UNIVERSIDADE FEDERAL DE UBERLÂNDIA

FACULDADE DE DIREITO

JOÃO VICTOR PIRES SILVEIRA

TUTELA JURÍDICA DOS DADOS PESSOAIS: SOB O CONTEXTO DA SOCIEDADE DIGITAL

Uberlândia - MG

2024

JOÃO VICTOR PIRES SILVEIRA

TUTELA JURÍDICA DOS DADOS PESSOAIS: SOB O CONTEXTO DA SOCIEDADE DIGITAL

Trabalho de Conclusão de Curso apresentado à Faculdade de Direito da Universidade Federal de Uberlândia como requisito parcial para obtenção do título de bacharel em Direito

Orientador: Prof. Dr. Almir Garcia Fernandes

Uberlândia - MG

2024

JOÃO VICTOR PIRES SILVEIRA

TUTELA JURÍDICA DOS DADOS PESSOAIS: SOB O CONTEXTO DA SOCIEDADE DIGITAL

Trabalho de Conclusão de Curso apresentado à Faculdade de Direito da Universidade Federal de Uberlândia como requisito parcial para obtenção do título de bacharel em Direito.

Uberlândia, 05 de abril de 2024.

Banca Examinadora:

_____

Prof. Dr. Almir Garcia Fernandes

Orientador - UFU

_____

Prof. Dr. Ricardo Padovani Pleti

Examinador Interno – UFU

AGRADECIMENTO

Gostaria de expressar meus sinceros agradecimentos a Deus, fonte inesgotável de sabedoria e inspiração, que iluminou meu caminho ao longo desta jornada acadêmica.

À minha mãe, Vanisonia Pires, cujo amor, apoio e sacrifícios incondicionais foram a força propulsora por trás de cada conquista. Sua dedicação incansável e encorajamento moldaram meu percurso e são uma constante inspiração.

Ao meu irmão, Victor Hugo Pires da Silveira, pela amizade, incentivo e compreensão. Sua presença constante trouxe alegria aos momentos desafiadores e significado às vitórias compartilhadas.

À minha namorada, Rafaela Vitor, pelo suporte emocional, compreensão e paciência demonstrados durante este período. Sua presença tornou cada desafio mais leve e cada sucesso mais significativo.

Ao professor orientador, Almir Fernandes, expresso minha gratidão pela orientação perspicaz, apoio acadêmico e conselhos valiosos. Sua dedicação ao meu crescimento acadêmico e profissional é verdadeiramente apreciada.

Cada um de vocês desempenhou um papel fundamental na minha jornada, contribuindo para o meu crescimento pessoal e acadêmico. Seu apoio foi crucial, e sou profundamente grato por cada momento compartilhado.

RESUMO

A sociedade contemporânea encontra-se imersa em uma era digital, onde a interconexão global é alimentada por uma abundância de dados que moldam não apenas a forma como vivemos, mas também como somos compreendidos e representados. Nesse cenário, a tutela de dados emerge como um tema central, exigindo uma análise profunda das complexas interações entre privacidade, ética, legislação e tecnologia.

A evolução tecnológica proporcionou inúmeros benefícios, mas também desencadeou desafios inéditos, especialmente no que diz respeito à proteção dos dados pessoais. Esta pesquisa se propõe a explorar as nuances da tutela de dados na sociedade digital, mergulhando nas teorias éticas, legais e sociais que norteiam essa questão premente.

A disseminação ubíqua de dispositivos conectados, às redes sociais onipresentes e as tecnologias emergentes de coleta e análise de dados têm transformado profundamente a maneira como os indivíduos interagem com o ambiente digital. Contudo, esse progresso não ocorre sem implicações significativas, levantando questões cruciais sobre a privacidade, autonomia e a preservação dos direitos individuais. Com fulcro na Lei Geral de Proteção de Dados e demais legislações aplicáveis, pretende-se dimensionar o nível de desenvolvimento experimentado no território nacional no tocante à proteção dos dados do cidadão.

Palavras-chave: Proteção de dados; LGPD (Lei Geral de Proteção de Dados); Sociedade Digital; Direito digital; Consentimento.

ABSTRACT

The contemporary society finds itself immersed in a digital era, where global interconnection is fueled by an abundance of data that shapes not only the way we live but also how we are understood and represented. In this scenario, data protection emerges as a central theme, demanding a profound analysis of the complex interactions between privacy, ethics, legislation, and technology.

Technological evolution has provided numerous benefits but has also triggered unprecedented challenges, especially concerning the protection of personal data. This research aims to explore the nuances of data protection in the digital society, delving into the ethical, legal, and social theories that guide this pressing issue.

The ubiquitous proliferation of connected devices, omnipresent social networks, and emerging technologies for data collection and analysis have profoundly transformed how individuals interact with the digital environment. However, this progress does not occur without significant implications, raising crucial questions about privacy, autonomy, and the preservation of individual rights. With a focus on the General Data Protection Law, the intention is to assess the level of development experienced in the national territory regarding the protection of citizen data.

Keywords: *Data protection; LGPD (General Data Protection Law); Digital Society; Digital Law; Consent.*

LISTA DE ABREVIATURAS E SIGLAS

- LGPD: Lei Geral de Proteção de Dados.
- CC: Código civil.
- CF: Constituição Federal.
- *GDPR: General Data Protection Regulation.*
- CDC: Código de Defesa do Consumidor.
- UE: União Europeia.
- MCI: Marco Civil da Internet.
- ANATEL: Agência Nacional de Telecomunicações.
- *IoT: Internet of Things*.
- SEBRAE: Serviço Brasileiro de Apoio às Micro e Pequenas Empresas.

SUMÁRIO

1. INTRODUÇÃO

O mercado como conhecemos hoje destoa daquele conhecido de um passado não muito distante[1] em que os vínculos comerciais dos modelos de negócio advinham majoritariamente das conexões estabelecidas por meios físicos.

As informações passaram a ser um ativo de grande valia a aqueles que desejam alcançar o público. O posicionamento digital de uma marca/empresa deixa de ser opcional e passa a ser obrigatório a sobrevivência ou evolução dela. Em suma, ou o empreendimento se posiciona digitalmente ou ele está em risco iminente de desaparecer ou pelo menos perder uma fatia de mercado extremamente considerável. Superou-se o passado breve em que as empresas se ocupavam-se de estarem presentes em listas telefônicas, exibir alguns cartazes pela cidade, panfletos, cartões de visitas, quando muito outdoors.

Com essa mudança paradigmática, assim como qualquer outra já observada pela humanidade, o surgimento de novos desafios é diretamente proporcional.

Em uma pesquisa apresentada pelo Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (SEBRAE):

> O *Marketing* Digital está dominando o mercado brasileiro e vem ganhando consistência ano a ano. O levantamento mostra que 94% das empresas no país escolheram esse tipo de estratégia para o crescimento da marca. (SEBRAE, 2022).

Vê-se como a digitalização de serviços, comunicações e transações financeiras resultou em um aumento significativo no volume de dados gerados e compartilhados *online*. Diante disso, passou a ser possível a criação de perfis de potenciais consumidores, tornando o processo de venda mais assertivo e barato. Sobre o tema, ainda que na retorica dos agentes, o usuário frente as opções que lhe são dadas, está ciente da disposição do bem tutelado, em uma pesquisa realizada pela Universidade da Pensilvania (2015), em que buscou-se identificar o nível de satisfação dos usuários frentes a essas práticas, quando questionados se estavam conscientes e satisfeitos ao trocar seus dados pessoais por serviços e produtos ‘gratuitos’ a pesquisa revelou

[1] O mercado entenda-se como modo em que as relações de consumo e comércio se dão.

um forte sentimento de injustiça entre os participantes, com 91% dos entrevistados expressando que seria injusto a troca de dados por serviços ou benefícios. Durante o levantamento da pesquisa, foi expressamente perguntado aos participantes da pesquisa a respeito da disponibilização troca de dados pessoais por *Wi-Fi* gratuito ou a criação de perfis para aprimorar serviços, com a maioria dos respondentes rejeitando essas práticas.

Com isso, o aumento exponencial de dados disponíveis e expostos gera preocupação sobre a privacidade e segurança dos usuários. Incidentes de violações de dados e uso indevido de informações pessoais destacam-se por cada vez mais se tornarem recorrentes. A lógica mercadológica de busca a maximização dos resultados impulsionou a coleta e tratamento de dados, formando um novo modelo de negócio bem como também fomentou o desenvolvimento de novas modalidades de publicidade. O que gera a necessidade de que os mecanismos de segurança bem como as regulamentações tentem evoluir na mesma velocidade.

A criação de legislações de proteção de dados pessoais, como a Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil, a qual estabeleceu o consentimento como um dos principais mecanismos para a legitimação do tratamento de dados pessoais, objetivou permitir o maior controle das informações pelo usuário. No entanto, a eficácia desse mecanismo tem sido questionada, revelando-se insuficiente para garantir a privacidade e a proteção efetiva dos dados pessoais dos indivíduos. O presente estudo investiga a problemática relativa à eficácia do consentimento enquanto mecanismo de legitimação do tratamento de dados pessoais sob a LGPD. Questionando: Em que medida o consentimento, tal como concebido e implementado na atual legislação de proteção de dados pessoais, é efetivo na proteção da privacidade e dos dados pessoais dos indivíduos.

O uso indiscriminado e muitas vezes opaco desses dados levanta questões éticas importantes. O que acontece com nossos dados depois que são coletados? Quem tem acesso a eles e com que finalidade são utilizados? Essas são perguntas que merecem reflexão, pois o uso indevido ou não autorizado de dados pessoais pode levar a violações de privacidade, discriminação e até mesmo manipulação comportamental.

Este trabalho tem como objetivo geral avaliar a eficácia do consentimento como mecanismo de proteção de dados pessoais sob a ótica da Lei Geral de Proteção de Dados Pessoais (LGPD), com a intenção de propor melhorias que garantam uma

proteção mais efetiva da privacidade dos indivíduos. Para alcançar tal finalidade, foram delineados objetivos específicos, incluindo a análise da natureza jurídica e os limites operacionais do consentimento tanto na LGPD quanto em legislações comparáveis. Essa análise foi fundamental para identificar os principais desafios enfrentados pelos titulares dos dados ao fornecer um consentimento que seja ao mesmo tempo informado e genuíno. Além disso, o estudo busca sugerir medidas e práticas alternativas ao consentimento, visando o fortalecimento da proteção de dados pessoais e a privacidade dos indivíduos.

No que tange à metodologia, a pesquisa optou por uma abordagem qualitativa, valendo-se da análise documental de legislação, doutrina e jurisprudência relevantes. Esta escolha metodológica incluiu também a revisão de literatura acadêmica sobre a proteção de dados pessoais e privacidade.

2. NORMATIVAS

Na era digital contemporânea, a sociedade está imersa em um ambiente interconectado, onde a abundância de dados molda não apenas nosso modo de vida, mas também nossa compreensão e representação. Diante desse cenário, a proteção de dados emerge como um tema central, exigindo uma análise profunda das complexas interações entre privacidade, ética, legislação e tecnologia.

O Marco Civil da *Internet* (MCI), Lei nº 12.965/2014, representou um marco inicial na tentativa de regular o comportamento na *internet,* visando proteger a privacidade dos usuários e estabelecer direitos e deveres para o uso da rede. No entanto, embora tenha avançado em algumas áreas, não abordou todos os aspectos necessários para lidar com os desafios contemporâneos da proteção de dados.

Diante da necessidade de uma legislação mais abrangente e específica, foi promulgada a Lei Geral de Proteção de Dados (LGPD), inspirada em legislações internacionais tendo como base o *General Data Protection Regulation* (GDPR) da União Europeia (UE). A LGPD estabelece princípios, direitos e obrigações relacionados ao tratamento de dados pessoais, fornecendo um quadro normativo sólido para lidar com as questões de privacidade na sociedade digital.

2.1 BASE LEGAL:

O MCI foi promulgado em 2014 e trouxe importantes avanços na proteção da privacidade dos usuários da *internet* no Brasil. Ele proibiu o uso e fornecimento de dados do usuário sem o seu consentimento, estabeleceu princípios para a coleta e tratamento de dados pessoais e determinou responsabilidades para os provedores de serviços *online*.

Além disso, o Marco Civil definiu os direitos e garantias dos usuários, incluindo o direito à privacidade e à proteção de dados pessoais. Ele também criou mecanismos de fiscalização e responsabilização, transferindo tal competência para agências reguladoras como a Agência Nacional de Telecomunicações (ANATEL).

No entanto, o MCI não conseguiu abordar todos os aspectos relacionados à proteção de dados na era digital. Sua regulamentação foi apenas o primeiro passo em direção a uma legislação mais ampla e detalhada.

Em paralelo à promulgação do Marco Civil da *internet*, iniciou-se, na Europa, a discussão acerca de uma legislação geral sobre proteção de dados. Desta forma, o GDPR apresentou-se como uma legislação abrangente da União Europeia (UE), promulgada em maio de 2018, como uma resposta ao contexto emergente de preocupações relacionadas à privacidade de dados em um ambiente digital em constante evolução. Sua gênese remonta a um período marcado pela fragmentação regulatória dentro do bloco europeu, onde as leis de proteção de dados variam consideravelmente entre os estados membros, resultando em lacunas e inconsistências no tratamento dos direitos de privacidade dos cidadãos.

O GDPR foi concebido com múltiplos objetivos. Primeiramente, visa fortalecer e consolidar os direitos individuais sobre os dados pessoais, conferindo aos cidadãos da UE um maior controle sobre o uso de suas informações pessoais. Além disso, busca simplificar o ambiente regulatório para as empresas que operam no mercado único europeu, estabelecendo um conjunto único de regras aplicáveis em todos os Estados membros. Por conseguinte, o GDPR estabelece diretrizes claras sobre a coleta, processamento e proteção de dados pessoais, fornecendo um quadro normativo sólido para a condução das práticas de tratamento de dados.

Os efeitos do GDPR têm sido substanciais tanto em termos práticos quanto normativos. Em nível prático, as organizações sujeitas ao escopo da lei foram compelidas a revisar e reformular suas práticas de gestão de dados, implementando

medidas de segurança robustas e adotando políticas de privacidade mais transparentes e informativas.

Em um levantamento realizado pelo *European Commision* e *a International Association of Privacy Professionals (IAPP)*, em quase um ano em vigor foram realizadas aproximadamente 144.376 reclamações às autoridades de proteção de dados europeias por supostas violações à GDPR e cerca de 89.271 notificações de data *breach* foram apresentadas para as autoridades europeias de proteção de dados (CONJUR,2019).

Ademais, a legislação instaurou um novo paradigma normativo global, influenciando a elaboração de legislações similares em outras jurisdições ao redor do mundo. Inspirados pela GDPR, vários países do globo adotaram ou reformaram suas próprias leis de proteção de dados para alinhar-se ou refletir os princípios estabelecidos pela GDPR. Exemplos incluem a Lei Geral de Proteção de Dados (LGPD) no Brasil, o *California Consumer Privacy Act* (CCPA) nos Estados Unidos e o *Personal Data Protection Bill* na Índia.

Em suma, representa um marco significativo na regulação da privacidade de dados, promovendo uma abordagem mais unificada e abrangente para a proteção dos direitos de privacidade dos indivíduos na era digital, ao mesmo tempo em que impõe exigências substanciais às organizações que lidam com dados pessoais.

Por fim, retomando o estudo à legislação nacional, a LGPD, inspirada no GDPR da União Europeia, foi promulgada em 2018 e representa uma evolução significativa na proteção de dados pessoais no Brasil. Ela estabelece princípios como o consentimento do titular dos dados, a finalidade e a transparência no tratamento de dados, além de direitos como o acesso, correção e exclusão de informações pessoais.

A Lei também impõe obrigações aos controladores e operadores de dados, exigindo medidas de segurança para proteger as informações pessoais contra acessos não autorizados e vazamentos. Além disso, prevê sanções para o descumprimento das normas, incluindo multas que podem chegar a 2% do faturamento da empresa[2].

Embora o Marco Civil da *Internet* tenha estabelecido alguns princípios e diretrizes importantes para a proteção de dados na *internet*, a legislação veio para complementar e aprimorar essa legislação. Enquanto o MCI tratava de forma mais

[2] limitadas a R$50 milhões por infração.

genérica da privacidade e proteção de dados, a LGPD detalha e regulamenta de maneira mais específica o tratamento de informações pessoais.

2.1.1 Impacto da Sociedade Digital na Privacidade

Com o avanço da tecnologia e a crescente digitalização da sociedade, as atividades de processamento de dados têm cada vez mais impacto na vida das pessoas. Hoje, vivemos em uma sociedade e economia orientadas por dados, onde as informações pessoais são usadas para diversos fins, desde publicidade direcionada até análises de comportamento do consumidor. Conforme preleciona o ilustre professor Gustavo Tepedino:

> Os dados disponíveis tornaram-se bem jurídico valiosíssimo, por vezes utilizados inescrupulosamente, contendo informações que permitem aos seus detentores conhecerem e traçarem perfis sobre hábitos de consumo, saúde, características genéticas e comportamentais de grande parte da população. (TEPEDINO, 2019 p. 13).

Diante desse contexto, a proteção da privacidade é uma questão fundamental, exigindo uma abordagem abrangente e multidisciplinar que leve em consideração não apenas aspectos legais, mas também éticos, sociais e tecnológicos.

O avanço da tecnologia e a proliferação de dispositivos conectados transformou radicalmente a maneira como interagimos com o mundo. Nessa sociedade altamente digitalizada, nossas atividades diárias deixam rastros digitais, gerando uma quantidade sem precedentes de dados pelo caminho. Esses dados, que incluem desde nossas preferências de compra até nossas interações nas redes sociais, são coletados, armazenados, processados e utilizados por empresas e organizações de diversas formas. Como resultado desse constante monitoramento e coleta de dados, a privacidade individual está cada vez mais em risco, a esse respeito, discorre Yuri Monnerat Lott:

> Considerando o atual dilema entre a necessidade de segurança e a consequente perda de privacidade com o compartilhamento de dados pessoais, no momento em que grande parte da população mundial marcha

> sobre a esteira globalizante e se torna cada vez mais dependente das novas tecnologias de informação e comunicação. (LOTT, 2015, p. 119).

A disseminação de dispositivos de monitoramento, como câmeras de segurança e dispositivos os quais se comunicam entre si, por meio *Internet of Things* (IoT) ou *internet* das coisas em uma tradução direta, explica que nossas atividades cotidianas estão sendo registradas e analisadas por razões econômicas e políticas. Além disso, a proliferação de aplicativos e serviços *online* coletam informações pessoais, muitas vezes sem o pleno conhecimento ou consentimento dos usuários.

Ademais, a assimetria de poder entre os indivíduos e as empresas ou governos que coletam e controlam esses dados é cada vez mais evidente. Conforme preleciona Bruno Bioni (2019, p.221) “Os consumidores mostram-se impotentes para fazer valer o seu desejo de controlar seus dados pessoais, sendo tal assimetria de poder a mola propulsora de tal resignação “.

Enquanto as organizações têm recursos e tecnologia para coletar, analisar e utilizar esses dados em seu benefício, os usuários médios têm pouco controle sobre suas próprias informações pessoais e pouca compreensão sobre como elas são usadas.

Diante desses desafios, a proteção legal e regulatória dos dados pessoais é crucial. Leis como o GDPR na União Europeia e a LGPD no Brasil visam garantir que os direitos dos indivíduos sejam respeitados e que suas informações pessoais sejam tratadas com transparência, segurança e responsabilidade. Essas legislações estabelecem princípios fundamentais, como o consentimento informado, a finalidade específica e a minimização de dados, que são essenciais para proteger a privacidade na era digital.

Um dos princípios norteadores da LGDP é o do consentimento, o qual assume-se como fator preponderante da tentativa de autotutela estabelecida. A ideia de consentimento livre é crucial na proteção da privacidade dos dados. Conforme destacado por Bruno Bioni (2019) à liberdade nesse contexto implica na capacidade do titular dos dados de fazer uma escolha sem qualquer forma de coerção ou pressão. O consentimento deve ser uma manifestação voluntária e informada, onde o indivíduo tem pleno conhecimento sobre o que está autorizando.

Especialistas em proteção de dados ressaltam a importância da granularidade do consentimento, nessa linha de raciocínio, Caio César C. Lima elucida que:

> É importante observar o que diz respeito à granularidade, por meio da qual não se pode ter como válido o consentimento manifestado no formato de ‘tudo ou nada’. Nesse sentido, nas situações em que houver coleta de dados para diferentes finalidades, o titular dos dados deve ter a possibilidade de escolher, uma a uma, a finalidade específica em relação à qual autoriza o tratamento de dados, sendo inválido se não houver essa opção. (LIMA, 2020, p. 28).

Um dos objetivos do consentimento é estabelecer uma relação transparente entre os indivíduos que fornecem seus dados e as empresas que os coletam, armazenam e tratam. Isso significa que as empresas devem informar claramente aos usuários sobre como seus dados serão utilizados, garantindo uma compreensão adequada das práticas de privacidade.

2.1.2 Proteção da Privacidade como Direito Fundamental

A proteção da privacidade dos dados é reconhecida como um direito fundamental, que deve ser respeitado e protegido pelas empresas e pelo poder público. A partir da Emenda Constitucional 115/2022, o Congresso promulga emenda à Constituição tornando a proteção de dados pessoais, inclusive nos meios digitais, um direito fundamental e a esse despeito, o autor Danilo Doneda previa:

> Certa ‘equalização’ entre uma série de direitos fundamentais que possuem repercussão direta sobre dados pessoais, como o direito à privacidade, o direito à informação e a transparência. A inserção de um direito à proteção de dados de forma explícita no rol de direitos fundamentais da Constituição da República proporcionaria, portanto, uma isonomia entre esses direitos que, formalmente, afigura-se fundamental para a proteção de liberdades fundamentais. (DONEDA, 2019, p. 269).

Em decorrência do amparo jurídico construído, as empresas são obrigadas a obter o consentimento dos usuários para a coleta e o tratamento de seus dados, conforme estabelecido em leis como a LGPD. Essas leis abrangem não apenas os meios digitais, mas também todos os outros setores que lidam com dados pessoais, estabelecendo sanções para aqueles que violarem as normas de privacidade.

Esses pontos destacam a importância do consentimento livre e informado na proteção da privacidade dos dados pessoais, bem como a necessidade de transparência e responsabilidade por parte das empresas que coletam e tratam esses dados. A legislação de proteção de dados, como a LGPD, desempenha um papel crucial ao estabelecer diretrizes claras para o tratamento ético e legal dos dados pessoais, garantindo assim os direitos fundamentais dos indivíduos na sociedade digital.

É evidente que as atividades de processamento de dados exercem uma influência significativa na vida das pessoas, conforme observado por Bruno Bioni (2019). Vivemos em uma sociedade e economia em que essas atividades orientam e movimentam as interações sociais e comerciais, utilizando os dados como signos identificadores do cidadão.

A discussão sobre a proteção de dados é de extrema relevância para o estudo do direito, uma vez que o conceito de dados pessoais desempenha um papel central na imputação de relevância jurídica a essas questões. Segundo Bruno Bioni (2019, p. 104), “a análise para determinar se um dado pode ser considerado pessoal depende do contexto e do tipo de informação que pode ser extraída de uma base de dados.”

Ao analisar as possibilidades de resolver os problemas associados à utilização e coleta de dados pessoais, surgem os chamados dados anônimos. Bruno Bioni (2019, p. 104), destaca que esses dados, em princípio, “seriam incapazes de identificar o sujeito. No entanto, por meio de técnicas como supressão, generalização e outras, as empresas tentam tornar os dados menos identificáveis”.

Apesar das tentativas de anonimização, a ideia de dados anônimos revela-se ineficaz. Empresas de tecnologia podem cruzar dados de diferentes fontes, tornando possível a identificação do usuário. Nesse sentido, o conceito mais apropriado para dados pessoais é o "conceito expansionista", conforme destacado por Bruno Bioni (2019, p. 108). “Esse conceito reconhece que as informações podem identificar um sujeito, mesmo que de forma indireta ou remota, abraçando uma definição mais ampla de dados pessoais”.

Essas considerações demonstram os desafios enfrentados na proteção da privacidade dos dados pessoais, bem como a necessidade de uma abordagem mais abrangente e atualizada para lidar com as questões relacionadas à identificação e anonimização dos dados na sociedade digital.

3. PRINCÍPIOS E CONCEITOS NA PROTEÇÃO DE DADOS PESSOAIS: UMA PERSPECTIVA JURÍDICA

A emergência da proteção de dados pessoais como um campo autônomo, distinto do direito à privacidade, reflete um reconhecimento crescente das nuances específicas impostas pelo ambiente digital sobre as liberdades individuais e a autodeterminação. A Lei Geral de Proteção de Dados (LGPD) no Brasil e o *General Data Protection Regulation* (GDPR) na União Europeia constituem marcos regulatórios que estabelecem um novo paradigma na gestão de informações pessoais, enfatizando a autonomia do titular dos dados e a responsabilidade dos agentes de tratamento.

A transição para uma concepção de proteção de dados centrada na autonomia do titular reflete um avanço significativo nas obrigações de transparência e consentimento. Historicamente, a gestão de dados estava predominantemente nas mãos do Estado ou de entidades corporativas, com pouca ou nenhuma preocupação à ingerência individual sobre como as informações pessoais eram coletadas, usadas ou compartilhadas, tal como na lição de Bruno Bioni (2019) o distintivo da geração inicial de leis de proteção de dados pessoais reside em sua concentração na regulação governamental, além da intenção de implementar regras estritas que regulamentassem a aplicação tecnológica.

Lys Nunes Lugati (2020) trabalha em sua obra de maneira didática e cronológica, apontando a evolução das chamadas ‘gerações’ das leis que desempenharam caráter regulatório da proteção da privacidade em escala mundial. Sendo possível auferir nesse esteio que as gerações[3] de leis relativas à proteção de

[3] Primeira Geração: surgiu na década de 70, para regular o crescente uso de bancos de dados por entidades governamentais e privadas, focando na coleta, armazenamento e processamento de dados pessoais para proteger a privacidade individual. Segunda geração: ampliaram o escopo da regulamentação, estabelecendo direitos explícitos para os titulares dos dados e criando autoridades independentes para supervisionar a conformidade. Terceira Geração: as leis de terceira geração responderam à globalização e ao avanço da internet, focando em temas como transferência internacional de dados, segurança da informação e a exigência de consentimento explícito, adaptando-se às novas realidades digitais. Quarta Geração: Inaugurada pela GDPR da UE em 2018, a quarta geração caracteriza-se por regulamentações de alcance global, princípios de 'privacidade desde a concepção', o direito ao esquecimento e sanções severas por violações, influenciando leis em várias jurisdições e marcando um movimento global em direção a uma proteção mais rigorosa dos dados pessoais.

dados transformaram de maneira pragmática o modo como se lida com as informações dispostas na contemporaneidade.

3.1 DESAFIOS NA ERA DA PUBLICIDADE COMPORTAMENTAL *ONLINE*

A categorização de dados pessoais, sensíveis e anonimizados reflete a complexidade e a diversidade das informações tratadas na esfera digital. A distinção entre essas categorias é fundamental para a aplicação adequada das proteções jurídicas. Dados sensíveis, em particular, requerem salvaguardas adicionais devido ao seu potencial discriminatório. Essa diferenciação normativa destaca a necessidade de um tratamento diferenciado baseado na natureza das informações, um princípio essencial para a proteção eficaz da privacidade e da dignidade humana no ambiente digital.

A evolução da publicidade digital, especialmente a publicidade comportamental *online*, exemplifica a intrincada relação entre tecnologia e privacidade. A capacidade que se tem, por meio dos instrumentos tecnológicos que hoje estão ao alcance dos operadores, de rastrear e analisar o comportamento online de indivíduos para fins de publicidade personalizada levanta questões significativas sobre a autodeterminação e o controle sobre os próprios dados. Conforme denota Victor Augusto Tateoki:

> Com a evolução das tecnologias da comunicação, e o grande aumento do fluxo de dados gerados pela sociedade da informação, aliado ao rápido avanço da tecnologia e do barateamento dos custos de coleta e armazenamento de dados a possibilidade de análise de dados para uma publicidade comportamental ficou mais fácil (TATEOKI, 2017, p. 70).

A publicidade contextual, enquanto ferramenta publicitária destinada a aumentar a eficiência das mensagens veiculadas ao preestabelecer um público-alvo destinatário da mensagem. Quanto maior volume de informação que o fornecedor detiver sobre o consumidor, maior a eficiência da publicidade contextual e, nos padrões atuais de tratamento de dados pessoais, é alarmante o grau de conhecimento que as empresas possuem sobre os consumidores (MACHADO e RUARO, 2017)

A eficácia do consentimento como mecanismo de proteção é desafiada pela complexidade e pela falta de transparência nas práticas de coleta e uso de dados.

Este cenário evidencia a necessidade de mecanismos regulatórios robustos que garantam não apenas a transparência e a responsabilidade dos agentes de tratamento, mas também meios efetivos para que os indivíduos exerçam controle sobre suas informações pessoais.

Diante do crescente mercado, bem como o desenvolvimento da ciência mercadológica, ferramentas foram criadas ou melhoradas visando atender aos interesses dos agentes e controladores de forma cada vez mais eficientes, tornando a publicidade cada vez mais assertiva.

Dentre estas ferramentas pode-se elencar os *cookies*, que fazem parte do cotidiano a importunação no canto da tela ao acessar um *website* pela primeira vez, informando que ao aceitar a utilização dos *cookies*, sua experiência ao utilizar o aplicativo (app) ou *website* tornaria-se melhor.

O rastreamento de informações na *internet* como um fenômeno cotidiano experimentado por usuários após uma simples busca por serviços ou produtos, ilustra a complexidade e a intrusividade das práticas de publicidade e *marketing* digital. Esse processo é majoritariamente viabilizado pelo uso de *cookies*, pequenos arquivos de texto que desempenham um papel crucial na navegação *online,* evidenciando um campo de tensão entre usabilidade e privacidade.

3.2 *COOKIES* E A DINÂMICA DO RASTREAMENTO *ONLINE*

Em um estudo publicado pelos pesquisadores Steven Englehardt e Arvind Narayanan, da Universidade de *Princeton* (2016). Através do monitoramento dos cerca de 1 milhão de *sites* mais acessados, concluíram pela presença de, pelo menos, 81.000 *third party*[4]. Além da predominância da prática de sincronização de *cookies*, sugerindo intensa troca de dados entre corporações e/ou organizações.

Por meio da aplicação dos *cookies*, cada clique na *internet* cria um retrato[5] e cada retrato é capaz de servir de amostra para diversos fins. Inicialmente cumprem demonstrar que, *cookies* são arquivos projetados para otimizar a experiência de navegação na *internet.* Eles permitem que *websites* 'lembrem' das ações e preferências dos usuários, como *login*, idioma, tamanho da fonte e outras

[4] Domínios que fogem da relação usuário-*website*, representando outras empresas que podem se beneficiar das informações coletadas.
[5] Uma coleta de cada clique, ou seja, monitora cada clique.

configurações de visualização, por um período, tornando desnecessário reconfigurar essas preferências a cada visita ao *site*. Ao mesmo tempo, os *cookies* têm a capacidade de registrar detalhadamente o comportamento de navegação dos usuários, coletando dados que podem ser utilizados para personalizar a experiência *online* e, mais criticamente, para direcionar publicidade.

First Party Cookies são aqueles configurados pelo próprio *site* visitado pelo usuário e geralmente coletam dados diretamente utilizados pelo proprietário do ambiente virtual para melhorar a funcionalidade e a experiência do usuário. Esses *cookies* podem incluir informações sobre preferências de navegação, itens adicionados ao carrinho de compras, entre outros dados pertinentes à interação direta com o sítio eletrônico.

Third Party Cookies diferentemente dos *cookies* de primeira parte, os de terceira parte são criados por domínios, que não o *site* que o usuário está visitando diretamente. Estes, são frequentemente usados para rastreamento transversal de usuários em vários *sites*, com o objetivo de coletar informações de navegação para direcionar publicidade específica, refletindo um nível mais profundo de coleta de dados e implicações potencialmente maiores para a privacidade dos usuários.

A compreensão dos fundamentos e funções dos *cookies* revela uma dualidade interessante em sua aplicação: enquanto servem para enriquecer a experiência do usuário *online*, facilitando a personalização e a memorização de preferências, também desempenham um papel crucial nas estratégias de *marketing* digital, especialmente na publicidade comportamental. Essa intrincada relação entre a funcionalidade dos *sites* e a coleta de dados para publicidade nos leva a explorar mais a fundo as tipologias de *cookies*, que se dividem em categorias específicas com base em quem os configura e para quais propósitos. A distinção entre *First Party Cookies* e *Third Party Cookies* ilumina ainda mais o espectro de uso desses pequenos arquivos de dados, evidenciando a complexidade das práticas de rastreamento *online* e suas implicações para a privacidade dos usuários. À medida que mergulhamos nessa diferenciação, fica claro que os *cookies*, dependendo de sua origem e uso, podem ter impactos variados na experiência *online* e na gestão da privacidade digital, sublinhando a necessidade de compreender as nuances dessas tecnologias e as responsabilidades que acompanham seu uso.

3.3 IMPLICAÇÕES LEGAIS E ÉTICAS

A prevalência de *cookies* na *internet,* particularmente os *Third Party*, levanta questões significativas sobre consentimento informado, transparência e controle do usuário sobre seus dados pessoais. Normativas de proteção de dados estabelecem diretrizes rigorosas sobre o consentimento dos usuários para o tratamento de seus dados pessoais, incluindo o uso de *cookies*. Essas regulamentações exigem que os usuários sejam claramente informados sobre a coleta e o uso de seus dados e que lhes seja oferecida a opção de aceitar ou recusá-lo, não sendo estritamente necessários para a operação do *site.*

Diante da situação, vários países implementaram ou reforçaram regulamentações de proteção de dados, visando proteger os direitos dos usuários em relação ao uso de seus dados pessoais.

Com isso, busca-se a conscientização do usuário, para que este possa ser mais zeloso com suas práticas digitais, limitando a envergadura dos dados divulgados na *internet.*

As informações do usuário constantemente são moeda de troca em uma sociedade digitalizada. O ponto que importa aferir, na atual circunstância em que não se tem o real e fidedigno controle que os termos de uso nos fazem acreditar, ao passo que, a autotutela de dados pessoais presume a ideia de que, um homem médio seja capaz de definir o que pode ou não ser feito com seus dados, através de um ‘contrato de adesão’ visto que são termos pré-definidos que visam possibilitar a coleta de dados e os transformá-lo em mercadoria.

A partir da publicidade comportamental, campanhas publicitárias são traçadas com base em sua atividade de navegação, ou seja, pesquisas, cliques, palavras chaves escritas e até mesmo, por vezes por meio da captação de som advindo de alguma permissão que eventualmente é requisitada. Corriqueiramente é requisitado ao usuário o fornecimento de permissões de aplicativos, navegadores, entre outros *softwares* para que possamos acessar determinado conteúdo, função. Nessa esteira apps diversos solicitam acesso às funções que nem mesmo estão relacionadas com sua atividade final. De maneira geral, essas permissões que o usuário distribui a estes *softwares* são empregados com a finalidade de demonstrar o consentimento expresso daquele ora consumidor na relação estabelecida. Entretanto, a forma como se dá essa permissividade demonstra que de fato não há uma livre vontade das partes, e sim uma

obrigação imputada ao cliente, de modo que, ao não aceitar esses termos, ele se vê impossibilitado de acessar funções por vezes essenciais.

3.4 INFLUÊNCIA DAS *BIG TECHS* E O EQUILÍBRIO DE PODER

As grandes empresas de tecnologia, denominadas *Big Techs*[6] impressionam pela grande ascensão e seu vasto domínio sobre o ecossistema digital. Cenário que reforça a importância de uma regulação efetiva para assegurar a concorrência leal e a proteção dos direitos dos titulares dos dados. O impacto dessas corporações na definição de padrões tecnológicos e práticas de mercado exige uma reflexão crítica sobre o poder e a responsabilidade no tratamento de dados pessoais. A dinâmica entre inovação tecnológica, poder econômico e proteção de dados pessoais sublinha a necessidade de uma abordagem regulatória que promova a equidade, a transparência e a justiça no ambiente digital.

As *BigTechs* atualmente possuem tamanho poder econômico, social e político, que são capazes de dominar o mercado com práticas muitas vezes predatórias e prejudiciais ao mercado e sua organização. Não faltam exemplos, mas impressiona e convém ressaltar como nos casos de empresas emergentes, as chamadas *startups* que ao primeiro sinal de inovação são rapidamente incorporadas aos quadros dessas grandes empresas como é o caso da *Meta Platforms, Inc.*[7]. Acabando com qualquer possibilidade de concorrência. Muitas vezes cerceando o acesso às novas tecnologias, a medida de seu interesse em possibilitar a ascensão da inovação ou não.

Diante da complexidade crescente das tecnologias digitais e do poderio das empresas, apresentam-se os desafios substanciais à eficácia do consentimento como mecanismo de proteção. Isso sublinha a importância de regulamentações que não somente assegurem a transparência e responsabilização por parte dos agentes de tratamento, mas também fortaleçam a capacidade dos indivíduos de exercer um controle efetivo sobre seus dados pessoais, colocando-os em paridade.

Neste contexto, a influência predominante das *Big Techs* no ecossistema digital e o consequente desequilíbrio de poder reforçam a necessidade de uma regulação

---

[6] São as grandes empresas que exercem domínio no mercado de tecnologia e inovação, como a Apple, o Google, a Amazon, a Microsoft e a Meta.

[7] (Anteriormente Facebook, Inc.) é um conglomerado estadunidense de tecnologia e mídia social.

eficaz que promova a concorrência, proteja os direitos dos titulares de dados e assegure que o desenvolvimento tecnológico e a inovação não ocorram às custas da privacidade e da dignidade humana. A evolução da proteção de dados pessoais, portanto, não se trata apenas de uma questão legal ou técnica, mas de um imperativo ético e social que demanda uma reflexão contínua e o compromisso de todos os envolvidos para garantir que os avanços tecnológicos sejam compatíveis com os direitos fundamentais dos indivíduos.

4. O CONSENTIMENTO NA TUTELA DE DADOS

A ideia de colocar o indivíduo no centro do controle de sua proteção, ou seja, ser competente para consagrar os ditames de sua livre vontade enfrenta alguns percalços, como a complexidade técnica e a assimetria informacional.

A complexidade das tecnologias digitais e dos sistemas de coleta de dados operam em uma escala e opacidade tais que o usuário médio[8], sem conhecimento especializado, não consegue compreender plenamente. Essa assimetria informacional entre usuários e entidades que coletam e processam dados pessoais coloca os primeiros em uma posição desvantajosa, onde a capacidade de tomar decisões informadas sobre o uso de seus dados é significativamente prejudicada.

A temática do consentimento, enquanto pedra angular da tutela de dados pessoais, emerge como um aspecto controverso e debatido na doutrina contemporânea sobre proteção de dados. A complexidade em torno do consentimento reflete as tensões intrínsecas entre a autonomia do indivíduo e as práticas de coleta, uso e compartilhamento de informações pessoais na era digital. Diante dessa realidade, a análise crítica da eficácia do consentimento como mecanismo de proteção da privacidade é fundamental para entender as dinâmicas atuais da regulação de dados. A problemática central reside na questão: o modelo de consentimento atualmente adotado pelas legislações e a aplicação das práticas de mercado podem, de fato, assegurar a proteção efetiva dos direitos dos titulares de dados.

A concepção tradicional de consentimento, entendida como uma manifestação livre, informada e inequívoca da vontade do indivíduo, enfrenta desafios significativos em sua aplicabilidade prática no contexto digital. As dinâmicas da *internet* e dos

[8] cidadão com conhecimentos considerados comuns.

serviços *online*, caracterizadas por termos de uso complexos e extensos, colocam em xeque a capacidade dos usuários de exercer uma escolha verdadeiramente informada e livre.

A literatura especializada, incluindo as contribuições do autor Bruno Bioni, evidencia as críticas ao modelo de consentimento baseado em uma noção idealizada de autonomia individual.

Inicialmente, a assimetria[9] informacional entre usuários e provedores de serviços *online* compromete a capacidade dos primeiros de compreender plenamente o escopo e as consequências do tratamento de seus dados. Além disso, a prática de 'aceitar ou recusar' um contrato[10], sem a possibilidade de negociação ou personalização, sugere um cenário de 'tudo ou nada'[11] que distancia o consentimento de sua idealização como expressão da liberdade individual e revela o caráter do contrato firmado entre as partes.

De maneira prática, a capacidade da autotutela dos dados pessoais é minada em decorrência desse cenário. O usuário médio não tem conhecimento[12] sobre a amplitude e profundidade da informação coletada por *sites* e aplicativos, nem sobre os múltiplos atores envolvidos na cadeia de tratamento e comercialização desses dados. Essa invisibilidade da coleta e do fluxo de dados cria um ambiente no qual o usuário não pode exercer controle efetivo sobre suas informações pessoais.

Diante das limitações do consentimento enquanto mecanismo de legitimação do tratamento de dados pessoais, emerge a discussão sobre a necessidade de modelos alternativos ou complementares de proteção. A doutrina e as leis regulamentares têm explorado conceitos como o interesse legítimo, a anonimização efetiva e a minimização de dados como formas de equilibrar os interesses em jogo, reduzindo a dependência do consentimento e, por sua vez, mitigando o ônus sobre o indivíduo.

Ainda nessa esteira, a problemática do consentimento na tutela de dados pessoais coloca em evidência as complexidades da governança de informações na sociedade contemporânea. A reflexão crítica sobre as limitações do consentimento e a exploração de mecanismos alternativos de proteção são etapas essenciais para o

---

[9] A assimetria que se pressupõe em qualquer relação advinda de comércio e prestação de serviços.
[10] Os termos de uso são notadamente contratos de adesão.
[11] O usuário que não concorda tem seu acesso cerceado.
[12] Nem se espera que tenha. As informações deveriam ser de fácil compreensão para que os usuários pudessem tomar sua decisão de maneira livre e desimpedida.

desenvolvimento de um quadro normativo que respeite a autonomia do indivíduo, promova a transparência e assegure a efetiva proteção da privacidade e dos dados pessoais. Em última análise, o desafio reside em conceber um sistema de tutela de dados que seja ao mesmo tempo robusto, flexível e adaptado às realidades tecnológicas e sociais em constante evolução.

4.1 PRÁTICAS DE CONSENTIMENTO E TERMOS DE USO

Os mecanismos de consentimento, implementados através de ‘termos de uso’ longos e complexos, sequer são entendidos pelos usuários, por óbvio não são lidos integralmente diante do dinamismo ao qual se encontra inserida a sociedade digital. Em um levantamento realizado pela empresa de auditoria *Deloitte* constatou-se que “91% dos norte-americanos não leem políticas de uso e privacidade. Entre os jovens estadunidenses, a situação consegue ser pior, já que 97% deles fazem o mesmo”. Assim, a autonomia do usuário na gestão de seus dados pessoais é mais teórica do que prática. A empresa britânica *think money* também constatou em sua pesquisa o tempo médio que seria gasto para que o usuário realizasse a leitura efetivamente dos termos de uso. O trabalho demonstra de maneira elucidativa, a plataforma amplamente usada no período pandêmico de 2019, levariam cerca de duas horas e vinte sete minutos.

4.2 LIMITAÇÕES HUMANAS

Do ponto de vista cognitivo, os usuários enfrentam o que é conhecido como ‘fadiga de decisão’ ao navegar na *internet.* A constante necessidade de tomar decisões sobre a aceitação de *cookies*, configurações de privacidade e consentimento para o tratamento de dados é esmagadora, levando a escolhas menos informadas e por consequência o aceite passivo das práticas de coleta de dados. Essa sobrecarga de decisões dificulta a capacidade do usuário de proteger proativamente sua privacidade e dados pessoais. O modelo de negócios predominante na *internet*, que se baseia na coleta, análise e comercialização de dados pessoais para publicidade direcionada e outros fins, incentiva práticas que priorizam a maximização da coleta de dados em detrimento da proteção da privacidade do usuário. Essa lógica de mercado, aliada à dependência dos usuários de serviços digitais gratuitos ou de baixo custo,

cria um ambiente no qual o zelo ativo dos dados pessoais pelo usuário é desestimulado. Nas palavras dos autores Godoi e Araújo:

> O avanço da tecnologia tem proporcionado cada vez mais praticidade e facilidade nas tarefas do dia a dia. A Internet conecta pessoas em todas as partes do mundo, permitindo novas formas de comunicação, fácil acesso à informação e entretenimento. (GODOI e ARAUJO, 2019, p. 20)

Entretanto, cabe a reflexão em relação aos impactos que a praticidade impõe como contraprestação.

Ainda na esfera do impacto que a capacidade cognitiva possui sobre o consentimento, a tendência humana para a gratificação imediata[13]. É um princípio bem documentado na psicologia comportamental. No contexto digital, isso se manifesta na prontidão com que os usuários concedem acesso aos seus dados pessoais em troca de conteúdo gratuito, serviços e conveniências *online*. A promessa de gratificação instantânea obscurece a percepção das implicações a longo prazo, como a perda de privacidade e o potencial uso indevido desses dados.

4.3 DESAFIOS REGULATÓRIOS E DE FISCALIZAÇÃO

Embora legislações como o GDPR e a LGPD representam avanços significativos na proteção de dados pessoais, a aplicação e fiscalização dessas leis enfrentam desafios práticos. Segundo o estudo *IT Trends Snapshot* (2023), da *Logicalis*, “uma empresa global de soluções e serviços de TI, apenas 36% das empresas declararam estar em total conformidade com as regulamentações”. A capacidade das autoridades reguladoras de monitorar e penalizar todas as violações é limitada, e muitos usuários permanecem incertos sobre seus direitos ou os meios pelos quais podem exercê-los efetivamente.

Em pesquisa exclusiva feita pelo Anuário de Direito Empresarial (2023), em que advogados de departamentos jurídicos das maiores empresas do Brasil foram ouvidos a respeito da adequação de suas empresas à LGPD. Embora haja uma percepção majoritária do alto impacto da lei (opinião de 59% dos entrevistados), é relevante o

[13] uma preferência por recompensas presentes em detrimento de benefícios futuros mais significativos

número de executivos que avaliam que as novas regras trouxeram pouco ou nenhum impacto na governança (38%). O que demonstra que a legislação ainda enfrenta desafios quanto a sua aplicabilidade.

4.4 LIMITAÇÕES TÉCNICAS E A COMPLEXIDADE DO AMBIENTE DIGITAL

A infraestrutura da *internet* e das tecnologias digitais é intrinsecamente complexa e opaca para a maioria dos usuários. O funcionamento dos algoritmos, a lógica por trás da coleta de dados através de *cookies* e outras tecnologias de rastreamento, bem como as práticas de mineração e análise de *big* data, são aspectos técnicos que escapam ao entendimento comum. Essa complexidade técnica obstaculiza a capacidade do usuário de compreender como seus dados são coletados, processados e utilizados, dificultando a tomada de decisões informadas sobre sua privacidade *online*.

Porquanto, o modelo de negócios predominante na *internet*, baseado na oferta de serviços ‘gratuitos' em troca de dados pessoais, impõe limitações econômicas significativas à autotutela dos dados. Esse modelo cria uma relação de dependência, na qual os usuários, em busca de serviços digitais acessíveis, acabam por comprometer sua privacidade. A alternativa de optar por serviços pagos que não coletam dados pessoais de maneira invasiva é muitas vezes inviável para uma grande parcela da população, devido a barreiras econômicas.

A soma dessas limitações técnicas, informacionais, jurídicas, cognitivas e econômicas evidencia a complexidade da autotutela de dados pessoais na *internet.* A capacidade do usuário comum de exercer controle efetivo e informado sobre suas informações pessoais é profundamente comprometida, exigindo não apenas intervenções regulatórias robustas, mas também uma reavaliação dos modelos de negócios digitais e das práticas de *design* tecnológico, com o objetivo de restaurar o equilíbrio entre os direitos dos usuários e os interesses comerciais.

A complexidade e a opacidade das operações de tratamento de dados na *internet* contribuem para a dificuldade dos usuários em antecipar e terem a percepção das consequências imediatas de suas escolhas. A coleta, o compartilhamento e a análise de dados pessoais estendem-se além do momento inicial de consentimento, permeando múltiplos aspectos da vida do indivíduo de maneiras que não são

cristalinas ou diretas. Essa invisibilidade das ramificações a longo prazo enfraquece a capacidade do usuário de fazer escolhas informadas e ponderadas.

A avaliação de riscos associados ao compartilhamento de dados pessoais exige não apenas uma compreensão das tecnologias e práticas de coleta de dados, mas também a habilidade de projetar essas informações no futuro para prever possíveis danos. No entanto, o usuário médio, confrontado com a complexidade técnica e a ausência de informações claras e acessíveis, encontra-se em uma posição desvantajosa para realizar essa análise de risco de forma eficaz. A natureza abstrata e difusa dos riscos de privacidade contribui para a subestimação das consequências prejudiciais do compartilhamento de dados.

Empresas e plataformas digitais frequentemente empregam estratégias de *nudging*[14] para incentivar a partilha de dados. Embora essas práticas possam aumentar a usabilidade e a eficiência, elas também podem manipular a tomada de decisão, enfatizando os benefícios imediatos e minimizando a percepção dos riscos associados ao tratamento de dados pessoais. Essa manipulação do consentimento explora a incapacidade do usuário de ponderar adequadamente entre as recompensas imediatas e as consequências futuras. Além disso, por meio da otimização de experiência do cliente, as empresas conseguem direcionar o usuário para atender à vontade sem que ele perceba, como depreende-se do pensamento dos autores Zingales e Bakonyi (2022, p.117) “as pessoas possuem racionalidade limitada e, destarte, a título ilustrativo, são incapazes de assimilar e absorver todas as informações, estão suscetíveis à maneira como as coisas lhes são apresentadas.”

A dificuldade dos usuários em equilibrar a gratificação imediata com os potenciais efeitos invasivos e prejudiciais a longo prazo do compartilhamento de dados pessoais destaca uma vulnerabilidade fundamental na autotutela de dados na *internet*. Para mitigar esse problema, é essencial promover uma maior transparência nas práticas de coleta e uso de dados, implementar abordagens de consentimento mais informadas e desenvolver mecanismos regulatórios e tecnológicos que empoderem os usuários a fazer escolhas mais conscientes e ponderadas sobre seus dados pessoais. Essas medidas, combinadas com esforços contínuos de educação digital e conscientização sobre privacidade, são vitais para fortalecer a capacidade

[14] técnicas de arquitetura de escolha que influenciam sutilmente as decisões do usuário

dos indivíduos de proteger sua informação pessoal em um mundo cada vez mais orientado por dados.

5. CONCLUSÃO

À medida que avançamos na era digital, a questão do consentimento na tutela de dados pessoais emerge como um tema de complexidade e controvérsia sem precedentes, refletindo um embate central entre a autodeterminação individual e as engrenagens de um ecossistema digital intrinsecamente assimétrico e opaco. Esta análise abrangente revela que, apesar dos esforços regulatórios significativos representados pelo GDPR e pela LGPD, o consentimento — enquanto pedra angular da proteção de dados — enfrenta desafios substanciais que comprometem sua eficácia como mecanismo de proteção da privacidade na prática.

A problemática em torno do consentimento é multifacetada, enraizada não apenas nas limitações técnicas e na complexidade do ambiente digital, mas também na dinâmica das relações de poder que favorecem entidades corporativas e tecnológicas em detrimento do indivíduo. A assimetria informacional, uma característica marcante dessas relações, debilita a capacidade do usuário médio de compreender a amplitude, profundidade e consequências do tratamento de seus dados pessoais, minando assim a noção de um consentimento verdadeiramente livre e informado.

Além disso, a prática de solicitar consentimento por meio de termos de uso extensos e complicados — frequentemente aceitos sem uma leitura atenta ou compreensão plena — evidencia um abismo entre a teoria do consentimento informado e sua realização na realidade digital contemporânea. Essa discrepância ressalta a necessidade urgente de repensar o papel do consentimento dentro da arquitetura de proteção de dados, questionando sua posição como o fundamento exclusivo ou predominante para a legitimidade do tratamento de dados pessoais.

Diante dessas reflexões, torna-se evidente que a tutela efetiva de dados pessoais demanda uma abordagem mais holística e multidimensional, que não apenas reconheça, mas efetivamente responda às complexidades impostas pelo cenário digital. Isso implica ir além da simplificação do consentimento e abraçar modelos complementares de proteção de dados que valorizem princípios como a

minimização de dados, a anonimização efetiva, e o interesse legítimo, balanceando de maneira mais justa os interesses em jogo.

Portanto, o desafio que se coloca é o desenvolvimento de um *framework* de proteção de dados que, mantendo o consentimento como um de seus pilares, seja suficientemente ágil para adaptar-se às inovações tecnológicas e suficientemente robusto para garantir a proteção efetiva da privacidade e da autodeterminação informacional dos indivíduos. Neste contexto, a educação digital surge como uma ferramenta indispensável, capacitando os usuários a navegarem o ambiente digital de forma mais consciente e crítica, enquanto estratégias regulatórias e tecnológicas inovadoras — como a privacidade por *design* — oferecem promessas de um futuro em que a tutela de dados pessoais seja verdadeiramente centrada no indivíduo.

Em suma, enquanto navegamos pelas águas turbulentas da era digital, a questão do consentimento na tutela de dados pessoais permanece no cerne do debate sobre como conciliar os avanços tecnológicos com os direitos fundamentais dos indivíduos. Enfrentar esse desafio não é apenas uma questão de adequação legal, mas uma imperativa ética e social que requer um compromisso coletivo para redefinir as normas de proteção de dados em uma sociedade cada vez mais digitalizada. Somente assim poderemos assegurar que o progresso tecnológico sirva ao bem-estar humano, respeitando a dignidade, a liberdade e a privacidade de todos.

REFERENCIAS:

1 ano da GDPR**: o que podemos aprender com os erros e acertos da Europa**. *ConJur*. Disponível em: https://www.conjur.com.br/2019-mai-31/opiniao-podemos-aprender-europa-ano-gdpr/. Acesso em: [02/01/2024].

90% das pessoas não leem termos e condições de apps, revela estudo. *Showmetech*. Disponível em: https://www.showmetech.com.br/pessoas-nao-leem-termos-e-condicoes-de-apps/. Acesso em: [10/03/2024].

ÁVILA, Ana Paula Oliveira; WOLOSZYN, André Luis. **A tutela jurídica da privacidade e do sigilo na era digital: doutrina, legislação e jurisprudência**. *Revista de Investigações Constitucionais*, Curitiba, vol. 4, n. 3, setembro/dezembro 2017. ISSN 2359-5639. Núcleo de Investigações Constitucionais da UFPR.

BELO, Neuza Maria; BRASIL, Haroldo Guimarães. **Assimetria Informacional e Eficiência Semiforte do Mercado**. *Faculdades Pedro Leopoldo, FGV-RJ e Faculdade Pitágoras; Faculdades Pedro Leopoldo e IBMEC-MG*. Artigo recebido em 22 nov. 2005. Aprovado em 11 jun. 2006.

BORDONI, Jovina D'Avila. **A Colisão Entre Liberdade de Expressão e Direitos da Personalidade: Análise do Acórdão** Nº 694.260 do Tribunal de Justiça do Distrito Federal e Territórios. *Tribunal de Justiça do Distrito Federal e Territórios*.

BRASIL. **Código Civil.** Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406.htm. Acesso em: 27 de maio de 2023

BRASIL. **Constituição Federal de 1988.** Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 27 de maio de 2023]

BRASIL. **Lei Geral de Proteção de Dados**. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 27 de maio de 2023

BRASIL. **Marco Civil de Internet.** Disponível em; https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 27 de maio de 2023

DE GODOI, Maiko Gustavo; Araújo, Liriane Soares de. **A Internet das Coisas: evolução, impactos e benefícios**. Faculdade de Tecnologia de Catanduva (FATEC), São Paulo, Brasil, maio de 2019.

DONEDA, Danilo Cesar Maganhoto **Da privacidade à proteção de dados pessoais** [livro eletrônico] : elementos da formação da Lei Geral de Proteção de Dados / Danilo Cesar Maganhoto Doneda. -- 2. ed. -- São Paulo: Thomson Reuters Brasil, 2020.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. São Paulo (SP): Editora Revista dos Tribunais. 2021, Capítulo 1.

Em 5 anos, LGPD tem impacto regulatório, mas efeito prático é duvidoso. *ConJur*. Disponível em: https://www.conjur.com.br/2023-ago-14/anos-lgpd-muda-cultura-abre-horizonte-regulatorio/. Acesso em: [11/02/2024].

ENGLEHARDT, Steven; Narayanan, Arvind. Online Tracking: **A 1-million-site Measurement and Analysis.** Versão estendida do artigo apresentado na ACM CCS 2016. Princeton University. Disponível em: https://www.cs.princeton.edu/~arvindn/publications/OpenWPM_1_million_site_tracking_measurement.pdf. Acesso em: [14/03/2024]

Garantias do Consumo. **A proteção do consumidor digital em face das redes sociais**. *ConJur*. Disponível em: https://www.conjur.com.br/2021-dez-01/garantias-consumo-protecao-consumidor-digital-face-redes-sociais/. Acesso em: [02/03/2024].

LUGATI, Lys Nunes; Almeida, Juliana Evangelista de. **Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa**. *Revista de Direito, Viçosa*, v. 12, n. 02, 2020. ISSN 2527-0389. DOI: 10.32361/2020120210597.

PINHEIRO, P. P. **Direito digital**. 7. ed. São Paulo: Saraiva, 2021. E-book.

PIRES, Gabriel Duarte**. Prerrogativas e Limites no Manuseio dos Dados Pessoais: O Consentimento e suas Implicações**. 2023. 49 f. Trabalho de Conclusão de Curso (Graduação) – Escola de Direito, Negócios e Comunicação, Pontifícia Universidade Católica de Goiás (PUC GOIÁS), Goiânia, 2023.

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

ROCHA, Mariana Thamiris Silva. **Direito Digital e o Marco Civil da Internet: O Posicionamento da Lei 12.965/14 Diante dos Tratados Internacionais no Combate aos Conflitos Virtuais**. 2017. Trabalho de Conclusão de Curso (Bacharelado em Direito) - Centro Universitário Tabosa de Almeida - ASCES/UNITA, Caruaru, 2017.

SOUZA, Diego Chagas de; Lima, João Vitor Sangiacomo Meira. **O alcance do consentimento na proteção de dados pessoais: perspectivas sobre a sociedade de vigilância na era da informação**. *Revista Eletrônica da PJE RJ*, [volume], n. [número], p. [primeira página] - [última página], [ano]. 26p. Recebido em: 13 ago. 2021. 1° parecer em: 18 out. 2021. 2° parecer em: 29 out. 2021.

TATEOKI, Victor Augusto. **A proteção de dados pessoais e a publicidade comportamental**. *Revista Juris UniToledo*, v. 02, n. 01, p. 62-75, jan./mar. 2017, Araçatuba, SP.

TEIXEIRA, T. **LGPD e E commerce**. 2. ed. São Paulo: Saraiva, 2021. E-book.

TUROW, Joseph; Hennessy, Michael; Draper, Nora. **The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation**. Annenberg School for Communication, University of Pennsylvania; Annenberg Public Policy Center, University of Pennsylvania; Department of Communication, University of New Hampshire, Maio de 2015.

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

ZINGALES, Nicolo; BAKONYI, Erica. **Aceitabilidade do nudging: a necessidade de uma resposta multidimensional.** Direitos Fundamentais & Justiça, Belo Horizonte, ano 16, p. 115-143, out. 2022. Número especial.