



**FACULDADE DAMAS DA INSTRUÇÃO CRISTÃ
CURSO DE DIREITO**

STELLA CRYSTHINA FERREIRA DE CASTRO

**A RELAÇÃO ENTRE OS MECANISMOS REPRESSORES CONSTANTES NA
LGPD E A SUA EFETIVIDADE**

RECIFE

2023

STELLA CRYSTHINA FERREIRA DE CASTRO

**A RELAÇÃO ENTRE OS MECANISMOS REPRESSORES CONSTANTES NA
LGPD E A SUA EFETIVIDADE**

Monografia apresentada à
Faculdade Damas da Instrução
Cristã como requisito parcial para a
obtenção do título de Bacharel em
Direito.

Orientadora: Prof.^a Dra. Renata
Cristina Othon Lacerda de Andrade

RECIFE

2023

Catálogo na fonte
Bibliotecário Ricardo Luiz Lopes CRB-4/2116

C355r Castro, Stella Crysthina Ferreira de.
A relação entre os mecanismos repressores constantes na LGPD e a sua efetividade / Stella Crysthina Ferreira de Castro. - Recife, 2023.
50 f.

Orientador: Prof.^a Dr.^a Renata Cristina Othon Lacerda de Andrade.
Trabalho de Conclusão de Curso (Monografia - Direito) – Faculdade Damas da Instrução Cristã, 2023.
Inclui bibliografia.

1. Efetividade. 2. Lei geral de proteção de dados. 3. Mecanismos repressivos. 4. Titular de dados. 5. Vulnerabilidade. I. Andrade, Renata Cristina Othon Lacerda de. II. Faculdade Damas da Instrução Cristã. III. Título.

340 CDU (22. ed.)

FADIC (2023.1-017)

STELLA CRYSTHINA FERREIRA DE CASTRO

**A RELAÇÃO ENTRE OS MECANISMOS REPRESSORES CONSTANTES NA
LGPD E A SUA EFETIVIDADE**

Trabalho de conclusão do curso de bacharelado em Direito da Faculdade Damas da Instrução Cristã – FADIC, como requisito parcial para a obtenção do título de bacharel em Direito.

Aprovada em ____ de _____ de 2023.

BANCA EXAMINADORA:

Orientadora: **Prof. Dra. Renata Cristina Othon Lacerda de Andrade**

Faculdade Damas da Instrução Cristã – FADIC – Brasil

Examinadora: **Prof. Dra. Danielle Spencer Holanda**

Faculdade Damas da Instrução Cristã – FADIC – Brasil

Aos meus pais, Stênio e Euda Castro.

AGRADECIMENTOS

Agradeço primeiramente a Deus, que tem cuidado de mim e me guiado em direção ao sucesso.

Agradeço à minha família, em especial, aos meus pais, Stênio e Euda Castro e minha irmã, Sophia Castro, que são os maiores incentivadores dos meus sonhos.

Agradeço ao meu namorado, Álvaro Nunes, pelo incentivo e companheirismo sempre constantes.

Agradeço a minha orientadora, a Professora Renata Andrade, que me guiou nessa jornada de mais um sonho que se concretiza.

Agradeço à coordenação do curso de direito da FADIC, na pessoa de sua coordenadora, a professora Renata Celeste, pelo apoio e amizade durante todo o curso.

Agradeço à coordenação da cadeira de Orientação Monográfica, na pessoa de seu coordenador, o professor Leonardo Siqueira, pelo incentivo à conclusão desta etapa final.

Agradeço a minha turma, pelos momentos de leveza durante os nossos intervalos para o café, que aos poucos foi transformando colegas em amigos que levarei para sempre.

“Há uma força motriz mais poderosa que o vapor, a
eletricidade e a energia atômica: a vontade”

(Albert Einstein)

RESUMO

Essa pesquisa traz como objetivo analisar a efetividade dos mecanismos repressores constantes na Lei Geral de Proteção de Dados (LGPD), já que sua ineficácia poderia significar uma violação ao direito fundamental da proteção de dados. Como forma de contextualizar o tema, o trabalho primeiramente traz o conceito de dados pessoais e a sua importância diante da sociedade atual, a chamada sociedade informacional, além de apresentar o titular do dado pessoal e sua vulnerabilidade diante dos agentes de tratamento, demonstrando a necessidade de tutela do direito à proteção de dados. Em seguida, são apresentados os mecanismos de controle constantes na LGPD: o de responsabilização administrativa e o de responsabilização civil. Por fim, é feita uma análise jurisprudencial com palavras-chave: LGPD, responsabilidade civil, responsabilidade objetiva e responsabilidade ativa ou proativa na sua ementa, no Tribunal de Justiça de São Paulo (TJSP), para que se possa conferir a efetividade dos mecanismos. O resultado da pesquisa aponta no sentido de que, dentro do recorte jurisprudencial analisado, os mecanismos parecem estar sendo suficientemente efetivos na tutela do direito à proteção de dados pessoais.

Palavras-chave: Efetividade; Lei Geral de Proteção de Dados; Mecanismos repressivos; Titular de dados; Vulnerabilidade.

ABSTRACT

This research aims to analyze the effectiveness of the repressive mechanisms contained in the General Data Protection Law (LGPD), since their ineffectiveness could mean a violation of the fundamental right of data protection. As a way of contextualizing the theme, the work first brings the concept of personal data and its importance in today's society, the so-called informational society, in addition to presenting the holder of the personal data and his vulnerability in the face of treatment agents, demonstrating the need safeguarding the right to data protection. Next, the control mechanisms contained in the LGPD are presented: administrative accountability and civil accountability. Finally, a jurisprudential analysis is made with keywords: LGPD, civil liability, strict liability and active or proactive liability in its menu, in the Court of Justice of São Paulo (TJSP), so that the effectiveness of the mechanisms can be verified. The result of the research points to the fact that, within the jurisprudential framework analyzed, the mechanisms seem to be sufficiently effective in protecting the right to the protection of personal data.

Keywords: Effectiveness; General Data Protection Law; Repressive mechanisms; Data holder; Vulnerability.

LISTA DE ABREVIATURAS E SIGLAS

ANDP – Autoridade Nacional de Proteção de Dados

CF – Constituição Federal

CNJ – Conselho Nacional de Justiça

EC – Emenda Constitucional

LGPD – Lei Geral de Proteção de Dados

TJSP – Tribunal de Justiça de São Paulo

SUMÁRIO

1 INTRODUÇÃO	10
2 OS DADOS PESSOAIS MEDIANTE A SOCIEDADE DA INFORMAÇÃO	14
2.1 OS DADOS PESSOAIS	14
2.2 A SOCIEDADE DA INFORMAÇÃO	16
2.3 OS DADOS PESSOAIS MEDIANTE A SOCIEDADE DA INFORMAÇÃO	17
2.4 A VULNERABILIDADE DO TITULAR DO DADO PESSOAL	19
2.4.1 O TITULAR DO DADO PESSOAL	19
2.4.2 A VULNERABILIDADE DO TITULAR DO DADO PESSOAL	20
2.4.3 A VULNERABILIDADE DO TITULAR DO DADO PESSOAL SENSÍVEL	22
3 A EFETIVIDADE DOS MECANISMOS DE CONTROLE TRAZIDOS PELA LGPD	25
3.1 OS MECANISMOS DE CONTROLE DA LGPD	25
3.1.1 O PRIMEIRO MECANISMO: RESPONSABILIZAÇÃO ADMINISTRATIVA ...	25
3.1.2 O SEGUNDO MECANISMO: RESPONSABILIZAÇÃO CIVIL	30
3.1.2.1 A RESPONSABILIDADE CIVIL SUBJETIVA DOS AGENTES DE TRATAMENTO DE DADOS	32
3.1.2.2 RESPONSABILIDADE CIVIL OBJETIVA DOS AGENTES DE TRATAMENTO DE DADOS	33
3.1.2.3 RESPONSABILIDADE CIVIL OBJETIVA DOS AGENTES DE TRATAMENTO NAS RELAÇÕES DE CONSUMO	34
3.1.2.4 RESPONSABILIDADE CIVIL ATIVA OU PROATIVA DOS AGENTES DE TRATAMENTO DE DADOS	35
4 ANÁLISE JURISPRUDENCIAL (ADMINISTRATIVAS E JUDICIAIS)	37
4.1 TRIBUNAL DE JUSTIÇA DE SÃO PAULO AUTOS Nº 1000794- 59.2021.8.26.0554	37
4.2 TRIBUNAL DE JUSTIÇA DE SÃO PAULO AUTOS Nº 1049037- 81.2021.8.26.0506	39
4.3 TRIBUNAL DE JUSTIÇA DE SÃO PAULO AUTOS Nº 1082876- 88.2021.8.26.0100	39
4.4 TRIBUNAL DE JUSTIÇA DE SÃO PAULO AUTOS Nº 1042935- 03.2021.8.26.0002	40
4.5 OUTROS JULGADOS	41
5 CONCLUSÃO	44
REFERÊNCIAS	47

1 INTRODUÇÃO

A partir da segunda metade do século XX, com o acelerado avanço tecnológico experimentado pela humanidade, dados pessoais passaram a circular livremente, principalmente após o advento da internet, que acelerou a globalização e consequentemente, o tráfego de dados.

De posse dessas informações pessoais, conglomerados econômicos poderosos conseguem constituir um provável perfil de cada indivíduo e esses perfis são verdadeiros ativos para as empresas privadas, ou seja, são bens que ela possui e que podem ser convertidos em dinheiro.

Sem saberem o poder dessas informações, as pessoas acabam fornecendo-as de forma voluntária, principalmente através das redes sociais, contudo, essa exposição acontece também de forma involuntária, na interação entre o cidadão e o Estado, e entre o cidadão e os estabelecimentos comerciais, como condição para aquisição de produtos e serviços, desde os mais supérfluos aos mais essenciais à sobrevivência e manutenção da vida.

Após a coleta, esses dados são transformados em algoritmos, para que possam ser armazenados em enormes conjuntos de informações, posteriormente relacionados, agrupados e contextualizados, permitindo que um perfil pessoal de cada indivíduo seja traçado.

E esses perfis, traçados através dos dados pessoais de cada pessoa, que à primeira vista parecem ser sem relevância e sem valor, são na realidade, capazes de estimular comportamento desejados, de acordo com os interesses e preferências da empresa que os detém, que os utiliza de maneira indiscriminada, ou seja, são uma verdadeira matéria prima preciosa.

Visando apenas o lucro, as empresas privadas detentoras dos dados pessoais, acabam violando princípios constitucionais de extrema importância, tais quais os princípios da dignidade da pessoa humana, da individualidade, da honra, da privacidade e da intimidade.

Diante do contexto apresentado, de coleta e utilização indiscriminada dos dados pessoais dos cidadãos, impulsionadas pelo acelerado avanço tecnológico experimentado nos últimos anos, é possível perceber o importante papel do Direito em balancear o avanço tecnológico e a proteção dos direitos fundamentais. Desta

maneira, além do tratamento constitucional já existente, foi promulgada, em agosto de 2018, a Lei Geral de Proteção de Dados, a LGPD.

Após a entrada em vigor da LGPD e diante da necessidade de se garantir uma proteção ainda mais robusta aos dados pessoais, o Congresso reconheceu que a ausência dessa salvaguarda representava sérios riscos às liberdades e garantias individuais, e promulgou a Emenda Constitucional (EC) nº 115/2022, que incluiu a proteção de dados de forma taxativa no rol dos direitos fundamentais, tendo sido uma importante conquista para garantia da privacidade e da segurança do indivíduo na era digital, já que cada vez mais, os dados pessoais têm sido utilizados para fins comerciais, políticos e, até mesmo, criminosos, tornando-se um assunto de relevância global.

Para LEFOSSE (2022), o reconhecimento da proteção de dados como um direito fundamental autônomo na Constituição teve as seguintes consequências práticas: 1) status normativo superior em relação a toda legislação brasileira; 2) condição de direito fundamental autônomo, pois existe independente de outros direitos fundamentais; 3) status de cláusula pétrea; e 4) aplicabilidade imediata aos casos concretos, dispensando qualquer regulamentação.

Dessa forma, com a promulgação da EC nº 115, a proteção de dados foi elevada à categoria de direito fundamental, com status cláusula pétrea, não podendo ser alterada nem mesmo por emenda constitucional, o que é de grande valor quando se quer garantir a segurança e a integridade desse direito, e, ainda, garantir que não sofrerá ataques e inovações que provoquem a destruição do seu núcleo essencial.

Tendo em vista a importância de se proteger os dados pessoais, surge o questionamento: os mecanismos repressivos constantes na LGPD são suficientes para proteger o titular dos dados pessoais?

Partiremos da premissa de que quando o titular dos dados busca os mecanismos repressivos, sejam administrativos ou civis, para que possa ter uma punição do agente de tratamento de dados como forma de compensação por um dano sofrido, tal fato provocará uma retroalimentação negativa, o que tende a diminuir eventos danosos, uma vez que a sanção tem, para além da função da realização de justiça, a função de prevenção geral, na medida que serve de exemplo para outros agentes de tratamento de dados, bem como a função de prevenção especial, que tem a finalidade de evitar a reincidência do próprio agente sancionado.

Assim, o estudo tem como objetivo principal analisar as decisões da Autoridade Nacional de Proteção de Dados (ANPD), sobre a responsabilidade administrativa e decisões judiciais acerca da violação à legislação de proteção de dados pessoais. Quanto às decisões da ANPD, buscaremos analisar quantas sanções foram aplicadas, qual porte das empresas sancionadas (notório poderio econômico), e qual tipo de sanção, e em se tratando da aplicação de multa, se seu valor foi suficiente alto, nos moldes do art. 52 da LGPD, de forma a inibir a prática do ilícito.

Quanto às decisões judiciais, faremos uma pesquisa jurisprudencial sobre o assunto no banco de jurisprudência do maior Tribunal de Justiça, qual seja, Tribunal de Justiça de São Paulo (TJSP). Inicialmente serão realizadas buscas que contenham as palavras-chaves: LGPD, responsabilidade civil, responsabilidade objetiva e responsabilidade ativa ou proativa na ementa do julgado. Faremos esse filtro com o intuito do resultado nos direcionar para decisões que realmente tratassem do tema proteção de dados de forma principal.

Após isso, passaremos a estudar cada um dos julgados, analisando qual tipo de responsabilidade civil foi reconhecida como aplicável ao caso, se houve a inversão do ônus da prova, se alguma sanção foi efetivamente aplicada, e finalmente, se houve consenso acerca de que tipo de responsabilidade civil (objetiva, subjetiva ou a ativa ou proativa) deve ser considerada quando envolver à legislação que trata de proteção de dados pessoais.

Quanto à metodologia de pesquisa, utilizaremos fontes bibliográficas e documentais e jurisprudencial acerca de casos concretos, disponíveis na pesquisa de jurisprudência, como já referido, do Tribunal de Justiça de São Paulo (TJSP).

Com intuito de desenvolver da maneira mais eficiente possível este trabalho, a pesquisa será descritiva, aplicada e bibliográfica, com abordagem metodológica qualitativa, método dedutivo e técnicas de observação, comparação, descrição, análise e síntese.

Frente ao questionamento descrito anteriormente, o presente trabalho trará tanto a hipótese de suficiência dos mecanismos repressivos da LGPD, não sendo necessária a tomada de outras medidas para a proteção dos dados pessoais, quanto a sua insuficiência e, por consequência, necessidade de complementação, seja por meio de uma legislação complementar, seja por meio da efetiva aplicação da legislação já existente.

Diante do que se foi exposto, para que o problema em pauta seja respondido, o presente trabalho contará com três capítulos. O primeiro capítulo trará o conceito de dados pessoais, o contexto histórico do surgimento da sociedade digital, a influência desses dados nessa sociedade, e a vulnerabilidade do titular do dado pessoal. O segundo capítulo tratará da efetividade dos mecanismos de controle trazidos pela LGPD. E o terceiro e último capítulo trará uma análise jurisprudencial, tanto administrativa, quanto judicial.

2 OS DADOS PESSOAIS MEDIANTE A SOCIEDADE DA INFORMAÇÃO

É essencial para o presente trabalho discorrer sobre o tratamento e a proteção dos dados pessoais frente a sociedade digital, no entanto, antes de relacioná-los, é necessária uma análise isolada dos termos: dados pessoais e sociedade da digital.

Toda essa análise importa para situar o leitor diante da configuração de sociedade nos dias atuais e como os dados pessoais se comportam nesse contexto, para que mais adiante seja debatida a efetividade dos mecanismos repressores da Lei Geral de Proteção de Dados (LGPD).

2.1 OS DADOS PESSOAIS

Primeiramente é preciso entender as diferenças entre os termos “dados” e “informações”, que comumente são tratados como sinônimos, e embora essas palavras tenham seus significados se sobrepondo, suas distinções são significativas, em se tratando do tema trabalhado.

Dados são o que constitui a matéria prima da informação, são o conhecimento bruto que de maneira isolada não conseguem transmitir uma mensagem clara, nem identificar um indivíduo. Já informações são os dados tratados e analisados, com significados práticos que produzem conhecimento relevante sobre certo indivíduo, conseguindo individualizar a pessoa.

Ou seja, o dado é matéria prima da informação, a partir daquele se chega a esta, em outras palavras, o dado é um conceito amplo que engloba o conceito de informação.

Da mesma maneira entende Bioni (2020) sobre os conceitos mencionados:

De início, cabe destacar que dados e informação não se equivalem, ainda que sejam recorrentemente tratados na sinonímia e tenham sido utilizados de maneira intercambiável ao longo deste trabalho. O dado é o estado primitivo da informação, pois não é algo per se que acresce conhecimento. Dados são simplesmente fatos brutos que, quando processados e organizados, se convertem em algo inteligível, podendo ser deles extraída uma informação. (BIONI, 2020, p. 31-32).

O legislador, ao escolher a palavra dado, em lugar da palavra informação, acabou por assimilar uma proteção mais ampla ao indivíduo, pois mesmo que o titular dos dados não seja identificado, estará igualmente protegido pela lei, diferentemente se tivesse escolhido a palavra informação, que em muitos casos deixaria o titular dos dados desamparado e vulnerável.

Os dados pessoais se tornaram uma nova identificação da pessoa e esse fato tem seus lados positivos e negativos. Do ponto de vista positivo, facilita a vida das pessoas no cotidiano, que tem acesso a tudo que precisam de identificação de maneira célere e prática, por outro lado, essas pessoas acabam ficando expostas, pois quem detém essas informações pode utilizá-las de maneira inadequada, seja deixando esses dados desprotegidos, expondo a vida íntima do titular dos dados ou lucrando com essas informações.

Existem diferentes tipos de dados, os quais, são diferenciados pela LGPD, são eles: os dados pessoais e os dados sensíveis. Segundo a referida lei, dado pessoal é a informação relacionada à pessoa natural identificada, como por exemplo, nome, sobrenome, RG e CPF, ou identificável, como no caso dos dados de geolocalização (GPS), endereço IP, identificação de dispositivo dentre outros, enquanto os dados pessoais sensíveis são os que se referem aos dados de 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. Define ainda que os dados pessoais objeto de tratamento têm como titular a pessoa natural a quem estes dados se referem (art. 5º da LGPD, I, II e V).

Dados pessoais sensíveis são informações que revelam a intimidade e privacidade das pessoas, e são considerados sensíveis porque possuem um risco maior de serem usadas de forma discriminatória, preconceituosa ou até mesmo, criminosa. Como os dados pessoais sensíveis são particularmente vulneráveis, a sua coleta e o processamento devem ser limitados, juntamente com medidas de segurança mais rígidas para sua proteção.

Fica clara, então, a vulnerabilidade do titular dos dados pessoais perante quem os detém, e por esse motivo, surge a necessidade da criação de uma lei específica que regule essa relação. Surge, por consequência, em 2018, a LGPD, no entanto muito antes dela haviam outras legislações não específicas que acabavam sendo utilizadas em lides referentes ao tema em questão.

Entendido o conceito e a amplitude e relevância dos dados pessoais, agora se faz necessário entender o contexto em que se inserem e o seu papel diante da sociedade digital.

2.2 A SOCIEDADE DA INFORMAÇÃO

No final do século XX, houve uma intensa transformação da sociedade, por conta dos avanços tecnológicos da época, sobretudo pelo surgimento da internet, que trouxe como consequência positiva a ruptura das barreiras geográficas, promovendo a globalização e aproximando os países que antes não tinham contato cultural, econômico e social.

A internet foi, então, o que transformou a sociedade tal qual ela é hoje e também impulsionou a difusão e publicação de informações a nível mundial. A Revolução Tecnológica da Informação trazida pela internet foi tamanha, que Castells (1999, p.67), equiparou a grandiosidade da revolução tecnológica à da Revolução Industrial ocorrida no século XVIII.

Nesse cenário digital, a informação, que sempre existiu, impulsionada pela internet, passou a ser coletada, armazenada, processada e transmitida em todo o globo terrestre, de maneira rápida, desordenada e em grande quantidade. Assim, como consequência, a informação tomou o lugar de recursos que antigamente mantinham sociedades mais antigas e passou a ter importância primordial na detenção de poder e riquezas.

Nesse mesmo sentido, Bioni (2020, p.39), afirma que a sociedade é atualmente organizada através da informação, sendo ela o elemento central do desenvolvimento da economia e essa nova organização surge exatamente por conta da evolução tecnológica, que foi capaz de armazenar e transmitir informações em alta velocidade e quantidade.

O autor Bioni (2020, p. 44), ainda reforça o considerável papel das informações no desenvolvimento da economia, quando acrescenta que os dados são o combustível que permite o empreendimento mais eficiente e produtivo do mercado, porque a medida que conhecem o comportamento das pessoas através de informações pessoais, acabam melhorando desde a concepção de um produto ou serviço até a publicidade para promovê-los.

É a informação que por ser matéria prima da economia atual, quem passa a ditar a lógica de acúmulo de capital. E diante desse contexto, é preciso colocar em destaque que juntamente com as vantagens trazidas pelo poder das informações, surgem também as problemáticas.

Essas problemáticas surgem ao passo que com o tratamento de dados pessoais, há a possibilidade de exposição, utilização abusiva e comercialização de informações das pessoas, podendo esses dados tanto expor o indivíduo, quanto apresentar sobre ele uma informação diversa da realidade, o que pode vir a prejudicar a vida de quem teve seus dados tratados.

2.3 OS DADOS PESSOAIS MEDIANTE A SOCIEDADE DA INFORMAÇÃO

A era digital é caracterizada pelos avanços tecnológicos, a formação de redes, a globalização e a velocidade da informação e essa era gera um direto impacto na vida privada, na produção de produtos, na prestação de serviços e no acúmulo de capital, sendo a informação o principal subsídio de toda a sociedade atual.

Assim, nesse contexto digital, o dado é o protagonista, que dita as regras do mundo contemporâneo, à medida que transforma a economia e dá lugar a um mercado mais especializado e direcionado aos gostos e personalidades de cada indivíduo.

Essa era digital é chamada de sociedade informacional pelo estudioso do assunto, Castells (1999, p. 107-109), que apresentou seus aspectos centrais, sendo eles: a informação como matéria prima da economia; a penetração da tecnologia na vida das pessoas; a adaptação dessa tecnologia às complexidades da humanidade; a flexibilidade da tecnologia da informação diante da mudança constante da sociedade; e um sistema cada vez mais integrado.

A sociedade informacional, no entanto, tem seu lado positivo e seu lado negativo. O lado positivo foi exatamente o que foi abordado anteriormente nesse trabalho: a transmissão de informações de maneira rápida e sua utilização em prol do indivíduo e da sociedade, entre outras coisas.

O lado negativo, no entanto, é que pode ser bastante perigoso já que guarda relações diretas com a vida privada do titular desses dados pessoais, como educação, saúde e finanças, além de suas relações sociais e de trabalho.

Por estar presente num âmbito tão íntimo, a coleta, armazenamento e processamento de dados pessoais gera uma gritante vulnerabilidade do titular dessas informações em relação a quem os detém, há um verdadeiro desequilíbrio entre as duas partes. Como lado negativo, essas informações privadas tem a possibilidade de serem expostas e utilizadas de forma indevida, afetando diretamente seus titulares.

Os dados pessoais são como uma nova identificação da pessoa, são inclusive considerados uma mercadoria, que não interfere apenas na esfera individual de cada um, mas afeta toda uma sociedade e por esse motivo ser objeto de proteção do Estado.

Então, Estado, diante da necessidade de proteção individual e da sociedade, perante a sociedade informacional, toma a iniciativa de criação de uma legislação específica capaz de proteger o lado mais vulnerável dessa relação, surge então, a Lei Geral de Proteção de Dados (LGPD), que além da premissa de proteção dos dados pessoais, vem com o papel de salvaguardar direitos fundamentais que antes estavam ameaçados.

Assim como consta no artigo 1º da LGPD:

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (BRASIL, 2018).

Além dos mencionados direitos fundamentais, está também presente na lei o direito à intimidade, à vida privada, à honra e à dignidade da pessoa humana.

Importante mencionar que embora a LGPD tenha sido a primeira regulamentação específica sobre o tema de proteção de dados, esse tema já havia sido tratado anteriormente em outras legislações, como ocorreu na proteção constitucional do direito à intimidade, vida privada, honra e dignidade da pessoa humana, além do Código de Defesa do Consumidor, o pioneiro no assunto de proteção de dados do consumidor. O Código Civil também trata de assuntos que se aproximam bastante da proteção de dados, embora não trate de forma específica do tema.

Logo em seguida, através da Declaração de Santa Cruz de La Sierra, houve o reconhecimento do direito fundamental de proteção de dados pessoais. Quase dez anos depois, foram promulgadas as leis do Cadastro Positivo e Marco Civil da Internet, que trouxeram em seu conteúdo, temas como informações em bancos de dados e o direito do titular de dados frente a utilização de suas informações.

A LGPD traz, respaldada no direito fundamental de liberdade, a manifestação de vontade do indivíduo como fator determinante na utilização de seus dados pessoais. Embora, em se tratando dos dados pessoais, o consentimento acaba por criar um vínculo entre o titular das informações e o agente de tratamento, que é quem

manipula esses dados, pois quando o primeiro manifesta seu consentimento para que o segundo manipule seus dados, é automaticamente criada uma relação de direitos e obrigações.

Frazão, Oliva e Tepedino (2019) trazem a reflexão no mesmo sentido:

O consentimento representa instrumento de manifestação individual no campo dos direitos da personalidade e tem o papel de legitimar que terceiros utilizem, em alguma medida, os dados de seu titular. Ele compreende a liberdade de escolha, sendo meio para a construção e delimitação da esfera privada. Associa-se, portanto, à autodeterminação existencial e informacional do ser humano, mostrando-se imprescindível para a proteção do indivíduo e a circulação de informações. (FRAZÃO, OLIVA e TEPEDINO, 2019)

A Lei Geral de Proteção de dados também dá a definição de consentimento, em seu artigo 5º, inciso XII:

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

XII – consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. (BRASIL, 2018)

O consentimento, é, portanto, tratado como a manifestação livre, informada e inequívoca da vontade do titular. Entretanto, a vontade sozinha não basta, é preciso estar em concordância com o restante do ordenamento, para que assim produza os efeitos do negócio.

2.4 A VULNERABILIDADE DO TITULAR DO DADO PESSOAL

Diante do contexto de sociedade informacional analisado no capítulo anterior, agora é preciso apresentar a figura central desse estudo, o titular dos dados pessoais e entender a extensão da sua vulnerabilidade diante de toda a sociedade.

É importante demonstrar a vulnerabilidade do titular dos dados pessoais ao passo que quanto maior a vulnerabilidade, mais efetivo deve ser o controle desses dados.

Deixar de utilizar os serviços que exigem os dados pessoais não é uma opção plausível, já que ao fazer isso, o titular dos dados acaba sendo excluído da convivência em sociedade e deixa de ter acesso a diversos produtos e serviços.

2.4.1 O TITULAR DO DADO PESSOAL

O titular dos dados pessoais é a pessoa física a quem os dados se referem. Em outras palavras, é a pessoa que tem seus dados pessoais coletados, armazenados, processados ou utilizados por uma empresa, organização ou entidade pública.

A titularidade dos dados pessoais pertence ao titular deles, assim como afirma o artigo 17 da LGPD:

Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei. (BRASIL, 2018)

Um aspecto que merece destaque é o fato referente a impossibilidade de desvinculação dos dados pessoais da pessoa do seu titular, não importando se eles passaram ou não a serem tratados pelo controlador ou operador. Desta forma, ainda que o titular, por livre e espontânea vontade, disponibilize seus dados, não importando se publicamente ou não, há um liame indissociável que a titularidade jamais deixa de ser dele.

Como titular dos dados, uma pessoa tem o direito de estar ciente de como suas informações pessoais estão sendo coletadas, utilizadas e protegidas. Ela tem o direito de ser informada sobre as finalidades do processamento de seus dados e sobre qualquer compartilhamento dessas informações com terceiros. Além disso, em conformidade com o artigo 18 da LGPD, o titular dos dados tem o direito de acessar, corrigir, excluir ou limitar o processamento de seus dados pessoais, caso necessário.

Empresas e organizações têm a responsabilidade de tratar os dados pessoais dos titulares de forma segura e em conformidade com as leis de proteção de dados aplicáveis. Isso envolve garantir a privacidade, confidencialidade e integridade dos dados, bem como obter o consentimento adequado, quando necessário, para processar as informações pessoais.

2.4.2 A VULNERABILIDADE DO TITULAR DO DADO PESSOAL

A vulnerabilidade do titular dos dados pessoais é uma preocupação cada vez mais relevante na sociedade contemporânea, marcada pela ampla coleta e uso de informações pessoais e com o avanço da tecnologia e o surgimento da sociedade da informação, os indivíduos se tornaram mais suscetíveis a riscos relacionados à privacidade e segurança de seus dados.

Um dos principais aspectos da vulnerabilidade do titular dos dados pessoais é a assimetria de poder entre indivíduos e as entidades que coletam e processam suas informações. As empresas, organizações e até mesmo governos têm acesso a um volume significativo de dados pessoais, enquanto os indivíduos muitas vezes têm pouca influência ou controle sobre como suas informações são utilizadas.

Da mesma forma corrobora Marculino (2021, p.26), ao mencionar que existe a necessidade de maiores debates em face da vulnerabilidade do cidadão frente aos agentes de tratamento que possuem mais expertise de suas atividades e até mesmo frente ao Estado.

Essa assimetria pode criar uma situação na qual os titulares dos dados pessoais têm menos capacidade de proteger sua privacidade, controlar o uso de suas informações e tomar decisões informadas sobre o compartilhamento de dados. Eles muitas vezes estão sujeitos a práticas de coleta de dados invasivas, falta de transparência sobre como seus dados são usados e a potenciais violações de segurança que podem resultar em roubo de identidade, fraudes financeiras ou outros abusos.

Além disso, a vulnerabilidade do titular dos dados pessoais é agravada pelo fato de que as informações pessoais podem ser usadas para a criação de perfis detalhados e a tomada de decisões automatizadas que afetam a vida das pessoas. A análise de dados pode resultar em discriminação, exclusão social ou impactos negativos na obtenção de empregos, seguros, serviços financeiros e outros aspectos importantes da vida cotidiana.

Outro ponto relevante é a falta de conhecimento e conscientização por parte dos titulares dos dados. Muitas pessoas não têm plena compreensão dos riscos associados à divulgação de suas informações pessoais, bem como dos direitos e mecanismos disponíveis para proteger sua privacidade. Isso pode levar a um consentimento inadequado ou desinformado ao compartilhar dados, ampliando ainda mais sua vulnerabilidade.

A LGPD em seu artigo 7º, inciso I, traz o consentimento como um pré-requisito para o tratamento de dados pessoais.

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular. (BRASIL, 2018)

O artigo 5º, inciso XII da mesma lei traz a definição de consentimento como uma manifestação livre, informada e inequívoca de concordância do titular com o tratamento de seus dados.

Art. 5º Para os fins desta Lei, considera-se: XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. (BRASIL, 2018)

O consentimento é o ato jurídico em que a pessoa natural, o titular dos dados pessoais, manifesta o seu aceite para que seus dados sejam tratados, mas com uma finalidade específica e informada. O substantivo “finalidade” não deve passar despercebido ao titular, já que é uma manifesta condição ao tratamento de dados e sem a finalidade informada, os dados poderiam ser utilizados como o controlador bem entendesse.

A respeito do consentimento no contexto de proteção de dados pessoais, Mendes (2014, p.61), coloca que:

[...] na medida em que consentimento do indivíduo permite o processamento dos seus dados, na eventual hipótese de violação ao seu direito à privacidade, como poderia ele reivindicar a reparação daquela violação, se tinha autorizado o tratamento de seus dados pessoais? (MENDES 2014, p.61)

Sobre o questionamento de Mendes, mesmo que o consentimento tenha sido dado de maneira livre, informada e inequívoca, junto a ele é preciso estar respeitado o pré-requisito da finalidade, ou seja, a reparação da violação do direito de privacidade na esfera do tratamento de dados seria suficientemente justificada pela distorção da finalidade desse tratamento.

Portanto, para Mendes (2014, p.61-62), “é fundamental compreender que o consentimento não representa a ausência de interesse do indivíduo na tutela dos dados pessoais, mas constitui um ato de escolha no âmbito da autodeterminação individual”.

2.4.3 A VULNERABILIDADE DO TITULAR DO DADO PESSOAL SENSÍVEL

Na LGPD o tratamento de dados pessoais sensíveis se encontra numa seção separada do tratamento dos demais dados, justamente devido a sua importância e potencial de impacto na privacidade e na intimidade das pessoas.

Esse tipo de dado se difere dos demais, à medida que se referem a informações mais íntimas e pessoais, que podem revelar características específicas e sensíveis de um indivíduo.

No tocante aos dados sensíveis, Doneda (2021, p. 160) esclarece que:

A prática do direito da informação deu origem à criação de uma categoria específica de dados, a dos dados sensíveis. Estes seriam determinados tipos de informação que, caso sejam conhecidas e processadas, prestar-se-iam a uma potencial utilização discriminatória ou particularmente lesiva e que apresentaria maiores riscos potenciais que a média, para a pessoa e não raro para a coletividade. Alguns destes dados seriam as informações sobre raça, credo político ou religioso, opções sexuais, o histórico médico ou os dados genéticos de um indivíduo. (DONEDA 2021, p. 160)

Santos (2001), entende que com a mesma cautela que são tratados os dados sensíveis, devem ser tratados também os dados “públicos”, como número de RG e CPF, endereço profissional, entre outros, isto porque dependendo do meio e maneira de divulgação, podem causar lesões igualmente gravosas aos dados sensíveis.

A definição de dado pessoal sensível se encontra no artigo 5º, inciso II da LGPD:

Art. 5º Para os fins desta Lei, considera-se: II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. (BRASIL, 2018)

Em meio a essa era digital, muitos usuários expõem informações pessoais em redes sociais e outros meios online, tanto para se inserirem socialmente e conseguirem se conectar com outros indivíduos, quanto para a utilização de produtos e serviços básicos.

O grande problema se encontra no consentimento “forçado” que os titulares se deparam, já que o acesso aos serviços básicos, como saúde e serviço bancário exigem o fornecimento de dados pessoais como um pré-requisito obrigatório para uso ou acesso a praticamente todos os serviços, sob pena do consumidor, titular dos dados, não ter acesso.

Como visto anteriormente, o consentimento, segundo a própria LGPD (art. 5º, II), é a manifestação livre, informada e inequívoca do titular dos dados. Ou seja, “obrigar” o titular a fornecer os dados em troca de um serviço é ir de contra a legislação.

Mais especificamente, em relação ao consentimento de dados sensíveis (art. 11, I da LGPD), além das exigências dos demais dados, há a exigência que o

requerimento de concessão seja feito de forma específica e destacada, para que não passe de forma despercebida pelo titular.

Dentre os dados sensíveis elencados no artigo 5º da LGPD, merece especial destaque os dados biométricos, os quais foram posteriormente detalhados pelo Decreto 10.046/2019, que em seu artigo 2º, inciso II, traz que “características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar”.

Eles merecem esse destaque pelo fato de serem considerados únicos e permanentes, o que torna a sua utilização mais eficaz e ao mesmo tempo perigosa. A coleta de dados biométricos é uma realidade cada vez mais frequente, na qual os titulares são obrigados a fornecer esses dados tão sensíveis em troca de acessar quase todos os lugares, como por exemplo, academias, condomínios, hospitais, clínicas, empresariais, aeroportos e bancos, sob a justificativa da necessidade de controle de acesso para segurança do próprio usuário.

Mesmo com as vantagens oferecidas por essas tecnologias biométricas, é importante considerar os riscos associados à coleta e armazenamento desses dados, já que se por descuido ou má fé vazarem, podem dar prejuízos financeiros e a honra dos titulares.

Assim, é fundamental que haja regulamentação e medidas de segurança adequadas para garantir a proteção de todo e qualquer tipo de dado pessoal, em especial os dados sensíveis.

3 A EFETIVIDADE DOS MECANISMOS DE CONTROLE TRAZIDOS PELA LGPD

Diante da vulnerabilidade dos cidadãos frente “obrigatoriedade” do fornecimento indiscriminado de dados, sob pena do consumidor, titular dos dados, não ter acesso ao produto ou serviço, como já foi discutido no capítulo anterior, a Lei Geral de Proteção de Dados trouxe uma série de mecanismos repressivos que visam punir empresas e organizações que não cumprem as regras de proteção de dados. Entretanto, a efetividade dos mecanismos repressivos é essencial para garantir a proteção das informações dos titulares diante da sua vulnerabilidade.

3.1 OS MECANISMOS DE CONTROLE DA LGPD

Considerando todas as vulnerabilidades que acometem o titular dos dados, fica patente a necessidade de controle, assim a Lei Geral de Proteção de Dados trouxe uma série de mecanismos repressivos que visam punir empresas e organizações que não cumprem as regras de proteção de dados. O primeiro mecanismo é a aplicação de sanções pela Autoridade Nacional de Proteção de Dados (ANPD), chamada de responsabilização administrativa, as sanções podem ir de advertência, multa até eliminação de dados pessoais. O segundo mecanismo é a responsabilização civil e o ressarcimento de danos, que deve ser buscado por meio de ações que serão apreciadas pelo Poder Judiciário.

Da mesma forma leciona Monteiro (2019), ao afirmar que a LGPD possui dois mecanismos repressivos de proteção de dados pessoais, sendo o primeiro, de responsabilização administrativa com sanções como advertência, multa, publicização da infração, bloqueio e eliminação de dados pessoais, aplicadas pela autoridade nacional (ANPD), e o segundo mecanismo, sendo o de responsabilização civil e o ressarcimento de danos, através do poder Judiciário.

3.1.1 O PRIMEIRO MECANISMO: RESPONSABILIZAÇÃO ADMINISTRATIVA

Um dos principais mecanismos repressivos é a imposição de sanções administrativas, que são impostas às empresas que descumprem as regras da LGPD, as quais podem ser multadas em até 2% do faturamento da empresa, com um máximo de R\$ 50 milhões por infração. Além disso, a LGPD prevê a possibilidade de as empresas serem obrigadas a publicar a decisão que determinou a infração e a

penalidade imposta, e ainda podem ser penalizadas com advertência, bloqueio e eliminação de dados pessoais.

As referidas sanções administrativas constam do art. 52 da LGPD, in verbis:

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II; IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração; (BRASIL, 2018)

Antes da aplicação de sanção, faz-se necessário a instauração do procedimento administrativo e a observação dos parâmetros descritos no § 1º do art. 52, a fim de balizar a dosimetria da infração, a saber:

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)

O art. 53 determinou à autoridade nacional à regulamentação acerca das sanções administrativas, in verbis:

Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa. (BRASIL, 2018)

Para cumprir o art. 53 da LGPD, a ANPD publicou a Resolução CD/ANPD nº 4 de 24 de fevereiro de 2023, que trata da aplicação das sanções administrativas em virtude de infração à LGPD, assim, o tão aguardado regulamento finalmente foi disponibilizado.

Coelho (2023) explica que a Resolução CD/ANPD nº 4/2023, elaborada com diversas contribuições da sociedade, busca garantir a proporcionalidade entre a sanção aplicada e a gravidade da conduta do agente, visando, ainda, proporcionar segurança jurídica aos processos fiscalizatórios e garantir o direito ao devido processo legal e ao contraditório, essenciais ao direito administrativo sancionador.

Conforme a gravidade e a natureza das infrações, estas serão classificadas em leve, média ou grave, conforme descrito no art. 8º do referido regulamento:

Art. 8º As infrações são classificadas, segundo a gravidade e a natureza das infrações e dos direitos pessoais afetados, em:

I - leve;

II - média; ou

III - grave.

§ 1º A infração será considerada leve quando não verificada nenhuma das hipóteses relacionadas nos §§ 2º ou 3º deste artigo.

§ 2º A infração será considerada média quando puder afetar significativamente interesses e direitos fundamentais dos titulares de dados pessoais, caracterizada nas situações em que a atividade de tratamento puder impedir ou limitar, de maneira significativa, o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação; violação à integridade física; ao direito à imagem e à reputação; fraudes financeiras ou uso indevido de identidade, desde que não seja classificada como grave.

§ 3º A infração será considerada grave quando:

I - verificada a hipótese estabelecida no § 2º deste artigo e cumulativamente, pelo menos, uma das seguintes:

a) envolver tratamento de dados pessoais em larga escala, caracterizado quando abranger número significativo de titulares, considerando-se, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica do tratamento realizado;

b) o infrator auferir ou pretender auferir vantagem econômica em decorrência da infração cometida;

c) a infração implicar risco à vida dos titulares;

d) a infração envolver tratamento de dados sensíveis ou de dados pessoais de crianças, de adolescentes ou de idosos; e) o infrator realizar tratamento de dados pessoais sem amparo em uma das hipóteses legais previstas na LGPD;

f) o infrator realizar tratamento com efeitos discriminatórios ilícitos ou abusivos; ou

g) verificada a adoção sistemática de práticas irregulares pelo infrator;

II - constituir obstrução à atividade de fiscalização (BRASIL, 2018)

Grossmann (2023, p.1) nos ensina que o após classificar a infração, o regulamento traz uma tabela para definição do grau de dano, que vão de 0 (danos insignificantes aos titulares) a 3 (lesões com impactos irreversíveis ou de difícil reversão, ou litigância de má-fé), com os graus 1 e 2 relativos à escala progressiva do 0 a 3.

Além disso, O regulamento também traz o rol das circunstâncias agravantes e atenuantes nos artigos 14 e 15, e ainda a forma de cálculo da multa, que para a sua

a fixação, o Regulamento determina que a ANPD deverá observar se há no caso concreto a presença de circunstâncias agravantes e/ou atenuantes, que impactarão no aumento ou na redução do valor da multa.

Ressaltamos, ainda, que a ANPD, desde de 2021, editou o Regulamento, que tem por objetivo estabelecer os procedimentos inerentes ao processo de fiscalização e as regras a serem observadas no âmbito do processo administrativo sancionador pela Autoridade Nacional de Proteção de Dados (ANPD), por meio da publicação da Resolução CD/ANPD nº 1/2021, sendo o Regulamento importante na medida que define procedimentos para fiscalização, traz a forma do processo administrativo sancionador, e define a aplicação subsidiária das disposições da Lei 9.784/99 ao próprio Regulamento, como observamos nos seus artigos 1º e 2º:

Art. 1º Este Regulamento tem por objetivo estabelecer os procedimentos inerentes ao processo de fiscalização e as regras a serem observadas no âmbito do processo administrativo sancionador pela Autoridade Nacional de Proteção de Dados (ANPD).

§ 1º As disposições deste regulamento aplicam-se aos titulares de dados, aos agentes de tratamento, pessoas naturais ou jurídicas, de direito público ou privado e demais interessados no tratamento de dados pessoais, nos termos do art. 13.

§ 2º As disposições da Lei nº 9.784, de 29 de janeiro de 1999, aplicam-se subsidiariamente a este Regulamento.

Art. 2º A fiscalização compreende as atividades de monitoramento, orientação e atuação preventiva, conforme os procedimentos previstos neste Regulamento.

§ 1º A aplicação de sanção ocorrerá em conformidade com a regulamentação específica, por meio de processo administrativo sancionador, definido neste Regulamento.

§ 2º A atividade de fiscalização da ANPD terá por finalidade orientar, prevenir e reprimir as infrações à Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD). (BRASIL, 2018)

Dessa forma, como podemos observar, existem vários regulamentos para fiscalização e aplicação das sanções administrativas, editados pela ANPD, mas impende verificar se, diante da possibilidade de aplicação de sanções administrativas, já houve aplicação de sanções pela ANPD.

No dia 1º de agosto de 2021, entraram em vigor as sanções administrativas da Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD), ocorre que, passado um ano da vigência das sanções, ainda não havia sido aplicada nenhuma multa em pecúnia, isso porque a Autoridade Nacional de Proteção de Dados (ANPD),

estava atuando apenas de forma educativa e visando conscientizar a população sobre os direitos dos titulares, assim como afirmam Rego e Campos (2023).

Ainda, segundo Grossmann (2023), a ANPD já recebeu desde da publicação da LGPD, cerca de 7 mil denúncias e que no 27/2/23, dia da publicação do Regulamento - Resolução CD/ANPD nº 4/2023, havia oito processos administrativos sancionadores em curso à espera da nova norma.

No 31/05/23, a Coordenação-Geral de Fiscalização da Autoridade Nacional de Proteção de Dados – ANPD divulgou uma lista contendo os 16 processos e as 27 instituições que estão sob investigação da ANPD quanto a sua adequação à Lei Geral de Proteção de Dados Pessoais – LGPD. Na referida lista constam empresas privadas como: Tik tok, Telegram Messenger Inc., Claro S.A. e Serasa S.A., WhatsApp LLC, entre outras, além de órgãos e empresas públicos como: Serviço Federal de Processamento de Dados – Serpro, Ministério da Justiça e Segurança Pública, Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP), Instituto Nacional do Seguro Social (INSS) e Dataprev, entre outros, ou seja, os processos ainda estão em tramitação, não tendo sido ainda aplicada nenhuma sanção administrativa pela Autoridade Nacional de Proteção de Dados, além disso, por meio de uma análise superficial, percebemos que o número de processos autuados é pequeno se comparado às denúncias.

Entretanto, acreditamos que tal fato não reflete, verdadeiramente, uma inefetividade deste órgão, mas, tão somente, por ser um órgão novo (criado pela Medida Provisória nº 869/2018, convertida na Lei nº 13.853/2019, mas que só passou a funcionar efetivamente com a nomeação de seu primeiro Diretor-Presidente, em novembro de 2020), ainda não está funcionando com a sua inteira capacidade, mas que, pelo que tudo indica, em breve estará em pleno funcionamento. Prova disso, são as diversas medidas tomadas, a saber:

- Definição e aprovação da estrutura regimental e o quadro de cargos da Autoridade (Decreto nº 10.474/2020).

- Transformação da Autoridade Nacional de Proteção de Dados em autarquia de natureza especial (A Lei nº 14.460/2022);

- Vinculação da ANPD ao Ministério da Justiça e Segurança Pública (Decreto nº 11.401/2023);

- Aprovação do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados (Resolução CD/ANPD Nº 1/2021);

- Aprovação do Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte (Resolução CD/ANPD Nº 2/2022);

- Instituição do Comitê de Governança Digital da Autoridade Nacional de Proteção de Dados (Resolução CD/ANPD Nº 3/2023);

- Aprovação do Regulamento de Dosimetria e Aplicação de Sanções Administrativas (Resolução CD/ANPD Nº 4/2022).

Além disso, ANPD possui autonomia técnico-decisória, patrimônio próprio.

Pois bem, como podemos perceber a regulamentação da Dosimetria e Aplicação de Sanções Administrativas só ocorreu em fevereiro deste ano, e a ANPD não se poderia aplicar sanções sem essa regulamentação, talvez, também seja um dos motivos que em maio ainda não havia decisões do órgão acerca de infrações. Entretanto, pensamos que, logo em breve, a ANPD funcionará plenamente, com total capacidade de ser um mecanismo repressor efetivo na aplicação da LGPD.

3.1.2 O SEGUNDO MECANISMO: RESPONSABILIZAÇÃO CIVIL

Outro mecanismo possível é a responsabilização civil e o ressarcimento de danos, já que há na lei a previsão de ajuizamento de ações judiciais por danos morais e patrimoniais em caso de violação de dados. Isso significa que as pessoas que tiverem seus dados violados podem acionar o Judiciário para buscar reparação pelos danos sofridos, como perda financeira ou comprometimento da sua privacidade, como podemos depreender dos artigos 22 e 42 da LGPD:

Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.”

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)

Sobre a Responsabilidade Civil, antes de adentrar ao tema, cumpre-nos explanar, mesmo que de forma superficial, sobre os seus tipos e os elementos que compõe cada uma.

Assim, quanto a origem ela pode ser dividida em 1) Responsabilidade Civil Contratual, que advém da existência de um contrato entre as partes e, 2) Responsabilidade Civil Extracontratual (Aquiliana), que advém da conduta do infrator ao descumprir a lei vigente.

Assim, a doutrina especializada separou a ilicitude em subjetiva (dolo ou culpa) e objetiva (aquela em que apenas ocorre o prejuízo, sem analisar se a conduta foi intencional ou não).

Pereira (2023, p.1), nos ensina que responsabilidade subjetiva, é composta pela conduta humana, nexo-causal, dano e culpa (esta em sentido amplo, inclui tanto o dolo como a culpa em sentido estrito, que é a quebra do dever de cuidado). Enquanto a responsabilização objetiva tem os mesmos pressupostos, exceto a culpabilidade, ou seja, é composta pela conduta humana, nexo-causal, dano e risco (reconhece-se no agente um dever prévio de cuidado, é responsável, a priori, porque não observou aquele dever de cuidado que lhe era intrínseco).

Feita essa breve revisão dos tipos de responsabilidade, passemos a discorrer acerca de qual responsabilidade Civil que deve ser aplicada quando há o descumprimento dos ditames da LGPD, presente no capítulo VI da lei, intitulado “Da Responsabilidade e do Ressarcimento de Danos”. Apesar, disso, não deixou explícito qual o tipo de responsabilidade deve ser aplicado nos casos relacionados a danos sofridos pelos titulares dos dados. Importante destacar, como bem nos alerta Capanema (2023, p. 2), que dependendo da relação jurídica, a LGPD deve ser preterida, devendo-se utilizar normas específicas, como o Código de Defesa do Consumidor, como expressamente traz o art. 45 da LGPD, in verbis:

Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente. (BRASIL, 2018)

Além disso, o legislador não deixou explícito qual o tipo de responsabilidade deve ser aplicada nos casos relacionados a danos sofridos pelos titulares dos dados, se será uma responsabilidade subjetiva, aquela que necessita de comprovação de culpa por não cumprimento do dever imposto ao agente de tratamento, ou uma responsabilidade objetiva, aquela que é aplicada independentemente de culpa, já que

se baseia no risco da atividade do agente; ou, ainda, a responsabilidade civil ativa ou proativa, defendida por alguns como sendo uma nova modalidade trazida pela LGPD, como nos ensina Oliveira (2022, p. 34):

(...)existe uma discussão doutrinária sobre se a responsabilidade indicada na LGPD seria uma responsabilidade objetiva ou não, sendo que há argumentos válidos em ambos os posicionamentos. Esse fato fez surgir nova ideia de responsabilização, chamada "responsabilidade ativa ou proativa", a qual não se encaixaria especificamente nos conceitos de responsabilidade objetiva ou subjetiva (...) (OLIVEIRA, 2022, p. 34)

Diante disso, faz-se necessário caracterizar quais os tipos de responsabilidade civil dos agentes de tratamento são trazidos pela doutrina, para aplicação nas relações de consumo. Para que possibilite um melhor entendimento acerca das discussões jurisprudenciais que trataremos mais adiante.

3.1.2.1 A RESPONSABILIDADE CIVIL SUBJETIVA DOS AGENTES DE TRATAMENTO DE DADOS

O ar. 42 da LGPD traz a obrigação de reparação do dano, patrimonial ou extrapatrimonial, causado pelos agentes de tratamento (controlador ou operador), em razão do exercício de atividade, vejamos:

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)

Na responsabilidade civil subjetiva é necessário comprovar que o agente que causou o dano agiu com culpa ou dolo, ou seja, que houve uma conduta negligente ou intencional para que a responsabilização ocorra.

Para Gondim (2021, p. 7), o legislador se omitiu ao não estabelecer na LGPD o tipo de responsabilidade, e tal omissão leva a conclusão de que se está diante de responsabilização subjetiva:

Ao se omitir, a primeira conclusão é de que estaria inserida na regra geral da responsabilização subjetiva, uma vez que, para afastar o pressuposto da culpa, a conduta deve estar prevista em lei ou importar em atividade de risco (art. 927 do Código Civil).

Uma leitura do art. 927 do Código Civil, percebemos que o caput trata da responsabilidade subjetiva, enquanto o seu parágrafo único traz a responsabilidade objetiva, em que a reparação do dano ocorrerá independente de culpa, mas "*nos casos especificados em lei*". Isso nos leva, realmente, a concordar com Gondim, pois, *como a LGPD não foi explícita, estaríamos diante da responsabilidade subjetiva, na qual é necessária provar a culpa, in verbis*:

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

Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem. (BRASIL, 2002)

Sobre a questão discorre Maldonado apud Landim (2022, p. 34/35):

(...) o sistema jurídico brasileiro (Código Civil) é a um só tempo adepto da responsabilidade civil subjetiva e objetiva, mister ressaltar que o parágrafo único do artigo 927, do Código Civil, ao mencionar que “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”, o termo risco da atividade ou do negócio está em sua essência atrelado ao risco associado ao produto ou serviço principal do fornecedor, não sendo o tratamento aos dados pessoais uma atividade, propriamente, de risco, mas, sim, um elemento acessório e de apoio ao negócio (...)

E mais, o inciso II, do art. 43, da LGPD uma excludente de responsabilidade, que permite que o agente de tratamento a invoque, desde que prove que não agiu com dolo ou culpa, e que cumpriu os deveres impostos pela lei, falando a favor da responsabilidade civil subjetiva, a saber:

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

(...)

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

(...) (BRASIL, 2018)

3.1.2.2 RESPONSABILIDADE CIVIL OBJETIVA DOS AGENTES DE TRATAMENTO DE DADOS

Como já dito no tópico anterior, a responsabilidade objetiva é trazida pelo parágrafo único do art. 927 do CC.

Segundo Danilo Doneda e Laura Mendes APOUD Mulholland, (2023, p. 1), o legislador optou na LGPD pelo regime da responsabilidade civil objetiva na LGPD, por considerar que os dados pessoais são de natureza de direito personalíssimo e de direito fundamental, sendo assim, a atividade de tratamento de dados traz um risco intrínseco, já que tem potencialidade danosa considerável em caso de violação desses direitos. Defende também, que na medida que inciso III do artigo 6, impõe a necessidade de limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados, vinculando o exercício da atividade de tratamento de dados pessoais a um risco inerente, potencialmente

causador de danos a seus titulares, o que também reforça a adoção do regime de responsabilidade objetiva.

Outra questão a se considerar é que se a relação entre o titular dos dados e o agente de tratamento de dados é não isonômica, deve-se considerar o titular do dado pessoal com sendo hipossuficiente, ou seja, a parte mais fraca da relação, e nesse modo de pensar, o regime de responsabilidade objetiva seria adequado.

Sobre a responsabilidade objetiva Landim (2023) leciona:

“(...) a teoria objetiva, na visão dos doutrinadores que a defendem se mostra mais coerente de tal modo que o risco da atividade possui como fundamento o potencial lesivo aos direitos de outrem, sendo certo que o tratamento aos dados pessoais do titular é um risco por si só e é inerente à atividade normalmente desempenhada pelo fornecedor, ao ponto que não se questiona se a ação do agente de tratamento causador do dano foi imprudente, negligente ou dolosa, ao contrário, haverá obrigação de reparar ao titular, desde que o agente de tratamento tenha criado o risco decorrente de suas atividades.”

Por outro lado, Bodin de Moraes (2019, p. 3) adverte que adoção do regime objetivo apresentaria, para alguns especialistas, um empecilho ao desenvolvimento de novas tecnologias tão bem-vindas para o usuário.

Landim (2023) corrobora com o que advertiu Bodin de Moraes. Para ele, a adoção da responsabilidade civil objetiva, a qual considera o risco da atividade, seria um empecilho ao crescimento de mercado e a inovação tecnológica, uma vez que ao titular restaria demonstrar o dano sofrido para fins de reparação, independentemente da conduta do agente de tratamento.

Novakoski e Naspolini (2023, p.13) defendem o regime da responsabilidade civil objetiva, pois, para os autores, a legislação de proteção de dados traz mecanismos de responsabilidade preventiva, com o intuito de impedir o dano, então parece contraditório subordinar a reparação de danos decorrentes de lesão a dados pessoais, ao regime da responsabilidade civil subjetiva, com todas as dificuldades a ele inerentes, principalmente se considerando que os dados pessoais são um direito humano básico.

3.1.2.3 RESPONSABILIDADE CIVIL OBJETIVA DOS AGENTES DE TRATAMENTO NAS RELAÇÕES DE CONSUMO

Nas relações de consumo, a responsabilidade civil é objetiva, fundada na teoria do risco do negócio, bastando comprovar o dano e o nexo de causalidade, neste

sentido: (Acórdão 1227623, 07084454020188070009, Relatora: GISLENE PINHEIRO, Sétima Turma Cível, data de julgamento: 29/1/2020, publicado no DJE: 10/2/2020.):

(...) a responsabilidade civil decorrente de relação de consumo é de natureza objetiva, não dependendo de culpa para sua ocorrência, possuindo como requisitos apenas a comprovação do dano, a prestação de serviço defeituoso e o nexo de causalidade entre o dano e os defeitos relativos à prestação do serviço.”

O legislador não estando alheio a necessidade de uma maior proteção nas relações de consumo, previu a coexistência da LGPD com outras normas, as quais devem se sobrepôr. Assim, às regras do Código de Defesa do Consumidor devem ser aplicadas para resguardar o direito do titular dos dados, ou seja, deverá aplicar a responsabilidade objetiva, nas relações de consumo, nos moldes dos artigos 45 e 64 da LGPD.

Frise-se ALFREDO ATTIÉ, relator da Apelação Cível nº: 1000794-59.2021.8.26.0554do, pensa do mesmo modo: “Frisa-se, ainda, não haver qualquer antinomia da LGPD como outras legislações, como, por exemplo, o Código de Defesa do Consumidor. Em havendo violação à legislação consumerista, se aplicam as regras do art. 14 e seguintes do Código de Defesa do Consumidor e o regime da responsabilidade civil objetiva.”

DANIELA MENEGATTI MILANO, Relatora **Processo nº 1022003-46.2021.8.26.0405, reconheceu a aplicação da** responsabilidade civil objetiva *na relação de consumo*:

“Evidente a relação de consumo havida entre as partes e, portanto, a responsabilidade objetiva da fornecedora em relação aos danos provenientes de falha na prestação do serviço.”

3.1.2.4 RESPONSABILIDADE CIVIL ATIVA OU PROATIVA DOS AGENTES DE TRATAMENTO DE DADOS

Segundo Bodin de Moraes (2019), a LGPD trouxe um novo regime de responsabilização, nos artigos 42 a 45, o de responsabilidade civil ativa ou proativa, o qual busca prevenir e evitar a ocorrência de danos e não apenas determinar o ressarcimento de danos causados, configurando-se como uma novidade da lei.

A responsabilidade civil ativa se refere ao dever da empresa de tomar todas as medidas necessárias para evitar que ocorram danos aos titulares dos dados,

enquanto a responsabilidade civil proativa consiste em agir antecipadamente, prevenindo possíveis riscos e garantindo que as informações pessoais dos usuários estejam sempre seguras.

A LGPD estabelece que as empresas devem adotar medidas técnicas e organizacionais para proteger os dados pessoais de seus clientes e usuários, incluindo a implementação de políticas de privacidade claras e transparentes, a adoção de medidas de segurança para prevenir ataques cibernéticos e o treinamento de funcionários para lidar com informações pessoais de forma segura.

Bodin de Moraes (2019), afirma que esse novo tipo de responsabilização é importante para a exigência de demonstração do cumprimento, por parte do agente, da adoção das medidas trazidas pela LGPD, indo muito além da mera determinação do ressarcimento de danos causados, buscando prevenir e evitar a ocorrência desses danos.

É importante mencionar que para a configuração de indenização a partir desse novo regime, além da violação de algum dispositivo da LGPD, é preciso que esse dano tenha sido causado por um agente de tratamento de dados, ou seja, apenas esses agentes de tratamento podem ser obrigados a reparar esse dano.

Sobre o tema, Bodin de Moraes (2019) conclui que o legislador, ao passo que não optou pelo regime subjetivo e nem pelo regime objetivo, e elaborou um novo regime pautado na prevenção, defendeu a ideia de evitar em primeiro lugar, que os danos sejam causados.

4 ANÁLISE JURISPRUDENCIAL (ADMINISTRATIVAS E JUDICIAIS)

Com já discutido anteriormente, com a vigência da Lei Geral de Proteção de Dados (LGPD), a Lei 13.709/2018, questões sobre sua aplicação ainda causam dúvida, por conta das novidades que trouxe para o ordenamento jurídico no que se refere à forma que o direito brasileiro pretende proteger dados pessoais em ambientes digitalizados. Por não ter ainda no ordenamento jurídico uma quantidade robusta de decisões acerca do tema, é natural que a comunidade jurídica questione como será a aplicação da referida lei pelo judiciário, qual teoria de responsabilidade civil deve ser aplicada aos agentes de tratamento, como será sua fiscalização, como será a aplicação de sanções para os que infringem da norma, entre tantas outras indagações. Entretanto, como já esclarecido, o escopo desse trabalho foi analisar a decisões da ANPD sobre a responsabilidade administrativas e as decisões judiciais acerca da violação à legislação de proteção de dados pessoais.

Quanto à análise das decisões da Autoridade Nacional de Proteção de Dados, esta restou prejudicada, considerando que até o mês de maio deste ano nenhuma sanção administrativa havia sido aplicada pela Autoridade Nacional de Proteção de Dados.

Passaremos a analisar as decisões proferidas pelo TJSP. Procedemos à pesquisa jurisprudencial no banco de jurisprudência, buscando decisões que contivessem as palavras-chaves: LGPD, responsabilidade civil, responsabilidade objetiva e responsabilidade ativa ou proativa na sua ementa. Desta pesquisa, retornaram um total de 62 decisões, sendo: 33 acerca de “LGPD e responsabilidade civil”; 10 acerca de “LGPD e responsabilidade civil objetiva”; 16 acerca de “LGPD e responsabilidade objetiva”; e 3 acerca de “LGPD e responsabilidade ativa proativa”.

4.1 TRIBUNAL DE JUSTIÇA DE SÃO PAULO AUTOS Nº 1000794-59.2021.8.26.0554

Este julgado trata de pedido de indenização por danos morais, proposta pela consumidora (titular dos dados) contra a Eletropaulo Metropolitana Eletricidade de São Paulo S.A., sob a alegação que teve seus dados pessoais transmitidos a terceiros, sem o seu consentimento, causando-lhe constrangimentos, como recebimento de mensagens e propagandas indesejadas, além de ligações telefônicas

desconhecidas. Alega, ainda, que a proteção dos dados é irrecuperável e que a indevida exposição de sua intimidade, autoriza a condenação da ré em danos morais, com fundamento no art. 42 e seguintes da Lei nº 13.709/18 (LGPD).

Já a ré, em resumo, alegou em sua defesa: que há o risco de possível efeito cascata se acolhido o pedido indenizatório; que os fatos ainda estão sob investigação; que houve a adoção de medidas relacionadas à ampla divulgação do vazamento; inexistência de dano in re ipsa, entre outras.

O relator começou esclarecendo que o art. 5º traz a definição de dado pessoal, dado pessoal sensível, controlador, operador e tratamento, conceitos que são decisivos para a compreensão do regime de responsabilidade civil aplicável ao caso, e para a delimitação da extensão dos danos, em caso de violação aos preceitos adotados na LGPD, bem como em outras legislações, como o Código de Defesa do Consumidor. Explicou, também, que a responsabilidade dos controladores e operadores (agentes de tratamento) está disposta nos art. 42 a 45 da LGPD, e que tal responsabilidade é do tipo ativa e proativa:

Frisou que não há qualquer antinomia da LGPD como outras legislações. E, em havendo violação à legislação consumerista, se aplicam as regras do art. 14 e seguintes do Código de Defesa do Consumidor e o regime da responsabilidade civil objetiva.

Esclareceu, inclusive, que com a LGPD e a adoção de um regime objetivo de responsabilização civil, é falsa a premissa de que haveria uma ampliação do número de demandas indenizatórias, inibindo o desenvolvimento e a indústria, bem como de novas tecnologias.

Relata que é incontroverso que a autora teve dados pessoais não sensíveis (nome, número de CPF, data de nascimento, idade, telefones fixo e celular e endereço de e-mail) expostos indevidamente pela ré.

No caso concreto, não condenou a ré por danos morais, pois não restou demonstrada a lesão a qualquer dos componentes da dignidade humana da autora (igualdade, integridade psicofísica, liberdade e solidariedade), diferente do seria a hipótese de vazamento de dados sensíveis, estes autorizariam a condenação por danos morais in re ipsa (presumido).

No mesmo sentido, os processos: 1022003-46.2021.8.26.0405; 1024481-61.2020.8.26.0405; 1000417-50.2021.8.26.0405; 1000407-06.2021.8.26.0405;

1000331-24.2021.8.26.0003; 1008308-35.2021.8.26.0704 e 1024016-54.2020.8.26.0405.

4.2 TRIBUNAL DE JUSTIÇA DE SÃO PAULO AUTOS Nº 1049037-81.2021.8.26.0506

Trata de pretensão à exclusão de dados pessoais do demandante de sítios eletrônicos da ré, os quais foram inseridos sem o seu consentimento, bem como indenização por danos morais.

O relator explica que as informações constantes da referida página têm finalidade exclusiva de proteção ao crédito, ou seja, são destinadas exclusivamente à análise do risco na concessão de crédito. Além, disso, os dados constantes (nome, CPF, telefone, endereço, nome da mãe, data de nascimento, gênero e renda) não são dados sensíveis, mas dados compartilhados pelos próprios indivíduos em diversos ambientes.

Pontua também que o autor não demonstrou nenhuma situação que configurasse dano psicológico ou à sua personalidade, não havendo em que se falar em indenização por dano moral.

O acórdão foi assim ementado: “OBRIGAÇÃO DE FAZER E INDENIZATÓRIA. Pretensão à exclusão de dados pessoais do demandante de sítios eletrônicos da ré, bem como indenização por danos morais. Impossibilidade. Inserção de dados cadastrais, não sensíveis, conforme o disposto no art. 5º, I e II, da LGPD. Informações destinadas à proteção do crédito, que independem do consentimento do autor. Aplicação do art. 7º, §4º, da LGPD. As inserções impugnadas também são autorizadas pela Lei nº 12.414/2011. Questão objeto de repercussão geral, objeto do Tema 710, do STJ, que deu origem à Súmula 550, do mesmo tribunal. Precedentes. Ausência de danos morais a indenizar. Sentença mantida. RECURSO DESPROVIDO.”

No mesmo sentido, os processos: 1065252-58.2022.8.26.0002; 1049552-19.2021.8.26.0506; 1049037-81.2021.8.26.0506; 1048206-33.2021.8.26.0506; 1044581-72.2021.8.26.0576; e 1044748-08.2021.8.26.0506.

4.3 TRIBUNAL DE JUSTIÇA DE SÃO PAULO AUTOS Nº 1082876-88.2021.8.26.0100

O relator explicou que os fatos deste processo envolvem o chamado e que assim se tornou conhecido dossiê dos antifas, isto é, a compilação de centenas de nomes, imagens e dados de pessoas pretensamente ligadas a movimento dito antifascista. A autora reclama de se terem divulgado sua imagem e alguns dados neste dossiê, ademais associado ou seus integrantes pelo réu à prática de ilícitos.

Continuou relatando que o réu, Deputado Estadual que, se não elaborou o dossiê, amplificou sua divulgação e instou seus seguidores a lhe fornecer dados para tanto, além de ter associando as pessoas constante do dossiê a grupo terrorista.

Asseverou, ainda, que o dossiê é um catálogo organizado de pessoas e entidades ligadas a movimentos ou correntes de esquerda, e é neste catálogo que foram inseridos os dados da autora (nome, data de nascimento, sua imagem e seus endereços nas redes sociais). Ou seja, tratando seus dados com base em supostas preferências políticas (dado sensível), que é uma afronta ao direito à identidade.

Assim, considerou o dano moral configurado, arbitrando indenização.

Já no processo 1049658-35.2021.8.26.0100, o relator votou no mesmo sentido do julgado acima, tendo ainda esclarecido que na vulneração a direito da personalidade, o dano moral se evidencia em in re ipsa, ou seja, o ilícito resta configurado pela própria conduta de violação, sendo necessária a indenização para cumprir seu papel preventivo.

No mesmo sentido, os processos: 1049658-35.2021.8.26.0100; 1012674-37.2021.8.26.0008; e 1034681-38.2021.8.26.0100

4.4 TRIBUNAL DE JUSTIÇA DE SÃO PAULO AUTOS Nº 1042935-03.2021.8.26.0002

Trata-se de recurso de apelação interposto contra a sentença que julgou parcialmente procedente os pedidos formulados em ação indenizatória proposta contra DECOLAR.COM LTDA e AZUL LINHAS AÉREAS BRASILEIRAS S/A, as quais foram condenadas solidariamente no pagamento de danos morais.

Inconformada, a Decolar.com recorreu sob o argumento que os fatos narrados decorreram de fraude perpetrada por terceiros. Diz que não estão presentes os danos morais pleiteados, haja vista que não concorreu para os fatos narrados e sequer foi beneficiada pela conduta ilícita praticada.

O relator pontuou que o conjunto probatório dá conta de que a corré apelante realizou a venda de passagem aérea e emitiu bilhete em nome do autor apelado. Foram utilizados os dados pessoais do autor, além de terem sido encaminhadas mensagens referentes à compra para seu e-mail particular.

Ainda explicou que os danos morais pleiteados pelo autor (recorrido), no entanto, não se viram presentes, haja vista que os fatos alegados como ensejadores da ofensa não são capazes de enquadrar a situação de efetivo dano extrapatrimonial, na medida em que sequer demonstrados quaisquer abalos ou prejuízos impostos ao autor por força da compra de passagem por terceiro em seu nome.

Além disso, asseverou que à luz do disposto na Lei Geral de Proteção de Dados, mais especificamente em seu artigo 5º, II, não houve vazamento de dados pessoais sensíveis, o que não implica automaticamente em ofensa aos direitos da personalidade, tampouco em dano moral presumido.

Recurso provido para afastar a indenização por dano moral.

No mesmo sentido deste julgado, temos o 1002843-25.2022.8.26.0009, que a responsabilidade civil objetiva deveria ser aplicada ao caso, reconheceu que houve vazamento de dados, que o réu descumpriu o ônus da prova, quanto às exigências normativas da LGPD relativas à segurança dos dados, e que o ato ilícito restou caracterizado. Entretanto, deixou de aplicar sanção, tendo em vista a inexistência de dano.

E ainda: processo 1022003-46.2021.8.26.04045, infração, pela ré, de dever inculcado na Lei Geral de Proteção de Dados (LGPD), configuração de responsabilidade objetiva. Inexistência, contudo, de demonstração de dano. Dano moral que exige prova de sua ocorrência. Não aplicação de sanção.

4.5 OUTROS JULGADOS

Quanto ao segundo mecanismo, responsabilização civil, observamos que em todos os julgados que analisamos, o TJSP reconheceu que, quando a relação entre as partes é de consumo, deve-se aplicar as normas do CDC, como bem asseverou o relator do processo nº 1000794-59.2021.8.26.0554, quando disse que não há qualquer antinomia da LGPD como outras legislações. E, em havendo violação à legislação consumerista, se aplicam as regras do art. 14 e seguintes do Código de Defesa do Consumidor e o regime da responsabilidade civil objetiva.

Entretanto, mesmo diante da responsabilidade civil objetiva, o dano e o nexo de causalidade devem estar sobejamente caracterizados (1014245-32.2019.8.26.0196). Este foi na verdade o motivo de que, embora aquela corte tenha reconhecido a infringência da LGPD numa relação consumerista, e, também, reconhecido a aplicação da responsabilidade civil objetiva, deixou de condenar a ré, por falta de comprovação do dano patrimonial ou extrapatrimonial sofrido.

Em outra decisão, apesar de ter reconhecido a aplicação do CDC e a responsabilidade civil objetiva, deixou de inverter o ônus da prova (art. 6º, VIII do CDC), por não se demonstrar verossimilhança. (1010692-66.2022.8.26.0003).

Quanto à responsabilidade ativa ou proativa, ela foi citada em três julgados que analisamos daquela corte, tais decisões consideraram que a doutrina tem razão quando imputam essa responsabilidade aos agentes de tratamento de dados, uma vez que estão obrigados a prevenir e evitar a ocorrência de danos. Entretanto, nos referidos processos, foi reconhecida que cabia a responsabilidade objetiva (1000331-24.2021.8.26.0003; 1008308-35.2020.8.26.0704; 1000794-59.2021.8.26.0554).

Quanto à responsabilidade civil subjetiva, o relator do processo 1000407-06.2021.8.26.0405 esclarece que a responsabilidade atribuída pela LGPD aos agentes de tratamento de dados não é objetiva, mas que esta incide nas relações de consumo, e neste caso, comporta as exceções constantes no inciso II, do art. 14 do CDC e do inciso III do art. 43 da LGPD.

Através das pesquisas jurisprudenciais, citadas ao decorrer do capítulo, foi possível verificar que regra geral a corte paulista tem considerado a responsabilidade subjetiva como aplicável como regra à LGPD, sendo necessária a comprovação de dolo ou culpa. Entretanto, TJSP considerou, em todos os casos analisados, que em caso de relação consumerista, a responsabilidade civil é objetiva, portanto, uma exceção à regra, tendo aplicado sanção desde que se provasse dano.

Já em se tratando de vazamento de dados sensíveis, o dano moral foi considerado presumido, sendo desnecessária a demonstração de prejuízos concretos ou a comprovação do efetivo abalo moral. Em relação os dados pessoais não sensíveis, considerados meramente cadastrais, aquela corte só aplicou sanção quando houve a efetiva demonstração de dano.

Quanto à teoria da responsabilidade ativa ou proativa, que diz respeito à imposição de deveres voltados a prevenção dos danos, esta foi citada encontrada em

três julgados, como sendo uma teoria doutrinária, mas efetivamente, nos referidos julgados, a teoria considerada foi a de responsabilidade civil objetiva, pois os casos eram referentes à relação de consumo.

5 CONCLUSÃO

O desenvolvimento do presente trabalho foi impulsionado pela notada vulnerabilidade do titular de dados pessoais frente ao agente de tratamento, fazendo surgir a pergunta que guiou a pesquisa, qual seja: “Os mecanismos de repressivos constantes na Lei Geral de Proteção de Dados (LGPD) são suficientes para proteger o titular dos dados pessoais? ”.

Antes de ser possível responder a este complexo questionamento, se fez necessário entender que a sociedade impulsionada pela tecnologia, se transformou na chamada sociedade informacional, na qual os dados pessoais são os novos ativos das empresas privadas, ou seja, são bens que podem ser convertidos em dinheiro.

A partir do elevado valor material conferido aos dados pessoais, a coleta e utilização deles passou a acontecer de forma excessiva e descontrolada, violando os princípios constitucionais da dignidade da pessoa humana, da individualidade, da honra, da privacidade e da intimidade.

Notória a necessidade de interferência direta do Estado, foi promulgada a LGPD, objetivando a tutela do dos direitos fundamentais mencionados, assim como o direito à privacidade de dados e a proteção aos que se encontravam mais vulneráveis nessa relação, os titulares de dados.

Mesmo após a entrada em vigor da LGPD, se fez necessária uma proteção ainda mais robusta aos dados pessoais, desta forma, foi promulgada a Emenda Constitucional nº 115/2022, a qual incluiu a proteção de dados no rol dos direitos fundamentais.

Diante do status de direito fundamental, a proteção de dados ganhou ainda mais importância e como forma de cercear essa garantia, a LGPD trouxe dois mecanismos de controle. O primeiro é a responsabilização administrativa aplicada pela Autoridade Nacional de Proteção de Dados (ANPD), em que as sanções previstas vão desde advertência até a eliminação de dados pessoais, e o segundo mecanismo é a responsabilização civil e o ressarcimento de danos através da jurisdição do Poder Judiciário.

Muito além de haver uma previsão em legislação específica sobre a proteção de dados e os mecanismos de controle, é essencial que para uma verdadeira efetividade da lei, seja verificada a existência de fiscalização e aplicação dos mencionados mecanismos. Exatamente como foi feito em seguida no presente trabalho.

Em se tratando do primeiro mecanismo de controle, o de responsabilização administrativa, foi constatado através da divulgação de uma lista pela ANDP, que até maio de 2023, o número de processos administrativos autuados é extremamente pequeno se comparado ao número de denúncias à Autoridade Nacional e até o presente momento, os processos ainda estão em tramitação, não tendo sido ainda aplicada nenhuma sanção administrativa pela Autoridade Nacional de Proteção de Dados.

O segundo mecanismo de controle, o de responsabilização civil, é um pouco mais complexo, pois como a LGPD não deixa explícito qual tipo de responsabilidade civil deve ser aplicado nos casos relacionados a danos sofridos pelos titulares dos dados, há uma discussão doutrinária se a responsabilidade seria objetiva ou subjetiva, surgindo ainda, a partir da LGPD, um novo tipo de responsabilidade, a responsabilidade ativa ou proativa, que busca prevenir e evitar a ocorrência de danos, não se limitando a determinar o ressarcimento de danos causados. O único tipo de responsabilidade civil trazida de forma expressa pela LGPD, é a responsabilidade objetiva quando se tratar de relações de consumo.

De maneira a verificar como está ocorrendo a aplicação da LGPD pelo judiciário, bem como qual teoria de responsabilidade civil está sendo aplicada aos agentes de tratamento e suas respectivas sanções no caso concreto, foi feita uma análise jurisprudencial do TJSP, através das palavras-chaves: LGPD, responsabilidade civil, responsabilidade objetiva e responsabilidade ativa ou proativa na sua ementa.

Através da pesquisa jurisprudencial, acima citada, foi possível verificar que regra geral o Tribunal de Justiça de São Paulo (TJSP), tem considerado a responsabilidade subjetiva como aplicável à LGPD, mas desde que tenha havido a efetiva demonstração de dano. Em se tratando de relação consumerista, que é uma

exceção à regra, o tribunal aplicou em todos os casos a responsabilidade civil é objetiva. Tratando-se de vazamento de dados sensíveis, a corte paulista considerou dano moral presumido, ou seja, sem a necessidade de demonstração dos prejuízos concretos do vazamento. Quanto a teoria de responsabilização civil trazida pela LGPD, a responsabilização ativa ou proativa, ela foi utilizada juntamente com a teoria objetiva, já que em todos os casos, se tratava de relação consumerista.

Por fim, quanto a pergunta central da monografia, se os mecanismos de controle trazidos pela LGPD estão efetivamente protegendo o titular de dados e por consequência promovendo a justiça, é plausível concluir que quanto ao primeiro mecanismo, o de responsabilização administrativa, apesar de a Agência Nacional de Proteção de Dados (ANPD), até o presente momento, não ter tomado nenhuma decisão e aplicado a sanção cabível, isto se dá pelo fato de que ainda não houve tempo hábil para a conclusão dos processos e tal fato não reflete a inefetividade deste órgão, pois diante das diversas medidas tomadas por ele, tudo indica que em breve estará em pleno funcionamento com total capacidade de ser um efetivo mecanismo repressor.

Quanto ao segundo mecanismo, o de responsabilização civil, dentro do recorte feito na pesquisa, é razoável admitir que o mecanismo tem se mostrado bastante efetivo, uma vez que em todos os casos relacionados a dados pessoais não sensíveis (cadastrais) em que houve comprovação do dano (moral ou material), foi aplicada sanção e, nos casos de dados sensíveis, o dano moral foi presumido, não havendo necessidade de prova, sendo aplicada sanção; já em relação ao dano material devido ao vazamento de dado sensível, desde que provado, houve sanção.

REFERÊNCIAS

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2020.

BODIN DE MORAES, M. C. LGPD: um novo regime de responsabilização civil dito proativo. **civilistica.com**, v. 8, n. 3, p. 1-6, 15 dez. 2019. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/448>. Acesso em: 20 mai. 2023.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Centro Gráfico, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20 de mar. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 3 de abr. 2023.

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. **Cadernos Jurídicos: Direito Digital e proteção de dados pessoais, ano**, v. 21, p. 163-170, 2020. Disponível em: <https://core.ac.uk/reader/322682320>. Acesso em 14 jun. 2023.

CARVALHO, Gustavo Robichez de; NASSER, Rafael; MULHOLLAND, Caitlin. **A LGPD e o Novo Marco Normativo no Brasil**. Porto Alegre: Arquipélago Editorial, 2020. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=IDjnDwAAQBAJ&oi=fnd&pg=PT2&dq=A+LGPD+e+o+Novo+Marco+Normativo+no+Brasil.+&ots=P0UdWZjiaV&sig=2b7OsWUQdQh0sNypMQyH59YWp9g#v=onepage&q=A%20LGPD%20e%20o%20Novo%20Marco%20Normativo%20no%20Brasil.&f=false>. Acesso: 23 de maio de 2023.

CASTELLS, Manuel. **A sociedade em rede**. 24. ed. São Paulo: Paz e Terra, 2013.

COELHO, Carolina. Publicado, enfim, o regulamento para aplicação de sanções por infração à LGPD. **Revista Consultor Jurídico**, 5 de março de 2023, 7h05. Acesso em: <https://www.conjur.com.br/2023-mar-05/carolina-coelho-regulamento-aplicacao-sancoes-infracao-igpd#:~:text=%5B1%5D%20Artigo%2053.,base%20das%20san%C3%A7%C3%B5es%20de%20multa>. Acesso em: 05 de junho de 2023.

CNJ. **Resolução nº 46, de 18 de dezembro de 2007**. Cria as tabelas processuais unificadas do poder judiciário e dá outras providências. Disponível em: https://atos.cnj.jus.br/files/resolucao_46_18122007_04042019134854.pdf. Acesso em: 8 de jun. 2023.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters, 2021.

FRAZÃO, Ana; OLIVA, Milena Donato; TEPEDINO, Gustavo. **Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro**. 3. ed. São Paulo: Revista dos Tribunais, 2019.

GONDIM, Glenda Gonçalves. A responsabilidade civil no uso indevido dos dados pessoais. **Revista IBERC**. v. 4, n. 1, p. 19-34, jan./abr. 2021. Disponível em: <https://revistaiberc.emnuvens.com.br/iberc/article/view/140/119>. Acesso em: 15 jun. 2023.

GROSSMANN, Luís Osvaldo. ANPD publica regulamento de sanções e tem 8 processos na fila de multas. **Revista Convergência Digital**, 27/02/2023. Disponível em: <https://www.convergenciadigital.com.br/Governo/ANPD-publica-regulamento-de-sancoes-e-tem-8-processos-na-fila-de-multas-62596.html#:~:text=A%20ANPD%20j%C3%A1%20recebeu%20cerca,%C3%A0%20espera%20da%20nova%20norma>. Acesso em: 15 de mai. 2023.

LANDIM NETO, José Emiliano Paes. **Responsabilidade civil dos agentes de tratamento à luz da lei geral de proteção de dados**: análise jurisprudencial dos Tribunais Estaduais. 2022. Disponível em: https://repositorio.idp.edu.br/bitstream/123456789/4234/5/DISSERTA%c3%87%c3%83O_Jos%c3%a9%20Emiliano%20Paes%20Landim%20Neto.pdf. Acesso em: 13 jun. 2023.

LOPES, Alan Moreira. **Direito Digital e LGPD na Prática**: advocacia digital prática. 1. ed. São Paulo: Rumo Jurídico, 2021.

MAIMONE, Flávio Caetano. **Responsabilidade Civil na LGPD**: efetividade na proteção de dados pessoais. 1. ed. Rio de Janeiro: Foco, 2022.

MARCULINO, Karoline Silveira. **Vulnerabilidade do titular de dados pessoais e a responsabilidade dos agentes de tratamento**. 2021. Disponível em: <https://lume.ufrgs.br/handle/10183/237640>. Acesso em: 2 abr. 2023.

MENDES, Laura Schertel. **Privacidade, Proteção de Dados e Defesa do Consumidor**: linhas gerais de um novo direito fundamental. 1. ed. São Paulo: Saraiva, 2014.

MINISTÉRIO DA JUSTIÇA. **ANPD divulga lista de processos de fiscalização em andamento**, 31/05/2023, 19h01. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-lista-de-processos-de-fiscalizacao-em-andamento>. Acesso em: 7 de junho de 2023.

MONTEIRO, Yasmin Sousa. **A efetividade dos mecanismos de proteção de dados pessoais na lei 13.709/2018**. 2019. Disponível em: <https://repositorio.uniceub.br/jspui/bitstream/prefix/13383/1/21486829.pdf>. Acesso em: 22 de mai. 2023.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, v. 19, n. 3, p. 159-180, 2018. Disponível em: <https://dialnet.unirioja.es/servlet/articulo?codigo=8697583>. Acesso em: 26 mai. 2023.

NOVAKOSKI, André Luis Mota; NASPOLINI, SHDF. Responsabilidade civil na LGPD: problemas e soluções. **Conpedi Law Review**, v. 6, n. 1, p. 158-174, 2020. Disponível em: <https://scholar.archive.org/work/ljqjsbpmb5bojeafhj2sefzm4q/access/wayback/https://i>

ndexlaw.org/index.php/conpedireview/article/download/7024/pdf. Acesso em: 11 jun. 2023.

OLIVEIRA, Helena Saiuri Cato Mendes de. **Responsabilidade civil e a possibilidade de aplicação de limitação e excludentes da responsabilidade civil diante de ataques às bases de dados de empresas privadas: uma análise sob a luz da LGPD e do CDC.** Disponível em: <https://dspace.mackenzie.br/handle/10899/32615>. Acesso em: 23 mai. 2023.

PALHARES, Felipe et al. **Estudos Sobre Privacidade e Proteção de Dados.** 1. ed. São Paulo: Thomson Reuters, 2020.

PEREIRA, Marcus Vinicius Mariot. Responsabilidade Civil: Resumo doutrinário e principais apontamentos. **Jusbrasil**, 17 de abril de 2023. Disponível em: <https://www.jusbrasil.com.br/artigos/responsabilidade-civil-resumo-doutrinario-e-principais-apontamentos/405788006>. Acesso em: 22 mai. 2023.

REGO, Maria Beatriz Torquato; CAMPOS, Lucas Cruz. O que esperar das primeiras multas da LGPD aplicadas pela ANPD. **Revista Consultor Jurídico**, 17 de agosto de 2022, 13h02. Disponível em: <https://www.conjur.com.br/2022-ago-17/rego-campos-primeiras-multas-anpd>. Acesso em: 30 de mai. 2023.

RODRIGUEZ, Daniel Piñeiro. **O Direito Fundamental à Proteção de Dados: vigilância, privacidade e regulação.** 1. ed. Rio de Janeiro: Lumen Juris, 2021.

SANTOS, Antonio Jeová. **Dano moral na internet.** Editora Método, 2001.

SÃO PAULO. Tribunal de Justiça de São Paulo. **Acórdão.** Apelação Cível nº: 1000794-59.2021.8.26.0554. Lei geral de proteção de dados pessoais (LGPD) e direito do consumidor. Ação com preceitos condenatórios. 27ª Câmara de Direito Privado do Tribunal de Justiça de São Paulo. Relator: Alfredo Attié, 30 de novembro de 2021. Disponível em: <https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=15239289&cdForo=0>. Acesso em: 9 jun. 2023.

SÃO PAULO. Tribunal de Justiça de São Paulo. **Acórdão.** Apelação Cível nº: 1049037-81.2021.8.26.0506. Pretensão à exclusão de dados pessoais do demandante de sítios eletrônicos da ré, bem como indenização por danos morais. Impossibilidade. 14ª Câmara de Direito Privado do Tribunal de Justiça de São Paulo. Relator: Anna Paula Dias da Costa, 7 de dezembro de 2022. Disponível em: <https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=16307356&cdForo=0> Acesso em: 13 jun. 2023.

SÃO PAULO. Tribunal de Justiça de São Paulo. **Acórdão.** Apelação Cível nº: 1082876-88.2020.8.26.0100. Responsabilidade civil. Dossiê, chamado Antifas, compilando indevidamente dados pessoais, e sensíveis, nos termos da LGPD, relativos a pessoas identificadas por suas preferências políticas. 1ª Câmara de Direito Privado do Tribunal de Justiça de São Paulo. Relator: Claudio Godoy, 1 de fevereiro de 2022. Disponível em: <https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=15367031&cdForo=0>. Acesso em: 9 jun. 2023.

SÃO PAULO. Tribunal de Justiça de São Paulo. **Acórdão**. Apelação Cível nº: 1042935-03.2021.8.26.0002. Apelação. Ação indenizatória. Contrato de transporte aéreo nacional. Sentença de parcial procedência. Compra de passagem aérea em nome do autor por terceiro sem o seu conhecimento. Danos morais não configurados. 14ª Câmara de Direito Privado do Tribunal de Justiça de São Paulo. Relator: César Zalaf, 8 de setembro de 2022. Disponível em: <https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=16030120&cdForo=0>. Acesso em: 10 jun. 2023.

SÃO PAULO. Tribunal de Justiça de São Paulo. **Acórdão**. Apelação Cível nº: 1022003-46.2021.8.26.0405. APELAÇÃO CÍVEL Prestação de serviços (energia elétrica) Vazamento de dados do consumidor. Ação de indenização por danos morais Sentença de improcedência Inconformismo do autor Vazamento de dados incontroverso. Infração, pela ré, de dever insculpido na Lei Geral de Proteção de Dados (LGPD). Responsabilidade objetiva. 19ª Câmara de Direito Privado do Tribunal de Justiça de São Paulo. Relator: Daniela Menegatti Milano, 24 de março de 2022. Disponível em: <https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=15516070&cdForo=0>. Acesso em: 10 jun. 2023.

SÃO PAULO. Tribunal de Justiça de São Paulo. **Acórdão**. Apelação Cível nº: 1014245-32.2019.8.26.0196. Responsabilidade civil objetiva extracontratual. Lei Geral de Proteção de Dados LGPD. Autor que reclama prejuízo moral em razão de inserção de seus dados pessoais em “site” administrado pela ré, passando a receber ligações indevidas. 27ª Câmara de Direito Privado do Tribunal de Justiça de São Paulo. Relator: Daise Fajardo Nogueira Jacot, 26 de novembro de 2022. Disponível em: <https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=15223083&cdForo=0>. Acesso em: 12 jun. 2023.

SÃO PAULO. Tribunal de Justiça de São Paulo. **Acórdão**. Apelação Cível nº: 1010692-66.2022.8.26.0003. Declaratória e indenizatória Violação à Lei Geral de Proteção de Dados (LGPD). 18ª Câmara de Direito Privado do Tribunal de Justiça de São Paulo. Relator: Henrique Rodriguero Clavisio, 6 de março de 2023. Disponível em: <https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=16527307&cdForo=0>. Acesso em: 12 jun. 2023.

VÉLIZ, Clarissa. **Privacidade é Poder**: por que e como você deveria retomar o controle de seus dados. 1. ed. São Paulo: Contracorrente, 2021.

VILELA, Naiara Aparecida Lima. **O Comércio de Dados Pessoais e a (Des)proteção da Privacidade**. 1. ed. São Paulo: Tirant Lo Blanch, 2020.

ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância**: a luta por um futuro humano na nova fronteira do poder. 1. ed. Rio de Janeiro: Intrínseca, 2021.