

**INSTITUTO BRASILEIRO DE ENSINO, DESENVOLVIMENTO E PESQUISA – IDP
ESCOLA DE DIREITO – EDB
CURSO DE GRADUAÇÃO EM DIREITO**

Simone Rodrigues de Oliveira Takaku

**OS DESAFIOS ASSOCIADOS À PROTEÇÃO DOS TITULARES DE DADOS NOS
CONTRATOS POR ADESÃO: UMA ANÁLISE DO DIREITO À PRIVACIDADE
DIANTE DA ASSIMETRIA INFORMACIONAL DO CONSUMIDOR**

**BRASÍLIA
2022**

SIMONE RODRIGUES DE OLIVEIRA TAKAKU

**OS DESAFIOS ASSOCIADOS À PROTEÇÃO DOS TITULARES DE DADOS NOS
CONTRATOS POR ADESÃO: UMA ANÁLISE DO DIREITO À PRIVACIDADE
DIANTE DA ASSIMETRIA INFORMACIONAL DO CONSUMIDOR**

Trabalho de Conclusão de Curso apresentado
como requisito para a conclusão da graduação
em Direito do Instituto Brasileiro de Ensino
Desenvolvimento e Pesquisa - IDP

**ORIENTADORA: MARIA CRISTINE BRANCO
LINDOSO**

**BRASÍLIA
2022**

SIMONE RODRIGUES DE OLIVEIRA TAKAKU

**OS DESAFIOS ASSOCIADOS À PROTEÇÃO DOS TITULARES DE DADOS
NOS CONTRATOS POR ADESÃO: UMA ANÁLISE DO DIREITO À
PRIVACIDADE DIANTE DA ASSIMETRIA INFORMACIONAL DO
CONSUMIDOR**

Trabalho de Conclusão de Curso
apresentado como requisito para a
conclusão da graduação em Direito do
Instituto Brasileiro de Ensino
Desenvolvimento e Pesquisa – IDP

Brasília, 25 de novembro de 2022.

Prof. Msc. Maria Cristine Branco Lindoso
Professora Orientadora

Prof. Msc. Janete Ricken Lopes de Barros
Membro da Banca Examinadora

Prof. Dr. Flavio José Roman
Membro da Banca Examinadora

**OS DESAFIOS ASSOCIADOS À PROTEÇÃO DOS TITULARES DE DADOS
NOS CONTRATOS POR ADESÃO: UMA ANÁLISE DO DIREITO À
PRIVACIDADE DIANTE DA ASSIMETRIA INFORMACIONAL DO
CONSUMIDOR**

**THE CHALLENGES ASSOCIATED WITH THE PROTECTION OF DATA
HOLDERS IN ADHESION CONTRACTS: AN ANALYSIS OF THE RIGHT TO
PRIVACY BEFORE CONSUMER INFORMATION ASYMMETRY**

Simone Rodrigues de Oliveira Takaku

SUMÁRIO: 1. Introdução; 2. Direito à Proteção de Dados, Fundamentos e Marcos regulatórios; 2.1. Uma breve análise do conceito de Privacidade e Vulnerabilidade; 2.2. A Assimetria Informacional do Consumidor; 3. A Problemática dos Contratos por Adesão diante da Assimetria informacional e da Vulnerabilidade do titular de dados; 4. O Conceito de *Privacy by Design* aplicado à LGPD; 4.1. Os Desafios da Proteção de Dados no Ordenamento Jurídico; 5. Considerações Finais.

RESUMO

O presente artigo acadêmico tem o objetivo de analisar em que medida a Lei Geral de Proteção de Dados poderá garantir a efetiva proteção dos titulares de dados, usuários da internet, nos contratos por adesão quanto à legitimidade da coleta de dados e seu tratamento, diante de um contexto multicultural no qual estão presentes a assimetria informacional e a extrema vulnerabilidade do consumidor brasileiro. A metodologia usada na abordagem do problema foi a pesquisa bibliográfica de doutrinas jurídicas e pesquisa documental da legislação em função do caráter teórico argumentativo deste artigo. A inquietação surge a partir do avanço tecnológico que se torna um grande desafio para a sociedade em função dos riscos apresentados no campo da ética, da transparência,

da privacidade e da governança dos dados. Nesse viés, a pesquisa busca demonstrar os avanços da regulamentação jurídica e de que forma o ordenamento jurídico brasileiro conseguirá acompanhar as mudanças sociais, alcançar a velocidade das inovações e garantir a efetiva proteção dos titulares de dados nos contratos por adesão e conclui com a hipótese da aplicação do conceito de *Privacy by Design* na esfera de proteção da privacidade dos dados pessoais como forma de minimizar os efeitos decorrentes da assimetria informacional e da vulnerabilidade presente nas relações consumeristas.

Palavras-chave: proteção de dados, privacidade, vulnerabilidade, assimetria informacional, Código de Defesa do Consumidor - CDC, Lei Geral de Proteção de Dados – LGPD e *Privacy by Design*.

ABSTRACT

The present academic article has the objective of analyze in which measure the General Data Protection Law may ensure the effective protection of the data holders, internet users, in the adhesion contracts by adherence to the legitimacy of the data collection and its handling, against a multicultural context in which are present the informational asymmetry and the extreme vulnerability of the Brazilian consumer. The methodology used in the approach of the problem was the bibliographic research of judicial doctrines and the documentary research of the legislation in the argumentative character of this article. The concern emerges from the technological progress that becomes a great challenge for the society in function of the risks shown in the fields of ethics, transparency, privacy and data governance. In this bias, the research seeks to prove the legal regulation advances and in what way the Brazilian juridical ordering will be able to follow the social changes, reaching the speed of the innovations and guarantying the effective protection of the data holders in the contracts by adherence and concludes with the hypothesis of concept application of *Privacy by Design* in the realm of personal data privacy protection as means of minimizing the arising effects of informational asymmetry and present vulnerability in consumer relations.

Keywords: data protection, privacy, vulnerability, information asymmetry, Consumer Protection Code – CDC, General Data Protection Law – LGPD and *Privacy by Design*.

1. INTRODUÇÃO

Nas últimas décadas, quase tudo o que percebemos como mudança, inovação e transformações, está associado de alguma forma ao avanço digital e tecnológico, a partir da transformação digital, desde o ano 2000, a velocidade de transmissão de dados deu um salto quantitativo e qualitativo e o número de pessoas com acesso à internet passou de 4% para 63% da população mundial, de acordo com o estudo Digital 2022.¹ Com isso, o comércio, os serviços, o entretenimento, a educação e a informação tornaram-se *online* e a alguns cliques de distância entre consumidor e fornecedor.

Diante dos avanços e da evolução da tecnologia digital a cada dia surgem novas aplicações de inteligência artificial, *machine learning*,² e do uso de algoritmos pelas empresas, os quais elevam a cognição e possibilitam um maior monitoramento dos usuários da internet e conseqüentemente uma maior acurácia na compreensão do perfil do consumidor.

Nesse cenário de crescente informatização tecnológica, manifestada pela intensidade do fluxo de dados e maior propagação da informação por meios eletrônicos, é válida a preocupação da doutrina no que concerne à privacidade e os dados pessoais da pessoa, na medida em que estes estão dentre os campos mais afetados pela evolução da tecnologia digital, os quais se tornaram bens jurídicos valiosos e por vezes utilizados de maneira inadequada e até inescrupulosas.

Conforme salienta Shoshana Zuboff, na economia atual prospera o sistema de "capitalismo de vigilância",³ no qual os dados pessoais extraídos e colhidos pelas plataformas *online* são utilizados para geração de riqueza, desde o simples direcionamento de anúncios para indução do comportamento na esfera do consumo e até mesmo para prever os nossos desejos.

¹ DATAREPORTAL (2022). **Digital 2022 Global Digital Overview**. Disponível em: <https://datareportal.com/reports/digital-2022-global-overview-report>. Acesso em: 5 jun. 2022.

² Aprendizado de máquina, quando o algoritmo se retroalimenta a partir de informações obtidas por ele próprio.

³ Nas palavras de Shoshana Zuboff traduzido por Fernanda Bruno, o termo "Capitalismo de Vigilância" faz referência ao *big data*, componente fundamental de uma nova lógica de acumulação intencional, o capitalismo de informação, que procura prever e modificar o comportamento humano como meio de produzir receitas e controle de mercado. ZUBOFF, Shoshana. Big Other. Capitalismo de vigilância e perspectivas para uma civilização de informação. In: BRUNO, Fernanda *et al.* **Tecnopolíticas da vigilância: Perspectivas da margem**. São Paulo: Boitempo Editorial, 2019. (Coleção Estado de Sítio) p. 17-68.

Na contramão da evolução digital, um estudo recente publicado pela PwC em parceria com o Instituto Locomotiva traçou um retrato preocupante das iniciativas do país para o futuro:

Teremos grandes dificuldades de avançar no processo de digitalização enquanto o acesso à internet permanecer amplamente desigual, os equipamentos disponíveis não forem adequados para a formação digital e o sistema de educação básica continuar a formar um grande contingente de brasileiros incapazes de interpretar textos, sem conhecimentos suficientes de matemática e do idioma inglês.⁴

Considerando o contexto em que o Brasil apresenta uma das maiores desigualdades sociais do mundo⁵, não somente no aspecto econômico, mas também cultural, percebe-se que essa disparidade socioeconômica exterioriza no acesso a oportunidades, na garantia dos direitos fundamentais, como ainda promove um grande desequilíbrio de informação entre consumidores e fornecedores, a chamada assimetria informacional.

Assim, a partir desse contexto, este artigo pretende analisar como o ordenamento jurídico brasileiro, especialmente o Código de Defesa do Consumidor e a Lei Geral de Proteção de Dados Pessoais, poderá proporcionar uma efetiva proteção dos titulares de dados nos contratos por adesão, quanto à privacidade e a legitimidade da coleta e tratamento de dados num cenário multicultural e diante da assimetria informacional e de extrema vulnerabilidade do consumidor brasileiro, bem como avaliar formas para minimizar os efeitos decorrentes desta assimetria e da vulnerabilidade presente nas relações.

O capítulo 2 fornece um panorama do direito à proteção de dados, e seus principais marcos regulatórios no ordenamento jurídico, trazendo a pluralidade e interdependência das fontes normativas, ainda, será explanado o conceito de vulnerabilidade, suas classificações e a assimetria informacional.

No capítulo 3 serão apresentados o conceito de contrato por adesão e a problemática da legitimidade da coleta e tratamento de dados diante da assimetria

⁴ PRICEWATERHOUSECOOPERS BRASIL LTDA. **O abismo digital no Brasil**: Saiba como desigualdade de acesso à internet, a infraestrutura inadequada e a educação deficitária limitam as nossas opções para o futuro. PwC. Disponível em: https://www.pwc.com.br/pt/estudos/preocupacoes-ceos/mais-emas/2022/O_Abismo_Digital.pdf. Acesso em: 5 jun. 2022.

⁵ GIFE. **O aumento da desigualdade social no Brasil, segundo pesquisas**. O Gife. 2022. Disponível em: <https://gife.org.br/desigualdade-social-no-brasil/>. Acesso em: 25 abr. 2022.

informacional e da reconhecida vulnerabilidade do titular de dados, diante da natureza adesiva imposta unilateralmente no contrato de adesão a partir de cláusulas padronizadas e previamente definidas pelo fornecedor.

No quarto capítulo, a partir das análises, será examinado e proposto a aplicação do conceito de *Privacy by Design* na esfera de proteção da privacidade dos dados pessoais como forma de minimizar os efeitos decorrentes da assimetria informacional e da vulnerabilidade presente nas relações consumeristas.

2. DIREITO A PROTEÇÃO DE DADOS, FUNDAMENTOS E MARCOS REGULATÓRIOS

A proteção dos direitos individuais no Brasil está vinculada à história das Constituições brasileiras, marcadas por avanços e retrocessos. A Constituição Federal de 1988⁶, além de arrolar os direitos fundamentais e garantias individuais, também elenca um vasto rol de direitos coletivos, sociais, políticos e insere disposições relacionadas especificamente ao Direito do Consumidor.⁷

Com o reconhecimento da tutela constitucional na esfera do direito do consumidor, em 1990 foi instituído por meio da Lei nº 8.078/90 o Código de Defesa do Consumidor, abarcando cláusulas gerais com arcabouço teórico de natureza multidisciplinar e principiológica, que tem como função, regular as relações de consumo por meio de normas de proteção e defesa do consumidor, no intuito de assegurar a proteção do consumidor considerado como a parte vulnerável no sistema consumerista.

Assim, o Código de Defesa do Consumidor na qualidade de direito fundamental e de norma de ordem pública, por meio do estabelecimento da política nacional das relações de consumo, constitui um instrumento de harmonização dos interesses nas relações entre fornecedores e consumidores, visando equilibrar a relação e estabelecer condições de igualdade ao consumidor.

⁶ BRASIL. **Constituição Federal**. República Federativa do Brasil de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/ConstituicaoCompilado.htm. Acesso em: 30 abr. 2022.

⁷ Art. 5º, XXXII, da Constituição Federal, o Estado promoverá, na forma da lei, a defesa do consumidor; art. 170, V, a ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, tem por fim assegurar a todos, existência digna, conforme os ditames da justiça social, observados os seguintes princípios [...] de defesa do consumidor; e Art. 48, do ADCT – Ato das Disposições Constitucionais Transitórias. O Congresso Nacional, dentro de cento e vinte dias da promulgação da Constituição, elaborará código de defesa do consumidor.

De acordo com Laura Schertel, "o caráter principiológico das normas do CDC se mostra aberto para oferecer soluções para os novos conflitos relacionados a tecnologia da informação" e ao desenvolvimento de mecanismos de proteção da personalidade do consumidor contra os riscos advindos do processamento de dados pessoais, de forma a garantir a inviolabilidade da intimidade e da vida art. 5º, X da CF.⁸

Sob essa perspectiva, a implementação do CDC trouxe importante inovação nas relações contratuais, viabilizando novas formas de contratos, maior proteção aos hipervulneráveis e inserindo o primeiro marco legislativo relacionado a proteção de dados no Brasil, com uma seção específica que trata sobre banco de dados e cadastro de consumidores, seção IV, art. 43:

Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

§ 1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.

§ 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.

§ 3º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.

§ 4º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.

Nesse contexto, o direito do consumidor se transforma num importante instrumento de desenvolvimento social, e constitui-se em uma das vertentes do direito social e do processo de intervenção estatal na economia⁹, além de prevenção e reparação de danos, contudo, diante das disrupções do mundo atual, das crescentes mudanças sociais e do avanço acelerado da tecnologia, dada a necessidade de regulação e relevância do tema, vários outros diplomas legais sobrevieram, destacando-se a Lei de Acesso à

⁸ MENDES, Laura Schertel. A vulnerabilidade do consumidor quanto ao tratamento de dados pessoais. **Revista de Direito do Consumidor**. vol. 102. ano 24. São Paulo: Ed. RT, nov-dez. 2015. p. 19-43.

⁹ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental, São Paulo: Saraiva, 2014. (Série IDP: linha pesquisa acadêmica) p. 195.

Informação (Lei nº 12.527/2011)¹⁰, o Marco Civil da Internet (Lei nº 12.965/2014),¹¹ e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018).¹²

A respeito do tema, dispõe Laura Schertel Mendes:

Na economia atual, caracterizada pela flexibilidade e customização da produção, bem como pela avidez das empresas por informações pessoais, inúmeras são as ameaças à privacidade nas relações de consumo. Nesse sentido, diante do processamento de dados pessoais dos consumidores pelo setor privado, é fundamental analisar quais os mecanismos jurídicos necessários para o estabelecimento do equilíbrio entre ambos. O tratamento de dados pessoais no âmbito do relacionamento entre o consumidor e a empresa consiste numa relação de direito privado, mais especificamente numa relação de consumo, sujeita a uma pluralidade de normas do ordenamento jurídico, como a Constituição Federal, o Código de Defesa do Consumidor e diversas outras leis. Essas normas, muitas vezes aplicáveis concomitantemente, devem ser interpretadas de forma dialógica, buscando a harmonia e a integridade do sistema jurídico.¹³

Em relação a Lei de Acesso à Informação, dialogando com o CDC, trouxe em seus dispositivos, seção específica sobre o tratamento das informações pessoais em que dispõe na seção V, art.31:

Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.

§ 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem: II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.

Da mesma forma, o Marco Civil da Internet estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e também assegura a proteção dos dados pessoais e as hipóteses de tratamento e de fornecimento, conforme disposto nos artigos 3º e art. 7º:

Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: I - garantia da liberdade de expressão, comunicação e

¹⁰ BRASIL, **Lei n. 12.527**, de 18 de novembro de 2011. Lei de Acesso a Informação. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm. Acesso em: 12 ago. 2022.

¹¹ BRASIL, **Lei n. 12.965**, de 23 de abril de 2014. Marco Civil da Internet. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 12 ago. 2022.

¹² BRASIL, **Lei n. 13.709** de 14 de agosto de 2018. Lei Geral de Proteção de Dados: Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em 10 out. 2022.

¹³ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. (Série IDP: linha pesquisa acadêmica). p. 191.

manifestação de pensamento, nos termos da Constituição Federal; II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei;

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

Igualmente, a Lei Geral de Proteção de Dados Pessoais - LGPD Lei nº 13.709/2018 influenciada pelo regulamento europeu GDPR – *General Data Protection Regulation*,¹⁴ consolidou outra importante inovação ao inserir um regime de proteção e de responsabilidades ao direito brasileiro, dialogando com as demais leis mencionadas anteriormente e em conjunto com o Código de Defesa do consumidor, viabilizou uma elevação de garantias individuais, tendo como fundamento o livre desenvolvimento da personalidade dos titulares de dados.

Dentre as principais inovações trazidas pela LGPD estão a definição de conceitos relacionados a dados pessoais sensíveis e o estabelecimento de obrigações e as possibilidades para o tratamento dos dados.

Cumprido destacar que o Código de Defesa do Consumidor foi recepcionado pela LGPD, dado que ambos possuem princípios e mecanismos protetivos similares. Importante ressaltar que a proteção de dados no Direito do Consumidor, no Marco Civil da Internet e na Lei Geral de Proteção de Dados são complementares, sendo assim, a LGPD converge no mesmo sentido de proteger os direitos fundamentais da liberdade, da privacidade e dos direitos de personalidade dos indivíduos.

De forma análoga, a LGPD ao dispor sobre o tratamento de dados pessoais das pessoas naturais, realizado por pessoas físicas ou jurídicas, define as hipóteses em que tais dados podem legitimamente ser utilizados por terceiros e tem como fundamento a autodeterminação informativa, ou seja, a pessoa tem o controle de como seus dados vão ser utilizados, embora, a lei estabeleça mecanismos para proteger os titulares dos dados contra o uso inadequado, o campo das relações de consumo frente a autodeterminação

¹⁴Regulamento Geral sobre Proteção de Dados do direito Europeu. Disponível em: <https://gdpr-info.eu/>. Acesso em 30 ago. 2022.

informativa, ainda é considerado como um dos pontos sensíveis diante da vulnerabilidade do adquirente de produtos e serviços.

Conforme disposto no art. 2º da LGPD, "a proteção de dados tem como fundamentos: (I) o respeito à privacidade; (II) autodeterminação informativa; (III) liberdade de expressão, de informação, de comunicação e de opinião; (IV) inviolabilidade da intimidade, da honra e da imagem; (V) desenvolvimento econômico e tecnológico e a inovação; (VI) livre iniciativa, a livre concorrência e a defesa do consumidor; (VII) direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Os dados pessoais hoje são um grande ativo na economia da informação, são utilizados por governos nas políticas públicas e pelo setor privado para fins econômicos. Nesse cenário, o tratamento de dados pessoais deverá observar os princípios da boa-fé estabelecido no Código de Defesa do Consumidor, bem como os demais princípios que estruturam a LGPD, conforme art. 6º da lei 13.709/18, princípio da finalidade, da adequação, da necessidade, do livre acesso, da qualidade de dados, da transparência, da segurança, da prevenção, da não discriminação, e da responsabilização e prestação de contas.

Para melhor compreensão e avanço no tema, os autores Tarcísio Teixeira e Ruth Guerreiro discorrem sobre a LGPD e os princípios que norteiam sua aplicação. Segundo os autores, de acordo com o princípio da finalidade, a realização do tratamento dos dados pessoais deverá ocorrer para propósitos legítimos, específicos, explícitos e informados ao titular, não há possibilidade de se obter autorização do titular para um tratamento específico e posteriormente alterar esse tratamento para uma forma incompatível com a estabelecida inicialmente, para que a coleta seja considerada legalmente, terá que respeitar essa finalidade.¹⁵

Pelo princípio da adequação, a compatibilidade do tratamento dos dados deverá ocorrer conforme as finalidades informadas ao titular, de acordo com o contexto do cadastro e seu tratamento.¹⁶

Conforme o princípio da necessidade, os agentes deverão limitar o tratamento dos dados ao mínimo necessário para a realização de suas finalidades, com abrangência

¹⁵ TEIXEIRA, Tarcísio; GUERREIRO, Ruth M. **Lei Geral de Proteção de Dados Pessoais (LGPD): Comentada Artigo por Artigo**. 4. Ed. - São Paulo: Editora Saraiva, 2022. p. 17-20.

¹⁶ Idem, Ibidem. p.17-20.

dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento. Os princípios da finalidade, adequação e necessidade, somados, resultam no chamado mínimo essencial, ou seja, à real necessidade de se obter determinado dado pessoal para se atingir a finalidade pretendida.¹⁷

Em relação ao princípio do livre acesso é garantido aos titulares a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.¹⁸

O princípio da qualidade de dados estabelece a garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.¹⁹

De acordo com o princípio da transparência, aos titulares há garantia de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.²⁰

Conforme o princípio da segurança as empresas deverão utilizar medidas técnicas, administrativas e organizativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.²¹

O princípio da prevenção estabelece a necessidade de adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. Ressalta, uma maior exigência em relação aos dados pessoais considerados sensíveis, tais como, 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 vinculados a pessoa natural.²²

Pelo princípio da não discriminação, é vedado a utilização de dados pessoais, de modo a promover discriminação para fins abusivos ou ilícitos, conforme Tarcísio Teixeira e Ruth Guerreiro, "a não discriminação encontra respaldo no princípio constitucional da igualdade, em que todos são iguais perante a lei e na lei, sendo vedado

¹⁷ Idem, Ibidem. p.17-20.

¹⁸ Idem, Ibidem. p.17-20.

¹⁹ Idem, Ibidem. p.17-20.

²⁰ Idem, Ibidem. p.17-20.

²¹ Idem, Ibidem. p.17-20.

²² Idem, Ibidem. p.17-20.

ao agente de tratamento qualquer tratamento de dados para fins discriminatórios, ilícitos ou abusivos".²³

Por fim, o princípio da responsabilização e prestação de contas, o qual consiste na demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.²⁴

Segundo Bruno Bioni, grande parte destes princípios tem a centralidade no indivíduo, conforme ressalta "É uma carga principiológica que procura conformar, justamente, a ideia de que o titular dos dados pessoais deve ser empoderado com o controle de suas informações pessoais e, sobretudo, na sua autonomia da vontade".²⁵

As bases legais para tratamento de dados pessoais estão previstas no art. 7º da referida lei, para análise proposta no artigo, o enfoque se dará no inciso I que estabelece como regra para tratamento de dados pessoais o consentimento do titular, art. 7º, I.²⁶ esse consentimento é definido pelo art. 5º, XII – o consentimento é interpretado como a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Conforme expõe Danilo Doneda, a proteção de dados pessoais no ordenamento jurídico se estruturou com objetivo de corrigir a assimetria informacional entre os titulares de dados e os agentes de tratamento:

Estruturalmente, a Lei Geral de Proteção de Dados caracteriza-se como um instrumento normativo de natureza protetiva, isto é, elaborado com o objetivo de corrigir um desequilíbrio conjuntural em seu determinado âmbito, qual seja a missão de corrigir a assimetria informacional entre os titulares de dados pessoais e os agentes de tratamento, a partir da constatação do acúmulo de poder nas mãos destes últimos como resultado da configuração das tecnologias de informação. Esta natureza protetiva, especificamente, é voltada direta e unicamente para a proteção da pessoa, no caso quando caracterizada como titular de dados pessoais.²⁷

²³ Idem, Ibidem. p.17-20.

²⁴ Idem, Ibidem. p.17-20.

²⁵ BIONI, Bruno Ricardo. **Proteção De Dados Pessoais**: a função e os limites do consentimento. 3ª ed. rev. atual, Rio de Janeiro: Forense, 2021. p.130.

²⁶ Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular. [...]

²⁷ DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel. **Estudos sobre Proteção de Dados pessoais**: Direito, Tecnologia, Inovação e Proteção de Dados num Mundo em Transformação. Expressa, 2022. p.31.

Segundo Guilherme Magalhães Martins, como forma de trazer maior eficiência na proteção de dados do indivíduo, a LGPD trouxe foco e centralidade na pessoa humana:

A Lei de Proteção de Dados coloca em primeiro plano a pessoa humana, ou seja, o titular de dados pessoais, que tem reconhecidos seus direitos, no artigo 18, em especial: à confirmação da existência de tratamento (inciso I); ao acesso aos dados (inciso II); à correção de dados incompletos, inexatos ou desatualizados (inciso III); à anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na mesma lei (inciso IV); à portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados o segredo comercial e industrial, de acordo com a regulamentação do órgão controlador (inciso V); à eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei (inciso VI); à informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados (inciso VII); à informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa (inciso VIII); à revogação do consentimento, nos termos do parágrafo quinto do artigo 8º desta Lei (inciso IX). Destaca-se ainda o direito de o usuário requisitar seus dados independentemente de judicialização, tendência louvável se comparada ao Marco Civil da Internet no regime de responsabilidade dos provedores por conteúdo inserido por terceiros, condicionada à difícil via judicial.²⁸

Consoante a relevância social do tema e entendimentos jurisprudenciais, por meio da Emenda Constitucional nº 115, de 10.02.2022²⁹, a proteção de dados pessoais ganha status de direito fundamental ao ser introduzido no rol de direitos e garantias fundamentais da Constituição Federal, "art. 5º LXXIX, a proteção de dados pessoais é assegurada, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais".

Neste viés, é notória a constante preocupação no âmbito regulatório, no sentido de que o direito sempre acompanhe as mudanças sociais e a evolução tecnológica de forma a garantir a proteção dos direitos e garantias fundamentais, reforçando a liberdade e a privacidade dos indivíduos.

²⁸ MARTINS, Guilherme Magalhães. A Lei Geral de Proteção de Dados Pessoais (LEI 13.709/2018) e a Proteção dos Consumidores. *In*: MARQUES, Claudia Lima. **Direito do Consumidor: 30 anos do CDC**: Da consolidação como Direito Fundamental aos atuais desafios da sociedade. Rio de Janeiro: Forense, 2020. cap. 16, p. 430.

²⁹BRASIL. **Constituição Federal**. Emenda Constitucional 115. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 23 out. 2022.

2.1 Uma breve análise do conceito de Privacidade e Vulnerabilidade

A tutela da privacidade esteve ligada diretamente à proteção de intromissões indesejadas na esfera da vida pessoal das pessoas, limitada à esfera patrimonialista, com o progresso da tecnologia e na medida que surgiram novos desafios no ordenamento jurídico a partir do tratamento informatizado dos dados e diante dos recentes incidentes de vazamento de dados com potencial violação da privacidade e exposição indesejada da pessoa, constata-se a transformação do conceito de privacidade ligada à proteção de dados, que passa a ser considerado uma garantia de controle do indivíduo sobre suas próprias informações.³⁰

Conforme Laura Schertel, "percebe-se uma alteração não apenas do conteúdo do direito à privacidade, mas também do seu léxico, passando a ser denominada privacidade informacional, proteção de dados pessoais, autodeterminação informativa, entre outros".³¹

Sob essa perspectiva, em razão da nova concepção de privacidade, relacionada a busca de igualdade, da liberdade de escolha, do anseio em não ser discriminado, atrelada à personalidade da pessoa e ao seu desenvolvimento³², surgem os questionamentos, em que pese a existência de pluralidade de fontes normativas relacionadas ao tema, à luz da vulnerabilidade e diante de uma acentuada assimetria de informações do titular de dados, em que medida a proteção dos titulares de dados consegue alcançar uma aplicabilidade efetiva.

Danilo Doneda observa de forma crítica a questão do contexto político e social do Brasil trazendo à tona a vulnerabilidade social do país, alinhado a preocupação da violação da privacidade destes perfis individuais, aponta a necessidade da regulação da proteção de dados de forma coletiva.

Certamente, algumas particularidades históricas podem apontar os motivos dessa determinada configuração da matéria no Brasil; como o pode, até certo ponto, o próprio perfil social do país – que, dada a existência de problemas estruturais de maior gravidade, poderia sugerir que a proteção de dados pessoais seja, ao menos em termos

³⁰ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. (Série IDP: linha pesquisa acadêmica) p. 32.

³¹ Idem, *Ibidem*, p. 32.

³² DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados - e-book**. São Paulo: Editora Revista dos Tribunais. 2021. P. RB 1.1.

quantitativos, uma demanda de menos apelo. Uma demanda pela proteção dos dados pessoais não é sentida de forma uniforme em uma população de perfil socioeconômico bastante heterogêneo como a brasileira, pelo simples motivo de que a percepção da relevância da sua tutela desenvolve-se somente depois que uma série de outras necessidades básicas sejam satisfeitas. A grande parcela de brasileiros que possui menor poder de compra, por exemplo, reflete no fato de que suas informações pessoais possam eventualmente ser de menor interesse para entes privados, que focalizam a coleta de informações nos extratos com maior poder econômico – o que, por si só, afasta a demanda pela tutela, ao menos por esse motivo e em uma determinada faixa da população. Confirma-se, assim, que a necessidade de uma sociedade em estabelecer mecanismos de proteção de dados pessoais varia conforme o padrão médio de consumo de sua população, assim como de outros fatores como sua educação e a própria penetração da tecnologia no cotidiano.³³

A ideia de vulnerabilidade num conceito amplo consiste em uma fragilidade ou debilidade, do ponto de vista jurídico estabelecido pelo Código de Defesa do Consumidor, o conceito de vulnerabilidade se aplica àqueles indivíduos que não possuem condições de conhecer técnica ou faticamente os produtos e serviços que são colocados à sua disposição, conforme o art. 4º, I, do Código de Defesa do Consumidor, um exemplo de um princípio norteador do direito do consumidor na medida que reconhece os riscos e a fragilidade entre consumidor e fornecedor e orienta a interpretação e a aplicação das normas legais de forma a tentar reequilibrar essa relação assimétrica.

Art. 4º A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios - I - reconhecimento da vulnerabilidade do consumidor no mercado de consumo.

Diante do princípio da vulnerabilidade em relação ao consumidor, a doutrina classifica a vulnerabilidade em quatro espécies, vulnerabilidade técnica, vulnerabilidade jurídica, vulnerabilidade fática e vulnerabilidade informacional, uma quinta categoria ainda não reconhecida é apresentada pelo autor Bruno Miragem "o reconhecimento da vulnerabilidade digital".³⁴

³³ Idem, *Ibidem*, cap. 1, p. RB 1.1.

³⁴ MIRAGEM, Bruno, *Princípio da Vulnerabilidade: Perspectiva atual e funções no direito do consumidor contemporâneo*. In: MARQUES, Claudia Lima. **Direito do Consumidor: 30 anos do CDC**: da

De acordo com a vulnerabilidade técnica, o consumidor não detém condições e conhecimentos técnico especializado sobre os produtos e serviços objetos da relação contratual e de consumo.

A vulnerabilidade jurídica diz respeito à falta de conhecimento dos direitos e deveres inerentes à relação de consumo, aos termos do contrato e as condições e os efeitos jurídicos incidentes da legislação.

A vulnerabilidade fática é a mais ampla, trata do reconhecimento da fragilidade e da debilidade do consumidor frente ao fornecedor, distinguindo-se em vulnerabilidade econômica e vulnerabilidade agravada ou hipervulnerabilidade do consumidor que requer cuidado e proteção especial.

A vulnerabilidade informacional, associada a assimetria informacional, se traduz na dificuldade do consumidor em obter informações relevantes sobre a contratação ou sobre o produto ou objeto contratado.

Por fim, a vulnerabilidade digital, apresentada pelo autor Bruno Miragem, como a ausência de habilidade ou familiaridade do consumidor com o ambiente digital. Sob esse enfoque, ressaltam-se os riscos em que o consumidor digital está submetido, suscetível à estímulos emocionais e sensoriais do meio digital que podem afetar seu comportamento de compra e expostos a ameaças e fraudes eletrônicas.

Quanto aos novos modelos de oferta, o comércio eletrônico – inclusive por plataformas digitais – assim como o tratamento de dados pessoais dos consumidores para a definição de perfis de consumo, alteram o modo de consumir. Por outro lado, o surgimento de bens digitais, a aplicação crescente de inteligência artificial e o desenvolvimento da internet das coisas, acrescentando automação dos produtos e serviços, modificam substancialmente o objeto do consumo. Será este o contexto que justifica o reconhecimento de outra dimensão da vulnerabilidade informacional, que não se resume à falta ou à pouca qualidade da informação prestada, mas a ausência de habilidade ou familiaridade com o ambiente digital. A internet revela-se ambiente propício a uma nova estratégia de comunicação, tendo em conta que as escolhas do consumidor não serão totalmente racionais, mas influenciadas por cores, formatos, design, discurso e outros elementos da apresentação de produtos, serviços ou do próprio contrato, formando incentivos sensoriais ou emocionais direcionados à tomada de decisão.³⁵

consolidação como direito fundamental aos atuais desafios da sociedade. Rio de Janeiro: Forense, 2020. p. 247.

³⁵ Idem, *Ibidem*. p. 248.

2.2 A Assimetria Informacional do Consumidor

Segundo os autores Amanda Oliveira e João Accioly, "a assimetria da informação consiste na situação em que uma parte da relação detém mais informações do que a outra sobre fatores determinantes da transação que ambas consideram fazer"³⁶, com isso, a assimetria informacional gera um desequilíbrio na relação contratual intensificando a vulnerabilidade do consumidor. O conceito da assimetria informacional se traduz exatamente nessa disparidade das informações sobre bens e serviços conhecidas pelos fornecedores e consumidores.

A informação permite que o consumidor tenha mais condições de avaliar o produto ou serviço e a sua probabilidade da compra considerando os riscos atinentes ao negócio, contudo, geralmente o consumidor não dispõe dessa informação, ficando a mercê do fornecedor que detém a informação no intuito de proteger seu negócio. Um grande desafio que temos enquanto agente numa economia de dados é justamente a assimetria informacional, ela atinge todos os campos, seja do usuário e consumidor e do próprio poder regulatório.

3. A PROBLEMÁTICA DOS CONTRATOS POR ADESÃO DIANTE DA ASSIMETRIA INFORMACIONAL E DA VULNERABILIDADE DO TITULAR DE DADOS

Quando um usuário da internet acessa um *site*, por mais que esse *site* seja considerado seguro e confiável, ele armazena *cookies*³⁷ que monitoram a navegação, seja

³⁶ OLIVEIRA, Amanda Flávio, ACCIOLY, João C. Andrade Uzêda, Direito do Consumidor e Análise Econômica do Direito. In: MARQUES, Cláudia Lima. **Direito do Consumidor: 30 anos do CDC**: da consolidação como direito fundamental aos atuais desafios da sociedade. Rio de Janeiro: Forense, 2020. p. 395.

³⁷ Os *cookies* são marcadores digitais, inseridos nos discos rígidos do computador do usuário de internet pelos *websites* visitados, que permitem a identificação e o armazenamento da navegação do internauta. Ao mesmo tempo que são úteis, por possibilitar a memorização de senhas e a personalização de serviços, os *cookies* podem trazer riscos à privacidade, quando o computador passa a ser associado a um determinado usuário, a partir dos dados pessoais fornecidos a um *site*. Além disso, se armazenados por um longo período de tempo, esses marcadores podem rastrear o comportamento do usuário *online* em diversos *sites*. MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: Linhas gerais de um novo direito fundamental. São Paulo. Saraiva, 2014. (Série IDP Linha Pesquisa Acadêmica) p.102.

para melhoramentos da página ou para avaliação do usuário e seus hábitos de navegação e consumo ou para transmitir informações a terceiros.

Citando como exemplo a página da empresa aérea Gol, um *site* de compras de passagens aéreas acessada por muitos usuários, ao visitar o endereço www.voegol.com.br, os *cookies* de terceiros são exibidos no bloqueador do navegador, caso o usuário não os desabilite ou não efetue a configuração de restrição e bloqueio de *cookies*, os domínios .360yield.com, .3lift.com, .adnxs.com, .afilio.com.br, secure.afilio.com.br, .bidswitch.net, .bing.com, .bat.bing.com, .c.bing.com, .bluekai.com, .casalemedia.com, .clarity.ms, .c.clarity.ms, www.clarity.ms, .creativecdn.com, .criteo.com, .demdex.net, .dnacdn.net, .doubleclick.net, neo.dynaton.com.br, .getblue.io, .krxid.net, .liadm.com, .media.net, exchange.mediavine.com, .omnitagjs.com, .outbrain.com, ct.pinterest.com, .pubmatic.com, .trends.revcontent.com, .rlcdn.com, .rubiconproject.com, .sharethrough.com, .smaato.net, .smartadserver.com, .socdm.com, .t.co, .taboola.com, .tiktok.com, .tremorhub.com, .twitter.com, tm.uol.com.br, .yahoo.com, .yieldmo.com, .ads.yieldmo.com, teriam acesso à navegação desse usuário.



Nessa seara, apesar da empresa ter uma política de privacidade clara e transparente, contudo, essa mesma política de privacidade não é aplicada aos *sites* de terceiros. Surge então a inquietação relacionada a privacidade e a proteção de dados diante da assimetria informacional e a vulnerabilidade do consumidor e usuário, diante do exposto, propõe-se a analisar os contratos de adesão e as hipóteses para a mitigação da vulnerabilidade.

Primeiramente o Código de Defesa do Consumidor como forma de tutelar o interesse do consumidor em função das constantes mudanças e transformações das relações contratuais na sociedade, inseriu em seu art. 54 o conceito de contrato por adesão, definindo-o como aquele cujas cláusulas tenham sido aprovadas pela autoridade competente ou estabelecidas unilateralmente pelo fornecedor de produtos ou serviços, sem que o consumidor possa discutir ou modificar substancialmente seu conteúdo. Os

termos de uso e as políticas de privacidade possuem a natureza de contrato por adesão, são contratos assinados eletronicamente pelo usuário.

Nesse contexto, diante da natureza adesiva imposta no contrato de adesão a partir de cláusulas padronizadas e previamente definidas pelo fornecedor, levanta-se outra problemática em relação ao livre consentimento do titular dos dados e o legítimo interesse da empresa, em que medida os termos de uso e as políticas de privacidade, enquanto contrato de adesão, estão adequadas aos parâmetros de proteção de dados, e, em especial quanto a cláusula do consentimento.

Considerando que o usuário da internet e de plataformas ao acessar um serviço ou produto on-line ele necessariamente precisa ler e concordar com a política ou termos de uso definidos unilateralmente pelo fornecedor, observa-se aí uma relação desigual de poder diante da vulnerabilidade e assimetria de informações do usuário.

Para Laura Schertel Mendes, os consumidores e usuários ao navegar na internet muitas vezes ficam suscetíveis aos estímulos e apelos das ações de *marketing* e muitas vezes sem conhecimento de termos técnicos, consentem com a utilização e tratamentos de seus dados pessoais para quaisquer fins, ficando expostos inclusive a ameaças cibernéticas.

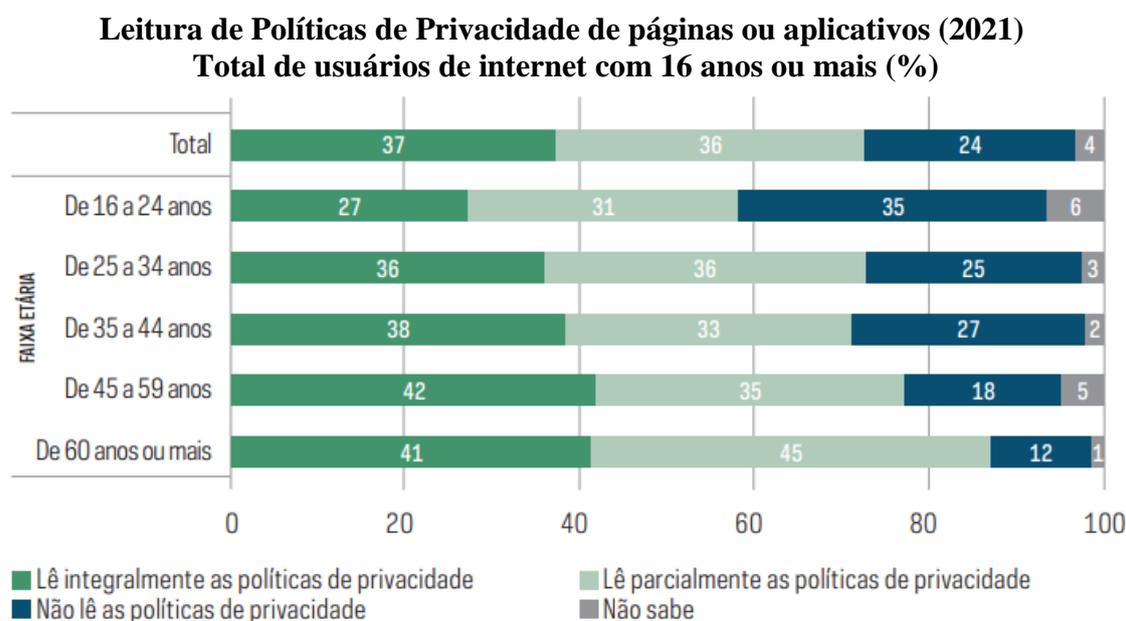
Li e aceito os termos "Ao navegar pela Internet, é bastante comum se deparar com essa frase ao fim de um longo texto, com letras pequenas e linguagem técnica. Não por acaso, estudos têm indicado que muitos usuários não leem esses termos e, quando o fazem, acabam por não os entender ou levam um tempo significativo para tanto. Mais do que isso, caso o usuário não concorde com os termos apresentados, é comum que sua única opção seja a de não desfrutar importantes produtos e serviços on-line. Entretanto, assim fazendo, acaba enfrentando elevados custos sociais na medida em que esses produtos e serviços penetram, cada vez mais, a vida social e as dinâmicas político-econômicas dos cidadãos com o Estado, com empresas privadas e com a comunidade na qual estão inseridos".³⁸

Nessa mesma linha, um estudo realizado pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação – Cetic.br e NIC.br, aponta a mesma situação de vulnerabilidade, segundo o levantamento, a maior parte dos usuários da internet não fazem a leitura integral dos termos e políticas de privacidade, contudo,

³⁸ MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da. Proteção de dados para além do consentimento: Tendências de materialização. In: DONEDA, Danilo *et al.* **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. 90.

consentem com o aceite dos termos e políticas definidos pelo fornecedor, bem como das configurações de *cookies*, para o acesso ao conteúdo e serviços, conforme demonstrado no gráfico abaixo:³⁹

Gráfico 1 – Indicador de Usuários que leem os termos e políticas de privacidade



Fonte: Comitê Gestor da Internet no Brasil/Núcleo de Informação e Coordenação do Ponto BR – NIC.br

Ainda, de acordo com Laura Schertel Mendes, as empresas utilizam das informações cotidianas dos consumidores por meio de monitoramento de seus hábitos de consumo, interesses e características pessoais, conhecido como *profiling*⁴⁰ ou perfilamento, ou seja, a depender da página visitada, buscas na internet, interações nas redes sociais, o usuário é classificado e encaixado em um determinado perfil, seja para adaptação de produtos e serviços para diferentes segmentos, publicidades direcionadas

³⁹ COMITÊ GESTOR DA INTERNET NO BRASIL. **Privacidade e proteção de dados pessoais**: perspectivas de indivíduos, empresas e organizações públicas no Brasil. São Paulo. Núcleo de Informação e Coordenação do Ponto BR, 2022. p. 61. Disponível em: https://cetic.br/media/docs/publicacoes/2/20220817110001/privacidade_protecao_de_dados_pessoais_2021_livro_eletronico.pdf. Acesso em: 03 out. 2022.

⁴⁰ O *profiling* é uma espécie de tratamento de dados pessoais que envolve a construção de perfis a partir da análise automatizada de grandes quantidades de dados coletados acerca de um indivíduo ou de um grupo, com o objetivo de se tomar uma decisão em relação ao sujeito perfilado. Assim como a maioria das tecnologias, observa-se ganhos importantes com seu uso, principalmente em termos de eficiência e eficácia de análises preditivas. Porém, o uso irrestrito pode significar importantes efeitos prejudiciais ao desenvolvimento da vida privada dos indivíduos, por possibilitar previsões de comportamento ou de características de um sujeito de maneira invasiva à sua privacidade, assim como a discriminação de pessoas submetidas a um perfil estereotipado.

ou até mesmo para comercialização dos dados, com isso, elas obtêm um alto grau de lucratividade e estabilidade comercial, minimizando seus riscos, e a consequência disso é a classificação das pessoas em categorias de acordo com a avaliação de seus riscos e a discriminação do acesso a determinados bens e serviços.⁴¹

Se, por um lado, ao monitorar os usuários, as empresas obtêm lucratividade, minimizam seus riscos e geram riqueza, por outro lado, as pessoas têm sua privacidade exposta a riscos a partir do uso indevido de seus dados, e se tornam ainda mais vulneráveis e suscetíveis as manipulações.

4. O CONCEITO DE *PRIVACY BY DESIGN* APLICADO A LGPD

O conceito de *Privacy by Design* foi criado pela canadense Ann Cavoukian, o qual estabelece que as regras de privacidade e proteção de dados pessoais devem ser implementadas em cada estágio de desenvolvimento do produto e serviços desde a sua concepção com o objetivo de garantir privacidade e permitir que os indivíduos tenham controle sobre seus dados pessoais. Os pilares que sustentam esse modelo estão ancorados em um conjunto de sete princípios fundamentais:⁴²

O primeiro princípio estabelece que na metodologia de *Privacy by Design* o fornecedor deve ser proativo ao invés de reativo, e preventivo, e não corretivo, com objetivo de prevenir os incidentes antes que eles ocorram, norteia toda a organização para que ela tenha uma postura preventiva em relação aos incidentes relacionados à proteção de dados, de forma a evitá-los ao invés de ter uma postura reativa.

O segundo princípio se refere ao *Privacy by Default*, a privacidade é tida como uma configuração padrão, mediante a qual a proteção dos dados pessoais deve ser garantida em todos os momentos, sem a necessidade de configurações por parte das pessoas.

O terceiro princípio está relacionado à incorporação da privacidade ao *design*, ao processo e na arquitetura de sistemas de Tecnologia da Informação, ou seja, a

⁴¹ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. (Série IDP Linha Pesquisa Acadêmica) p.111.

⁴² SIMONETTE, Marcel. *Privacy by Design e Privacy by Default*. **CEST. Boletim - Volume 6, Número 06**, 2021. Disponível em: www.cest.poli.usp.br/pt/boletins/. Acesso em: 19 jun. 2022.

privacidade não pode ser considerada apenas como algo a mais no projeto, ela é parte do que será desenvolvido.

O quarto princípio se refere à funcionalidade total (soma positiva, não somatório) com a ideia de trazer benefícios e resultados para empresa e consumidor.

O quinto princípio prevê a adoção de medidas de segurança de ponta a ponta, desde a coleta, uso, acesso, armazenamento, compartilhamento e descarte, ou seja, proteção total em todo seu ciclo de vida. Todas as funcionalidades possíveis devem estar completas e protegidas, gerando um benefício mútuo, para as pessoas e para a empresa.

O sexto princípio ordena a visibilidade e a transparência, o fornecedor deverá manter disponível ao usuário, informações sobre políticas e práticas de privacidade dos dados pessoais, além de informá-lo sobre o motivo da coleta dos dados e quem tem acesso à informação.

Por último, estabelece o princípio do respeito pela privacidade do usuário, manter a centralidade nos interesses e necessidades do usuário.

O conceito de *Privacy by Design* foi incorporado no artigo 25 do Regulamento Geral sobre Proteção de Dados da União Europeia - GDPR (General Data Protection Regulation),⁴³ na LGPD este conceito está previsto no art.46 § 2º, como se nota, a lei brasileira possui conceitos semelhantes relacionados à proteção de dados, e em ambas as leis o consentimento é um requisito indispensável para a coleta de dados.

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. § 2º As medidas de que trata o caput deste artigo

⁴³ 1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. 2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. 3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article. Disponível em: <https://gdpr-info.eu/art-25-gdpr/>. Acesso em 15 out. 2022.

deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Conforme aponta Thiago Sombra na tabela abaixo, a Lei Geral de Proteção de Dados brasileira teve forte influência da GDPR, em muitos dos seus pontos são quase idênticas:⁴⁴

Tabela 1 – Comparativo do Consentimento presente na LGPD e na GDPR

LGPD	GDPR
Consentimento deve ser:	Consentimento deve ser:
Prévio	Prévio
Livre	Livre
Informado	Informado
Para uma finalidade determinada	Específico
Inequívoco	Indicação inequívoca por declaração ou ação afirmativa
Por escrito ou outro meio que demonstre a vontade do titular	
Se para dados sensíveis, também deve ser:	Se para dados sensíveis, também deve ser:
Específico	Explícito
Em destaque	
Consentimento pode ser revogado a qualquer tempo	Consentimento pode ser revogado a qualquer tempo
Consentimento deve ser manifestado de maneira apartada de outros termos	Consentimento deve ser manifestado de maneira apartada de outros termos

Fonte: Tabela extraída da tese de Thiago Sombra.

A ideia dos princípios de *Privacy by Design* incorporado à LGPD, busca minimizar a vulnerabilidade presente nas relações contratuais em relação ao consumidor, bem como elevar a tutela da proteção de dados dos mais vulneráveis, a partir da aplicação de técnicas e modelagem do produto e serviço desde a sua concepção se orientando pela privacidade, transparência e em linguagem acessível ao usuário.

Assim, essa metodologia quando implantada pelas empresas, garante além da adequação à LGPD, novas medidas que respeitam a privacidade desde a concepção do produto e serviço.

⁴⁴ SOMBRA, Thiago Luís Santos. **Direito à Privacidade e Proteção de Dados no Ciberespaço: A Accountability como fundamento da Lex Privacy**. Brasília, 2019, Tese. Universidade de Brasília, Brasília, 2019, p.113.

No Brasil, considerando a vulnerabilidade social do país, onde a disparidade socioeconômica se exterioriza no acesso a oportunidades, na garantia dos direitos fundamentais, como promove um grande desequilíbrio de informação entre consumidores e fornecedores, alinhado a preocupação da violação da privacidade e do consentimento aparente⁴⁵ nos contratos de adesão, percebe-se que a implantação do conceito de *Privacy by Design* coordenado às regulamentações do Código de Defesa do Consumidor e da Lei Geral de Proteção de Dados contribuiria para ampliar as garantias e proteção de direitos.

Como afirma Thiago Sombra, "a imposição de mecanismos de *accountability*, transparência, escolha e sistemas operacionais acessíveis (*privacy by design e privacy by default*) são mais eficientes na proteção da privacidade do que a simples ampliação da camada de requisitos em torno do consentimento".⁴⁶

4.1 Os Principais Desafios da Proteção de Dados no Ordenamento Jurídico

Conforme apresentado nos capítulos anteriores, diante do exponencial avanço tecnológicos que se torna um grande desafio da sociedade em função dos riscos apresentados no campo da ética, da transparência, da privacidade e da governança de dados, a legislação brasileira também apresenta um grande desafio de acompanhar essa evolução e as mudanças sociais de forma a superar as insuficiências em relação ao consentimento do titular diante da assimetria de poderes e da vulnerabilidade presente nas relações.

De acordo com Bruno Bioni, faz-se necessário compreender e reavaliar a função e os limites do consentimento de modo a compreender a autodeterminação informacional, ou seja, o controle que o indivíduo tem sobre seus dados pessoais. O autor avalia que o controle sobre os dados pessoais deve ir além do consentimento, propõe uma maior intervenção no fluxo informacional para reduzir a assimetria e limitar a autonomia da vontade diante da situação de hipervulnerabilidade do titular de dados.⁴⁷

⁴⁵ Ocorre quando o consumidor é constrangido a dar o seu consentimento para que determinado serviço ou produto não lhe seja negado. Benedikt Buchner denomina tal situação de "*take it or leave it*", isto é, pegar ou largar, o que denota que a liberdade de consentir nesse caso fica prejudicada. MENDES, Laura Schertel. A vulnerabilidade do consumidor quanto ao tratamento de dados pessoais.

Revista de Direito do Consumidor. vol. 102. ano 24. São Paulo: Ed. RT, nov.-dez. 2015.p.29.

⁴⁶ SOMBRA, Thiago Luís Santos. **Direito à Privacidade e Proteção de Dados no Ciberespaço: A Accountability como fundamento da Lex Privacy**. Brasília, 2019, Tese. Universidade de Brasília, Brasília, 2019, p.119.

⁴⁷Nas palavras de Bruno Bioni "o consentimento do titular dos dados continua a exercer um papel normativo de protagonismo, mas sob um novo roteiro que inclui a atuação de atores coadjuvantes importantes: novas

Outra ideia, trabalhada por Thiago Sombra, é a investigação dos modelos regulatórios da correção, autorregulação e da regulação estatal, com intuito de compreender a privacidade e a proteção de dados, associada a insuficiência do consentimento e a pluralidade de mecanismos de proteção, tais como, a anonimização,⁴⁸ pseudonimização,⁴⁹ *data protection officer*,⁵⁰ de modo a evidenciar como a policontextualidade poderá contribuir para uma regulação mais efetiva.

O modelo de regulação estatal é exclusivo do Estado, compreende a implementação de políticas públicas, criação de incentivos, elaboração de normas gerais de proteção de dados, e a criação de órgãos governamentais responsável pela fiscalização e imposição de sanções, a exemplo, no Brasil, da ANPD – Autoridade Nacional de Proteção de Dados.⁵¹

formas para operacionalizá-lo, levando-se em conta a arquitetura (de vulnerabilidade) da rede; o relato normativo complementar da privacidade contextual que o limita e o readapta diante de um solo epistemológico que esfacela a técnica tradicional da autodeterminação baseada de declaração de vontade do titular dos dados; e o cidadão também exerce domínio sobre seus dados, se estes forem tratados de forma previsível de acordo com suas legítimas expectativas." BIONI, Bruno Ricardo. **Proteção De Dados Pessoais: a função e os limites do consentimento**. 3ª ed. Rio de Janeiro: Forense, 2021. p. 276.

⁴⁸ Anonimização conforme definido no art. 5º, III, da LGPD é o processo por meio do qual os dados pertencentes a um titular não são mais passíveis de identificação e associação direta ou indireta àquele indivíduo, tornando-se um dado anônimo e consequentemente deixam de ser protegidos pela lei. Nesse sentido, Maria Cristine Lindoso ressalta que a anonimização de dados pressupõe um grande risco assumido pelo agente, que tem a responsabilidade em proteger a privacidade, caso contrário, assume o risco de violar a privacidade do usuário no caso do processo de anonimização puder ser revertido. LINDOSO, Maria Cristine Branco. **Discriminação de Gênero no Tratamento Automatizado de Dados Pessoais: Como a automatização incorpora vieses de gênero e perpetua a discriminação de mulheres**. Rio de Janeiro: Processo, 2021. p.162.

⁴⁹ De acordo com opiniões tratadas no WORKING PARTY 29, **Opinion 5/2014 on Anonymisation Techniques** *Apud* Thiago Sombra, a pseudonimização é um processo voltado a disfarçar a identificação de um titular de dados pessoais, de forma a garantir maior nível de segurança, mediante a substituição de um atributo exclusivo do titular por outro tipo de registro. Ao contrário do que muitos sustentam, dados pseudonimizados são considerados dados pessoais, ou seja, não envolvem um processo de anonimização, na medida em que o controlador ainda tem condições de identificar o titular. Na pseudonimização, o controlador tem informações adicionais capazes de refazer toda a cadeia de identificação até se chegar novamente no titular dos dados. SOMBRA, Thiago Luís Santos. **Direito à Privacidade e Proteção de Dados no Ciberespaço: A Accountability como fundamento da Lex Privacy**. Brasília, 2019, Tese. Universidade de Brasília, Brasília, 2019, p.140.

⁵⁰ DPO - *data protection officer* ou encarregado de proteção de dados pessoais, é o responsável pela difusão da cultura de proteção de dados, implementação de boas práticas e realização de constantes treinamentos. Importante ressaltar que os DPOs podem ser pessoas físicas ou jurídicas e não são pessoalmente responsáveis pelos atos praticados pelo controlador, pois sua única atribuição é demonstrar as condições em que a atividade de processamento de dados pessoais ocorre. Se for um empregado do controlador, o DPO deve ter acesso a recursos, independência e autonomia para exercer suas atividades, de sorte que não poderá estar submetido a orientações superiores para exercer suas funções precípuas e nem ser demitido ou punido por desempenhá-las corretamente. *Idem*, *Ibidem*. p. 193.

⁵¹ A ANPD foi criada pela Medida Provisória n. 869, de 27 de dezembro de 2018 como sendo uma autoridade de natureza jurídica transitória, em um primeiro momento ela foi um órgão da administração pública federal, vinculada à Presidência da República, posteriormente a medida provisória foi convertida na Lei n. 13.853, de 14 de agosto de 2019. Por sua vez, o Decreto 10.474, de 26 de agosto de 2020, aprovou a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança

No modelo de correção o Estado atua mediante a elaboração de normas e diretrizes gerais, as leis asseguram uma margem de atuação e complementação por entes privados dos diversos setores da economia.

A autorregulação permite que as empresas elaborem regras próprias para disciplinar as suas atividades, como exemplo do código de conduta, selos, políticas, padrões tecnológicos e arranjos contratuais, dotados de flexibilidade e capazes de facilmente se adaptarem à evolução tecnológica.⁵²

Um dos desafios levantados por Thiago Sombra em sua tese é a necessidade de um novo modelo para a tutela efetiva da proteção de dados, de um modo "responsivo e inovador, capaz de compreender as manifestações de pluralismo jurídico e as autonomias das redes de comunicação, com a devida mescla da correção e autorregulação, mediante o estabelecimento de normas gerais de proteção de dados e maior margem para a atuação da iniciativa privada".

Afirma na sua análise que "o modelo de correção tem sido mais adequado frente aos desafios inerentes à tutela da privacidade e proteção dos dados pessoais, sobretudo porque permite a conciliação entre atuação estatal e fomento à inovação tecnológica". Propõe um modelo de correção policontextual que perpassa pela internalização da cultura e proteção de dados e tutela da privacidade em todas as camadas de uma organização.⁵³

Nesse viés, o autor defende que para uma regulação mais efetiva seria interessante uma abordagem considerando os diversos atores e o emprego da

da ANPD, com entrada em vigor na data de publicação da nomeação do Diretor-Presidente da ANPD no Diário Oficial da União, ocorrida em 06 de novembro de 2020, quando, então, a ANPD efetivamente iniciou suas atividades. Em 13 de junho de 2022, foi editada a MP n. 1.124, que transformou a autoridade nacional em uma autarquia de natureza especial, mantida a estrutura organizacional e suas competências, a medida provisória foi convertida na lei nº 14.460, de 25 de outubro de 2022, que manteve a autoridade nacional como uma autarquia de natureza especial. Entre as principais competências da ANPD, estão as seguintes: elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação; promover na população o conhecimento das normas e das políticas públicas sobre o assunto; estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais; editar regulamentos e procedimentos; deliberar sobre a interpretação da LGPD. Disponível em: <https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes-2013-anpd#c2>. Acesso em: 03 dez. 2022.

⁵² SOMBRA, Thiago Luís Santos. **Direito à Privacidade e Proteção de Dados no Ciberespaço: A Accountability como fundamento da Lex Privacy**. Brasília, 2019, Tese. Universidade de Brasília, Brasília, 2019. p. 74.

⁵³ Idem, Ibidem. p. 199

*accountability*⁵⁴ como meio de fiscalização e controle da tutela da privacidade e proteção de dados, e por oportuno, apresenta um modelo regulatório híbrido denominado de *Lex Privacy*, na qual, a regulação estatal e a correção são complementares.

Na mesma linha, de acordo com Pamela Samuelson, *apud* Thiago Sombra, para uma tutela efetiva de proteção dos dados é necessário compreender a policontextualidade do processo regulatório e adaptá-las ao contexto:

O processo de regulação segundo as diretrizes da policontextualidade deve considerar quando é possível aplicar as leis existentes, quando será necessário adaptá-las ou quando novas deverão ser elaboradas. Deve considerar, ainda, o modo de formulação razoável e proporcional da regulação, além de ter em mira que o processo legislativo deve resultar em normas flexíveis e facilmente adaptáveis às novas circunstâncias. Por fim, deve considerar os direitos fundamentais a despeito das pressões econômicas e tecnológicas, bem como coordenar com os demais países a construção de uma governança transnacional da internet em torno de leis e políticas públicas, de modo a proporcionar um ambiente virtual global mais seguro.⁵⁵

No cenário brasileiro, alinhado ao desenvolvimento de novas tecnologias e disruptões nos produtos e serviços, o Banco Central do Brasil em conjunto com a CVM, iniciou a implantação do modelo de *Sandbox* Regulatório,⁵⁶ um ambiente experimental em que as empresas selecionadas têm flexibilidade regulatória para o desenvolvimento de produtos e serviços inovadores, alinhados às necessidades dos usuários e clientes desde à sua concepção, nota-se nesse modelo a incorporação do conceito de *Privacy by Design* como forma de reduzir a assimetria informacional e a vulnerabilidade do consumidor.

⁵⁴ A *accountability* na proteção de dados tem sete elementos centrais: liderança e direção; análise de risco; políticas e procedimentos; transparência; treinamento e consciência; monitoramento e verificação; responsividade e enforcement (CIPL – Centre for Information Policy Leadership. What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations’ Practices to the CIPL Accountability Framework. Report of the CIPL Accountability Mapping Project, May 2020) *Apud* MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da. Proteção de dados para além do consentimento: Tendências de materialização. *In*: DONEDA, Danilo *et al.* **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. 112.

⁵⁵ SAMUELSON, Pamela, *Apud* Thiago Sombra, SOMBRA, Thiago Luís Santos. **Direito à Privacidade e Proteção de Dados no Ciberespaço**: A *Accountability* como fundamento da *Lex Privacy*. Brasília, 2019, Tese. Universidade de Brasília, Brasília, 2019, p.57.

⁵⁶ O *Sandbox* Regulatório é um ambiente em que entidades são autorizadas pelo Banco Central do Brasil para testar, por período determinado, projeto inovador na área financeira ou de pagamento, observando um conjunto específico de disposições regulamentares que amparam a realização controlada e delimitada de suas atividades. Objetivos do *Sandbox* regulatório do BC, estimular a inovação e a diversidade de modelos de negócio, estimular a concorrência entre os fornecedores de produtos e serviços financeiros e atender às diversas necessidades dos usuários, no âmbito do Sistema Financeiro Nacional (SFN) e do Sistema de Pagamentos Brasileiro (SPB), assegurando a higidez desses sistemas. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/sandbox>. Acesso em: 22 out. 2022.

Nesse ambiente de testes a autoridade reguladora monitora e acompanha os riscos associados aos novos produtos e serviços, desde a concepção já existem regras claras e transparentes para adequação às leis vigentes e aprimoramento do arcabouço regulatório, diante das ponderações, pode-se constatar que o *Sandbox* Regulatório tem aderência ao modelo regulatório híbrido, proposto pelo autor Thiago Sombra, trazendo na prática a ideia da necessidade de complementariedade da regulação estatal e a da correção.

Nesse aspecto, retomando ao problema do consentimento e acesso aos termos de uso e políticas de privacidade que ainda é muito prejudicado pelo fato de serem longos e de difícil interpretação pelo usuário, a proposta de aplicação do modelo regulatório híbrido, complementar à LGPD e coordenado ao conceito de *Privacy by Design*, seria um mecanismo aderente para garantir que os controladores de dados reformulem seus termos de aceite e políticas de privacidade com uma abordagem acessível para todos os usuários.

No âmbito da LGPD dada sua característica de transversalidade na medida que esta afeta todos os setores da economia e entes públicos e privados, é possível vislumbrar que haja espaço para um ambiente regulatório estruturado nos moldes do *Sandbox* regulatório do Banco Central. À luz desse tema, ressalta Miriam Wimmer, diretora da ANPD:

___cingindo-se a análise apenas à esfera do poder público, já é possível vislumbrar de imediato a coexistência de diferentes atores institucionais dotados de competências que de alguma maneira tocam na proteção de dados, para além da própria Autoridade Nacional de Proteção de Dados, dotada de um papel central nessa temática. Em adição à pluralidade de órgãos reguladores no âmbito do Estado, é preciso observar que a sistemática da LGPD pressupõe a permeabilidade a outras instâncias de produção regulatória, como regras de boas práticas e códigos de conduta pactuados pelos próprios agentes de tratamento. A Lei cria, ainda, uma sistemática favorável à tutela coletiva da proteção de dados, abrindo espaço para que entidades representativas atuem em defesa dos direitos do titular de dados.⁵⁷

⁵⁷ GEN Jurídico. **Leia o prefácio do livro Regulação e Proteção de Dados Pessoais, de Bruno Bioni, por Miriam Wimmer.** 2022. Disponível em: <http://genjuridico.com.br/2022/08/19/prefacio-do-livro-regulacao-e-protecao-de-dados-pessoais/>. Acesso em: 05 dez. 2022.

5. CONSIDERAÇÕES FINAIS

Este estudo teve a pretensão de analisar como o ordenamento jurídico brasileiro, especialmente o Código de Defesa do Consumidor e a Lei Geral de Proteção de Dados Pessoais, poderão proporcionar uma efetiva proteção dos titulares de dados nos contratos por adesão diante da exposição da privacidade, da releitura do consentimento e da legitimidade da coleta e tratamento de dados, frente à assimetria informacional e a vulnerabilidade do consumidor.

A inquietação surge a partir do avanço tecnológico observado nos últimos anos, o qual, proporcionou maior intensidade do fluxo de dados, bem como, maior propagação de informações por meios eletrônicos, e, diante das novas possibilidades trazidas com a utilização de inteligência artificial e uso de algoritmos, permitiu às empresas um constante monitoramento do comportamento do consumidor e usuário da internet, atrelado à esses fatos, as ameaças à privacidade do titular de dados se tornaram evidentes.

De fato, o tema da proteção de dados figura entre os campos afetados pela evolução da tecnologia digital em função dos riscos apresentados no campo da ética, da transparência, da privacidade e da governança dos dados do titular, uma vez que os dados pessoais se tornaram bens jurídicos valiosos e por vezes utilizados de maneira inadequada e até inescrupulosas.

Nesse viés, a pesquisa busca demonstrar os avanços da regulamentação jurídica no tema proteção de dados e como o ordenamento jurídico brasileiro na esfera da proteção de dados e da privacidade, vem historicamente acompanhando as mudanças sociais de modo a alcançar a velocidade das inovações e garantir a efetiva proteção dos titulares de dados nos contratos por adesão.

É interessante notar que ao longo dos marcos regulatórios sempre houve preocupação em conferir ao consumidor o direito de controlar seus dados, ou seja, a autodeterminação e consentimento dado pelo titular, em contraponto, num cenário multicultural e diante da assimetria informacional e de extrema vulnerabilidade do consumidor brasileiro, busca-se novas formas complementar para minimizar os efeitos decorrentes desta assimetria e da vulnerabilidade presente nas relações.

Diante da abordagem e das considerações trazidas na doutrina, constata-se que para o ambiente regulatório acompanhar as disrupções e inovações trazidas com a revolução tecnológica, faz-se necessário que o sistema normativo contenha normas flexíveis, de ordem principiológica, e facilmente adaptáveis às novas circunstâncias e que seja capaz de perpassar entre regulação estatal e correção no intuito de aumentar a proteção do titular de dados.

Constata-se, portanto, que tanto o Código de Defesa do Consumidor, quanto a Lei Geral de Proteção de Dados, dado o caráter principiológico de ambas as leis, se amoldam as mudanças sociais e inovações tecnológicas do atual contexto brasileiro.

Diante das considerações, o estudo tenta demonstrar que para uma efetiva proteção dos titulares de dados, faz-se necessário a aplicação do conceito de *Privacy by Design* na esfera de proteção da privacidade e proteção de dados, nos sistemas, códigos, arquiteturas e nos procedimentos tecnológicos desde a fase de concepção do produto e serviços até a sua execução, como forma de prevenir e minimizar os efeitos decorrentes da assimetria informacional e da vulnerabilidade presente nas relações consumeristas.

Por fim, corroborando com o tema, Thiago Sombra, Bruno Biondi, Laura Schertel apresentam instrumentos de *accountability* para uma efetiva proteção dos titulares de dados, focado na transparência, no desenvolvimento da inteligência artificial com deveres éticos e compromissos baseados no respeito aos direitos humanos, à segurança e proteção de dados pessoais, a privacidade dos indivíduos.

Desse modo, conclui-se que a implementação de um modelo regulatório híbrido, com a participação de órgãos públicos e privados, a exemplo do modelo do *sandbox* regulatório, complementar a legislação, coordenado ao conceito e aos princípios de *Privacy by Design*, seria um mecanismo capaz de aperfeiçoar e monitorar constantemente a adequação e a padronização dos contratos de adesão, de forma a garantir que os controladores de dados reformulem seus termos de aceite e políticas de privacidade com uma abordagem padronizada e acessível para todos os usuários.

6. REFERÊNCIAS BIBLIOGRÁFICAS

BANCO CENTRAL DO BRASIL, **SandBox Regulatório**, Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/sandbox>. Acesso em: 22 out. 2022.

BRASIL. **Constituição Federal**. República Federativa do Brasil de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/ConstituicaoCompilado.htm. Acesso em: 13 out. 2022.

BRASIL. **Constituição Federal: Emenda Constitucional 115**. República Federativa do Brasil de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 23 out. 2022

BRASIL. **Lei n. 8.078**, de 10 de setembro de 1990. Código de Defesa do Consumidor. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm. Acesso em: 29 abr. 2022.

BRASIL, **Lei n. 12.527**, de 18 de novembro de 2011. Lei de Acesso a Informação. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm. Acesso em: 12 ago. 2022.

BRASIL, **Lei n. 12.965**, de 23 de abril de 2014. Marco Civil da Internet. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 12 ago. 2022.

BRASIL. **Lei n. 13.709** de 14 de agosto de 2018. Lei Geral de Proteção de Dados: Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em 10 out. 2022.

BRASIL. **Lei n. 14.460** de 25 de outubro de 2022. Autoridade Nacional de Proteção de Dados: Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Lei/L14460.htm#art7. Acesso em 03 dez. 2022.

BRASIL. Presidência da República. **Autoridade Nacional de Proteção de Dados**: Disponível em: <https://www.gov.br/anpd/pt-br/aceso-a-informacao/perguntas-frequentes-2013-anpd#c2>. Acesso em: 03 dez. 2022.

BIONI, Bruno Ricardo. **Proteção De Dados Pessoais**: a função e os limites do consentimento. 3ª ed. Rio de Janeiro: Forense, 2021.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Privacidade e proteção de dados pessoais**: perspectivas de indivíduos, empresas e organizações públicas no Brasil. São Paulo. Núcleo de Informação e Coordenação do Ponto BR, 2022. Disponível em: https://cetic.br/media/docs/publicacoes/2/20220817110001/privacidade_protecao_de_dados_pessoais_2021_livro_eletronico.pdf. Acesso em: 03 out. 2022.

DATAREPORTAL (2022). **Digital 2022 Global Digital Overview**. Disponível em: <https://datareportal.com/reports/digital-2022-global-overview-report>. Acesso em: 5 jun. 2022.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais e-book**: Fundamentos da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Thomson Reuters Brasil, 2021. (Revistas dos Tribunais).

DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel. **Estudos sobre Proteção de Dados pessoais**: Direito, Tecnologia, Inovação e Proteção de Dados num Mundo em Transformação. Expressa, 2022.

GEN JURÍDICO. **Leia o prefácio do livro Regulação e Proteção de Dados Pessoais, de Bruno Bioni, por Miriam Wimmer**. Disponível em: <http://genjuridico.com.br/2022/08/19/prefacio-do-livro-regulacao-e-protacao-de-dados-pessoais/>. Acesso em: 5 dez. 2022.

GIFE. **O aumento da desigualdade social no Brasil, segundo pesquisas**. O Gife. 2022. Disponível em: <https://gife.org.br/desigualdade-social-no-brasil/>. Acesso em: 25 abr. 2022.

LINDOSO, Maria Cristine Branco. **Discriminação de Gênero no Tratamento Automatizado de Dados Pessoais**: Como a automatização incorpora vieses de gênero e perpetua a discriminação de mulheres. Rio de Janeiro: Processo, 2021.

MARTINS, Guilherme Magalhães. A Lei Geral de Proteção de Dados Pessoais (LEI 13.709/2018) e a Proteção dos Consumidores. *In*: MARQUES, Claudia Lima. **Direito do Consumidor: 30 anos do CDC**: Da consolidação como Direito Fundamental aos atuais desafios da sociedade. Rio de Janeiro: Forense, 2020.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. 1ª Edição. São Paulo: Saraiva, 2014. (Série IDP: linha pesquisa acadêmica).

MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da. Proteção de dados para além do consentimento: Tendências de materialização. *In*: DONEDA, Danilo *et al.* **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

MENDES, Laura Schertel. A vulnerabilidade do consumidor quanto ao tratamento de dados pessoais. **Revista de Direito do Consumidor**. vol. 102. ano 24. p. 19-43. São Paulo: Ed. RT, nov-dez. 2015.

MIRAGEM, Bruno. Princípio da Vulnerabilidade: Perspectiva atual e funções no direito do consumidor contemporâneo. *In*: MARQUES, Claudia Lima. **Direito do Consumidor: 30 anos do CDC**: Da consolidação como Direito Fundamental aos atuais desafios da sociedade. Rio de Janeiro: Forense, 2020.

OLIVEIRA, Amanda Flávio, ACCIOLY, João C. Andrade Uzêda, Direito do Consumidor e Análise Econômica do Direito. *In*: MARQUES, Claudia Lima. **Direito do**

Consumidor: 30 anos do CDC: da consolidação como direito fundamental aos atuais desafios da sociedade. Rio de Janeiro: Forense, 2020.

PRICEWATERHOUSECOOPERS BRASIL LTDA. **O abismo digital no Brasil:** Saiba como desigualdade de acesso à internet, a infraestrutura inadequada e a educação deficitária limitam as nossas opções para o futuro. PwC. Disponível em: https://www.pwc.com.br/pt/estudos/preocupacoes-ceos/mais-temas/2022/O_Abismo_Digital.pdf. Acesso em: 5 jun. 2022.

SAMUELSON, Pamela, Apud SOMBRA, Thiago Luís Santos. **Direito à Privacidade e Proteção de Dados no Ciberespaço:** A Accountability como fundamento da Lex Privacy. Brasília, 2019 Tese. Universidade de Brasília, Brasília, 2019.

SIMONETTE, Marcel. *Privacy by Design e Privacy by Default*. **CEST. Boletim - Volume 6, Número 06**, 2021. Disponível em: www.cest.poli.usp.br/pt/boletins/. Acesso em: 19 jun. 2022.

SOMBRA, Thiago Luís Santos. **Direito à Privacidade e Proteção de Dados no Ciberespaço:** A Accountability como fundamento da Lex Privacy. Tese. Universidade de Brasília, 2019. Disponível em: <https://repositorio.unb.br/handle/10482/35752>. Acesso em: 23 out. 2022.

TEIXEIRA, Tarcísio; GUERREIRO, Ruth M. **Lei Geral de Proteção de Dados Pessoais (LGPD): Comentada Artigo por Artigo**. 4ª Edição. São Paulo: Editora Saraiva, 2022.

UNIÃO EUROPÉIA. **General Data Protection Regulation - GDPR**. Disponível em: <https://gdpr-info.eu/>. Acesso em: 30 ago. 2022.

UNIÃO EUROPÉIA. **General Data Protection Regulation - GDPR**. Disponível em: <https://gdpr-info.eu/art-25-gdpr/>. Acesso em 15 out. 2022.

ZUBOFF, Shoshana. Big Other: Capitalismo de vigilância e perspectivas para uma civilização de informação. *In:* BRUNO, Fernanda *et al.* **Tecnopolíticas da vigilância:** Perspectivas da margem. São Paulo: Boitempo Editorial, 2019. (Coleção Estado de Sítio).