UNIVERSIDADE FEDERAL DO PARÁ
INSTITUTO DE CIÊNCIAS JURÍDICAS
FACULDADE DE DIREITO

LUANA MARRON DA SILVA CARDOSO

O DILEMA SOBRE A TEORIA DA RESPONSABILIDADE CIVIL ADOTADA PELA LGPD NO CONTEXTO DE INEFICIÊNCIA DO CONSENTIMENTO COMO BASE LEGAL APTA Á TUTELA DA AUTODETERMINAÇÃO INFORMACIONAL

BELÉM
2024

LUANA MARRON DA SILVA CARDOSO

O DILEMA SOBRE A TEORIA DA RESPONSABILIDADE CIVIL ADOTADA PELA LGPD NO CONTEXTO DE INEFICIÊNCIA DO CONSENTIMENTO COMO BASE LEGAL APTA Á TUTELA DA AUTODETERMINAÇÃO INFORMACIONAL

Trabalho de Conclusão de Curso apresentado à Faculdade de Direito, vinculada ao Instituto de Ciências Jurídicas, da Universidade Federal do Pará, como requisito parcial para obtenção do título de Bacharela em Direito.

Orientadora: Prof.ª Dra. Pastora do Socorro Teixeira Leal.

BELÉM
2024

O DILEMA SOBRE A TEORIA DA RESPONSABILIDADE CIVIL ADOTADA PELA LGPD NO CONTEXTO DE INEFICIÊNCIA DO CONSENTIMENTO COMO BASE LEGAL APTA Á TUTELA DA AUTODETERMINAÇÃO INFORMACIONAL

THE DILEMMA OVER THE THEORY OF CIVIL LIABILITY ADOPTED BY LGPD IN THE CONTEXT OF CONSENT'S THE INEFFICIENCY AS A LEGAL BASIS ABLE TO PROTECT INFORMATIONAL SELF-DETERMINATION

Orientanda Luana Marron da Silva Cardoso[1]
Discente concluinte do curso de Direito na Universidade Federal do Pará
Orientadora Prof.ª Dra. Pastora do Socorro Teixeira Leal
Professora adjunta da Faculdade de Direito da Universidade Federal do Pará

RESUMO

O presente trabalho tem o intuito de analisar qual teoria da responsabilidade civil foi adotada pela Lei Geral de Proteção de Dados (LGPD): teoria objetiva ou subjetiva. Questiona-se se a teoria da responsabilidade adotada é adequada ao deslinde de problemáticas envolvendo a adoção da base legal do consentimento, especialmente considerando a pífia efetividade dessa base legal para promoção da autodeterminação informacional dos titulares de dados e a situação de vulnerabilidade desses titulares. A pesquisa desenvolvida tem caráter teórico-descritivo e viés qualitativo, que é proposto dentro de uma perspectiva crítica e reflexiva. Utiliza-se o método dedutivo, de procedimento de revisão de literatura e a técnica de pesquisa bibliográfica especializada no assunto pesquisado. O artigo se desenvolve a partir da divisão das temáticas abordadas em três itens: no primeiro são apresentadas e analisadas criticamente definições conceituais importantes previstas na LGPD, com destaque para o conceito de dados pessoais e dados pessoais sensíveis, para a definição de consentimento e para a previsão do direito à autodeterminação informacional; no segundo, explana-se sobre os problemas envolvendo a utilização da base legal do consentimento; e, finalmente, o último item aborda as controvérsias envolvendo o entendimento de três autores sobre a teoria da responsabilidade civil prevista na LGPD. Como resultado da pesquisa, concluiu-se por intermédio da análise de várias disposições da LGPD que a teoria adotada foi a teoria subjetiva em razão de diversas previsões voltadas à consideração da culpa do agente de tratamento. Contudo, o estudo sugere

[1] Matrícula 201906140017, e-mail: luanamarron19@gmail.com.

que a teoria da responsabilidade objetiva é a mais viável para tutelar as partes mais vulneráveis da relação, que são os titulares de dados pessoais.

Palavras-chave: responsabilidade civil; LGPD; tutela informacional.

ABSTRACT

This article aims to analyze which theory of civil liability was adopted by the Lei Geral de Proteção de Dados (LGPD): objective or subjective theory. The question is if the theory of liability adopted is adequate to resolve issues involving the adoption of the legal basis of consent, especially considering the poor effectiveness of this legal basis for promoting the informational self-determination of data subjects and the vulnerability of these subjects. The research has a theoretical-descriptive profile and a qualitative bias, which is proposed within a critical and reflective perspective. This article was deleveloped by the deductive method, the literature review procedure and the bibliographic research technique specialized in the subject. The article is divided in three items: the first presents and critically analyzes important conceptual definitions envisaged by LGPD, with emphasis on the concept of personal data and sensitive personal data, the definition of consent and the legal provision of the right to informational self-determination; the second item explains the problems involving the use of consent as a legal basis; and finally, the last item addresses the controversies involving the understanding of three authors regarding the theory of civil liability provided by LGPD. The research has concluded that the theory adopted was the subjective theory due to several provisions aimed at considering the fault of the data processing′s agent. However, the study suggests that the theory of objective liability is the most viable to protect the most vulnerable parties in the relationship, which are the personal data subjects.

Key-words: civil liability; LGPD; informacional protection.

1. INTRODUÇÃO

A proteção de dados pessoais ganhou relevância no cenário jurídico nos últimos anos em razão do avanço do compartilhamento, coleta e tratamento de dados promovido pela constante evolução das tecnologias de informação. Diante disso, inovações legais precisaram ser realizadas a fim de tutelar os titulares de dados pessoais, assegurando-lhes direitos, garantias e mecanismos necessários a sua proteção.

Nesse sentido, foi promulgada a Emenda Constitucional (EC) 115/2022, no dia 10 de fevereiro de 2022, que acrescentou o inciso LXXIX ao art. 5º da Constituição da República Federativa do Brasil (CRFB/88), segundo o qual "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais" (BRASIL, 2022). Como se trata de uma norma de eficácia limitada, o papel de garantir a efetiva aplicação do direito nela previsto foi exercido pela Lei nº 13.709, de 14 de agosto de 2018, ou seja, a Lei Geral de Proteção de Dados (LGPD), que dispõe de forma mais aprofundada sobre os direitos e obrigações dos titulares e dos agentes de tratamento. Além de estabelecer disposições procedimentais quanto à maneira de realização da coleta e tratamento, a LGPD desenvolveu direitos correlatos ao direito fundamental à proteção de dados, como é o caso da autodeterminação informacional.

Contudo, alguns entraves relacionados às disposições legais da LGPD foram identificados ao longo de sua aplicação. Destacam-se as dúvidas e discussões sobre qual teoria da responsabilidade civil a lei teria elegido e sobre qual teoria se adequaria melhor aos problemas envolvendo a garantia dos direitos dos titulares de dados pessoais, considerando suas vulnerabilidades e a necessidade de assegurar o direito fundamental à autodeterminação.

Ademais, cumpre sublinhar que, entre os obstáculos à tutela dos titulares de dados, a ineficiência da adoção do consentimento, uma das principais bases legais autorizadoras do tratamento de dados, merece especial atenção na medida em que se relaciona com a abordagem utilizada pela LGPD para dispor sobre os riscos da atividade de tratamento e oferece implicações significativas ao direito à autodeterminação.

Em face disso, propõe-se tecer um estudo crítico acerca da temática da responsabilidade civil na LGPD, sob a perspectiva da tutela desses titulares sujeitos às complicações relativas ao consentimento e ao exercício de seu direito à autodeterminação, buscando identificar se foi eleita a teoria objetiva ou subjetiva.

O artigo se desenvolve a partir da divisão das temáticas abordadas em três itens: no primeiro, são apresentadas e analisadas criticamente definições conceituais importantes previstas na LGPD, com destaque para o conceito de dados pessoais e dados pessoais sensíveis, para a definição de consentimento e para a previsão do direito à autodeterminação informacional; no segundo, explana-se sobre os problemas envolvendo a utilização da base legal do consentimento; e, finalmente, o último item aborda as controvérsias envolvendo o entendimento de três autores sobre a teoria da responsabilidade civil prevista na LGPD.

A pesquisa desenvolvida tem caráter teórico-descritivo e viés qualitativo, que é proposto dentro de uma perspectiva crítica e reflexiva. Utiliza-se o método dedutivo, de procedimento de revisão de literatura e a técnica de pesquisa bibliográfica especializada no assunto abordado.

2. DADOS NÃO SENSÍVEIS, DADOS SENSÍVEIS E A BASE LEGAL DO CONSENTIMENTO DO TITULAR: SEUS CONCEITOS E SUAS IMPRECISÕES.

O dado pessoal, segundo a LGPD, é a informação relacionada à pessoa natural identificada ou identificável (Art. 5º, I). Alguns exemplos de dados são o nome, CPF, endereço e e-mail.

Segundo a teoria reducionista, a presença de dados que se repetem, a exemplo de homônimos, não permitiria que houvesse a individualização precisa de uma parcela das pessoas inseridas em um banco de dados de base relacional (que organiza os dados relacionando-os entre si), caso não houvesse outros dados considerados identificadores (ou seja, dados únicos) como, por exemplo, o CPF (Bioni, 2019, p. 103).

Noutro lado, a teoria expansionista entende que não necessariamente exige-se um dado identificador para que a pessoa se torne identificável uma vez que a agregação de novas informações dentro de uma mesma base de dados tende a eliminar as incertezas, tendo, em última análise, o potencial para individualizar o titular dos dados coletados. Voltando ao exemplo dos homônimos, a agregação de informações sobre a localização geográfica poderia tornar esse grupo de titulares de dados identificáveis (Bioni, 2019, p. 104).

Independentemente da teoria adotada, ambas coincidem ao considerar que a definição de uma informação como um dado pessoal depende de uma análise das circunstâncias nas quais essa informação está inserida, a partir de um estudo contextual.

Segundo Bioni (2019, p. 108-109), via de regra, prevalece o conceito expansionista no contexto do advento da proteção de dados como um direito fundamental, de modo que o dado pessoal equivale a uma informação que, direta ou indiretamente, identifica um sujeito. Tal definição abarca as informações que têm o potencial de identificar alguém, ainda que de maneira remota, e não limita os dados pessoais a uma projeção imediata, mas inclui um referencial mediato que pode ter ingerência na esfera de uma pessoa.

A LGPD definiu, em seu art. 5º, II, uma espécie de dado contida no gênero dado pessoal anteriormente conceituado, a qual consiste nos dados pessoais sensíveis, que são dados pessoais 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. Os dados sensíveis recebem proteção específica, buscando tutelar o princípio da isonomia, em razão da possibilidade de seu tratamento dar ensejo a algum tipo de vulnerabilidade e discriminação (Bioni, 2019, p. 119).

Da mesma forma como ocorre com os dados pessoais, as informações sobre o usuário só podem ser definitivamente entendidas como dados pessoais sensíveis por meio de uma análise circunstancial, especialmente no sentido de constatar se há potencialidade discriminatória em relação a esses dados haja vista que, a depender do tratamento utilizado, um dado "trivial" pode se tornar um dado sensível (Mulholland, 2021, p. 1-5). Os dados relativos à atividade do usuário em determinada aplicação, tais como histórico de pesquisa e conteúdos mais consumidos, quando devidamente relacionados, podem propiciar que o controlador identifique informações sensíveis acerca do titular.

Esses conceitos são a peça central para o entendimento da proteção de dados como um direito fundamental, elencado no art. 5º, LXXIX, da CRFB/88 e diretamente relacionado ao direito à privacidade e à inviolabilidade da intimidade (art. 5º, X, da CRFB/88).

Ademais, o dado pessoal está atrelado à imagem de seu titular, enquanto pessoa, por se caracterizar como uma projeção, extensão ou dimensão desse titular, especialmente quando tratamos de dados sensíveis. Em virtude disso, a proteção desses dados se insere como um direito da personalidade na medida em que são caracteres incorpóreos que conformam a projeção da pessoa humana e se relacionam ao nome, à honra, e à integridade física e psíquica da pessoa humana (Bioni, 2019, p. 99). Corroborando com tal entendimento, o art. 1º da LGPD estabelece como um de seus objetivos a proteção aos direitos fundamentais de liberdade e de privacidade e ao livre desenvolvimento da personalidade da pessoa natural.

É evidente que a LGPD regulamentou a proteção de dados e especificou outros direitos relacionados a essa garantia fundamental. Assim, destaca-se a autodeterminação informacional, que é, resumidamente, o poder de controle sobre os próprios dados, a fim de que os titulares sejam capazes de determinar, por eles mesmos, quando, como e em qual extensão suas informações pessoais seriam comunicadas aos outros (Westin, 1970). A

autodeterminação está relacionada ao livre desenvolvimento da personalidade em razão de sua correlação com os direitos à liberdade e à privacidade no âmbito da coleta e tratamento de dados.

Um dos mecanismos empregados pela LGPD para frear a coleta massiva de dados e, consequentemente, propiciar um melhor exercício do direito à autodeterminação pelo titular foi a adoção das bases legais elencadas no art. 7º, I a X, como hipóteses autorizadoras da coleta e tratamento de dados dos usuários.

Dessa forma, o tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: a) mediante o fornecimento de consentimento pelo titular; b) para o cumprimento de obrigação legal ou regulatória pelo controlador; c) pela administração pública para execução de políticas públicas; d) para a realização de estudos por órgão de pesquisa; e) para execução de um contrato do qual o titular é parte; f) para o exercício regular de direitos em processo judicial, administrativo ou arbitral; g) em caso de necessidade para a proteção da vida ou da incolumidade física do titular ou de terceiro; h) para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; i) quando necessário para atender aos interesses legítimos do controlador ou de terceiro; j) para a proteção do crédito.

A base legal do consentimento recebe destaque especial em razão da forma como se desenvolveu a proteção de dados ao longo da história e da evolução mundial da regulamentação sobre proteção de dados, principalmente considerando a atuação da Corte Constitucional Alemã.

Resumidamente, a primeira geração de leis sobre proteção de dados foi marcada pelo foco na atuação da esfera governamental e na regulação rígida da própria tecnologia empregada. Entretanto, diante da inviabilidade dessa estratégia regulatória, a segunda geração legislativa optou por transferir ao titular de dados a responsabilidade pela proteção e o consentimento passou a ser um meio pelo qual o cidadão expressa sua escolha quanto à coleta, uso e compartilhamentos dos próprios dados. Na geração subsequente, busca-se assegurar a ampla participação do indivíduo no processo de tratamento de seus dados almejando o máximo controle do indivíduo sobre o fluxo de suas informações e aumentando o protagonismo do consentimento. A quarta geração inovou ao relativizar a centralidade do consentimento, entretanto não eliminou o seu protagonismo e adicionou a adjetivação – livre, informado, inequívoco, explícito e/ou específico (Bioni, 2019, p. 170-173).

No contexto brasileiro, a LGPD segue a quarta geração evolutiva e define consentimento, em seu artigo 5º, XII, como a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinados, sendo que tais dados pessoais consistem na informação relacionada a pessoa natural identificada ou identificável (artigo 5º, I), e o seu tratamento é toda operação referente a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (artigo 5º, XII).

Por sua vez, o artigo 7º, I da referida lei determina que o fornecimento de consentimento é uma das hipóteses que permitem a realização do tratamento de dados pessoais, contanto que tal consentimento seja livre, informado, inequívoco e diga respeito a uma finalidade determinada de forma geral, e, em alguns casos, deve ser, ainda, específico.

O tratamento de dados sensíveis por meio do consentimento do titular exige que esse consentimento seja realizado de forma específica e destacada, para finalidades específicas (artigo 11, I, LGPD), ou seja, afasta-se a possibilidade de autorização do tratamento de dados sensíveis por meio de consentimento genérico e/ou cuja finalidade do tratamento não esteja bem delimitada (Mulholland, 2021, p. 15-18).

Ademais, a LGPD (artigo 9º, § 2º, e artigo 18) determina que, quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular deverá ser informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados – os quais a) são obter do controlador a confirmação da existência de tratamento; b) acesso aos dados; c) correção de dados incompletos, inexatos ou desatualizados; d) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na lei; e) portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; f) eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no artigo 16 da mesma lei; g) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; h) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; i) revogação do consentimento.

Sobre o compartilhamento e a comunicação de dados pessoais sensíveis entre controladores para obter vantagem econômica, a LPGD apenas considera a possibilidade de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências (artigo 11, § 3º). Até o presente momento, não foi realizada tal regulamentação pela ANPD.

Teoricamente, o consentimento é o mecanismo pelo qual se confere efetividade ao direito da autodeterminação informativa, pois, ao ofertar ao indivíduo a possibilidade de participação no tratamento de seus dados, o desenvolvimento de sua personalidade é, neste aspecto, salvaguardado. O direito à autodeterminação informativa funcionaria como uma "mola propulsora" da estrutura de proteção de dados, a qual pode ser entendida como um elemento atual indispensável a concretizar a cidadania do novo milênio (Rodotá, 2008, p. 17).

Contudo, a prática diverge da teoria por esbarrar em aspectos que dificultam a plenitude do consentimento. A priori, verifica-se que há uma incerteza sobre a terminologia utilizada pela legislação brasileira, que prejudica o entendimento sobre como determinado dado deve ser tutelado. Isso se dá porque o entendimento sobre os conceitos de dado pessoal ou de dado pessoal sensível e, consequentemente, sobre as estratégias regulatórias possíveis para a sua definição é algo fluido, que somente é entendido com maior precisão a partir de uma análise mais concreta da situação na qual tais dados estão inseridos, com a demonstração das diferenças e das consequências práticas entre tais estratégias regulatórias distintas (Bioni, 2019, p. 102).

Dessa forma, desenha-se uma incerteza jurídica quanto à aplicação da legislação na rotina dos titulares, que é ampliada pelas limitações dos usuários de tecnologias sobre o seu funcionamento, impossibilitando um exercício concreto da autodeterminação informacional.

Somada a essa incerteza conceitual, verifica-se que a legislação não oferta um definição dos termos "livre, informado, inequívoco, explícito e/ou específico", deixando a cargo dos controladores e titulares a descrição do consentimento pleno, o que permite questionar em quais situações o consentimento segue os moldes da lei em termos práticos.

3. A PROBLEMÁTICA DA APLICAÇÃO SOBRECARREGADA DA BASE LEGAL DO CONSENTIMENTO.

Existem alguns impedimentos ao exercício de livre consentimento, como a limitação intelectiva dos titulares de dados de avaliar os riscos e benefícios da ação durante sua tomada

de decisão. Entre as limitações psicológicas para a tomada de decisão, a teoria da decisão da utilidade subjetiva postula que, nas considerações iniciais sobre o consentimento, o ganho imediato pesa mais do que as futuras perdas, ainda que as ramificações dessa perda sejam consideráveis (Kerr; Berrigar; Burkell, 2006, p. 7), o qual, no caso de consentimento para compartilhamento dos dados com terceiros, consistiria no benefício imediato de usufruir determinado serviço online, enquanto há futuras perdas na privacidade do consumidor e na sua autodeterminação.

Bioni (2019, p. 210-222) aponta uma sobrecarga do consentimento a partir de conclusões advindas de sua análise de estudos empíricos das Universidades de Stanford e Carnigie Mellon (Cranor; Mcdonald, 2010, p. 1), Universidade de Berkeley (Hoofnagle *et al*., 2012, p. 273) e Universidade da Pensilvânia (Turow; Hennessy; Draper, 2015, p. 13). Resumidamente, as conclusões obtidas pelo autor demonstram que a falta de conhecimento sobre as tecnologias de coleta de dados e publicidade comportamental é um fator que dificulta a plenitude do consentimento, – especialmente, quanto consideramos o desconhecimento sobre sua nocividade à livre escolha – o que é intensificado pela constante atualização do arsenal tecnológico, impedindo a obtenção desse conhecimento em razão da liquidez inerente à tecnologia e da assimetria das relações entre titulares de dados e empresas possuidoras das tecnologias da informação.

Outrossim, a análise do autor confirma a teoria da utilidade subjetiva, acrescentando que a economia informacional se usa dessa vulnerabilidade dos cidadãos para favorecer a coleta de dados. Também foi possível concluir que há uma resignação das pessoas em relação à economia de dados pessoais, ainda que a maioria discorde dessa lógica dessa espécie de atuação, de modo que acataram algo que é indesejável, mas, ao mesmo tempo, inevitável.

Entretanto, tais indivíduos afirmam o desejo de ter controle sobre seus próprios dados de maneira que a resignação é fruto da descrença dessa habilidade. Entende-se que essas conclusões põem em xeque a ideia de autogestão diante de um problema estrutural, segundo o qual as diversas oportunidades na sociedade atual estão condicionadas ao fornecimento dos dados pessoais e, ao mesmo tempo, constata-se a existência de uma relação assimétrica geradora de uma vulnerabilidade específica.

É pertinente citar o caso do aplicativo WhatsApp, considerando que, mesmo após a mudança de privacidade permitindo a coleta de dados em 2015, continua sendo o aplicativo de mensagem mais utilizado no Brasil, estando presente em 98% dos smartphones em 2021,

enquanto o aplicativo de mensagens Telegram, seu concorrente, é utilizado por 45% dos usuários desses aparelhos (Statista, 2021).

A resignação dos usuários em face do descontrole sobre o uso de seus dados por terceiros, somado à fragilidade do consentimento como forma de promoção de autodeterminação informacional, demonstra que a legislação de proteção de dados transferem para o indivíduo grande parte da responsabilidade para promover sua autogestão, sem que haja a devida atenção para o padrão de comportamento desses titulares em meio ao caráter tipo de abordagem utilizada pelos controladores do tratamento de dados.

Somado a isso, a maioria das organizações continuam a tratar o consentimento como um momento transacional¸ utilizando os acordos cuja forma genérica é baseada na afirmação "li e concordo com os termos e condições", chamados de contratos de adesão, como um meio de obter consentimento abrangente para coleta, uso e divulgações excessiva dos dados pessoais (Kerr; Berrigar; Burkell, 2006, p. 10).

Isso ocorre principalmente nas situações relacionadas à monetização a partir do tratamento de dados por meio dos *freemiuns*, que são modelos de negócios que permitem acesso livre e gratuito a determinado serviço ou produto online em sua versão limitada ou básica e, para acessar a versão completa ou *premium*, exige contraprestação pecuniária direta, entretanto migrar para uma versão *premium* não exclui a possiblidade de rentabilizar os dados dos usuários, bem como o titular de dados desconhece o custo efetivo da transação que está realizando e o processo de tratamento de seus dados (Bioni, 2019, p. 49-50).

Frisa-se que é comum que o aceite do uso e do compartilhamento dos dados pessoais seja uma condição para que o usuário usufrua das funcionalidades oferecidas, situação que torna nítida a disposição sobre os dados pessoais como uma moeda de troca no contexto de aplicações e sites gratuitos.

Uma forma de ilustrar a relação entre pagamento pelo serviço e comercialização de dados corresponde à venda do aplicativo de mensagem WhatsApp para a rede social Meta, outrora Facebook. O Whatsapp, que antes possuía como proposta a proteção dos dados pessoais de seus usuários contra a publicidade comportamental, cogitou o pagamento de U$ 1,00 ao ano para utilização do serviço, todavia mudou sua política de negócio em 2015 ao instituir uma nova política de privacidade que passou a compartilhar os dados do usuário com um grupo de empresas do grupo, aumentando seu rendimento para U$12,00 ao ano por usuário (Insider, 2014). Também convém citar o exemplo do faturamento em mídia do

Instagram em 2019, que foi próximo aos 20 bilhões de dólares, sendo esta receita diretamente relacionada ao valor dos dados dos seus usuários (Isto é dinheiro, 2019).

Considerando que os usuários não pagam uma quantia monetária (*zero-price*) pelo produto ou serviço, a contraprestação deriva do fornecimento de seus dados pessoais, que possibilita o direcionamento de conteúdo publicitário, e cuja receita pagará, indiretamente, pelo bem de consumo (*advertisement business model*), qual seja o serviço ou produto fornecido pelo provedor (Bioni, 2019, p. 49).

Entende-se, portanto, que essa economia baseada na monetização de dados, denominada, sob complementar perspectiva, pela terminologia *zero-price advertisement business model*, consiste na cadeia de relações de troca que se forma a partir da contraprestação por parte do titular dos mesmos dados – o qual fornece seus dados a fim de utilizar o serviço teoricamente gratuito – e, uma vez coletados pelo prestador do serviço, a cadeia segue com a venda dos dados a terceiros, situação na qual observa-se contraprestação monetária. Essa cadeia constitui uma relação plurilateral, caracterizada pela presença dos anunciantes publicitários – distanciando da tradicional relação bilateral que envolve basicamente usuário do serviço e fornecedor entorno de uma transação econômica direta aperfeiçoada pela transferência pecuniária (Bioni, 2019, p. 47).

Verifica-se que essa realidade intensifica a vulnerabilidade do titular de dados na medida em que se perfila por intermédio de uma complexa rede de relações, com atores externos à relação controlador-titular, sobre os quais sequer o titular tem conhecimento, o que, em conjunto com as limitações do titular sobre os termos técnicos que permeiam essas relaçãos, prejudica novamente a autogestão de dados.

Diante disso, constata-se que há uma situação na qual o agente de tratamento obtém vantagens econômicas por meio do tratamento de dados de pessoas naturais obtidos mediante o fornecimento de consentimento sobrecarregado e ineficiente como medida de proteção desses indivíduos, submetendo os titulares a riscos relativos à violação de seus direitos fundamentais. Esse é um dos fatores determinantes à necessidade de aplicação da teoria do risco da atividade em caso de responsabilidade por eventuais danos provenientes desse tratamento, conforme será explanado posteriormente.

4. OS QUESTIONAMENTOS SOBRE A ADOÇÃO DA TEORIA DA CULPA PELO REGRAMENTO DA RESPONSABILIDADE CIVIL DA LGPD E A VIABILIDADE DE SUA SUBSTITUIÇÃO PELA APLICAÇÃO DA TEORIA DO RISCO DA ATIVIDADE.

A seção III "Da Responsabilidade e do Ressarcimento de Danos" abarca os arts. 42 a 45. Seguindo um modelo de cláusula geral, o art. 42 *caput*¸ determina que "o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo" (BRASIL, 2018).

O art. 44 da LGPD trata sobre a ocorrência de tratamento irregular de dados quando o agente de tratamento (i) deixar de observar a legislação ou (ii) não oferecer a segurança que o titular dele pode esperar, ou seja, sua legítima expectativa; consideradas as circunstâncias relevantes, enumeradas não exaustivamente nos incisos I a III: o modo pelo qual o tratamento é realizado; o resultado e os riscos que razoavelmente dele se esperam; e as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado. O parágrafo único do referido artigo dispõe que respondem pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46, der causa ao dano.

Analisando o art. 44, a noção de "tratamento irregular" mostra-se ambígua no texto da LGPD, na medida em que abarca a responsabilidade por violação da legislação (art. 44, *caput*) e por violação da segurança (art. 44, parágrafo único). Dessa forma, a disposição dessas determinações parece sugerir uma conexão mais estreita da noção de regularidade do tratamento para com a violação da segurança, do que para com a violação à legislação da proteção de dados, apesar da existência de uma excludente específica em caso de estrito cumprimento da legislação (art. 43, II) (Bioni; Dias, 2020, p. 10), a qual será melhor explicada mais à frente.

Segundo Bioni e Dias, o "tratamento irregular" não é noção autônoma, e o não fornecimento da segurança que o titular pode esperar (art. 44, *caput*) deve coincidir com "deixar de adotar as medidas de segurança" aptas a proteger os dados pessoais (art. 44, parágrafo único, c/c art. 46, *caput*)" (Bioni; Dias, 2020, p. 12).

Diante disso, o critério de "não fornecimento da segurança que o titular pode esperar do tratamento" (art. 44, *caput*), isoladamente, parece oferecer apenas diretrizes na elaboração do seu conteúdo ao invés de delimitar um critério para identificar a ocorrência de responsabilidade. Isso se deve ao fato de o critério da adoção de tratamentos aptos a proteger os dados pessoais ser demasiadamente amplo, conferindo apenas um critério mínimo uma vez que o cabedal de medidas aptas é extremamente vasto (Bioni; Dias, 2020, p. 13).

Nesse sentido, o esclarecimento do conceito de "não fornecimento da segurança que o titular pode esperar do tratamento" exigiria um filtro jurídico, ora representado pelas "expectativas juridicamente legítimas de segurança", que é um conceito indeterminado cujo sentido deve ser concretizado pelos tribunais em vista das circunstâncias do caso concreto. Somado a isso, faz-se necessário identificar o sujeito ao qual a lei intitulou "titular" nesse contexto, sendo possível adotar o critério subjetivo, no qual o titular seria a pessoa em causa, aumentando o relativismo da previsão legal; ou adotar o critério objetivo, tal qual faz o Código de Defesa do Consumidor, a partir do qual esse "titular" representaria um grupo abstrato de pessoas (Bioni; Dias, 2020, p. 13).

Segundo Bioni e Dias (2020, p. 14), as hipóteses de circunstâncias relevantes dos incisos I a III do art. 44 são calibradas pelo art. 50, §§ 1º e 2º, da LGPD, que, resumidamente, prevê que o operador e o controlador devem considerar algumas características em relação ao tratamento e aos dados ao estabelecer as boas práticas e implementar programas de governança, estabelecendo que a conduta a ser adotada poderá variar de acordo com a variação do potencial lesivo das mais diferentes atividades de tratamento de dados. Dessa forma, o texto da LGPD não nivela toda e qualquer atividade de tratamento de dados como sendo de risco exacerbado em face da multiplicidade de efeitos colaterais distintos, o que deve ser analisado caso a caso.

Outro critério de análise da noção de "tratamento irregular" que merece destaque são "as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado", circunstância relevante prevista no inciso III do art. 44, a qual foi inspirada na definição de produto ou serviço defeituoso do CDC (art. 12, § 1º, III e art. 14, § 1º, III) – o produto ou serviço será defeituoso quando não fornecer a segurança que o consumidor dele pode esperar, considerando as circunstâncias relevantes, a exemplo do risco que razoavelmente se espera e da época em que foi colocado em circulação ou fornecido.

Dessa maneira, o parâmetro determinante para definir as técnicas de tratamento disponíveis seria o da diligência média dos agentes de tratamento, o que deve ser avaliado no caso concreto. Frisa-se que, ao contrário do CDC, não há previsão de exclusão da culpa análoga. Bioni e Dias defendem que é possível conceber que o parâmetro almejado é, assim como no CDC, mais rigoroso do que o da culpa em razão da inspiração proveniente da legislação consumerista (Bioni; Dias, 2020, p. 16-18), contudo essa conclusão pressupõe uma interpretação que extrapola a previsão do texto legal.

À primeira vista, é possível concluir que as disposições mais gerais da LGPD sobre responsabilidade dos agentes e das irregularidades do processo de tratamento de dados se mostram amplas e por vezes ambíguas. Ao estipular várias disposições que se propõem adequar ao caso completo, a legislação tangencia a vagueza de seus conceitos e esbarra na falta de uma quantidade razoável de casos judicializados e concluídos para que possa haver o balizamento dessas disposições.

Observa-se que esse quadro tende a ser intensificado a partir da imprecisão de outros conceitos basilares anteriormente citados, a exemplo da própria definição de dados sensíveis e dados não sensíveis ou das características do consentimento.

Além disso, não se pode negar que, como a própria lei dispõe nos seu art. 50, as atividades de tratamento de dados figuram como atividades de risco. Em outras palavras, o risco é intrínseco à atividade de tratamento de dados, apesar de ser possível graduar esse risco em escalas de prováveis danos ao titular, que, em regra, figura como a parte mais vulnerável da relação por não dominar a tecnologia e os métodos utilizados nesse tratamento, bem como ter pouca ou nenhuma noção sobre os conceitos legais estruturantes dessa atividade. Vale ressaltar que os possíveis danos estão relacionados a direito fundamentais de titulares, evidenciando ainda mais sua vulnerabilidade, haja vista que há uma potencialidade danosa considerável em caso de violação desses direitos, caracterizados principalmente por sua natureza de direito personalíssimo e de direito fundamental (Mulholland, 2021, p. 14), a exemplo do direito à autodeterminação.

Diante dos riscos inerentes ao tratamento de dados e da vulnerabilidade dos titulares, entende-se que a teoria da responsabilidade objetiva, baseada na teoria do risco da atividade, seria a mais adequada a ser adotada no contexto da proteção de dados, especialmente com o intuito de garantir o pleno exercício da autodeterminação. Todavia, isso esbarra em outra

inexatidão da LGPD, que consiste na dúvida sobre qual tipo de teoria da responsabilidade foi adotada pelo legislador durante a produção do texto legal.

Essa dúvida está relacionada principalmente às hipóteses excludentes de ilicitudes previstas no art. 43, I a III, segundo o qual os agentes de tratamento não serão responsabilizados quando provarem que i) não realizaram o tratamento de dados pessoais que lhes é atribuído; ii) que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou iii) que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro. Tais excludentes contrastam com a previsão do art. 44 sobre o tratamento irregular que, embora não trate expressamente sobre responsabilidade objetiva, utiliza vários conceitos e construções normativas provenientes do CDC.

Antes de analisar a teoria da responsabilidade atualmente adotada pela LGPD, cumpre dizer que durante o processo de produção e aprovação dessa lei várias mudanças foram empreendidas em seu texto. A primeira versão do anteprojeto da LGPD adotou expressamente a teoria da responsabilidade objetiva baseada na teoria do risco da atividade em seu art. 6º, utilizando como referência o CDC.

Contudo, ao longo do processo legislativo, essa previsão foi excluída do texto e, adotou-se a análise do elemento de culpa como uns pressupostos a responsabilidade ao adicionar a possibilidade de eximir a responsabilização dos agentes de tratamento de dados caso comprovem “que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados” (art. 43, II) (Bioni; Dias, 2020, p. 5-7).

Outros aspectos da lei que reforçam a discussão da culpa são o princípio da *accountability* e a previsão de “relatórios de impacto à proteção de dados pessoais” (RIPD), especialmente para atividades de tratamento de dados que fossem de “alto risco”.

Em resumo, o princípio da *accountability*, previsto no art. 6º, X, da LGPD, exige que o controlador não apenas cumpra a lei, mas também que documente e demonstre esse cumprimento, objetivando-se garantir a transparência e a confiança no tratamento de dados pessoais. Já os relatórios de impacto à proteção de dados pessoais (art. 5º, XVII) tratam-se da documentação do controlador com a descrição dos processos de tratamento de dados pessoais

que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Esses elementos, somados ao Capítulo VII da LGPD, que trata sobre segurança e boas práticas, demonstram a existência de uma estrutura normativa que prioriza um juízo de valor em torno da conduta do lesante, diferenciando essa conduta por meio de uma análise sobre o risco que cada atividade de tratamento pode oferecer ao titular de dados (Bioni; Dias, 2020, p. 8).

Atualmente, não há consenso entre os autores dedicados ao estudo da responsabilidade na LGPD. A seguir, apresenta-se um breve apanhado das interpretações de alguns desses autores.

Bruno Bioni e Daniel Dias defendem que há uma presunção automática-legal da (i) a autoria do tratamento por parte do agente a quem o tratamento é atribuído; (ii) a violação à legislação de proteção de dados ou irregularidade do tratamento. Essa presunção automática, em conjunto com a possibilidade de inversão do ônus da prova em favor do titular (art. 42, § 2º, da LGPD) e a flexibilidade de outros elementos legais, tornaria extremamente difícil que o agente de tratamento de dados consiga afastar a sua culpa, apesar de ser adotada a responsabilidade subjetiva, representando uma erosão bastante significativa dos filtros da responsabilidade civil em favor do titular dos dados (Bioni; Dias, 2020, p. 18-20).

Existem alguns questionamentos válidos a serem pontuados sobre tal presunção automática-legal. Primariamente, impõe-se dizer que não há previsões expressas na lei sobre tal presunção. Os autores chegaram a essa conclusão por entenderem que, uma vez que a lei estabelece que os agentes de tratamento devem provar tais circunstâncias para evitar a responsabilização, a regra seria a presunção do descumprimento da legislação em caso de dano, o que facilitaria a responsabilização dos agentes e favoreceria os titulares e aproximaria a legislação de aspectos mais ligados à responsabilidade objetiva.

Contudo, analisando mais especificamente o inciso II do art. 43, segundo o qual percebe-se que a erosão no filtro da culpa pode ser mais favorável ao agente, e não ao titular. Isso porque é possível que os agentes tenham realizado o tratamento de dados pessoais que lhes é atribuído sem violação à legislação de proteção de dados, sendo possível aplicar a excludente de ilicitude, e que ainda assim haja o dano e a conduta do agente mediante culpa. Como destacado ao longo do presente trabalho, a legislação é repleta de conceitos

indeterminados, o que representa uma margem interpretativa para que o agente empreenda danos e ainda esteja dentro dos moldes legais.

A exemplo dessa situação, retoma-se a sobrecarga do consentimento do titular. Os agentes se valem da falta de requisitos que definam com exatidão a qualificação do consentimento como uma manifestação livre, informada e inequívoca, utilizando-se de manifestações meramente formais para embasar o tratamento de dados na hipótese do inciso I do art. 7º e gerando danos à autodeterminação ao empreender a uma complexa economia de dados pessoais que torna impossível a autogestão dos dados pessoais por seus titulares e que gera lucro aos agentes.

Explorando um viés diverso do apresentado anteriormente, as autoras Gisela Guedes e Rose Meireles (2023, p. 223) entendem que a LGPD adotou claramente a teoria subjetiva da responsabilidade civil, exigindo a prova da culpa do agente de tratamento na ocasião do dano, uma vez fundamentada (i) na omissão na adoção de medidas de segurança para o tratamento adequado dos dados (“quando não fornecer a segurança que o titular dele pode esperar,”); (ii) no descumprimento das obrigações impostas na lei (“em violação à legislação de proteção de dados pessoais” ou “quando deixar de observar a legislação”).

Ao contrário de Bioni e Dias, Guedes e Meireles entendem que na análise das excludentes de responsabilidade, o inciso II do art. 43 indicaria a adoção de uma excludente tipicamente relacionada às hipóteses de responsabilidade civil subjetiva uma vez que a violação da lei seria elemento subjetivo da obrigação de indenizar e indicaria a conduta culposa do agente de tratamento de dados. Desse modo, não haveria obrigação de indenizar quando o agente de tratamento de dados tiver demonstrado que observou o padrão esperado de atuação e, se o dano ocorreu, não foi em razão de sua conduta.

Para Caitlin Mulholland (2021, p. 15-19), a LGPD, pela inteligência dos arts. 42 e 44, adota a teoria da responsabilidade civil objetiva. A autora fundamenta essa conclusão ao defender que, na hipótese de violação de segurança (art. 46, parágrafo único), o legislador buscou abarcar situações danosas decorrentes de incidentes de segurança, ou seja, acontecimentos relacionados ao risco intrínseco da atividade de tratamento de dados, como vazamentos não intencionais e invasão de sistemas e bases de dados por terceiros não autorizados.

Uma proposta diferente é apresentada por Maria Celina Bodin de Moraes na forma da teoria ativa ou proativa da responsabilidade civil. Segundo essa teoria, a LGPD inaugurou um viés positivo sobre a responsabilidade civil, determinado pela necessidade de adoção de posturas voltadas à prevenção de danos, o que torna excepcional a obrigação de indenizar. Dessa maneira, o regime de responsabilidade adotado pela LGPD não poderia ser tratado nem como objetivo, nem como subjetivo, apesar da autora entender que há uma aproximação maior deste último, mas como uma responsabilização "proativa".

A partir desses posicionamentos, verifica-se que a legislação não define claramente o regime a ser adotado. Todavia, assiste razão às autoras Gisela Guedes e Rose Meireles ao afirmar que a responsabilidade adotada pela LGPD é a subjetiva uma vez que vários elementos remetem a análise da culpa do agente de tratamento, em especial quando consideramos a excludente de ilicitude relacionada a não violação da legislação (art. 43, II).

Por outro lado, não há como negar que várias previsões legais foram inspiradas no CDC, que expressamente adota a responsabilidade objetiva e cujas previsões refletem essa teoria. Dessa forma, algumas disposições da LGPD remontam um sistema de responsabilização independente de culpa, como pontua Caitlin Mulholland. Um exemplo que foi anteriormente citado é o inciso III do art. 44 da LGPD. Todavia, a retirada da previsão expressa da responsabilidade objetiva durante o processo legislativo e os dispositivos relacionados à análise da culpa do agente permitem concluir que o legislador não elegeu tal teoria para a proteção de dados.

Quanto à proposta da teoria da responsabilidade civil proativa, admite-se que a legislação de proteção de dados focou de forma mais veemente em exigir uma postura preventiva dos agentes de tratamento, impondo-lhes boas práticas de segurança. Contudo, essa abordagem, sem a adoção de previsões legais mais diretas quanto à obrigação de reparar possíveis danos, não atende a realidade de tratamento de dados presente no Brasil, contexto no qual o direito a proteção de dados ainda se mostra incipiente e a maioria dos titulares ainda não tem domínio técnico capaz de identificar possíveis violações às boas práticas.

Reafirma-se o posicionamento segundo o qual a atividade de tratamento de dados oferece riscos intrínsecos aos titulares vulneráveis, especialmente considerando o contexto da falha do consentimento como uma base legal apta a proteger o direito à autodeterminação desses indivíduos.

Verifica-se que, por meio desse consentimento, fornecido a partir da aceitação dos termos e condições do tratamento, sem o conhecimento adequado sobre suas consequências e sob a égide de uma legislação de não tutela satisfatoriamente determinadas vulnerabilidades, os titulares assumem tais riscos intrínsecos através de uma voluntariedade viciada.

Nesse cenário, a responsabilidade objetiva baseada na teoria do risco é a mais adequada em razão da urgência em garantir os direitos dos titulares e tutelar suas vulnerabilidades de forma efetiva, realocando a responsabilidade pelos riscos para as partes que estão explorando seus benefícios de forma mais efetiva, quais sejam os agentes.

5. CONSIDERAÇÕES FINAIS

Com base no conteúdo apresentado, verifica-se que a inexatidão conceitual presente na LGPD e a sobrecarga de sua base legal do consentimento podem ampliar as assimetrias que permeiam as relações entre titulares e agentes de tratamento, prejudicando o exercício da autodeterminação informacional e ampliando a vulnerabilidade dos titulares.

Dessa forma, ao adotar uma abordagem baseada na responsabilidade subjetiva com base na análise de culpa, permite-se questionar a eficácia da LGPD como meio jurídico capaz de tutelar os titulares diante da realidade tecnológica na qual o consentimento frequentemente não reflete a real compreensão dos titulares sobre as implicações do uso de seus dados.

Nesse sentido, a responsabilidade objetiva, fundamentada na teoria do risco da atividade, é proposta como uma solução mais adequada para lidar com os danos potenciais provenientes do tratamento de dados pessoais. Dada à característica do risco intrínseco da atividade de tratamento, a responsabilização dos agentes independentemente do exame da culpa teria o condão de equilibrar as relações desbalanceadas e de tutelar de forma mais eficaz os direitos dos titular nas hipóteses de danos.

Por fim, conclui-se que a LGPD, embora tenha dado importantes passos rumo à proteção dos dados pessoais e à autodeterminação informacional, ainda necessita de aperfeiçoamentos. A adoção de uma responsabilidade objetiva seria um avanço no sentido de garantir maior segurança jurídica aos titulares de dados, ao mesmo tempo em que fortaleceria o exercício dos direitos fundamentais consagrados na Constituição, assegurando a proteção da privacidade e a autogestão de dados pessoais.

REFERÊNCIAS

BIONI, Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. Civilistica.com, Rio de Janeiro, v. 9, n. 3, p. 1–23, 2020. p. 10. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/662>. Acesso em: 28 set. 2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidente da República, 2022. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 28 set. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Diário Oficial da União, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 28 set. 2024.

CRANOR, Lorrie Faith; MCDONALD, Aleecia M. Beliefs and Behaviors: InternetUsers' Understanding of Behavioral Advertising, **TPRC**, 2010. p. 1. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989092>. Acesso em 23 set. 2024.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau, "**Término do tratamento de dados**", IN: Tepedino, Gustavo; Frazão, Ana; Oliva, Milena Donato. Lei Geral de Proteção de Dados Pessoais. Ed. 3. Editora RT: São Paulo, 2023.

HOOFNAGLE, Chris Jay; SOLTANI, Ashkan; GOOD, Nathan; WAMBACH, Dietrich James; AYENSON, Mika. Behavioral advertising: the offer you cannot refuse. **Harvard Law & Policy Review**, v. 6, p. 273, Aug. 2012; UC Berkeley Public Law Research Paper n. 2137601, p. 273-296. Disponível em: <http://ssrn.com/abstract=2137601>. Acesso em 23 set. 2024.

INSIDER. **The Chart That Shows WhatsApp Was A Bargain At $19 Billioon**, 2014. Disponível em: <https://www.businessinsider.com/price-per-user-for-whatsapp-2014-2>. Acesso em 8 ago. 2024.

ISTO É DINHEIRO. **Instagram fatura US$ 20 bilhões com anúncios em 2019**. Disponível em: <https://istoedinheiro.com.br/instagram-fatura-us-20-bilhoes-com-anuncios-em-2019/>. Acesso em: 4 out. 2024.

KERR, Ian R., ; BARRIGAR, Jennifer ; BURKELL, Jacquelyn; BLACK, Katie. Soft Surveillance, Hard Consent. **Personally Yours**, Vol. 6, pp. 1-14, 2006. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=915407>. Acesso em 23 set. 2024.

MULHOLLAND, Caitlin. Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (lei 13.709/2018). **Revista Jur. Puc**. Rio, 2021. Disponível em: <https://www.jur.puc-rio.br/wp-

content/uploads/2021/07/IBERC_Responsabilidade-civil-e-dados-sensi%CC%81veis.pdf>. Acesso em 30 set. 2024.

RODOTÀ, Stefano. **A vida na sociedade da vigilância – a privacidade hoje**. Org. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

STATISTA, Statista Global Consumer Survey. **Penetration of selected mobile messaging apps among smartphone owners in Brazil from 2018 to 2021**, 2021. Disponível em: <https://www.statista.com/statistics/798131/brazil-use-mobile-messaging-apps/>. Acesso em 8 ago. 2024.

TUROW, Joseph; HENESSY, Michael; DRAPER, Nora. The tradeoff fallacy: how marketers are misrepresenting and opening them up to exploitation. **TPRC**, 2015. Disponível em: <https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf>. Acesso em 23 set. 2024.

WESTIN, Alan F. **Pivacy and Freedom**. E-book. New York: Atheneum, 1970.