de processos de certificação, um dos meios pelos quais a LGPD aponta para a consecução do princípio da responsabilização e prestação de contas, com o objetivo de ver a aplicação efetiva da Lei e facilitar a construção probatória (PALMEIRA, 2020, pp. 336-337).

As vantagens do desenvolvimento de programas de boas práticas e códigos de conduta têm relação direta com o grau das eventuais sanções a serem impostas em caso de violação do direito dos titulares de dados pela ANPD (PALMEIRA, 2020, p. 338). Caberá aos agentes de tratamento de dados, então, definir um conjunto de boas práticas internamente às instituições, que deverá ser seguido por todos os colaboradores, com a implementação dos processos

relativos à proteção de dados pessoais em todos os departamentos da instituição (GIOVANNINI JÚNIOR, 2019, pp. 88-89).

Essas medidas irão demonstrar o grau de comprometimento e a preocupação do controlador na manutenção de seus processos internos de acordo com a Lei, bem como a adoção de medidas aptas à proteção dos dados, que deverão ser revisadas e atualizadas regularmente (GIOVANNINI JÚNIOR, 2019, p. 89). Já os padrões técnicos mínimos para a proteção dos dados pessoais e o tempo de comunicação e remediação em caso de acidentes serão definidos por orientação da Autoridade Nacional de Proteção de Dados, como será adiante abordado.

5.2 A ATUAÇÃO DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS E A UNIFORMIZAÇÃO JURISPRUDENCIAL

Como visto no segundo capítulo, o texto original previsto no Projeto de Lei nº 53 de 2018 previa que a Autoridade Nacional de Proteção de Dados seria um órgão integrante da Administração Pública Federal Indireta, submetida a regime autárquico especial, vinculada ao Ministério da Justiça, com independência administrativa, mandato fixo e autonomia financeira (OLIVEIRA, 2020, p. 380).

Em virtude da edição da Medida Provisória nº 869 de 2018, que modificou o texto original da Lei e converteu-se na Lei nº 13.853, foi estabelecida a ANPD como integrante da Presidência da República, e, mais recentemente, a MP nº 1.124 de 2022 concedeu-lhe autonomia de autarquia de natureza especial, com a criação de um cargo comissionado de diretor-presidente, sem aumento de despesas; não obstante, suas competências e estrutura organizacional permaneceram as mesmas (BRASIL, 2022).

O objetivo da ANPD, portanto, é zelar, implementar e fiscalizar o cumprimento da LGPD no território nacional, mediante aplicação de sanções a seus infratores, e suas atividades incluem dispor sobre os padrões e técnicas a serem utilizadas em processos de anonimização de dados; determinar o término de tratamentos irregulares de dados; regulamentar a portabilidade de dados de um agente a outro; e assegurar os direitos dos titulares de dados (MORAES; QUEIROZ, 2019, p. 123).

Uma das formas de orientar a aplicação da responsabilidade proativa dos agentes de tratamento diante do dever de indenizar em caso de ocorrência de danos aos titulares é encontrada no § 1º do art. 46 da Lei:

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

§ 1º **A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia**, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei (BRASIL, 2018) (Grifo nosso).

Com efeito, espera-se da ANPD uma participação ativa, com a demonstração de boas práticas para os distintos setores da economia (MENKE; GOULART, 2021, p. 625), sendo um órgão fiscalizador e sancionador, disciplinado em um capítulo próprio - “Da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade” -, bem como é peça fundamental à implementação da Lei (BRANCO, 2020, p. 41).

A LGPD provocou importantes modificações nos setores público e privado e, diante disso, a definição final dos contornos da Lei é essencial para que os agentes de tratamento possuam uma maior segurança jurídica ao realizarem o tratamento dos dados pessoais (SOUZA *et al.*, 2020, p. 46).

A Lei estabeleceu que cabe exclusivamente à ANPD a aplicação das sanções previstas na LGPD e determinou a coordenação de sua atuação com os órgãos públicos competentes para aplicar sanções e normativas sobre o tema (OLIVEIRA, 2020, p. 381). No capítulo anterior ao da previsão da ANPD e de seu Conselho, há o capítulo “Da Fiscalização”, que prevê sobre as sanções administrativas em seus artigos 52 a 54, quais sejam advertência; multa simples de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no seu último exercício, excluídos os tributos, limitada a R\$ 50.000.000,00 por infração; multa diária, observado o limite anterior; publicização da infração; bloqueio dos dados pessoais a que se refere a infração; a eliminação desses dados; suspensão parcial do funcionamento do banco de dados; suspensão do exercício da atividade de tratamento; e proibição parcial ou total do exercício (BRASIL, 2018).

Essas sanções deverão estar de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios (art. 52, §1º):

- [...] I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
- II - a boa-fé do infrator;
- III - a vantagem auferida ou pretendida pelo infrator;
- IV - a condição econômica do infrator;
- V - a reincidência;
- VI - o grau do dano;
- VII - a cooperação do infrator;

VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
IX - a adoção de política de boas práticas e governança;
X - a pronta adoção de medidas corretivas; e
XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção. (BRASIL, 2018).

Além desses critérios, deverão ser observados os princípios da razoabilidade e proporcionalidade, já que a lei não é voltada exclusivamente à proteção dos indivíduos, mas também ao estímulo à inovação e às liberdades econômicas, tendo um propósito pedagógico (ALVES, 2020, p. 427).

Observa-se que, em consonância com o que foi visto no subcapítulo anterior, os incisos VIII e IX dispõem sobre a adoção de uma cultura corporativa de boas práticas, com a adoção de métodos preventivos e corretivos dos problemas, uma vez que os custos decorrentes desses incidentes serão analisados em proporção aos investimentos em cultura de proteção de dados e privacidade, ou ainda, de *compliance* (ALVES, 2020, p. 427). Nesse sentido, o art. 54 determina que o valor da sanção de multa diária aplicável às infrações deverá observar a gravidade da falta e a extensão do dano ou prejuízo causado (BRASIL, 2018).

A adoção de medidas técnicas e organizacionais é crucial para avaliar a conduta do agente de tratamento, caso este possua um sólido programa de segurança da informação não será tratado da mesma forma que outro que não tenha investido tanto na segurança de suas bases de dados; é nesse sentido que deverá se levar em conta o grau de conformidade com as medidas técnicas de segurança (MENKE; GOULART, 2021, p. 635).

Essa previsão aproxima-se da regra geral presente no art. 944, parágrafo único, do Código Civil, que prevê a redução equitativa da indenização, caso haja excessiva desproporção entre a culpa e dano, uma vez que poderá haver a redução das multas em situações de cumprimento adequado das normas e dos padrões de segurança (MENKE; GOULART, 2021, p. 635). Verifica-se novamente a necessidade de demonstrar que houve a adoção reiterada e demonstrada de mecanismos e procedimentos capazes de mitigar os danos.

A ANPD deve ter autonomia e independência para fiscalizar e propor sugestões de melhoria e correção de políticas e processos para a garantia dos direitos dos titulares de dados pessoais (GUTIERREZ, 2020, p. 449). Os três primeiros incisos do art. 55-J condensam o espírito da Lei (GUTIERREZ, 2020, p. 450) ao estipular que compete à ANPD zelar pela proteção dos dados pessoais; pela observância dos segredos comercial e industrial, observada a proteção dos dados pessoais e do sigilo das informações; e elaborar diretrizes para a Política Nacional de Proteção de Dados pessoais e da Privacidade (BRASIL, 2018). É importante que

a ANPD tenha ampla competência técnica para executar essas atribuições (GUTIERREZ, 2020, p. 450), com guias e orientações que demonstrem a sua postura colaborativa, por meio da estipulação de padrões boas práticas (CAMARGO, 2021, p. 59).

Além disso, o controlador deverá comunicar tanto à ANPD quanto ao titular de dados em caso de ocorrência de incidentes de segurança que possam acarretar riscos ou danos aos titulares (art. 48, LGPD), caso contrário, violará a Lei. Essa comunicação deverá demonstrar quais os dados afetados; quais os titulares envolvidos; as medidas técnicas e de segurança aplicadas; os possíveis riscos; se a comunicação não tiver sido imediata, o motiva da demora; e as medidas que foram ou serão adotadas para reverter a situação ou mitigar os prejuízos (§ 1º).

Quando notificada, a ANPD irá verificar a gravidade do incidente e, a partir disso, caso necessário, determinará ao controlador que promova a divulgação do fato (§ 2º) e adote medidas capazes de reverter ou minimizar os efeitos do incidente (art. 48, § 2º, II). Referidos fatores serão cruciais no juízo de gravidade do incidente, em conjunto com os incisos I a XI do § 1º do art. 52 da LGPD (VAINZOF, 2020, p. 156).

Diante disso, a defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente (art. 22, LGPD), com o objetivo de facilitar a tutela judicial dos direitos à proteção dos dados. Ademais, poderão os titulares reivindicar o cumprimento de seus direitos junto à ANPD (art. 18, § 1º, LGPD), que coordenará as atividades e terá poderes sancionatórios relacionados à proteção dos dados pessoais (SANTOS *et al.*, 2021, p. 6).

Em contrapartida, a Autoridade deverá observar os segredos comercial e industrial, sem que se confunda o que são dados pessoais e o que é um produto oriundo do tratamento desses, isto é, se um titular postular a portabilidade de seus dados, o órgão deverá encaminhar os dados coletados, mas não será obrigado a compartilhar os dados e as informações oriundas do seu tratamento, por meio de estudo de mercado e *softwares*, por exemplo (TEIXEIRA, 2021, p. 46).

Além disso, a jurisprudência possui uma grande importância no desenvolvimento interpretativo das normas de proteção de dados, tendo em vista que busca formar entendimentos consolidados e estabelecer a uniformização da interpretação legislativa, para combater a insegurança jurídica (TEIXEIRA, 2021, p. 60). A construção jurisprudencial e a orientação da ANPD são essenciais para que haja uma harmoniosa responsabilização dos agentes de tratamento; os processos de transformação digital e sua disruptividade passam a representar

novos desafios e obrigações, o que exige a existência de uma cultura orientada à proteção dos dados pessoais (KREMER, 2020, pp. 313-314).

Esse modelo regulatório visa dar efetividade para as leis de proteção de dados e a ANPD é primordial para a efetividade dos princípios e garantias previstas na legislação, com a função de elaborar diretrizes que assegurem uma verdadeira conscientização da sociedade civil sobre o tema (OLIVEIRA, 2020, p. 372). No Brasil, os valores da proteção de dados pessoais ainda estão pouco disseminados em relação a outros países, um dos desafios é a implementação dos princípios e da cultura de proteção dos dados pessoais e a efetividade da Lei (OLIVEIRA, 2020, p. 390).

Desse modo, a ANPD detém o relevante papel de criar diretrizes sólidas, fiscalizar, aplicar sanções e estabelecer uma cultura de responsabilidade civil (OLIVEIRA, 2020, p. 391). Na Europa já se percebe que as decisões dos tribunais e dos pronunciamentos das autoridades de proteção de dados dão contornos mais claros à legislação específica de cada um dos países, tendo a estrutura normativa sobre proteção de dados pessoais evoluído há décadas (CAMARGO, 2021, p. 12). É essencial que a ANPD desempenhe tais funções para que haja a congruência do sistema como um todo e que o tratamento dos dados pessoais seja realizado com transparência, efetividade e em consonância com as garantias e os princípios previstos na legislação (OLIVEIRA, 2020, p. 391).

5.3 RELATÓRIO DE IMPACTOS PELOS AGENTES DE TRATAMENTO DE DADOS

Como visto, um novo mapa de consequências foi introduzido em caso de descumprimentos da legislação pelos agentes de tratamento de dados, o que abre caminho a novas reivindicações de indenização (MORAES; QUEIROZ, 2019, p. 23). Em termos práticos, os agentes deverão analisar quais dados serão tratados; com que finalidade; e que tipos de operações serão aplicadas, por meio de atitudes conscientes, diligentes e proativas, para identificar os riscos e escolher e aplicar as medidas apropriadas a sua mitigação (MORAES; QUEIROZ, 2019, p. 23).

Nesse cenário, o Relatório de Impacto à Proteção dos Dados Pessoais (RIPD) é de fundamental importância, de forma a estimular e reforçar a capacidade dos agentes de tratamento à auto-organização de maneira mais ampla e geral, sendo um instrumento que vem ganhando, cada vez mais, protagonismo ao longo dos trabalhos preparatórios previstos na Lei (BIONI; DIAS, 2020, pp. 7-8). O RIPD é caracterizado pela Lei como a “documentação do

controlador que contenha a descrição dos processos de tratamento de dados pessoais que possam gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de riscos” (art. 5º, XVII).

Em seu art. 10, § 3º, a LGPD determina que a ANPD poderá solicitar ao controlador o relatório de impactos quando o tratamento tiver como fundamento o seu legítimo interesse e, ademais, poderá determinar ao controlador que elabore o relatório referente às operações realizadas (art. 38), devendo ser observados os segredos comercial e industrial (BRASIL, 2018). Desse modo, a ausência de elaboração do relatório é capaz de ensejar a aplicação de multas ou processos administrativos ou judiciais em desfavor do controlador por não se atentar ao tratamento regular dos dados conforme determina a legislação (SOUSA; FRANCO, 2020, p. 432).

O relatório será um documento gerado pelo controlador, com a descrição dos processos de tratamento de dados que poderão gerar riscos às liberdades civis e aos direitos fundamentais e com as medidas, salvaguardas e mecanismos de mitigação de riscos (SOUSA; FRANCO, 2020, p. 431). O fato de o RIPD poder ser exigido pela ANPD, ainda que não haja provas ou indícios de violações, deixa clara a potencialidade lesiva que a atividade de tratamento de dados poderá alcançar, por isso é imprescindível a existência do dever constante de informar quais os riscos que determinado tratamento está sujeito, bem como de descrever todos os procedimentos realizados, a metodologia da coleta e a indicação das medidas e mecanismos aplicados para mitigar os riscos (SANTOS *et al.*, p. 23).

A elaboração do RIPD irá viabilizar a avaliação dos critérios de segurança necessários e compatíveis com a natureza e o volume dos dados tratados (VAINZOF, 2020, p. 144). Com efeito, é aconselhável que os agentes de tratamento mantenham registros com descrição geral das medidas técnicas e organizativas de segurança aplicadas na atividade desempenhada (VAINZOF, 2020, p. 145), já que a função do relatório é expor todos os processos realizados, bem como a eficácia do tratamento e a conformidade com a Lei (MELLO; MIRAMONTES, 2021, p. 3).

Esse relatório apoia o princípio da responsabilização e prestação de contas, ajudando a comprovar a adoção de medidas técnicas e organizacionais apropriadas ao caso concreto; no entanto, não irá eximir a responsabilidade do agente, podendo resultar em multas e indenizações civis (MELLO; MIRAMONTES, 2021, p. 3). Ademais, é um dos instrumentos mais essenciais nos programas de governança e boas práticas, como forma de registrar a regularidade e legalidade das operações de tratamento de dados, para demonstrar que o controlador fez um

estudo prévio dos riscos e das medidas prudentes a serem aplicadas em questão (PALHARES, 2019, p. 138).

Contudo, o processo de avaliação do impacto do tratamento não deve ser visto simplesmente como uma documentação a ser elaborada pelo controlador gerada após um processo de conformidade, mas um instrumento de apoio às atividades de tratamento de uma organização, que vem da ideia de organização sistemática das operações, a fim de viabilizar a visualização de processos e procedimentos internos, para que seja possível prevenir e mitigar os riscos (GOMES, 2019, pp. 8-9).

Entretanto, ainda que a relevância de tal relatório seja evidente, a LGPD abordou o tema de forma extremamente genérica (PALHARES, 2019, pp. 138-139). Desse modo, alguns de seus elementos deverão ser delineados e regulamentados pela Autoridade Nacional de Proteção de Dados, como a definição de seu formato; o prazo de elaboração; os aspectos que deverão ser abordados por ele; os casos nos quais será obrigatório; além de grande parte de seu efetivo conteúdo (PALHARES, 2019, p. 140).

A título exemplificativo, várias autoridades de proteção de dados pessoais, como por exemplo a *Information Commissioner Officer (ICO)* do Reino Unido, disponibilizam informações, modelos e exemplos de como deverá ser a estrutura de um relatório de impacto (GOMES, 2019, p. 5). A ANPD, portanto, poderá dispor sobre os padrões técnicos mínimos a orientar os agentes de tratamento de dados, considerando a natureza das informações, as características específicas do tratamento e o estado atual da tecnologia (VAINZOF, 2020, p. 145).

De todo modo, são três as etapas consideradas essenciais para a elaboração do RIPD: o entendimento da organização e dos processos envolvidos, por meio do mapeamento dos dados pessoais utilizados no tratamento, com a consolidação de todas as informações presentes nos processos e atividades realizadas pela organização; a sua avaliação; e o gerenciamento de seus riscos (BRAZ JÚNIOR, 2019). O papel do relatório é avaliar, mapear, planejar, implementar e monitorar todo o processo de conformidade com a legislação e conseguir demonstrar a responsabilidade e prestação de contas perante a Autoridade Nacional (GOMES, 2019, pp. 11-12).

Entretanto, mister salientar que o RIPD não visa atender apenas à conformidade com a LGPD, mas também busca refletir uma avaliação dos possíveis impactos em virtude do tratamento, cuja base regulatória é a identificação dos riscos, que poderá ser realizada para diferentes propósitos, como avaliar os impactos de incidentes de segurança; novas tecnologias; ou produtos que possam gerar danos aos titulares de dados (GOMES, 2019, p. 12).

O seu objetivo fundamental, portanto, é ser uma ferramenta de governança de dados a ser internalizada no cotidiano da organização e não um documento a ser utilizado somente durante um processo de adequação regulatória (GOMES, 2019, p. 12). O Relatório de Impacto, nesse sentido, não deve ser enxergado como uma ferramenta burocrática, mas um documento que busca refletir um processo de aprendizado pelos agentes de tratamento de dados (GOMES, 2019, p. 14).

Sob a ótica dos agentes de tratamento, os custos despendidos nas adequações sistêmicas e procedimentais à conformidade perante a Lei, além das possíveis indenizações que serão determinadas diante de processos administrativos e judiciais, gera grande preocupação (ARAÚJO; FIGUEREDO, 2020, p. 338). Entretanto, a LGPD não pretende frear o desenvolvimento econômico e a inovação, pelo contrário, esse desenvolvimento é essencial para que novos mecanismos de proteção de dados sejam viabilizados; o que se busca, portanto, é a harmonia entre a tutela da livre iniciativa e das garantias fundamentais (SOUZA *et al.*, 2020, pp. 51-52).

Ao prever como um de seus fundamentos o desenvolvimento econômico e tecnológico e a inovação em seu inciso V do art. 2º, a Lei rompe com o antagonismo artificial entre a proteção de dados e a inovação, isto é, ao mesmo tempo que se protegem os dados pessoais, cria-se um mercado competitivo para que se ofereçam serviços mais seguros e protetivos dos dados pessoais alheios (SOUZA *et al.*, 2020, p. 52).

5.4 IMPACTOS NO DESENVOLVIMENTO ECONÔMICO E DE NOVAS TECNOLOGIAS

Um óbice que vem sendo levantado, principalmente pelos defensores da tese da responsabilidade civil subjetiva na Lei Geral de Proteção de Dados, é o fato de que a adoção da responsabilidade proativa (ou até mesmo da objetiva, para aqueles que a defendem), inibiria a competição e o desenvolvimento de novas tecnologias (NOVAKOSKI; NASPOLINI, 2020, p. 12). Além disso, asseveram que a sua aplicação também levaria à ampliação do número de demandas com viés ressarcitório, o que, da mesma forma, poderia inibir o desenvolvimento das novas tecnologias de tratamento de dados no Brasil (SANTOS *et al.*, 2021, p. 18).

Cuida-se, contudo, de falso dilema: a história já demonstrou que a adoção do regime de responsabilidade civil objetiva, sem a necessidade de comprovação de culpa e com hipóteses

de culpa *in re ipsa*, que tem o objetivo de facilitar o ônus probatório, não limitaram o desenvolvimento e a indústria (MORAES; QUEIROZ, 2019, p. 128).

Quando da promulgação do Código de Defesa do Consumidor e do próprio Código Civil em vigor, essa hipótese foi exaustivamente analisada (NOVAKOSKI; NASPOLINI, 2020, p. 12). Precedentemente a esse contexto, a liberdade era a regra e a responsabilidade a exceção; gradativamente o objetivo da responsabilidade civil deslocou-se da culpa para o dano, em virtude, justamente, da constatação de que as novas tecnologias estavam se tornando insuficientes para a aplicação de um regime de responsabilidade centrado sobre um juízo de reprovabilidade da conduta do agente causador do dano (SCHIREIBER, 2020, p. 579).

No início do processo de industrialização propugnava-se a exclusão da responsabilidade civil dos agentes que desempenhavam atividades perigosas no intuito de evitar que o progresso técnico viesse a ser dificultado em virtude das condenações ao pagamento de indenizações civis (MORAES; QUEIROZ, 2019, p. 128). Diante dessa realidade, em que os danos eram o efeito colateral de inovações importantes, tornou-se necessária a incidência de um novo regime de responsabilidade civil, qual seja o da responsabilidade objetiva, cuja demonstração de culpa vinha a ser cada vez mais difícil, diante da impessoalidade inerente ao funcionamento das novas tecnologias (SCHIREIBER, 2020, p. 579).

O ordenamento jurídico brasileiro, desse modo, organizou a reparação civil de uma forma mais moderna (ROSENVALD, 2017, p. 42), a partir de uma gradativa transformação, à medida que a comprovação da culpa provou ser ineficiente diante da realidade encarada, que se torna a cada dia mais complexa (FILHO, 2018 *apud* OLIVEIRA, 2019, p. 36).

Dessa forma, ao contrário do que afirmavam os recriminadores da aplicação do novo regime de responsabilidade civil, a imputação do regime de responsabilidade objetiva nas hipóteses estabelecidas nos diplomas não inibiu a inovação e o desenvolvimento das novas tecnologias, pelo contrário, as tornou mais seguras e mitigou os riscos e os danos decorrentes do desenvolvimento, imputando o dever de reparar ao agente e assegurando a efetiva proteção do direito das vítimas (NOVAKOSKI; NASPOLINI, 2020, p. 12).

Hoje em dia, ambas as responsabilidades convivem de maneira harmoniosa no ordenamento jurídico brasileiro, competindo ao legislador ou ao próprio juiz definir quais as atividades que se encontram sob a égide da responsabilidade objetiva e quais se encontraram sob a da subjetiva (SCHIREIBER, 2020, p. 579). Desse modo, o mesmo se espera com a implementação da responsabilidade proativa, no qual o eixo axiológico do instituto se deslocaria da reparação do dano para a sua prevenção de forma eficaz (NOVAKOSKI; NASPOLINI, 2020, p. 12).

Assim, da mesma forma que a responsabilidade objetiva não foi um óbice ao desenvolvimento, a aplicação da responsabilidade proativa também não seria, uma vez que o eventual aumento dos custos de proteção dos dados pessoais para as entidades não é decisivo, já que não se pode estimar que os interesses dos titulares ligados à proteção de seus dados pessoais sejam de *status* inferior aos interesses tecnológicos (RODOTÀ, 2008, p. 53).

A partir da orientação jurisprudencial dos Tribunais Superiores, em atenção às diretrizes que serão estipuladas pela Autoridade Nacional de Proteção de Dados, o Judiciário será capaz de uniformizar as suas decisões, a partir dos entendimentos consolidados que deverão ser respeitados, com o condão de delimitar as condenações dos agentes de tratamento perante os danos que vierem a causar aos titulares de dados, determinando a correta interpretação da Lei; os agentes de tratamento terão uma maior segurança jurídica perante a forma com que irão desempenhar as suas atividades e quais as medidas de segurança que deverão empregar; e os titulares terão o seu direito à proteção dos dados pessoais garantido a partir dessas determinações, podendo, se for o caso, receber as indenizações devidas em razão de eventuais danos decorrentes do tratamento irregular de seus dados pessoais.

Observa-se que, em comparação ao que ocorreu quando da implementação da responsabilidade objetiva à época da promulgação do Código de Defesa do Consumidor, os avanços tecnológicos permanecem em constante desenvolvimento e, em paralelo a isso, se mantém a possibilidade de garantir aos consumidores a proteção de seus direitos. Ademais, a partir dos entendimentos consolidados dos Tribunais Superiores, tem-se uma uniformização da jurisprudência, que irá determinar em quais situações deverão ocorrer a incidência do regime específico de responsabilização civil.

Com efeito, para que haja a implementação da responsabilidade proativa no ordenamento jurídico brasileiro, bastará as orientações da ANPD e a uniformização da jurisprudência sobre a interpretação da Lei, para que se possa sustentar simultaneamente o desenvolvimento tecnológico, a salvaguarda dos direitos dos titulares e o ensinamento dos agentes de tratamento sobre como deverão desempenhar as suas atividades.

Desde a promulgação da Lei, a sociedade vive a insegurança jurídica referente a diversas lacunas existentes no texto legislativo, em especial a respeito de qual regime de responsabilidade civil deverá ser aplicado e quais serão os limites que irão caracterizar as atividades de tratamento desempenhadas como irregulares ou, ainda, quais serão os parâmetros a serem utilizados para minorar ou maximizar os valores das sanções e indenizações.

É evidente, portanto, a importância de uma orientação harmoniosa da Autoridade Nacional de Proteção de Dados (que deverá determinar as medidas a serem empregadas pelos

agentes no desempenho de sua atividade e preencher as demais lacunas presentes na Lei) e do Poder Judiciário (por meio da consolidação dos entendimentos, que uniformizará as decisões dos tribunais brasileiros). Dessa forma, a história nos mostra que o desenvolvimento tecnológico não será afetado e os direitos dos titulares serão garantidos, sem haver prejuízo à celeridade processual na busca da resolução dos conflitos.

6 CONCLUSÃO

O direito à proteção dos dados pessoais tem alcançado um espaço cada vez maior no debate público, apesar de não ser algo novo, o processamento dos dados pessoais na atualidade é muito mais intenso e necessita de uma legislação específica para a proteção desse direito. A sociedade encara um novo estágio de desenvolvimento econômico e tecnológico disseminado mundialmente por meio da *internet*.

Em virtude disso, observou-se o incremento de falhas de segurança e a coleta e o uso irregular dos dados pessoais, passíveis de ensejar danos aos titulares de dados. Desse modo, o impacto do tratamento dos dados pessoais passou a ser regulamentado pela Lei Geral de Proteção de Dados Pessoais, com previsões acerca de sanções e responsabilização daqueles que exercem a atividade.

O ordenamento jurídico brasileiro, portanto, deve se adequar a esse cenário, com previsões legais suficientes à tutela do direito à proteção dos dados pessoais, principalmente em virtude do seu alcance ao *status* de direito fundamental.

Dessa forma, os agentes de tratamento de dados deverão observar os fundamentos estabelecidos pela Lei, a boa-fê e os princípios norteadores do tratamento e os requisitos estipulados no art. 7º da Lei. Contudo, para que haja a sua responsabilização civil em caso de tratamento irregular de dados pessoais, uma análise mais detida da Lei deve ser realizada.

Parte da doutrina entende que deveria imperar na Lei o regime de responsabilidade civil subjetiva, devendo ser constatada a culpa dos agentes de tratamento para que possa haver a sua condenação à indenização dos indivíduos. Outra parte acredita que deve imperar o regime de responsabilidade objetiva, uma vez que o tratamento de dados pessoais é uma atividade de risco, inexistindo a necessidade de comprovação da culpa.

Contudo, o presente estudo buscou demonstrar que, diante da análise mais abrangente e minuciosa da legislação, foi constatada a necessidade de abandono da lógica binária da responsabilidade civil, para que essa rigidez não afete a capacidade da Lei em apresentar mecanismos jurídicos eficientes perante o cenário atual.

Dessa forma, em análise aos artigos 42 a 46 da Lei, bem como de seus princípios da segurança, da prevenção e, sobretudo, da responsabilização e prestação de contas, foi possível observar a inauguração de um novo regime de responsabilidade civil adotado pela Lei, qual seja o regime da responsabilidade proativa.

Essa inovação determina que não bastará que os agentes demonstrem a aplicação da Lei propriamente dita, mas que sejam empregadas ao tratamento medidas técnicas e administrativas aptas a garantir a segurança dos dados pessoais e o direito dos titulares de dados.

Contudo, mister salientar que os aplicadores do direito deverão ponderar quais as medidas existentes à época do tratamento e a capacidade financeira das instituições, não bastando a constatação, ou não, da culpa dos agentes, mas uma reflexão e fundamentação de suas decisões a partir dos artigos e princípios da Lei e das medidas adotadas no tratamento, a depender de cada caso concreto.

Como forma de mitigar os danos inerentes ao processamento dos dados e a redução de eventuais sanções administrativas e responsabilizações civis, caberá aos agentes o emprego de boas práticas e governança e a elaboração de um Relatório de Impacto à Proteção dos Dados Pessoais, para que haja a instrução dos envolvidos e a conformidade da instituição perante a Lei.

Para isso, demonstrou-se a importância das orientações da Autoridade Nacional de Proteção de Dados Pessoais, para nortear a correta aplicação da legislação e sanar as lacunas presentes na Lei, bem como demonstrar aos agentes como deverá ser elaborado o Relatório de Impacto e qual o nível de segurança esperado das medidas técnicas e administrativas aplicadas ao tratamento.

Além disso, a uniformização jurisprudencial apresenta igual relevância, para que haja um entendimento consolidado por parte dos Tribunais Superiores e sua harmoniosa aplicação, trazendo segurança jurídica ao ordenamento brasileiro.

Por fim, refutou-se as alegações sobre a possibilidade de a implementação do novo regime de responsabilidade civil ser capaz de frear o desenvolvimento econômico e tecnológico brasileiro e obstruir a celeridade processual do Poder Judiciário.

O que se constatou é que tais asseverações são meramente falácias, uma vez que, em comparação com o que ocorreu quando da implementação da responsabilidade objetiva no Código de Defesa do Consumidor, o desenvolvimento econômico e tecnológico manteve-se em ascensão e houve a garantia dos direitos dos consumidores, que não devem ser vistos com um *status* inferior ao desenvolvimento em questão.

Ademais, foi observado que por meio da orientação da Autoridade Nacional de Proteção de Dados e com a uniformização jurisprudencial por meio dos entendimentos consolidados dos Tribunais Superiores, o direito à proteção de dados deverá ser aplicado simetricamente pelo Poder Judiciário, com as peculiaridades de cada caso concreto.

Assim, o presente estudo constatou a existência de um novo regime de responsabilidade civil, inaugurado pela Lei Geral de Proteção de Dados Pessoais, que se mostra em harmonia com o atual cenário brasileiro e eficiente diante dos novos desafios encarados pela sociedade.

REFERÊNCIAS BIBLIOGRÁFICAS

- ALVES, Fabrício da Mota. Da Fiscalização. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (org.). **Lei Geral de Proteção de Dados Comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. Cap. 8. p. 403-441.
- ARAÚJO, Vitor Eduardo Lacerda de; FIGUEREDO, Douglas Dias Vieira de. Análise jurídica dos incidentes de segurança e a responsabilidade civil no Brasil. *In*: 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**. Porto Alegre: Fi, 2020. Cap. 15. p. 337-358.
- BACHA, Carolina Just. **O compartilhamento de dados no Brasil como alternativa para o aumento da concorrência na era da *data-driven economy***. 2021. 193 f. Dissertação (Mestrado) - Curso de Direito, Centro de Ciências Jurídicas, Universidade Federal da Santa Catarina, Florianópolis, 2021.
- BARRETO JÚNIOR, Irineu Francisco; NASPOLINI, Samyra Haydêe dal Farra. Proteção de informações no mundo virtual: a LGPD e a determinação de consentimento do titular para tratamento de dados pessoais. *In*: CZYMMECK, Anja (ed.). **Proteção de dados pessoais: privacidade versus avanço tecnológico**. 3. ed. Rio de Janeiro: Cadernos Adenauer, 2019. Cap. 7. p. 137-155.
- BASAN, Arthur Pinheiro; FALEIROS JÚNIOR, José Luiz de Moura. A tutela do corpo eletrônico como direito básico do consumidor. **Revista dos Tribunais**, São Paulo, v. 1020, n. 1, p. 133-168, nov. 2020.
- BESSA, Leonardo Roscoe; NUNES, Ana Luisa Tarter. Instrumentos processuais de tutela individual e coletiva: análise do art. 22 da LGPD. *In*: BIONI, Bruno; MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otávio Luiz (org.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense Ltda., 2021. Cap. 34. p. 1169-1208.
- BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. **Revista do Advogado**: Associação dos Advogados de São Paulo (AASP), São Paulo, v. 39, n. 144, p. 22-32, nov. 2019.
- BIONI, Bruno *et al* (org.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense Ltda., 2021.
- BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. **Civilistica.com**, Rio de Janeiro, v. 9, n. 3, 23 p., out. 2020.
- BITELLI, Marcos Alberto Sant'Anna. A Lei 12.965/2014: o Marco Civil da Internet. **Revista de Direito das Comunicações**, São Paulo, v. 7, n. 1, jun. 2014.
- BOBBIO, Norberto. **A Era dos Direitos**. 7. ed. Rio de Janeiro: Nova, 2004. 96 p. Tradução de Carlos Nelson Coutinho.

BOMFIM, Vólia; PINHEIRO, Iuri. Os sujeitos da Lei Geral de Proteção de Dados. **Revista do Tribunal Regional do Trabalho da 10ª Região**, Brasília, v. 25, n. 1, p. 229-239, nov. 2021.

BRANCO, Sérgio. As hipóteses de aplicação da LGPD e as definições legais. *In*: MULHOLLAND, Caitlin (org.). **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago, 2020. Cap. 3. p. 15-42.

BRANDÃO, Luíza Couto Chaves. O Marco Civil da Internet e a Proteção de Dados: diálogos com a LGPD. *In*: CZYMMECK, Anja (ed.). **Proteção de dados pessoais: privacidade versus avanço tecnológico**. 3. ed. Botafogo: Konrad Adenauer Stiftung, 2019. Cap. 2. p. 35-48.

BRASIL. Agência Senado. Senado Federal. **MP concede autonomia de autarquia à Autoridade Nacional de Proteção de Dados**. 2022. Disponível em: <https://www12.senado.leg.br/noticias/materias/2022/06/14/mp-concede-autonomia-de-autarquia-a-autoridade-nacional-de-protacao-de-dados>. Acesso em: 18 jun. 2022.

BRASIL. Agência do Senado. Senado Federal. **Senado inclui proteção de dados pessoais como direito fundamental na Constituição**. 2021. Disponível em: <https://www12.senado.leg.br/noticias/materias/2021/10/20/senado-inclui-protacao-de-dados-pessoais-como-direito-fundamental-na-constituicao>. Acesso em: 08 abr. 2022.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acesso em: 20 jan. 2022.

BRASIL. Lei nº 8.078 de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor. **Código de Defesa do Consumidor**. Brasília, DF. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 22 jan. 2022.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Dispões sobre o uso da Internet no Brasil. **Marco Civil da Internet**. Brasília, DF, Disponível em: Acesso em 21 mar. 2022

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção dos dados pessoais no Brasil. **Lei Geral de Proteção de Dados (LGPD). (Redação dada pela Lei nº 13.853, de 2019)**. Brasília, DF, Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 18 jan. 2022

BRASIL. Proposta de Emenda À Constituição nº 17, de 21 de fevereiro de 2019. **Senado Federal**: Inclusão da proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Brasília, DF, Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1647518557360&disposition=inline>. Acesso em: 22 abr. 2022.

BRASIL. Supremo Tribunal de Justiça. **Tema Repetitivo nº 710**. Relator: Ministro Paulo de Tarso Sanseverino. Brasília, DF, 17 nov. 2014. Disponível em: https://processo.stj.jus.br/repetitivos/temas_repetitivos/pesquisa.jsp?novaConsulta=true&tipo_pesquisa=T&cod_tema_inicial=710&cod_tema_final=710. Acesso em: 11 jun. 2022.

BRASIL. **Supremo Tribunal Federal**. Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6.837. Relatora Ministra Rosa Weber, Brasília, DF, 07 de maio de 2020.

BRASIL. **Supremo Tribunal Federal**. Recurso Extraordinário nº 673.707. Relator: Ministro Luiz Fux. Voto Gilmar Mendes, pp. 34-40. Brasília, DF, 17 de junho de 2015.

BRAZ JÚNIOR, Marcílio. **Das etapas de elaboração de um DPIA**: propósito de um *data protection impact assessment* não é eliminar todos os riscos, mas minimizar a existência destes. 2019. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/das-etapas-de-elaboracao-de-um-dpia-27042019>. Acesso em: 22 jun. 2022.

BRUNO, Marcos Gomes da Silva. Dos Agentes de Tratamento de Dados Pessoais. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (org.). **Lei Geral de Proteção de Dados Comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019. Cap. 6. p. 346-371.

CAMARGO, Gustavo Xavier de. **Dados pessoais, vigilância e controle**: como proteger direitos fundamentais em um mundo dominado por plataformas digitais?. Rio de Janeiro: Lumen Juris, 2021. 250 p.

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

CARVALHO, Gustavo Robichez de; NASSER, Rafael; MULHOLLAND, Caitlin. Apresentação. *In*: MULHOLLAND, Caitlin (org.). **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipelago, 2020. Cap. 1. p. 7-10.

COSTA, Luiz. *Privacy and the Precautionary Principle*. **Computer Law & Security Review**, Namur, v. 28, n. 1, p. 14-24, fev. 2012.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais comentada**. 3. ed. São Paulo: Thomson Reuters, 2019. 75 p.

CZYMMECK, Anja. Apresentação. *In*: CZYMMECK, Anja (ed.). **Proteção de dados pessoais: privacidade versus avanço tecnológico**. 3. ed. Rio de Janeiro: Konrad Adenauer Stiftung, 2019. Cap. 1. p. 7-9.

DONEDA, Danilo Cesar Maganhoto. **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia**: caderno de investigações científicas. 2. ed. Brasília: Escola Nacional de Defesa do Consumidor, 2010. 124 p.

DONEDA, Danilo. Considerações sobre a tutela da privacidade e a proteção de dados pessoais no ordenamento brasileiro. *In*: CONRADO, Marcelo; PINHEIRO, Rosaline Fidalgo (org.). **Direito Privado e Constituição: ensaios para uma recomposição valorativa da pessoa e do patrimônio**. Curitiba: Juruá, 2009. Cap. 23. p. 87-108.

DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. *In*: BIONI, Bruno Ricardo (org.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense Ltda., 2021. Cap. 1. p. 36-67.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 1 ed. Rio de Janeiro: Renovar, 2006. 103 p.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019. 352 p.

FRAJHOF, Isabella; MANGETH, Ana Lara. As bases legais para o tratamento de dados pessoais. *In*: MULHOLLAND, Caitlin (org.). **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago, 2020. Cap. 3. p. 65-98.

FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (org.). **Lei Geral de Proteção de Dados e suas repercussões no Direito brasileiro**. São Paulo: Revista dos Tribunais, 2019. Cap. 1. p. 10-25.

GOMES, Maria Cecília Oliveira. Relatório de impacto à proteção de dados.: uma breve análise da sua definição e papel na LGPD. **Revista da Associação dos Advogados de São Paulo (AASP)**: Revista do Advogado, São Paulo, n. 144, p. 7-15, nov. 2019.

GOMES, Rodrigo Dias de Pinheiro. Considerações sobre a figura do encarregado pelo tratamento de dados pessoais na Lei Geral de Proteção de Dados. **OAB de Norte A Sul**, Rio de Janeiro, v. 1, n. 11, p. 75-78, jan. 2020.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro: Responsabilidade Civil**. 16. ed. São Paulo: Saraiva Educação, 2021. 608 p.

GONDIM, Glenda Gonçalves. A responsabilidade civil no uso indevido dos dados pessoais. **Revista Iberc**, Rio de Janeiro, v. 4, n. 1, p. 19-34, abr. 2021.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau. Término do Tratamento de Dados. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (org.). **Lei Geral de Proteção de Dados e suas repercussões no Direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. Cap. 8. p. 118-131.

GUTIERREZ, Andriei. Da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (org.). **Lei Geral de Proteção de Dados Comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. Cap. 9. p. 442-463.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC) (São Paulo). **Governança Corporativa**. Disponível em: <https://ibgc.org.br/conhecimento/governanca-corporativa>. Acesso em: 29 jun. 2022.

KLEE, Antonia Espíndola Longoni; PEREIRA NETO, Alexandre Nogueira (ed.). A Lei Geral de Proteção de Dados (LGPD): uma visão panorâmica. *In*: CZYMMECK, Anja (ed.). **Proteção de dados pessoais: privacidade versus avanço tecnológico**. Rio de Janeiro: Konrad Adenauer Stiftung, 2019. Cap. 1. p. 12-33.

KORKMAZ, Maria Regina Rigolon; SACRAMENTO, Mariana. Direitos do Titular de Dados: Potencialidades e Limites na Lei Geral de Proteção de Dados Pessoais. **Revista**

- Eletrônica da Procuradoria Geral do Estado do Rio de Janeiro**, Rio de Janeiro, v. 4, n. 2, 28 p., ago. 2021
- KREMER, Bianca. Os agentes de tratamento de dados pessoais. *In*: MULHOLLAND, Caitlin (org.). **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago, 2020. Cap. 12. p. 289-318.
- LEONARDI, Marcel. Principais bases legais de tratamento de dados pessoais no setor privado. **Caderno Especial LGPD**, São Paulo, p. 71-85, nov. 2019.
- LEONARDI, Marcel. **Tutela e Privacidade na Internet**. São Paulo: Saraiva, 2011. 402 p.
- LÉVY, Pierre. Informática, *cyberlaw*, *e-commerce*. *In*: LORENZETTI, Ricardo Luis. **Tratado de los contratos**. 3. ed. Argentina: Rubinzal-Culzoni, 2000. Cap. 67, p. 833.
- LIMA, Caio César Carvalho. Do Tratamento de Dados Pessoais. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (org.). **Lei Geral de Proteção de Dados Comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. Cap. 2. p. 201-241.
- LINKE, Sarah Helena. **Sociedade de Vigilância e Consumo: Proteção de Dados Pessoais relacionados à saúde em programas de fidelização de redes de farmácia**. 2019. 252 f. Dissertação (Mestrado) - Curso de Direito, Centro de Ciências Jurídicas, Universidade Federal da Santa Catarina, Florianópolis, 2019.
- LOPES, Tereza Ancona. Responsabilidade civil na sociedade do risco. **Revista da Faculdade de Direito da Universidade de São Paulo**, v. 105, São Paulo, dez. 2010. pp. 1223-1234.
- MALDONADO, Viviane Nóbrega. Dos Direitos do Titular. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (org.). **Lei Geral de Proteção de Dados Comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. Cap. 3. p. 242-274
- MELLO, Ana Paula; MIRAMONTES, Giovanna Coelho. LGPD: agentes de tratamento, responsável e ANPD. **Cadernos Jurídicos da Faculdade de Direito de Sorocaba: Edição Especial**, São Paulo, v. 1, n. 3, p. 73-80, dez. 2021.
- MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 13. ed. São Paulo: Saraiva Educação, 2018. 2892 p.
- MENDES, Laura Schertel *et al.* O Supremo Tribunal Federal e a Proteção Constitucional dos Dados Pessoais: Rumo a um Direito Fundamental Autônomo. *In*: BIONI, Bruno Ricardo (org.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense Ltda., 2021. Cap. 3. p. 139-198.
- MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. **Revista de Direito do Consumidor**, São Paulo, v. 120, 2018.
- MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, São Paulo, v. 120, n. 27, 15 p., dez. 2018.

MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otavio Luiz. Apresentação. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otavio Luiz (org.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense Ltda., 2020. Cap. 1. p. 23-28.

MENKE, Fabiano; GOULART, Guilherme Damasio. Segurança da informação e vazamento de dados. *In*: BIONI, Bruno; MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otávio Luiz (org.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense Ltda., 2021. Cap. 17. p. 615-650.

MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. **Revista dos Tribunais**, São Paulo, v. 108, n. 1009, p. 173-222, nov. 2019.

MORAES, Maria Celina Bodin de. LGPD: um novo regime de responsabilização civil dito proativo. **Civilistica.com**, Rio de Janeiro, v. 8, n. 3, p. 1-6, dez. 2019.

MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD. *In*: CZYMMECK, Anja (ed.). **Proteção de dados pessoais: privacidade versus avanço tecnológico**. 3. ed. Rio de Janeiro: Cadernos Adenauer, 2019. Cap. 6. p. 113-136.

MULHOLLAND, Caitlin. **A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco?** 2020. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tr%E2%80%A6>. Acesso em: 14 jun. 2020.

MULHOLLAND, Caitlin; FRAJHOF, Isabela Z.. Prefácio. *In*: MULHOLLAND, Caitlin (org.). **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago, 2020. Cap. 2. p. 11-14.

NOGAROLI, Rafaella; PAVAN, Vitor Ottoboni. Violação e Responsabilidade. *In*: NALIN, Paulo *et al* (org.). **Pós-Constitucionalização do Direito Civil: novas perspectivas do Direito Civil na Constituição Prospectiva**. Londrina: Thoth, 2021. Cap. 4. p. 105-154.

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

OLIVEIRA, Caio César de. A Autoridade Nacional de Proteção de Dados (ANPD) e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. *In*: MULHOLLAND, Caitlin (org.). **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago, 2020. Cap. 17. p. 371-392.

OLIVEIRA, Denis Lima de. **Agentes de Tratamento de Dados Pessoais e Encarregado: Guia Prático sobre suas atribuições, responsabilidades e boas práticas**. 2021. 148 f. Dissertação (Mestrado) - Curso de Direito, Centro de Ciências Jurídicas, Fundação Getúlio Vargas, São Paulo, 2021.

OLIVEIRA, Guilherme Henrique Gualtieri de. As bases legais para o tratamento de dados pessoais: muito além do consentimento. *In*: 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**. Porto Alegre: Fi, 2020. Cap. 2. p. 45-63.

OLIVEIRA, José Eduardo da Silva. **Responsabilidade Civil dos Agentes de Proteção de Dados no Brasil**. 2019. 49 f. TCC (Graduação) - Curso de Direito, Centro de Ciências Jurídicas, Universidade Federal da Paraíba, Santa Rita, 2019.

OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (org.). **Lei Geral de Proteção de Dados e suas repercussões no Direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. Cap. 2. p. 26-41.

PALHARES, Felipe. O relatório de impacto à proteção de dados pessoais. *In*: MALDONADO, Viviane Nóbrega. **Lei Geral de Proteção de Dados Pessoais Manual de Implementação**. São Paulo: Thomson Reuters Brasil, 2019. Cap. 7. p. 138-168.

PALMEIRA, Mariana de Moraes. A segurança e as boas práticas no tratamento de dados pessoais. *In*: MULHOLLAND, Caitlin (org.). **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago, 2020. Cap. 15. p. 319-342.

PERILLI, Paulo Roberto Godoy. Proteção de dados, privacidade e o Marco Civil da Internet. *In*: 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**. Porto Alegre: Fi, 2020. Cap. 9. p. 192-213.

PINCER, Pedro. **Autoridade Nacional de Proteção de Dados é transformada em autarquia**. 2022. Disponível em: <https://www12.senado.leg.br/noticias/audios/2022/06/autoridade-nacional-de-protacao-de-dados-e-transformada-em-autarquia>. Acesso em: 17 jun. 2022.

PINHEIRO, Patrícia Peck Garrido. Nova lei brasileira de proteção de dados pessoais (LGPD) e o impacto nas instituições públicas e privadas. **Revista dos Tribunais**, São Paulo, n. 1000, fev. 2019.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais: comentários à lei nº 13.709/2018 (lgpd)**. 3. ed. São Paulo: Saraiva Jur, 2021. 176 p.

RODOTÁ, Stefano. **A vida na sociedade de vigilância**. A privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Doneda. Rio de Janeiro: Renovar, 2008.

ROSENVALD, Nelson. **As funções da responsabilidade civil: a reparação e a pena civil**. São Paulo: Atlas, 2013. 241 p.

SAMPAIO, José Adércio Leite. **Direito à intimidade e à vida privada**. 1 ed. Belo Horizonte: Del Rey, 1997.

SANTOS, Andréia da Costa Pereira dos. Dos Direitos do Titular: Finalmente o empoderamento dos indivíduos enquanto titulares de seus dados. *In*: SANTOS, Regiane Martins dos; CARVALHO, Adriana Cristina F. L. de (org.). **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Comissão de Direito Digital, Tecnologia e Inteligência Artificial. OAB/SP - 116ª Subseção Jabaquara - Saúde, 2020. Cap. 4. p. 52-63.

SANTOS, Camila Ferrão dos; SILVA, Jeniffer Gomes da; PADRÃO, Vinicius. Responsabilidade civil pelo tratamento de dados pessoais na Lei Geral de Proteção de Dados. **Revista Eletrônica da Procuradoria Geral do Estado do Rio de Janeiro**, Rio de Janeiro, v. 4, n. 3, 31 p., dez. 2021.

SARLET, Ingo Wolfgang. Proteção de Dados Pessoais como Direito Fundamental na Constituição Federal Brasileira de 1988: Contributo para a Construção de uma Dogmática Constitucionalmente Adequada. **Direitos Fundamentais & Justiça**, Belo Horizonte, v. 14, n. 42, p. 179-218, jun. 2020.

SCHREIBER, Anderson. Responsabilidade civil na Lei Geral de Proteção de Dados. *In*: BIONI, Bruno *et al* (org.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense Ltda., 2020. Cap. 16. p. 576-614.

SLEIMAN, Cristina. Texto de Abertura à 3ª Edição. *In*: PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais: comentários à lei nº 13.709/2018 (Lgpd)**. 3. ed. São Paulo: Saraiva Jur, 2021. p. 15-18.

SOUZA, Carlos Affonso; MAGRANI, Eduardo; CARNEIRO, Giovana. Lei Geral de Proteção de Dados Pessoais: uma transformação na tutela dos dados pessoais. *In*: MULHOLLAND, Caitlin (org.). **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago, 2020. Cap. 2. p. 43-64.

SOUSA, Zilda A. Goncalves de; FRANCO, Igor da Silveira. Aplicação da Lei Geral de Proteção de Dados ao poder público. *In*: 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**. Porto Alegre: Fi, 2020. Cap. 20. p. 406-442.

TASSO, Fernando Antonio. A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor. **Cadernos Jurídicos: Direito Digital e proteção de dados pessoais**, São Paulo, n. 53, mar. 2020, p. 97-116.

TEIXEIRA, Helber Anastácio. **O regime de responsabilidade civil do controlador e do operador à luz da Lei Geral de Proteção de Dados Pessoais**. 2021. 73 f. TCC (Graduação) - Curso de Direito, Centro de Ciências Jurídicas, Universidade do Sul de Santa Catarina, Araranguá, 2021.

TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. Desafios da inteligência artificial em matéria de responsabilidade civil. **Revista Brasileira de Direito Civil**, Belo Horizonte, v. 21, n. 1, p. 61-86, set. 2019.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (org.). **Lei Geral de Proteção de Dados e suas repercussões no Direito brasileiro**. São Paulo: Revista dos Tribunais, 2019. Cap. 10. p. 164-187.

TEPEDINO, Gustavo. **Temas de direito civil**. 4. ed. Rio de Janeiro: Renovar, 2008, 598 p.

UNIÃO EUROPEIA. **General Data Protection Regulation**. Parlamento Europeu. Bélgica, 27 de abril de 2016. Disponível em: <<https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679>>. Acesso em 29 de jun. de 2022.

VAINZOF, Rony. Disposições Preliminares. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (org.). **Lei Geral de Proteção de Dados Comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. Cap. 1. p. 22-200.

VIOLA, Mário; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otavio Luiz; BIONI, Bruno (org.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense Ltda., 2021. Cap. 6. p. 231-284.

WALD, Arnaldo. Um novo direito para a nova economia: os contratos eletrônicos e o Código Civil. *In*: **Direito e Internet: relações jurídicas na sociedade informatizada**, Marco Aurelio Greco e Ives Gandra da Silva Martins (coords.). São Paulo: Revista dos Tribunais, 2001, pp. 9-30.