CENTRO UNIVERSITÁRIO FAEMA – UNIFAEMA

NATHAN IGOR DIAS FURLAN

BANALIZAÇÃO DO CONSENTIMENTO NO TRATAMENTO DE DADOS

ARIQUEMES - RO
2023

NATHAN IGOR DIAS FURLAN

BANALIZAÇÃO DO CONSENTIMENTO NO TRATAMENTO DE DADOS

Trabalho de Conclusão de Curso apresentado ao curso de Direito do Centro Universitário FAEMA – UNIFAEMA como pré-requisito para obtenção do título de bacharel em Direito.

Orientador (a): Prof. Me. Everton Balbo dos Santos.

ARIQUEMES - RO
2023

FI

FICHA CATALOGRÁFICA
Dados Internacionais de Catalogação na Publicação (CIP)

F985b Furlan, Nathan Igor Dias.
Banalização do consentimento no tratamento de dados. / Nathan Igor Dias Furlan. Ariquemes, RO: Centro Universitário Faema – UNIFAEMA, 2023.
60 f.

Orientador: Prof. Me. Everton Balbo dos Santos.
Trabalho de Conclusão de Curso – Graduação em Direito – Centro Universitário Faema – UNIFAEMA, Ariquemes/RO, 2023.

1. Direito Digital. 2. Consentimento. 3. Privacidade. 4. Proteção de dados. I. Título. II. Santos, Everton Balbo dos.

CDD 340

Bibliotecária Responsável
Herta Maria de Açucena do N. Soeiro
CRB 1114/11

NATHAN IGOR DIAS FURLAN

BANALIZAÇÃO DO CONSENTIMENTO NO TRATAMENTO DE DADOS

Trabalho de Conclusão de Curso apresentado ao curso de Direito do Centro Universitário FAEMA – UNIFAEMA como pré-requisito para obtenção do título de bacharel em Direito.

Orientador (a): Prof. Me. Everton Balbo dos Santos.

BANCA EXAMINADORA

Assinado digitalmente por: Camila Valera Reis Henrique
Razão: Professora Responsável pelo Documento
Localização: Ariquemes/UNIFAEMA
O tempo: 16-06-2023 15:22:59

Prof.ª Ma. Camila Valera Reis Henrique
Centro Universitário FAEMA – UNIFAEMA

Assinado digitalmente por: Everton Balbo dos Santos
Razão: Sou Responsável pelo Documento
Localização: UNIFAEMA - Ariquemes/RO

Prof. Me. Everton Balbo dos Santos
Centro Universitário FAEMA – UNIFAEMA

Assinado digitalmente por: Hudson Carlos Avancini Persch
Razão: Sou Responsável pelo Documento
Localização: UNIFAEMA - Ariquemes/RO
O tempo: 16-06-2023 15:53:55

Prof. Me. Hudson Carlos Avancini Persch
Centro Universitário FAEMA – UNIFAEMA

ARIQUEMES – RO
2023

RESUMO

Esta pesquisa teve como objetivo analisar a banalização do consentimento pelas políticas de privacidade no contexto do tratamento de dados sob a ótica da legislação brasileira. A pesquisa utilizou o método hipotético-dedutivo, com abordagem qualitativa teórica descritiva, dimensionando a extensão e natureza do problema mediante revisão bibliográfica da doutrina e ordenamento jurídico vigente, explicando como é promovida a proteção de dados no Brasil e suas particularidades. O presente trabalho abordou questões relativas à conceitualização de tecnologia e privacidade, os riscos do tratamento de dados e a demanda regulatória pela proteção de dados, e a banalização do consentimento. Verificou-se que apesar de a legislação estabelecer que o consentimento deva ser adquirido com a exposição transparente, clara e inequívoca das políticas de privacidade, isso não ocorre na prática. Redes sociais e aplicativos de aparelhos móveis coletam dados de seus usuários e os utilizam para personalização de anúncios sem seu conhecimento. Foi observado que os elementos instituídos pela Lei Geral de Proteção de Dados ainda não são universalmente aplicados e respeitados, em vista de que o consentimento é colhido mediante a apresentação de termos longos e complexos, e o indivíduo, constrangido, acaba utilizando tais produtos e serviços aceitando quaisquer condições, efetivando a banalização do consentimento.

Palavras-chave: consentimento; direito digital; privacidade; proteção de dados.

ABSTRACT

This research aimed to analyze the trivialization of consent by privacy policies in the context of data processing from the perspective of Brazilian legislation. The research used the hypothetical-deductive method, with a descriptive theoretical qualitative approach, measuring the extent and nature of the problem through a bibliographical review of the current doctrine and legal system, explaining how data protection is promoted in Brazil and its particularities. The present work addressed issues related to the conceptualization of technology and privacy, the risks of data processing and the regulatory demand for data protection, and the trivialization of consent. It was found that although the legislation establishes that consent must be acquired with the transparent, clear and unambiguous exposure of privacy policies, this does not occur in practice. Social networks and mobile device applications collect data from their users and also use it to customize ads without their knowledge. It was observed that the elements established by the General Data Protection Law are not yet universally applied and respected, given that consent is collected by presenting long and complex terms, and the individual, embarrassed, ends up using such products and services accepting any conditions, effecting the trivialization of consent.

Keywords: consent; digital law; privacy; data protection.

SUMÁRIO

1 INTRODUÇÃO

A presente pesquisa discutirá acerca do instituto do consentimento no âmbito do tratamento de dados e sua banalização ao longo do desenvolvimento das políticas de privacidade modernas.

O tema foi escolhido em vista do crescente debate concernente à proteção da privacidade na era digital, levando em consideração as práticas de organizações públicas e privadas mundo afora. É necessário que juristas e a sociedade em geral estejam atentos a essas mudanças e trabalhem juntos para desenvolver novas estratégias e soluções para proteger a privacidade dos indivíduos.

A informação é coletada por meio de técnicas de monitoramento e auxilia na criação de um perfil detalhado do titular dos dados. A coleta e tratamento desses dados permite individualizar os usuários na vasta rede mundial de computadores, o que pode ter implicações negativas em termos de privacidade e segurança. Essa exposição indesejada de informações pessoais pode ocorrer em diversas situações sem o consentimento do titular.

Desta feita, a problemática que orbita ao tema é diretamente relativa aos conceitos de privacidade e consentimento. Afinal, quais são os riscos advindos do tratamento de dados? Estaria o consentimento sendo banalizado em detrimento à exploração da informação?

A primeira seção deste trabalho abordará características estruturantes de um novo modelo de sociedade que, em um paralelo ao *commodities* do passado, possui em seu centro a informação. Nesta mesma linha, se buscará o conceito de privacidade e a relação deste direito fundamental com a proteção de dados e as novas tecnologias da informação. Após, será abordada a relevância jurídica da informação e explorado como o tratamento de dados lhe fornece valor econômico.

A segunda seção discutirá quanto aos riscos que o tratamento de dados impõe aos titulares dos dados pessoais, e como esta realidade promoveu a demanda por institutos regulatórios e consequente criação de leis. Nesta seção também serão feitas algumas considerações no que toca à Lei Geral de Proteção de Dados. Ademais, se realizará uma breve abordagem no que toca aos princípios gerais do tratamento de dados.

Na terceira e última seção desta pesquisa, se fará uma abordagem em relação à conceituação legal e doutrinária do consentimento, sua importância para o

contexto do tratamento e proteção de dados. Ao fim, se discutirá sobre a banalização do consentimento ante à exploração econômica da informação.

A abordagem a ser utilizada será o método hipotético-dedutivo. A pesquisa será qualitativa teórica descritiva, tendo como objetivo dimensionar a extensão da natureza do problema mediante revisão bibliográfica da doutrina e legislação vigente, explicando como o ordenamento jurídico brasileiro promove a proteção de dados e suas particularidades, assim como abordar a hipotética banalização do consentimento.

Dentre as hipóteses alavancadas, o Brasil se encontra preparado para promover uma proteção de dados eficaz, havendo formalizado políticas públicas e delimitado órgãos de fiscalização para observar o devido cumprimento da Lei Geral de Proteção de Dados. Ademais, a jurisprudência e a administração pública trabalham rigorosamente a fim de combater o uso indevido de dados e o respeito ao consentimento.

Por outro lado, o Brasil hipoteticamente se encontra defasado para promover uma proteção de dados, e, inobstante tenha recentemente criado legislação própria ao tema, não buscou implementar o efetivo cumprimento de suas disposições. A legislação brasileira, por mais que seja moderna, é ineficaz em comparação a seus pares, e em decorrência de sua má implementação o consentimento é desrespeitado diariamente pela extensiva utilização de políticas de privacidade ambíguas.

2 SOCIEDADE DA INFORMAÇÃO

O ilustre professor Bruno Ricardo BIONI (2019, p 34) aduz que as pessoas atualmente vivem naquilo que chama de “sociedade da informação”, na qual “[...] informação é o (novo) elemento estruturante que (re)organiza a sociedade, tal como o fizeram a terra, as máquinas a vapor e a eletricidade [...].”

Conforme explicita DONEDA (2020, p. 56), em seu primórdio, a *internet* foi desenvolvida como um sistema de compartilhamento de informações dedicado a aplicações governamentais e comerciais. O principal distintivo desse sistema era a sua impressionante capacidade de permitir a comunicação entre dois ou mais computadores em uma velocidade e distância até então sem precedentes.

Com o passar do tempo, a *internet* passou por uma evolução significativa e se tornou uma plataforma global para a interação humana, tornando-se cada vez mais acessível, permitindo que pessoas de todo o mundo se conectem e compartilhem informações de maneira cada vez mais eficiente.

> O surgimento da rede internet, por exemplo, decididamente alargou as possibilidades de comunicação e fez emergir um grande número de questões ligadas à privacidade. O impacto que a rede proporcionou, porém, já se encontrava de certa forma incubado em tecnologias anteriores, que provocaram fenômenos assemelhados e que, se hoje podem até parecer pálidos, devem ser considerados em relação ao que representaram à sua época – afinal, são justamente impressões como essas que o suceder das gerações costuma apagar da memória de uma sociedade. (DONEDA, 2020, p. 55-56).

Vários fatores foram relevantes no que concerne ao aumento da acessibilidade à *internet*, como o surgimento de sistemas operacionais desenvolvidos especialmente para uso doméstico, a implementação de interfaces mais intuitivas e a popularização dos computadores.

Nos dias atuais, a *internet* tornou-se presente no cotidiano de bilhões de pessoas ao redor do mundo, que a utilizam para diversos fins, desde pesquisas em motores de busca até o acesso aos seus canais favoritos em plataformas de vídeos.

> [...] a evolução da área em conjunto com a indústria das telecomunicações, notadamente da telefonia móvel, tornou a Internet acessível em escala quase planetária, assim como a presença explosiva da computação pervasiva deu lugar ao conceito de computação ubíqua, ou seja, a onipresença dos recursos relacionados ao processo de criação, produção,

> armazenamento, compartilhamento e uso da informação. (SILVA; CARDOSO; PINHEIRO, 2021, p. 03) .

Além disso, é comum que as pessoas se comuniquem com seus familiares e amigos por meio de aplicativos de mensagens instantâneas e redes sociais. Tudo isso foi alavancado pelos avanços tecnológicos que permitiram o desenvolvimento de smartphones e outros dispositivos de computação portáteis.

Por meio dos smartphones, as pessoas podem acessar a *internet* de forma ainda mais rápida e fácil, permitindo que elas realizem diversas atividades enquanto se deslocam de um lugar para outro. (SILVA; CARDOSO; PINHEIRO, 2021, p. 03)

Consoante BIONI (2019, p. 127), inobstante a *internet* e a tecnologia tenham trazido inúmeras vantagens e benefícios para nossas vidas diárias, também é indispensável estar ciente dos desafios e riscos associados ao seu uso. As ações realizadas pelos usuários na *internet* geram uma grande quantidade de informações e dados que podem ser utilizados para determinar suas preferências, opiniões políticas e outras características pessoais.

> A sociedade da informação imprime uma nova dinâmica e novos desafios para a proteção da pessoa humana, a começar pela monetização dos seus dados pessoais. Tais dados, além de consolidar uma nova forma de prolongamento da pessoa, passam a interferir em sua própria esfera relacional, reclamando, por isso, uma normatização específica que justifica dogmaticamente a autonomia do direito à proteção dos dados pessoais e os desdobramentos da sua tutela jurídica (e.g., direito de acesso e retificação dos dados e oposição a decisões automatizadas, em especial de práticas discriminatórias). (BIONI, 2019, p. 127-128).

Ante o exposto, é pertinente salientar que a privacidade e o sigilo de comunicações e dados são considerados direitos fundamentais, conforme dita a Constituição Federal em seu artigo 5º, incisos X e XII:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> [...]
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> [...]
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer

> para fins de investigação criminal ou instrução processual penal; [...]. (BRASIL, 1988).

Ademais, a Lei Geral de Proteção de Dados estabelece em seu artigo 2º, incisos I, IV e VIII que:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> [...]
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> [...]
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (BRASIL, 2018).

Consoante MULHOLLAND (2018, p. 171), "[...] pode-se compreender, por meio de uma leitura funcionalizada da Constituição Federal e de seus princípios e valores, que a tutela da privacidade é o locus constitucional da proteção dos dados pessoais."

Mas apesar dos riscos, ao utilizar serviços online, como redes sociais, plataformas de vídeo e aplicativos de mensagens, os usuários frequentemente concordam com os termos e condições de uso sem ler cuidadosamente as cláusulas que tratam da coleta e uso de seus dados pessoais. Essa aceitação tácita permite que as empresas coletem e utilizem as informações dos usuários para diversos fins.

> Cada vez mais, os usuários da Internet subvertem-se em consumidores, sendo uma clara amostra de tal afirmação o crescimento exponencial do comércio eletrônico. No Brasil, o e-commerce acumula taxas de crescimento significativas, tendo faturado a quantia expressiva de R$ 44,4 bilhões no ano de 2016. Assim, cresce, em igual importância, os anúncios publicitários on-line para induzir o usuário ao consumo. (BIONI, 2019, p. 43).

Estas informações coletadas, porém, poderão ser compartilhadas com terceiros, sem o conhecimento do usuário. Isso pode resultar em violações de privacidade e segurança, especialmente quando as informações compartilhadas incluem dados pessoais sensíveis, como informações bancárias, endereços e números de telefone.

> Informações pessoais estão cada vez mais vulneráveis na atual economia digital, especialmente nas redes sociais e nos cadastros de organizações que atuam virtualmente. Limitar o acesso aos dados pessoais por parte de terceiros depende muitas vezes do usuário, mas tem considerável influência

> da organização proprietária da rede social para manter a segurança do titular da informação. (PIURCOSKY et al., 2019, p. 90).

Portanto, embora as empresas de tecnologia e publicidade tenham a responsabilidade de proteger os dados dos usuários, é importante que os próprios usuários também tomem medidas para proteger sua privacidade online. Isso inclui ler cuidadosamente os termos e condições de uso dos serviços online, limitar a quantidade de informações pessoais compartilhadas publicamente e utilizar ferramentas de privacidade.

> A ampliação do conceito de privacy se deu, em grande medida, por conta da evolução das formas de divulgação e apreensão de dados pessoais. Com o advento de novas tecnologias, notadamente o desenvolvimento da biotecnologia e da Internet, o acesso a dados sensíveis e, consequentemente, a sua divulgação, foram facilitados de forma extrema. Como resultado, existe uma expansão das formas potenciais de violação da esfera privada, na medida em que se mostra a facilidade por meio da qual é possível o acesso não autorizado de terceiros a esses dados. Com isso, a tutela da privacidade passa a ser vista não só como o direito de não ser molestado, mas também como o direito de ter controle sobre os dados pessoais e, com isso, impedir a sua circulação indesejada. (MULHOLLAND, 2018, p. 172-173).

Em razão disso, é importante que os usuários estejam cientes do que são os metadados e como eles podem ser usados pelas empresas de tecnologia e publicidade. Além do mais, é fundamental que as empresas sejam transparentes sobre o uso de metadados e adotem medidas de segurança para proteger as informações pessoais dos usuários. De acordo com MULHOLLAND (2018, p. 164), “[...] os dados devem ser tratados para determinados propósitos, que devem ser informados ao titular de dados previamente, de maneira explícita e sem que seja possível a sua utilização posterior para outra aplicação.”

> Apesar da capacidade de comunicação promovida pela internet, os interesses corporativos acabam levando a política para outro lado, algo que Morozov (2018) indica como “fim da política”. A digitalização da vida promove uma contínua privação da posse das atividades do dia-a-dia, que acabam transformando a vida cotidiana em mercadoria, havendo um labor produtivo para essas grandes empresas no simples ato de se estar conectadas às redes. (FORNASIER; KNEBEL, 2021, p. 1011).

Para o jurista Danilo DONEDA (2020, p. 164), a temática da privacidade passou a se concentrar cada vez mais na proteção da informação e, mais especificamente, dos dados pessoais, e por meio da “[...] proteção de dados

pessoais, garantias [...] relacionadas com a privacidade passam a ser vistas em uma ótica mais abrangente, pela qual outros interesses devem ser considerados [...]" (Ibid., p. 164), portanto, ao lidar com questões relacionadas à privacidade e proteção de dados pessoais, é fundamental que o operador do Direito leve em consideração não apenas a violação direta da privacidade, mas também os interesses mais amplos envolvidos.

2.1 PRIVACIDADE E TECNOLOGIA

Indivíduos confiam informações pessoais às empresas diariamente, esperando que esses dados sejam mantidos em segurança e protegidos de acessos não autorizados. Essa confiança é estabelecida a partir de uma relação de confiança entre o indivíduo e a empresa, na qual o indivíduo acredita que as informações confiadas serão tratadas com responsabilidade e não serão compartilhadas com terceiros sem sua permissão. (SILVA; CARDOSO; PINHEIRO, 2021, p. 03)

No entanto, a crescente ameaça de violação de dados e o aumento da exposição pública de casos de compartilhamento inadequado de informações pessoais levantaram preocupações sobre a privacidade no contexto de proteção de dados.

> Em retrospecto, por difícil que seja cristalizar a problemática da privacidade em um único conceito, é, no entanto, razoavelmente natural constatar que ela sempre foi diretamente condicionada pelo estado da tecnologia em cada época e sociedade. Podemos, inclusive, aventar a hipótese de que o advento de estruturas jurídicas e sociais que tratem do problema da privacidade são respostas diretas a uma nova condição da informação, determinada pela tecnologia. (DONEDA, 2020, p. 57).

Empresas que coletam e armazenam informações pessoais devem ser transparentes sobre suas políticas de privacidade, e garantir que seus clientes estejam plenamente informados sobre como seus dados serão usados e protegidos. Além disso, as empresas devem adotar medidas eficazes de segurança cibernética para proteger as informações de acessos não autorizados e adotar práticas responsáveis de compartilhamento de dados, obtendo consentimento explícito dos indivíduos antes de compartilhar suas informações com terceiros.

É necessário esclarecer que a variedade de terminologias utilizadas pela doutrina brasileira para representar "privacidade", sendo frequentemente utilizados

outros termos, como: vida privada, intimidade, segredo, sigilo, recato, reserva e intimidade da vida privada.

De acordo com MULHOLLAND (2018, p. 172) conceito tradicional de privacidade se refere à ideia de que uma pessoa tem o direito de manter informações sobre si mesma em segredo, impedindo que terceiros tenham acesso a essas informações sem seu consentimento. Essa reserva de informação é vista como um aspecto fundamental da privacidade, permitindo que as pessoas controlem quais informações pessoais são compartilhadas com outras pessoas ou organizações.

> Este conceito habitual de privacidade está, contudo, superado. Se, tradicionalmente, o direito à privacidade (*right to privacy*) está associado ao direito de ser deixado só, contemporaneamente pode-se afirmar que a privacidade evoluiu para incluir em seu conteúdo situações de tutela de dados sensíveis, de seu controle pelo titular e, especialmente, de "respeito à liberdade das escolhas pessoais de caráter existencial". (MULHOLLAND, 2018, p. 172, apud LEWICK, 2003, p. 09).

Em suma, o conceito de privacidade é complexo e multifacetado, abrangendo diferentes aspectos da vida pessoal. A reserva de informação é um aspecto central da privacidade, mas a privacidade também inclui outras dimensões importantes que devem ser consideradas e protegidas para garantir que as pessoas possam desfrutar de seus direitos e liberdades fundamentais.

O professor e jurista especializado em proteção de dados e privacidade, Danilo DONEDA (2020, p. 31), entende que, por vezes, pode acontecer de nos depararmos com situações em que há uma discrepância entre o significado de um conceito e o que ele representa na prática. É nesse contexto que deve ser examinada a "defasagem" existente para compreender como a noção de privacidade se desenvolveu e evoluiu ao longo do tempo, juntamente com outros elementos, para dar origem à proteção de dados pessoais.

Na mesma linha de pensamento, o jurista aduz que a privacidade tem sido vista de diferentes maneiras ao longo da história, dependendo do contexto social e cultural em que se encontra. Inicialmente, a privacidade era associada principalmente à proteção da intimidade física e do espaço pessoal. Com o tempo, à medida que a sociedade evoluiu e novas tecnologias surgiram, a privacidade passou a incluir questões relacionadas à proteção de informações pessoais, tais como registros médicos, financeiros e dados biométricos.

A partir dessa evolução conceitual, a proteção de dados pessoais tornou-se uma questão central em todo o mundo. Hoje, a privacidade é vista como um direito fundamental, e muitos países adotaram leis e regulamentos específicos para proteger as informações pessoais dos indivíduos (Ibid., p. 31). Essas leis estabelecem padrões para a coleta, uso, armazenamento e compartilhamento de dados pessoais, bem como para a notificação e consentimento do usuário.

No entanto, posto isto, é interessante salientar que o jurista acredita que a defasagem entre o conceito e a realidade da privacidade ainda é um desafio contínuo que exige a revisão constante dos padrões regulatórios e o fortalecimento das práticas de proteção de dados pessoais.

> [...] as raízes e normas de privacidade são baseadas em estruturas sociais. O limite do compartilhamento de informações recai [...] em quem confiamos. Isso implica na existência de uma responsabilidade fiduciária daquele a quem foram compartilhadas as informações; por exemplo. confiamos que bancos, [...] seguradoras de saúde, dentre outros, não fornecerão acesso aos nossos dados para alguém sem nossa permissão explícita. Em todas estas situações, o compartilhamento da informação é necessário e nossa confiança nos receptores é inerente, no entanto, nós a fornecemos em contextos específicos. (SHARMA, 2020, p. 05, tradução nossa).

A falta de uma definição clara para a privacidade não é exclusividade da doutrina brasileira e do civil law. Mesmo a doutrina norte-americana, que possui um termo de certa forma consolidado (*privacy*), abrange diversas situações que podem não ser relacionadas à privacidade pelos juristas oriundos de demais sistemas adeptos ao common law, como o Reino Unido. No Brasil, por sua vez, o ordenamento jurídico brasileiro contempla a privacidade como um direito fundamental. (DONEDA, 2020, p. 77)

A Constituição Federal brasileira de 1988 estabeleceu a proteção da intimidade e da vida privada como garantias e direitos fundamentais em seu artigo 5º, juntamente à proteção da honra e da imagem, valores que a Lei Geral de Proteção de Dados também adotou em seu artigo 2º. A utilização destes termos deixa claro que o legislador desejou incorporar esses aspectos à proteção da pessoa humana, cabendo ao intérprete determiná-los. (DONEDA, 2020, p. 79)

Atualmente, as demandas que definem o perfil da privacidade são diferentes das que foram no passado. Estas novas demandas estão intimamente relacionadas com a tecnologia e a informação pessoal. A exposição não desejada de informações pessoais hoje ocorre com mais frequência por meio da divulgação de informações

pessoais na rede mundial de computadores, em contraste a métodos mais antigos como a intrusão residencial ou violação de correspondência. (DONEDA, 2020, p. 25)

Além disso, muitos sites e aplicativos coletam informações pessoais dos usuários sem seu conhecimento explícito ou consentimento. A localização geográfica, histórico de navegação e preferências pessoais são apenas alguns exemplos das informações que podem ser coletadas sem o conhecimento do usuário. (DONEDA, 2020, p. 25)

Ademais, esses dados podem ser usados pelas próprias empresas para direcionar anúncios personalizados, mas também podem ser vendidos para terceiros sem o conhecimento ou consentimento dos usuários. Esse tipo de coleta de dados sem consentimento explícito tem sido objeto de preocupação crescente em relação à privacidade.

> [...] as redes sociais acumulam os mais diversos dados pessoais dos seus usuários, que são extraídos ao longo de toda a sua interação com a aplicação. Uma vez logado, o usuário passa a fornecer um rico perfil de si, que é o que viabiliza o direcionamento da publicidade. (BIONI, 2019, p. 44).

Via de regra, ao longo da história da humanidade o Estado foi considerado a maior ameaça à privacidade, que nem sempre foi um direito. Hodiernamente, entretanto, o setor privado também compartilha esta característica, havendo se tornado um perigo em potencial.

> O potencial perigo para a privacidade dos cidadãos, representado inicialmente pelo Governo, deu lugar a outra ideia segundo a qual o setor privado representaria uma ameaça ainda maior. Permanecem, latentes e plausíveis, porém, as hipóteses de rastreamento e controle invisível por parte do governo como perigo potencial para um futuro, que inclusive pode tomar proporções trágicas caso sociedades totalitárias tenham acesso às tecnologias necessárias. (DONEDA, 2020, p. 37-38)

O fato de que a privacidade e a proteção de dados pessoais se tornaram temas recorrentes na agenda do direito é resultado de uma orientação estrutural do ordenamento jurídico, que busca garantir a proteção dos direitos fundamentais. Nesse contexto, o desenvolvimento tecnológico é um fator chave na definição de novos espaços que requerem regulamentação jurídica. (DONEDA, 2020, p. 44)

Os desafios relacionados à privacidade e proteção de dados pessoais exigem uma compreensão tanto da tecnologia quanto do seu impacto na sociedade. É essencial que os juristas tenham conhecimentos técnicos e teóricos sólidos para

abordar essas questões complexas. Isso inclui entender como a tecnologia opera e influencia a sociedade em diferentes níveis.

Nas relações jurídicas que envolvem a tecnologia, há um alto grau de incerteza e complexidade que torna a regulação jurídica um desafio significativo. Ainda assim, é fundamental que o direito se adapte aos avanços tecnológicos e busque formas de proteger os direitos fundamentais dos indivíduos no ambiente digital. (DONEDA, 2020, p. 44-45)

Os desafios envolvidos na regulamentação de tecnologias emergentes e sua relação com a proteção de dados pessoais exigem um esforço conjunto de vários setores da sociedade, incluindo governos, empresas, especialistas em tecnologia e juristas. A colaboração entre esses grupos é essencial para garantir que a regulamentação seja eficaz e proteja os direitos dos indivíduos no ambiente digital.

> A utilização da matéria-prima do comportamento humano é o que Couldry e Mejias (2018, p. 2-10) denominam “colonialismo dos dados”, pois a mercantilização dos dados combina o comportamento predatório do colonialismo — ao expropriar informações diretas das vidas das pessoas com os métodos abstratos de quantificação da computação — com efeitos transnacionais — sendo que os cidadãos do sul global restarão em mais ampla dependência de acordo com maiores taxas de extração de mais-valor, enquanto o retorno é menor ainda em relação aos cidadãos dos centros produtivos das big tech. (FORNASIER; KNEBEL, 2021, p. 1014)

A privacidade é um conceito complexo que sempre esteve intimamente relacionado com o estado da tecnologia em cada época e sociedade. Mediante análise, é possível verificar que a tecnologia tem sido um dos principais condicionantes da privacidade ao longo da história, uma vez que novas tecnologias podem criar novas formas de exposição ou de proteção da informação pessoal.

Para DONEDA (2020, p. 57), é possível aventar a hipótese de que o surgimento de estruturas jurídicas e sociais voltadas para a proteção da privacidade é uma resposta direta à nova condição da informação determinada pela tecnologia. Com a evolução das tecnologias de comunicação e informação, houve uma explosão de dados pessoais sendo coletados, processados e compartilhados em diferentes contextos, criando novas preocupações e desafios para a privacidade.

2.2 INFORMAÇÃO COMO BEM JURÍDICO

O discurso sobre a privacidade vem mudando ao longo do tempo, e cada vez mais se concentra em questões relacionadas aos dados pessoais e à informação. Atualmente, o que diferencia a informação de seu significado histórico é a maior facilidade na sua manipulação, que se estende desde a sua coleta e tratamento até a sua comunicação. A tecnologia tem um papel fundamental nesse processo, já que, ao incrementar a capacidade de armazenamento e comunicação de dados, amplia-se também a variedade de formas pelas quais a informação pode ser coletada, usada e apropriada. (DONEDA, 2020, p. 140)

Com isso, a informação passa a ser cada vez mais relevante em diversos aspectos da vida cotidiana, seja em relações comerciais, políticas ou sociais. Além disso, a crescente utilidade da informação aumenta suas possibilidades de influir na vida das pessoas, tornando-se um elemento fundamental para um crescente número de atividades.

No entanto, a informação pode estar objetivamente vinculada a uma pessoa, ou seja, pode revelar algo sobre ela e estar diretamente relacionada às suas características ou ações. Essa relação pode ser estabelecida de acordo com a lei, como no caso do nome civil ou do domicílio, que são informações que estão ligadas à pessoa de forma clara e objetiva. Além disso, informações provenientes de seus atos, como dados referentes ao seu consumo, também podem estar vinculados a uma pessoa de forma objetiva. (Ibid., p. 141)

A Lei Geral de Proteção de Dados define alguns tipos de dados, dentre outros conceitos relevantes:

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
> [...]
> XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo; (BRASIL, 2018).

Uma informação também pode se referir a uma pessoa indeterminada, se transformando em um dado anônimo, uma ferramenta útil para várias finalidades nas quais a informação referente a uma determinada coletividade ou grupo específico de indivíduos é valorizada, mas sem a necessidade de identificar as pessoas às quais se refere. Para DONEDA (2020, p. 142) “A chamada “anonimização” de dados pessoais [...] é um recurso que algumas leis de proteção utilizam para diminuir os riscos presentes no seu tratamento.”

Ainda segundo o mesmo autor (Ibid., p. 142-143), o desenvolvimento da matéria dependeu amplamente da figura do banco de dados, que desempenha um papel fundamental na organização e no armazenamento de informações de diferentes tipos e fontes. Os bancos de dados consistem em conjuntos de informações organizadas segundo uma determinada lógica.

Um banco de dados pode ser manual, mas o informatizado tem “[...] potencial antes inimaginável: é capaz de armazenar um grande volume de informações, de processá-las rapidamente, agregá-las e combiná-las dos mais diversos modos [...]” (Ibid., p. 143). Sua importância se tornou tamanha ao ponto de se tornar o elemento catalisador de um novo perfil de utilização de informações, levando grande parte das normas e procedimentos de proteção de dados a se concentrarem especificamente na regulação desse tipo de sistema.

Nesta linha de pensamento, o jurista aduz que essa ênfase na proteção de dados em bancos de dados reflete a crescente importância desses sistemas no mundo moderno, onde grandes volumes de dados são coletados, armazenados e processados por empresas, organizações governamentais e outras entidades. Com o aumento da quantidade de dados pessoais coletados, como informações de identificação pessoal, informações financeiras e médicas, a necessidade de proteger esses dados se torna cada vez mais importante.

No entanto, em vista do desenvolvimento da tecnologia e maturação da matéria, foi averiguada a necessidade de se abordar diretamente os dados pessoais, mesmo quando estes não estejam vinculados a um banco de dados.

> O conceito de banco de dados viria a perder a centralidade, o que fica mais claro quando verificamos que diversas modalidades de tratamento de dados pessoais não podem ser mais compreendidas a partir de grandes repositórios de informação, mas, sim, pelas técnicas utilizadas para sua coleta, agregação e utilização. (Ibid., p. 143).

A prática do direito da informação tem desencadeado uma série de discussões em torno da proteção de informações pessoais, dando origem a uma categoria específica de dados conhecidos como dados sensíveis. Esses dados referem-se a determinados tipos de informações que, caso sejam conhecidas e submetidas a tratamento, podem se prestar a uma potencial utilização lesiva e, por isso, apresentam maiores riscos potenciais do que outros tipos de informação. (Ibid., p. 144)

Dentre os dados sensíveis, destacam-se informações relacionadas à raça, credo político ou religioso, opções sexuais, histórico médico ou dados genéticos de um indivíduo. Esses tipos de informação têm o potencial de serem usados para discriminação, preconceito ou tratamentos injustos, e, por essa razão, sua coleta, armazenamento e uso devem ser tratados com cuidado especial e estritas medidas de segurança.

Neste ínterim, DONEDA (Ibid., p. 144-145) entende que há um desafio importante em relação à proteção de dados sensíveis: encontrar um equilíbrio entre a necessidade de proteger a privacidade das pessoas e o uso legítimo dessas informações por organizações que desempenham funções essenciais em nossa sociedade. A mera proibição da coleta e tratamento de dados sensíveis pode não ser uma solução viável, no entanto, é importante destacar que a coleta e o uso de dados sensíveis devem ser justificados e proporcionais.

O regime adotado em relação aos dados sensíveis pode variar de acordo com as concepções adotadas em cada ordenamento jurídico. A diferenciação conceitual dos dados sensíveis tem como objetivo estabelecer uma área em que a probabilidade de utilização discriminatória da informação é potencialmente maior. No entanto, é necessário reconhecer que há situações em que a discriminação pode ocorrer sem a utilização de dados sensíveis. Ademais, em algumas circunstâncias, o uso de dados sensíveis pode ser justificado para fins legítimos e lícitos. (Ibid., p. 145)

Neste diapasão, o autor afirma a existência de uma corrente doutrinária que defende o reconhecimento de um direito de propriedade sobre os dados pessoais como uma solução para o problema da proteção de dados. Essa corrente entende que a criação de um mercado para esses bens seria uma maneira eficiente de lidar

com a coleta e o uso de dados pessoais, utilizando mecanismos da teoria econômica para otimização de custos e benefícios.

Segundo essa perspectiva, a propriedade dos dados pessoais seria um direito exclusivo do indivíduo, que poderia decidir como e com quem compartilhar suas informações em troca de benefícios econômicos. Dessa forma, os indivíduos teriam mais controle sobre seus dados pessoais e poderiam negociar o uso dessas informações com empresas e outras organizações, garantindo que seus interesses fossem levados em conta.

No entanto, essa abordagem também é controversa, pois muitos argumentam que os dados pessoais não são bens tangíveis e não podem ser tratados como tal.

> Considerar a informação como um bem jurídico e estender a tutela de caráter patrimonial para os dados pessoais, no entanto, não parece uma solução adequada, em vista da multiplicidade de situações e interesses presentes em torno dos dados pessoais, que não se limitam a vetores patrimoniais e que seriam irremediavelmente prejudicados se considerados apenas – ou majoritariamente – a partir de seu valor econômico. (Ibid., p. 145-146).

Mas a questão vai além de uma mera discussão sobre a natureza jurídica dessas informações. O problema central é encontrar uma maneira eficaz de abordar a questão do tratamento e uso de dados pessoais dentro do ordenamento jurídico (Ibid., p. 146), de forma que os interesses envolvidos sejam devidamente considerados e respeitados.

De acordo com DONEDA (Ibid., p. 146-147), “Por força do regime privilegiado de vinculação entre a informação pessoal e a pessoa à qual ela se refere [...], tal informação deve ser entendida, portanto, como uma extensão da sua personalidade.”

Isso envolve a identificação clara dos valores em jogo na proteção de dados pessoais, como a privacidade, a autonomia e a dignidade humana. É preciso também considerar as diferentes formas de tratamento de dados pessoais, desde a coleta até a utilização e compartilhamento, bem como os diferentes tipos de organizações que podem ter acesso a esses dados, como empresas, governos, instituições de pesquisa, entre outros.

3 RISCOS DO TRATAMENTO DE DADOS E DEMANDA REGULATÓRIA

Segundo TEFFÉ e VIOLA (2020, p. 02), a Lei Geral de Proteção de Dados tem como premissa básica a valorização de todos os dados pessoais, considerando-os relevantes e importantes. Para tanto, adotou-se uma definição ampla de dados pessoais, nos moldes do regulamento europeu, segundo a qual tais dados seriam todas as informações relacionadas a uma pessoa natural, identificada ou identificável.

É importante ressaltar que, muitas vezes, dados que parecem não ter importância ou que não fazem referência direta a uma pessoa, quando transferidos, cruzados ou organizados, podem revelar informações bastante específicas e sensíveis sobre determinada pessoa. Por isso, a Lei Geral de Proteção de Dados busca garantir a proteção e a privacidade de todos os dados pessoais, independentemente de sua aparente relevância ou aparente falta de identificação direta. (SILVA; CARDOSO; PINHEIRO, 2021, p. 04)

Diante da complexidade do tema, o legislador zelosamente instituiu como regra em seu artigo 1º que qualquer pessoa que trate dados, seja ela natural ou jurídica, de direito público ou privado, deverá ter uma base legal para fundamentar os tratamentos de dados pessoais que realizar. (BRASIL, 2018)

> Isso importa dizer que não haverá necessidade de identificação de uma base legal apropriada apenas nos casos que se enquadrarem nas hipóteses de exclusão de aplicação da lei previstas no Art. 4º da LGPD. Mas, ainda assim,o tratamento de dados pessoais previsto no Art.4º, inciso III (para fins exclusivos de segurança pública; defesa nacional; segurança do Estado; ou atividades de investigação e repressão de infrações penais) "será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei". (TEFFÉ; VIOLA, 2020, p. 03).

Desta forma, não sendo caso de exclusão, o tratamento realizado deverá se adequar em ao menos uma das hipóteses legais da Lei Geral de Proteção de Dados para que ele seja considerado legítimo e lícito. TEFFÉ e VIOLA (2020, p. 03) aduzem que "Essas bases foram estipuladas de forma geral e variada, devendo

detalhes e adequações serem realizados especialmente pela Autoridade Nacional de Proteção de Dados, pelo Legislativo e Judiciário.”

No entanto, é possível verificar que até mesmo grandes empresas do setor de tecnologia, que lidam rotineiramente com os dados de bilhões de pessoas, às vezes falham em cumprir com as disposições de múltiplas regulamentações nacionais e internacionais relativas à proteção de dados.

Um exemplo é o escândalo de dados *Facebook-Cambridge Analytica*. Em março de 2018, jornais expuseram ao mundo que a empresa de mineração e análise de dados *Cambridge Analytica (UK) Ltd.* minerou e analisou dados de aproximadamente 50 milhões de contas da rede social *Facebook* sem o consentimento de seus donos. (MA; GILBERT, 2019, n.p.)

> Limitar o acesso aos dados pessoais por parte de terceiros depende muitas vezes do usuário, mas tem considerável influência da organização proprietária da rede social para manter a segurança do titular da informação. Entre os anos de 2014 a 2018, a empresa Cambridge Analytica obteve dados de perfis de usuários da rede social Facebook nos Estados Unidos e no Reino Unido, com o objetivo de influenciar eleitores em campanhas políticas. As informações obtidas foram coletadas por meio de testes de personalidade na própria página da rede social, sendo possível traçar o perfil das pessoas por meio de páginas curtidas e postagens realizadas. Mediante análise do comportamento do usuário na rede social, seria possível direcionar propagandas eleitorais de acordo com o perfil da pessoa. (PIURCOSKY et al., 2019, p. 90).

A empresa desenvolveu um aplicativo cujo consistia em um quiz, que utilizava as informações do perfil do *Facebook* da pessoa para mostrar a ela qual era sua personalidade. No entanto, o aplicativo coletava dados não só de seu perfil, mas também de todos os outros perfis que fossem seus amigos na rede social. (MA; GILBERT, 2019, n.p.)

No mês de abril do mesmo ano, a então *Facebook* revelou que o número de contas afetadas ultrapassou o número de 87 milhões; consoante relatório promovido pela empresa, 443.117 destas contas eram provenientes de usuários brasileiros. (META, 2018, n.p)

Para a *Cambridge Analytica*, o mais importante era traçar o perfil político dos usuários estadunidenses, a fim de criar uma plataforma de propaganda eleitoral mais eficiente para o então candidato à presidência dos Estados Unidos, Donald Trump. A campanha eleitoral de Trump então diversificava a propaganda de acordo com os dados obtidos, que eram aliados à informações geográficas para definir o

nível de apoio ao presidenciável em várias regiões do país. Em locais com maior apoio, se tinha uma propaganda específica, e no caso contrário, também. (LEWIS; HILDER, 2018, n.p.)

> Um regulador da UE comparou recentemente o Facebook [...] ao setor bancário, onde a desregulamentação só levou à desordem e ao colapso econômico. Essa comparação foi feita este ano, quando legisladores da União Europeia questionaram Mark Zuckerburg [...] sobre o escândalo da Cambridge Analytica. O tom dos legisladores da União Europeia refletiu o do público em geral – cheio de frustração. Embora os atos do Facebook não tenham sido ilegais, eles certamente foram uma clara violação da privacidade de seus usuários. (SHARMA, 2020, p. 05, tradução nossa).

Para FORNASIER e KNEBEL (2021, p. 1025), a forma como a vigilância é executada atualmente não se assemelha mais à abordagem totalitarista do passado, representada pelo famoso conceito do "big brother", mas sim a um novo paradigma que poderíamos chamar de "grande outro", pois a vigilância não depende mais de um controle político intenso. Em vez disso, ela se baseia em uma abstração tecnológica indecifrável que faz com que os usuários entreguem seus dados comportamentais pessoais como condição para usufruir de serviços cada vez mais necessários para a vida cotidiana.

Esse fenômeno de instrumentalização do poder informacional está profundamente enraizado na imensa desigualdade estrutural que existe no âmbito da capacidade tecnológica. Ou seja, há uma assimetria informacional, pois os usuários só têm a capacidade de entregar seus dados, enquanto as empresas têm a capacidade de interpretá-los devido ao uso de técnicas avançadas de aprendizado profundo e inteligência artificial.

O impacto da informática na sociedade contemporânea é inegável. A revolução digital transformou a maneira como as pessoas se relacionam, trabalham e consomem produtos e serviços. Porém, essa transformação não se limitou ao aspecto social, alcançando também a esfera jurídica. De acordo com DONEDA (2020, p. 148):

> O mero fato da informação ser processada por computadores representa, por si, uma mudança nas consequências de seu tratamento. Alguns destes efeitos são mensurados quantitativamente, isto é, são decorrência do maior volume de informação que pode ser processado. Porém, não é somente a quantidade de informação processada que diferencia o tratamento informatizado de dados, mas também novos métodos, algoritmos e técnicas

> podem ser utilizados para este fim, operando igualmente uma mudança qualitativa no escopo do tratamento de dados pessoais.

Com a crescente complexidade dos meios de armazenamento e processamento de dados, tornou-se mais viável economicamente explorá-los do que mantê-los em sigilo, o que DONEDA (2020, p. 148) entende como uma "[…] mudança qualitativa no tratamento de dados pessoais […] na utilização de novos métodos, algoritmos e técnicas".

O autor afirma que dentre estas técnicas, especializadas estão o *data mining* e o *profiling*, que servem não só para coletar, mas também correlacionar dados pessoais.

Data mining (mineração de dados), que se trata da "[…] busca de correlações, recorrências, formas, tendências e padrões significativos a partir de quantidades muito grandes de dados, com o auxílio de instrumentos estatísticos e matemáticos" (Ibid., 2020, p. 151) para identificar informações interessantes.

O *profiling* consiste na formação de um perfil de comportamento de uma pessoa com base nos dados disponibilizados por ela ou colhidos da mesma mediante sua utilização de um serviço e afins. O *profiling* não pode ser entendido como algo inédito da era informacional, afinal, se desenvolveu a partir da evolução da burocracia e da administração privada e estatal. O que ocorre é que, a digitalização da informação a tornou mais útil. (Ibid., p. 151)

> Uma vez que os eventos cotidianos de nossas vidas são sistematicamente armazenados em um formato legível por uma máquina. Esta informação ganha uma vida toda própria. Ela ganha novas utilidades. Ela se torna indispensável em operações comerciais. E ela usualmente é transmitida de um computador a outro, de um negócio a outro, e entre o setor privado e o governo. (DONEDA, 2020, p. 151, apud GARFINKEL, 2000, p. 75).

Com a evolução da ciência mercadológica (*marketing* e publicidade), os dados pessoais se tornaram ativos necessários para o funcionamento da economia na era da informação, e, melhorados os métodos de coleta e processamento de dados (*big data*), foi criado um mercado baseado na vigilância do cidadão, o colocando "[…] como um mero espectador de suas informações." (BIONI, 2019, p. 39)

> Essa onipresença da Internet permitiu, de forma acoplada com a possibilidade do monitoramento da localização geográfica (*global positioning*

> *system*/GPS) dos *smartphones*, que as publicidades também sejam direcionadas com base em tal informação. Leva-se, assim, em conta, a proximidade física do potencial consumidor ao bem de consumo ofertado, como, por exemplo, seria o caso de um restaurante. […] Não é, portanto, uma mera coincidência que surja um anúncio publicitário, cujo bem de consumo esteja bem próximo geograficamente do cidadão ao utilizar um *smartphone* do potencial consumidor é uma (nova) estratégia mercadológica. […] É uma realidade, portanto, a estruturação de bases de dados de emoções, a fim de personalizar ainda mais a ação publicitária. (BIONI, 2019, p. 45-46).

Em agosto de 2022, a Secretaria Nacional do Consumidor (Senacon) condenou o *Facebook* ao pagamento de multa avaliada em R$ 6,6 milhões em decorrência do vazamento de informações de mais de 443.000 brasileiros à Cambridge Analytica (MJSP, 2022). No caso em questão, os dados destes brasileiros e mais pessoas mundo afora, sofreram um tratamento a fim de se aperfeiçoar e melhor promover a campanha do candidato Donald Trump à presidência dos Estados Unidos da América, utilizando os dados para oferecer uma melhor localização aos algoritmos de serviços de publicidade digital.

Este é um exemplo de publicidade direcionada, forma na qual se pretende aumentar o êxito da indução ao consumo mediante a personalização da comunicação social (BIONI, 2019, p. 41).

> Há, por isso, uma vigilância imperativa das pessoas, em especial do potencial consumidor, o que varia desde os seus hábitos de navegação e comportamento na Internet às suas próprias emoções, tornando-o, totalmente, transparente. (BIONI, 2019, p. 46-47).

Desta forma, ao utilizar a internet o próprio indivíduo acaba se tornando um produto em potencial, em vista de que os serviços “gratuitos” presentes na rede exercem uma forma de *trade-off* onde usufruem do usuário para fins externos ao mesmo, coletando seus dados e lucrando em cima deles, naquilo que se converte em uma verdadeira monetização dos dados pessoais.

Ao notar as implicações da não regulamentação do uso e manipulação de dados, não tardou até que o Estado e demais organizações começassem a buscar uma solução para este novo problema, inerente às inovações tecnológicas que, de uma forma ou de outra, haviam vindo para ficar. Portanto, seria necessária a formulação de políticas que visassem garantir proteção à privacidade de dados pessoais.

Não obstante certos países já possuíam um histórico de legislação referente à proteção de dados, foi necessário modernizá-la a vista destes novos desafios. As mais atuais, chamadas de leis de quarta geração, buscam “[…] fortalecer a posição da pessoa em relação às entidades que coletam e processam seus dados, reconhecendo o desequilíbrio nesta relação […]” (DONEDA, 2020, p. 169).

Na União Europeia, foi implementado no ano de 2018 o *General Data Protection Regulation* ou Regulamento Geral sobre a Proteção de Dados, que trata da regulamentação da proteção de dados de pessoas físicas presentes no território multinacional da união. Em paralelo, a demanda regulatória pela proteção de dados pessoais no Brasil gerou debates por um longo período, até a aprovação da Lei Geral de Proteção de Dados em 2018.

3.1 LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA

Conforme discutido retro, a evolução tecnológica trouxe consigo a necessidade de adaptar as normas jurídicas existentes e criar novas legislações para lidar com os desafios do mundo digital, ao passo que a presença da informática no dia a dia das pessoas exige uma atenção especial por parte do poder público e da sociedade como um todo, a fim de garantir que os avanços tecnológicos sejam utilizados para o benefício de todos, sem violar direitos e liberdades individuais.

É o caso da Lei Geral de Proteção de Dados, a qual foi um importante marco na proteção da privacidade e dos direitos dos titulares de dados pessoais no Brasil, estabelecendo regras para o tratamento de dados pessoais pelas empresas e instituições públicas e privadas. (FORNASIER; KNEBEL, 2021, p. 1005)

A promulgação da Lei Geral de Proteção de Dados em 2018 foi uma resposta à crescente demanda por regulamentação do tratamento de dados pessoais, em defesa dos direitos fundamentais de liberdade e privacidade. A Lei Geral de Proteção de Dados estabelece um conjunto de regras e regulamentos que regem a coleta, uso, armazenamento e compartilhamento de dados pessoais no Brasil, com o objetivo de proteger a privacidade e os direitos dos titulares dos dados.

A referida lei foi inspirada no Regulamento Geral de Proteção de Dados da União Europeia, que estabeleceu um padrão para a proteção de dados em toda a Europa. A Lei Geral de Proteção de Dados exige que as empresas adotem medidas

de segurança adequadas para proteger os dados pessoais dos titulares, além de obter seu consentimento explícito antes de coletar ou usar seus dados.

A Lei Geral de Proteção de Dados é aplicável ao tratamento de dados pessoais em qualquer meio, seja ele físico ou digital, realizado por pessoa física ou jurídica de direito público ou privado. O conceito de tratamento de dados é amplamente definido pela lei e inclui diversas atividades relacionadas ao processamento de informações pessoais. De acordo com a Lei Geral de Proteção de Dados, é considerado tratamento de dados pessoais:

> [...] toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; [...] (BRASIL, 2018, artigo 5º, inciso X).

Além disso, a lei também define como tratamento de dados a realização de operações automatizadas que afetem os dados pessoais de um titular, como a criação de perfis e a tomada de decisões com base em algoritmos.

A Lei Geral de Proteção de Dados estabelece ainda uma série de princípios e requisitos para o tratamento de dados pessoais, como a necessidade de obtenção do consentimento do titular para a coleta e uso de seus dados, a obrigação de manter a segurança das informações, a necessidade de transparência e clareza no tratamento de dados e o respeito aos direitos dos titulares.

Vale ressaltar que as disposições da Lei Geral de Proteção de Dados não serão aplicáveis caso o tratamento seja realizado por pessoa física para fins exclusivamente particulares e não econômicos, ou quando efetuado para fins jornalísticos e artísticos ou acadêmicos (BRASIL, 2018, artigo 4º, incisos I e II). Também não será aplicável quando o tratamento for realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividade de investigação e repressão penal. (BRASIL, 2018, artigo 4º, inciso III)

Além disso, o disposto não será aplicado caso os dados sejam provenientes de fora do Brasil e que não sejam objeto de comunicação, uso compartilhado com agentes de tratamentos brasileiros ou objeto de transferência internacional de dados com país alheio ao de sua proveniência, conquanto o país proporcione grau de proteção de dados pessoais adequados ao previsto na Lei Geral de Proteção de Dados (BRASIL, 2018, artigo 4º, inciso IV).

MALDONADO e BLUM (2020, p. 77) afirmam que os requisitos previstos no artigo 4º, inciso IV, visam aumentar a competitividade internacional brasileira, estimulando a contratação de empresas nacionais para serviços de tecnologia da informação, evitando que o Brasil se torne um “paraíso de dados”.

Consoante o artigo 5º, incisos VI e VII, da Lei Geral de Proteção de Dados (BRASIL, 2018), o tratamento dos dados pessoais poderá ser realizado por dois agentes, o controlador e o operador. Compete ao controlador decidir as finalidades e meios do tratamento dos dados pessoais. Ao operador cabe realizar o tratamento em nome do controlador. (BRASIL, p. 10, 2020)

Ademais, em paralelo aos agentes responsáveis pelo tratamento, a lei estabelece também a figura do encarregado, consistente na “[...] pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados [...]”. (BRASIL, 2018, artigo 5º, inciso VIII)

A Lei Geral de Proteção de Dados regulamenta o tratamento de dados pessoais realizados por quaisquer agentes de tratamento, sejam do âmbito privado ou do Poder Público. Quanto ao Poder Público, a Lei Geral de Proteção de Dados o define como órgãos ou entidades dos entes federativos (União, Estados, Distrito Federal e Municípios) e dos três Poderes, inclusas as Cortes de Contas e do Ministério Público, os serviços notariais e de registro, as empresas públicas e as sociedades de economia mistas que não estejam em regime de concorrência. (ANPD, 2022a, p. 05)

O tratamento de dados efetuado pelo Poder Público pode incorrer nas hipóteses previstas nos arts. 7º e 11 da Lei Geral de Proteção de Dados, os quais devem ser interpretados sob a luz do art. 23 da mesma lei (ANPD, 2022a, p. 06), cujo dita que:

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:
> I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; […] (BRASIL, 2018).

Além disso, o tratamento de dados pelo Poder Público pode ser analisado de acordo com as seguintes bases legais: consentimento, legítimo interesse, cumprimento de obrigação legal e regulatória e execução de políticas públicas. (ANPD, 2022a, p. 06)

Atualmente, o ordenamento relativo à proteção dos dados pessoais se preocupa não só com a determinação do conteúdo destes dados, mas também com o estabelecimento de técnicas eficazes para sua tutela, como a instituição de agências reguladoras ou órgãos fiscalizadores. No que toca à fiscalização da Lei Geral de Proteção de Dados, esta recai à Autoridade Nacional de Proteção de Dados.

A Autoridade Nacional de Proteção de Dados é órgão da administração pública, integrante da Presidência da República, ao qual é assegurado a autonomia técnica e decisória, competência para zelar pela proteção dos dados pessoais, elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, e fiscalizar e aplicar sanções na hipótese de tratamento de dados realizado em descumprimento à legislação, dentre outras atribuições. (BRASIL, 2020, art. 2º)

Órgãos como a Autoridade Nacional de Proteção de Dados são necessários ao passo que o indivíduo não consegue sozinho proteger seus interesses sem perder uma gama de benefícios providos por diversos serviços, como relata DONEDA (2020, p. 310):

> A atuação de uma autoridade de garantia nos moldes da maioria das autoridades de proteção de dados hoje existentes merece atenção, em primeiro lugar, porque nesse caso a simples atuação do indivíduo para a proteção de seus interesses – o controle individual, como em algumas das concepções de proteção de dados pessoais que nós verificamos – não é capaz de projetar uma situação na qual o direito fundamental em questão receba tutela adequada. A impossibilidade de concretizar a autodeterminação informativa baseada meramente na ação singular de seu interessado é patente em vista da desproporção entre sua vontade e uma estrutura dirigida à coleta de seus dados e preparada a excluí-lo de certas vantagens caso decida por não fornecê-los. Assim, tal tutela singular reproduziria uma tradição elitista da privacidade, que não corresponde à sua atual posição na nossa carta constitucional nem referencia outros direitos que devem ser mensurados nessa situação como, por exemplo, a igualdade.

A atuação destes órgãos é indispensável à tutela dos dados pessoais, visto que o usuário não tem o poder necessário para realizar tal tarefa.

Inobstante o indivíduo tenha a opção de consentir ou não com o tratamento de seus dados, os termos de uso de um serviço eventualmente podem ser abusivos ou absurdos, e o não consentimento geralmente acarreta em consequências prejudiciais ao usuário, como o completo impedimento à utilização de quaisquer funções de um determinado serviço (DONEDA, 2020, p. 292). Em conhecimento disto, órgãos fiscalizadores tentam prevenir tais acontecimentos, verificando e punindo práticas abusivas ao consumidor.

3.2 PRINCÍPIOS GERAIS DO TRATAMENTO DE DADOS

Segundo BUCHAIN (2021, p. 108) “A finalidade do tratamento de dados deve corresponder a sua realização para propósitos lícitos, ou seja, legítimos, específicos, explícitos e informados.”

A partir da década de 1970, começaram a surgir em diferentes países normas e regulamentações específicas sobre o uso de informações pessoais e a privacidade dos indivíduos (MALDONADO; BLUM, 2020, p. 126). Essas normas são baseadas em princípios e técnicas comuns, que têm sido desenvolvidos desde a sua criação e ainda hoje são amplamente utilizados e respeitados em todo o mundo.

Houveram quatro gerações de leis de proteção de dados. Consoante MALDONADO e BLUM (2020, p. 126) a primeira geração durou até 1977, sendo personificada na *Bundesdatenschutzgesetz* (Lei Federal da República Federativa da Alemanha sobre proteção de dados pessoais), e tinha como foco a criação de bancos de dados pessoais e seu controle por órgãos públicos.

Ainda segundo os mesmos autores, a segunda geração de normas e regulamentações surgiu no final da década de 1970, em resposta à crescente disseminação dos bancos de dados informatizados. Essa disseminação levou a uma preocupação crescente com a privacidade e a proteção dos dados pessoais, que passou a ser vista como uma liberdade negativa a ser exercida pelo próprio cidadão.

> A segunda geração de leis de proteção de dados pessoais é caracterizada por uma mudança do âmago regulatório. Preocupa-se não somente com as bases de dados estatais, mas, também, com as da esfera privada. A figura do Grande Irmão (uma única e centralizada base de dados) é diluída pela de Pequenos Irmãos (bancos de dados dispersos no plano estatal e

> privado). Com isso, percebe-se que seria inviável a estratégia regulatória anterior em que incumbia ao Estado licenciar a criação e o funcionamento de todos os bancos de dados. A segunda geração de leis transfere para o próprio titular dos dados a responsabilidade de protegê-los. Se antes o fluxo das informações pessoais deveria ser autorizado pelo Estado, agora cabe ao próprio cidadão tal ingerência que, por meio do consentimento, estabelece as suas escolhas no tocante à coleta, uso e compartilhamento dos seus dados pessoais. (BIONI, 2019, p. 171).

Houve uma mudança central na forma como a privacidade era abordada, deixando de se concentrar no fenômeno computacional em si para se concentrar na proteção dos direitos individuais em relação aos dados pessoais. Foi criado um sistema que fornecia aos cidadãos instrumentos para identificar o uso indevido de suas informações pessoais e propor a sua tutela.

Desde então, o fornecimento de dados pessoais começava a se tornar um requisito para a participação do indivíduo na sociedade, e o que era exceção veio a se tornar regra. A partir disso, surgiu a terceira geração na década de 1980, com o objetivo de aprimorar ainda mais a proteção dos dados pessoais, mantendo o enfoque na proteção dos direitos individuais, mas ampliando seu escopo para além da mera liberdade de fornecer ou não informações pessoais. O objetivo agora era garantir efetivamente a manutenção desses direitos. (MALDONADO; BLUM, 2020, p. 126)

Com o surgimento da terceira geração de leis, tornou-se evidente a complexidade que o tema da proteção de dados pessoais havia adquirido com o decorrer do tempo, pois agora não se resumia apenas à liberdade do indivíduo em decidir se queria ou não compartilhar suas informações pessoais, mas também ao contexto em que o pedido para divulgar esses dados era feito (Ibid., p. 127).

A proteção de dados pessoais agora também estabeleceria meios de proteção para as ocasiões em que a liberdade do indivíduo fosse cerceada. Nesse contexto, buscou-se incluir o titular dos dados em todas as fases do processo de tratamento e utilização de sua informação por terceiros, garantindo a autodeterminação informativa.

> A amplitude desse papel de protagonismo do indivíduo na proteção dos dados pessoais é o divisor de águas para a terceira geração de leis. Nesse estágio, as normas de proteção de dados pessoais procuraram assegurar a participação do indivíduo sobre todos os movimentos dos seus dados pessoais: da coleta ao compartilhamento. Alcançar-se-ia, assim, o êxtase da própria terminologia da “autodeterminação informacional”, pois, com tal

> participação, possibilitar-se-ia que o sujeito tivesse um controle mais extensivo sobre as suas informações pessoais. (BIONI, 2019, p. 172).

De acordo com MALDONADO e BLUM (2020, p. 127), embora a autodeterminação informativa tenha sido reconhecida como um importante princípio na terceira geração de leis de proteção de dados, o seu exercício ainda estava limitado a uma minoria privilegiada. Por isso, uma quarta geração de leis de proteção de dados surgiu visando abordar de forma mais ampla o problema da informação e elevar o padrão coletivo de proteção de dados pessoais.

Essas leis de quarta geração foram elaboradas com o intuito de fortalecer a posição das pessoas em relação às entidades que coletam e processam seus dados, estabelecendo autoridades independentes para fiscalização e aplicação das normas de proteção de dados, como a Diretiva da UE 95/46.

Entre os princípios comuns que podem ser observados nas leis de proteção de dados da quarta geração estão a vinculação mais estreita com a proteção da pessoa e com os direitos fundamentais, a definição de medidas mais rigorosas para garantir a privacidade e a segurança dos dados pessoais, a previsão de sanções para o descumprimento das normas, e o fortalecimento da transparência e da prestação de contas por parte das entidades que coletam e processam os dados pessoais. (Ibid., 2020, p. 127-128)

O artigo 6º da Lei Geral de Proteção de Dados aduz que o tratamento de dados pessoais deverá se restringir à observância da boa-fé e outros princípios (BRASIL, 2018), como a finalidade, a adequação, a necessidade, o livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção, a não discriminação e a responsabilização e prestação de contas, e os define como disposto a seguir:

> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

> V - qualidade dos dados: 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;
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas 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 difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: 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; (BRASIL, 2018).

Para MALDONADO e BLUM (2020, p. 128), os três primeiros princípios da Lei Geral de Proteção de Dados, que são a finalidade, adequação e a necessidade, estão intimamente ligados entre si. Em conjunto com o princípio da transparência, esses princípios formam o núcleo da lei e são essenciais para garantir o respeito à proteção dos direitos fundamentais de liberdade e privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural, por meio da proteção dos seus dados pessoais.

O princípio da finalidade determina que os dados pessoais devem ser coletados para finalidades determinadas, explícitas e legítimas, não podendo ser tratados de maneira incompatível com essas finalidades. Já o princípio da adequação exige que o tratamento de dados pessoais seja adequado, relevante e limitado ao mínimo necessário para alcançar as finalidades para as quais eles foram coletados. (DONEDA, 2020, p. 171)

O princípio da necessidade estabelece que o tratamento de dados pessoais deve ser restrito ao mínimo necessário para alcançar as finalidades específicas para as quais os dados foram coletados. (MALDONADO; BLUM, 2020, p. 134)

A transparência, outro princípio fundamental, se relaciona diretamente com os princípios mencionados anteriormente. Ele determina que os titulares de dados devem ser informados de forma clara e transparente sobre o tratamento de seus dados pessoais, incluindo os propósitos, as formas de tratamento, os responsáveis pelo tratamento, entre outras informações relevantes. (BIONI, 2019, p. 246)

A observância desses princípios é essencial para assegurar a proteção dos direitos fundamentais dos indivíduos e garantir o livre desenvolvimento da

personalidade, ao mesmo tempo em que permite a utilização adequada e necessária dos dados pessoais.

4 CONSENTIMENTO NO TRATAMENTO DE DADOS

A regulação dos dados no Brasil foi abordada recentemente pela aprovação da Lei Geral de Produção de Dados, inspirada no regulamento europeu, representando um marco normativo importante para os processos sociais e econômicos relacionados aos dados digitais. Uma das principais características da é a utilização do consentimento do usuário e do legítimo interesse como meio de garantir a defesa de direitos privados e fundamentais, trazendo uma nova perspectiva para a proteção da privacidade e segurança dos dados pessoais no Brasil.

> Porém, é identificável uma ambiguidade nessa proteção, pois o texto da lei reconhece uma (hiper) vulnerabilidade dos usuários (titulares dos dados) ao mesmo tempo em que dá condições para que a entrega de dados ocorra. A condição de titular de dados pessoais é definida pela lei em seu artigo 5º, V, como: “pessoa natural a quem se referem os dados pessoais que são objeto de tratamento”, ou seja, é o sujeito de direito que cede dados ao controlador e ao operador — e essa condição de disponibilidade só é possível por meio do consentimento, definido no art. 5º, XII, como “manifestação livre, informada e inequívoca no qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”. (FORNASIER; KNEBEL, 2021, p. 1005).

A discussão em torno da figura jurídica do titular na Lei Geral de Proteção de Dados é controversa pois suscita uma posição dúplice. De um lado, ele é considerado um sujeito digno de proteção, mas, por outro lado, é visto como uma figura livre para discutir sobre a cessão de seus dados. Esse cenário teórico tem motivado pesquisas que identificam os limites do consentimento do titular. No entanto, a Lei Geral de Proteção de Dados não estabelece formas específicas de consentimento juridicamente eficazes. (FORNASIER; KNEBEL, 2021, p. 1005-1006)

Desta feita, embora a vigência da Lei Geral de Proteção de Dados represente um marco jurídico importante para a proteção de dados pessoais no Brasil, é fundamental compreendê-la dentro do contexto da economia política que a recebe, que é a da mercantilização dos dados em uma economia da vigilância.

Esse aspecto aponta para a necessidade de se adotar uma abordagem crítica e reflexiva em relação à proteção de dados pessoais, levando em conta não apenas os aspectos legais e normativos, mas também as dimensões políticas, econômicas e sociais envolvidas na questão da privacidade e segurança dos dados.

A instituição de um marco jurídico nacional formaliza direitos fundamentais concernentes à privacidade e à proteção dos dados pessoais, em benefício direto ao exercício da cidadania, a autodeterminação sobre os dados e à proteção da dignidade da pessoa humana, e consoante FORNASIER e KNEBEL (2020, p. 1017), ao mesmo tempo busca "[...] aprimorar os princípios da livre concorrência, ao propor uma natureza regulatória de dados cuja finalidade parece ser a de forjar uma cultura para as organizações de proteção aos dados pessoais [...]".

Conquanto tenham sido presenciados vários avanços legislativos, ainda verifica-se uma disparidade entre o texto legal e a realidade fática. FORNASIER e KNEBEL (2021, p. 1012) entendem que existe uma desigualdade entre titulares e os controladores:

> A assimetria informacional é o fator estrutural determinante dessa economia dos dados, justamente pela profunda desigualdade entre a capacidade de gerir e processar dados entre os usuários, titular dos dados pessoais, e quem os controla, as big techs. A "mediação digital de tudo" (MOROZOV, 2018, p. 163) só é possível com tecnologias de apropriação privada das corporações informacionais, em que a lógica do extrativismo de dados ocorre sob um consenso algoritmo forjado nos escritórios dessas empresas, sob princípios que considerados "bons para todos". O titular dos dados pessoais queda-se refém de uma estrutura social que lhe deixa ao restrito papel de rendição de seus dados, mascarada de voluntariedade, ou o ostracismo que impossibilita o trabalho ou o lazer.

Dessa forma, o titular sempre se encontra suscetível a aceitar termos ora prejudiciais aos mesmos, se tornando reféns de uma estrutura social enraizada no mundo digital. Assim se descobre que o legislador também preocupou-se com a viabilidade econômica da legislação.

Assim sendo, inobstante tenha seu preço, a Lei Geral de Proteção de Dados estabelece segurança jurídica para setores da economia que lidam com o processamento de dados pessoais, os qualificando para a instauração de uma cadeia produtiva firmada em dados e processos de decisões automatizados. (FORNASIER; KNEBEL, 2020, p. 1017)

> A regulação em torno da proteção de dados reconhece o problema do extrativismo de dados, mas fornece a segurança jurídica da liberdade contratual sob a disponibilidade desses dados. No Brasil, a LGPD é um marco de criação dessa figura, o titular de dados pessoais, sujeito de direito capaz de fornecer seus dados pessoais comportamentais por meio de um processo de consentimento. A autoderminação informativa é um dos fundamentos dessa lei; mas tal qual ocorre com a autonomia privada sob o manto da igualdade jurídica, esse sujeito carece de condições materiais

> para exercício de plena liberdade sobre os dados pessoais, pois a escolha está somente na forma de consentimento em que os dados serão rendidos aos prestadores de serviços digitais. (FORNASIER; KNEBEL, 2020, p. 1024).

O titular de dados pessoais, conforme definido pela lei, é o responsável por controlar o uso e a circulação de suas informações pessoais, garantindo que os seus dados não sejam utilizados de maneira indevida ou violadora de sua privacidade.

No entanto, a lei estabelece limites claros para o tratamento de dados pessoais, exigindo o consentimento expresso do titular, o que significa que as empresas devem obter autorização clara e específica para a coleta, uso e compartilhamento de informações pessoais. Além disso, também exige a transparência no processamento de dados, garantindo que os titulares tenham acesso às informações sobre o uso de seus dados e possam exercer o seu direito de solicitar a exclusão ou correção de informações incorretas.

Neste ínterim, é possível visualizar que a proteção adequada dos dados pessoais é um desafio que requer uma solução que promova a proteção da privacidade da pessoa e, ao mesmo tempo, estabeleça um equilíbrio para a circulação de informações. Isso pode ser feito por meio da aplicação dos requisitos de proteção de dados pessoais, que visam garantir que esses dados sejam tratados de forma justa, transparente e legal.

> Para tal tarefa, é de valia uma leitura de institutos que, situados em posição central na problemática dos dados pessoais, deem oportunidade ao intérprete de estabelecer critérios para o balanceamento dos interesses em jogo, auxiliado pela aplicação dos princípios de proteção de dados pessoais. (DONEDA, 2020, p. 291-292).

O sistema legal desenvolvido para abordar o tratamento de dados fornece ao titular instrumentos de controle sobre as suas informações pessoais e de garantia de direitos (TEFFÉ; VIOLA, 2020, p. 05).

Entre os diferentes institutos e princípios que têm um papel central nessa questão, o consentimento e o legítimo interesse para o tratamento de dados pessoais é fundamental, como previsto no artigo 7º, incisos I e IX da Lei Geral de Proteção de Dados:

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

> [...]
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; (BRASIL, 2018).

O consentimento se refere ao ato pelo qual a pessoa concorda com o uso de seus dados pessoais para determinada finalidade. Consoante o artigo 5º, inciso XII da Lei Geral de Proteção de Dados (BRASIL, 2018), o consentimento é a "[...] manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada", ou seja, a pessoa deve ser informada claramente sobre como seus dados serão usados e ter a liberdade de consentir ou não com esse uso.

O consentimento do titular é um dos pontos mais sensíveis e cruciais em relação à disciplina de proteção de dados pessoais. O consentimento é um dos principais mecanismos utilizados pelo direito civil para estruturar uma disciplina que leve em consideração a autonomia da vontade do titular dos dados, a circulação de dados e os direitos fundamentais envolvidos (DONEDA, 2020, p. 292).

Através do consentimento, é possível ajustar os efeitos do tratamento de dados pessoais à natureza dos interesses em questão. A fim de evitar abusos no tratamento de dados pessoais e garantir os direitos do titular, ele tem a possibilidade de revogar seu consentimento ou pleitear o direito à oposição. A revogação do consentimento é um direito do titular de dados pessoais que permite que ele retire o consentimento que havia concedido previamente para o tratamento de seus dados.

> Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
> [...]
> § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.
> [...]
> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.
> [...]
> § 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei. (BRASIL, 2018).

Verifica-se que o consentimento do titular dos dados recebeu bastante atenção pelo legislador, inobstante não seja “[...] a única hipótese legal para o tratamento de dados pessoais nem hierarquicamente superior às demais contidas no rol do Art. 7º” (TEFFÉ; VIOLA, 2020, p. 05).

Além disso, encontra-se positivado o direito à explicação, que concede ao titular o direito de solicitar a revisão de decisões “[...] tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses [...]” (Ibid., p. 04).

> Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (BRASIL, 2018).

Mediante análise, é possível observar que os princípios da legislação de proteção de dados pessoais se voltam ao exercício da autonomia humana, demonstrando a preocupação do legislador com a participação do indivíduo no fluxo de suas informações pessoais (TEFFÉ; VIOLA, 2020, p. 05).

Os princípios de proteção de dados pessoais, principalmente o consentimento, são fundamentais para a garantia dos direitos do titular de dados e para o estabelecimento de uma base ética e legal para o tratamento de informações pessoais. No texto legal, a caracterização do consentimento segue a linha do Regulamento Europeu e das normas mais atuais sobre o tema.

Como discutido retro, o consentimento deverá ocorrer, via de regra, em consonância à hipótese do artigo 7º, inciso I da Lei Geral de Proteção de Dados. No entanto, existem alternativas mais rígidas para hipóteses em que houverem dados sensíveis ou relativos à crianças.

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas
> [...]
> Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
> § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. (BRASIL, 2018).

O cuidado com o consentimento do titular de dados pessoais é de extrema importância no atual cenário tecnológico, marcado pela coleta em massa de informações pessoais e pela mercantilização desses dados por parte de diversas empresas e organizações.

Nesse sentido, é fundamental que a interpretação do consentimento ocorra de forma restritiva, ou seja, que o agente que coletou o consentimento não possa estender a autorização concedida para o tratamento de dados para outros meios além daqueles previamente pactuados, para momentos posteriores ou para finalidades distintas (TEFFÉ; VIOLA, 2020, p. 06).

A interpretação restritiva do consentimento do titular é fundamental para garantir a proteção de dados pessoais e evitar abusos no tratamento dessas informações, afinal, os titulares de dados pessoais devem ter controle sobre suas informações e devem ter a liberdade de escolher como e para que finalidades seus dados serão utilizados.

Nesse diapasão, seguindo a lógica do consentimento informado, o artigo 9º da Lei Geral de Proteção de Dados (BRASIL, 2018) dispõe o titular tem direito ao acesso facilitado às informações relativas ao tratamento de seus dados, como exposto adiante:

> Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:
> I - finalidade específica do tratamento;
> II - forma e duração do tratamento, observados os segredos comercial e industrial;
> III - identificação do controlador;
> IV - informações de contato do controlador;
> V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
> VI - responsabilidades dos agentes que realizarão o tratamento; e
> VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei. (BRASIL, 2018).

Em continuidade, a lei deixa explícito que o consentimento será considerado nulo caso as informações fornecidas ao titular sejam enganosas ou abusivas, ou caso não tenham sido apresentadas de forma transparente e inequívoca (BRASIL, 2018, art. 9º, § 1º). Ademais, caso houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento fornecido originalmente

pelo titular, o mesmo deverá ser informado quanto às mudanças de finalidade, lhe sendo permitido revogar o consentimento (BRASIL, 2018, art. 9º, § 2º).

Além dessas ocasiões, "[...] quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato [...]. (BRASIL, 2018, art. 9º, § 3º)

No que diz respeito ao legítimo interesse, assim dispõe a legislação:

> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
> I - apoio e promoção de atividades do controlador; e
> II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.
> § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
> § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse. (BRASIL, 2018).

O princípio do legítimo interesse é um instituto importante dentro da disciplina de proteção de dados pessoais, uma vez que permite a realização de tratamentos de dados que sejam relevantes e necessários para as atividades exercidas pelo controlador de dados, desde que haja uma justificativa válida para tal (TEFFÉ; VIOLA, 2020, p. 14).

Dessa forma, o princípio do legítimo interesse é uma das hipóteses legais que podem ser utilizadas para tratar dados pessoais, ao lado do consentimento e outras situações previstas em lei.

> Diante da flexibilidade dessa base legal, as expectativas do titular dos dados têm peso especialmente relevante para sua aplicação, devendo ser consideradas também a finalidade, a necessidade e a proporcionalidade da utilização dos dados. Quanto mais invasivo, inesperado ou genérico for o tratamento, menor será a probabilidade de que seja reconhecido o legítimo interesse. (TEFFÉ; VIOLA, 2020, p. 14)

Para TEFFÉ e VIOLA (2020, p. 15) "Mostrar que há um interesse legítimo significa que o controlador (ou um terceiro) deve ter algum benefício ou resultado claro e específico em mente", desta forma, deve ser esclarecido o que realmente se está tentando alcançar com uma determinada operação de tratamento de dados.

Os autores ainda argumentam que inobstante “[...] determinado objetivo possa ser potencialmente relevante, ele deverá ser legítimo. Qualquer interesse ilegítimo, antiético ou ilegal não será um interesse legítimo para a LGPD.” (Ibid., 2020, p. 15)

No entanto, é importante ressaltar que a aplicação do princípio do legítimo interesse não pode ser vista como uma carta branca para que os controladores de dados coletem e utilizem dados pessoais de forma indiscriminada.

É necessário que o controlador demonstre que o tratamento dos dados é realmente necessário para a consecução de sua atividade, que o interesse em questão é legítimo e que os direitos e garantias fundamentais dos titulares dos dados não são prejudicados. Além disso, é importante que a análise do legítimo interesse seja feita caso a caso, de forma individualizada, e que seja possível ao titular dos dados opor-se ao tratamento em questão, caso considere que seus direitos estão sendo prejudicados.

4.1 ASSIMETRIA INFORMACIONAL E A BANALIZAÇÃO DO CONSENTIMENTO

O desenvolvimento das leis de proteção de dados pessoais ao longo das gerações tem se caracterizado pela evolução das definições do consentimento, que passaram a incluir adjetivos como “inequívoco”, “expresso”, “informado”, “específico” e “livre”.

No entanto, BIONI (2020, p. 226) aduz que apesar dessas mudanças, é possível perceber uma certa falta de atenção por parte das normas em relação à maneira como o consentimento deve ser efetivamente colhido.

Nesta linha de pensamento, embora a legislação tenha avançado ao estabelecer que o consentimento do titular dos dados é fundamental para a utilização de suas informações pessoais, ainda não foram estabelecidas regras precisas sobre como esse consentimento deve ser obtido de forma adequada e eficiente. Isso pode gerar situações em que o consentimento não é realmente livre, informado ou inequívoco, e acaba sendo utilizado como uma mera formalidade para legitimar o uso dos dados pessoais sem a real concordância do titular.

> Na medida em que a informação se impõe como instrumento de distribuição de riquezas e combustível do progresso econômico, não é legítima a utilização desse recurso de forma ilimitada, sob o risco lesão ou violação de

> inúmeros outros valores correlatos de igual importância para a ordem jurídica. Cabe ao Direito estabelecer limites para a sua utilização, de modo a impedir que o manejo desse bem econômico venha a malferir quaisquer direitos, notadamente os direitos de personalidade. (MENEZES; COLAÇO, 2017, p. 2325).

Diante desse descompasso entre a evolução das leis de proteção de dados e a falta de regulamentação específica sobre a forma como o consentimento deve ser obtido, o próprio mercado acabou criando mecanismos de autorregulação. Um desses mecanismos é a política de privacidade, uma técnica contratual utilizada para colher o consentimento necessário para o tratamento dos dados pessoais. (BIONI, 2020, p. 226)

> A Política de Privacidade é necessária a todas as empresas que coletam informações pessoais. Ela Informa quais os dados serão coletados e como, após a autorização do aderente ao serviço proposto,serão utilizados e tratados pelo controlador e pelo operador (agentes no tratamento de dados, segundo a LGPD), ou se e como serão cedidos a terceiros. A Política de Privacidade também disporá sobre o armazenamento das informações, ressaltando que os dados não são apenas os inseridos pelo usuário, mas também aqueles captados por ferramentas, como *cookies* (arquivos de Internet, criados por sites visitados e salvos no navegador utilizado, sendo essas informações usadas para identificar o visitante em páginas que possuem relação com os cookies), o que também deve ser informado quando utilizados. (SEBASTIÃO, 2022, p.112-113).

No entanto, para BIONI (2020, p. 226) essa técnica tem mostrado algumas falhas significativas. Em primeiro lugar, ela pode reforçar a assimetria informacional presente no mercado, já que muitos usuários acabam concordando com os termos da política de privacidade sem realmente compreenderem suas implicações.

Em vista de que as pessoas agora possuem vidas tanto no mundo físico quanto no virtual, as informações pessoais compartilhadas nas redes digitais se tornaram valiosas. De acordo com MENEZES e COLAÇO (2020, p. 2320), “No afã de integrar o circuito da rede, as pessoas compartilham dados gerais e aqueles mais íntimos de sua personalidade”, assim, a personalidade, revelada no ambiente virtual, é transformada em dados que poderão ser tratados de maneira inadequada, contra a finalidade inicial.

Além disso, a política de privacidade não capacita de forma efetiva o cidadão para exercer controle sobre suas informações pessoais, já que muitas vezes os termos são complexos e difíceis de serem compreendidos pelos usuários comuns.

> A assimetria informacional é o fator estrutural determinante dessa economia dos dados, justamente pela profunda desigualdade entre a capacidade de gerir e processar dados entre os usuários, titular dos dados pessoais, e quem os controla, as big techs. A “mediação digital de tudo” (MOROZOV, 2018, p. 163) só é possível com tecnologias de apropriação privada das corporações informacionais, em que a lógica do extrativismo de dados ocorre sob um consenso algoritmo forjado nos escritórios dessas empresas, sob princípios que considerados “bons para todos”. O titular dos dados pessoais queda-se refém de uma estrutura social que lhe deixa ao restrito papel de rendição de seus dados, mascarada de voluntariedade, ou o ostracismo que impossibilita o trabalho ou o lazer. (FORNASIER;KNEBEL, 2020, p. 1011).

Observa-se que as políticas de privacidade são, essencialmente, contratos de adesão. Isso significa que as condições e os termos do contrato são estabelecidos pela empresa e o usuário não tem a possibilidade de negociá-los, tendo que aceitá-los integralmente ou desistir de utilizar o serviço.

> Essa dinâmica dos contratos de adesão assinala, sobretudo, a assimetria de forças das relações de consumo, na medida em que o seu elo mais forte fixa unilateralmente o programa contratual. Isso significa, em termos de proteção de dados pessoais, que será o fornecedor quem determinará os rumos do fluxo informacional dos seus usuários, eliminando, praticamente, qualquer faixa de controle a ser por eles operada. (BIONI, 2020, p. 227).

Essa massificação das relações contratuais de consumo é uma característica marcante no mercado informacional, onde os usuários são frequentemente confrontados com uma grande quantidade de termos e condições contratuais que são estabelecidos pelas empresas de tecnologia.

> Sob a primeira perspectiva, nota-se que as políticas de privacidade são, por excelência, um contrato de adesão. A massificação das relações contratuais ordinárias de consumo é também característica marcante no mercado informacional. (BIONI, 2020, p. 226).

O jurista BIONI (2020, p. 227) entende que ao consumidor cabe apenas decidir se irá aderir ou não às políticas de privacidade das empresas de tecnologia. A terminologia “adesão” expressa precisamente essa dinâmica contratual, na qual o usuário não tem poder de negociação, sendo obrigado a aceitar as condições estabelecidas pela empresa de tecnologia para poder utilizar o serviço.

Neste diapasão, os usuários acabam não tendo o poder de barganha necessário para impor as suas preferências de privacidade. Essa conjuntura aliada “[...] à proeminência de uma série de plataformas que condicionam a própria

participação social do cidadão, acaba por tornar falaciosa a prometida esfera de controle dos dados pessoais", banalizando o consentimento e a autodeterminação informacional. Desta forma, "políticas de privacidade, ora escoradas nesta dinâmica dos contratos de adesão, têm sido uma ferramenta inapropriada para garantir ao consumidor o controle dos seus dados pessoais." (Ibid., p. 227)

Verifica-se que as políticas de privacidade são ferramentas contratuais que em sua finalidade última afastam o empoderamento do usuário consumidor. BIONI (2020, p. 229) afirma que "[...] seus textos longos e de difícil compreensão são incapazes de sequer estabelecer uma comunicação adequada para [...] racionalizar um processo de tomada de decisão."

> As redes sociais proporcionam um formato de interação e expressão que permite aos usuários a constituição de uma identidade digital própria (RESTA, 2014, p. 324), que também recebe proteção, exteriorizada na criação de perfis pessoais os quais, muitas vezes, revelarão traços específicos da personalidade não expostos no ambiente palpável. Permite-se que as pessoas conectadas em rede vivam uma espécie de second life (segunda vida), na qual "as regras de interação social são construídas e não recebidas; o caminho é sinalizado pelo computador, o horizonte é aquele da rede " (RODOTÀ, 2008, p. 119). O preço por essa possibilidade de conexão é a informação que é levada a depositar. (MENEZES; COLAÇO, 2017, p. 2329-2330).

Após a segunda geração de leis de proteção de dados pessoais, o titular assumiu um papel de protagonista no que se refere à proteção de suas informações, ao passo que lhe fornecia as ferramentas necessárias para efetivar a proteção de seus próprios dados (BIONI, 2020, p. 187).

Essa nova diretriz geracional formalizou o direito do indivíduo de controlar seus dados pessoais, o que levou à exigência legal do consentimento do titular dos dados para a coleta, uso, compartilhamento e qualquer outra etapa do tratamento dessas informações.

Essa abordagem reconhece que os dados pessoais são uma extensão da personalidade do indivíduo e, portanto, ele deve ter o poder de decidir como seus dados serão coletados, armazenados e utilizados. O consentimento do titular dos dados é, portanto, visto como uma medida fundamental para garantir que suas informações pessoais sejam tratadas de forma justa e adequada.

> Em que pese ter sempre havido dúvidas em torno da racionalidade e do poder de barganha dos titulares dos dados pessoais para que eles empreendessem um controle efetivo sobre seus dados pessoais, o

> consentimento permaneceu sendo o elemento nuclear da estratégia regulatória da privacidade informacional. A sua adoração pode ser traduzida pelo ciclo de adjetivações recebido ao longo desse trajeto. Seja no direito comunitário europeu [...], seja no que diz respeito às leis setoriais e geral de proteção de dados pessoais no Brasil [...], o consentimento tido como informado, livre, expresso, específico ou inequívoco confirma esse processo de veneração. (BIONI, 2020, p. 188).

BIONI (2020, p. 208) aduz que existem barreiras psicológicas que entorpecem o indivíduo, limitando seu controle sob suas informações pessoais. Uma dessas barreiras seria fundamentada na teoria da decisão da utilidade subjetiva.

De acordo com essa teoria, “O ser humano tem a tendência de focar nos benefícios imediatos, o que [...] é representado pelo acesso a um produto ou serviço on-line [...]” (Ibid., p. 208), e por este motivo o indivíduo faz vista grossa aos virtuais prejuízos à sua própria privacidade, ao passo que os considera improváveis e distantes no futuro.

Ainda segundo o jurista, “[...] uma vez feita tal escolha, é pouco provável que o sujeito volte atrás, revogando o consentimento para o tratamento dos dados pessoais” (Ibid., p. 209). Neste sentido, o “[...] processo de tomada de decisão tende a se levar pelo contexto de que as perdas são maiores do que os ganhos.” (Ibid., p. 209-210)

> Apesar da capacidade de comunicação promovida pela internet, os interesses corporativos acabam levando a política para outro lado, algo que Morozov (2018) indica como “fim da política”. A digitalização da vida promove uma contínua privação da posse das atividades do dia-a-dia, que acabam transformando a vida cotidiana em mercadoria, havendo um labor produtivo para essas grandes empresas no simples ato de se estar conectadas às redes (BELLER, 2013, p. 213-232). (FORNASIER;KNEBEL, 2020, p. 1011).

Neste ínterim, o usuário que teve acesso a um produto ou serviço apresentará uma tendência em privilegiar seus benefícios em detrimento ao controle de seus dados. Desta maneira, o serviço ou produto gratuito acaba sendo ainda mais valorizado, ao passo que “Nesse jogo de ganhos e perdas, o ser humano tende a procurar uma ‘zona de conforto’ para não se culpar em torno do prejuízo por ele suportado.” (BIONI, 2020, p. 209)

> Trata-se das chamadas dissonâncias cognitivas em que o sujeito procura um alívio para simetricamente compensar um desconforto. É nesse contexto que se insere o denominado “paradoxo da privacidade”. Em que pese as pessoas valorarem a proteção de seus dados pessoais, elas empreendem

> ações dissonantes a tal apreço. As suas condutas contradizem o que elas estimam, surgindo-se uma relação de incoerência entre o que elas praticam e o que elas enxergam como ideal. (BIONI, 2020, p. 209).

Integrar-se ao meio virtual talvez já não seja somente uma opção, mas sim uma necessidade, ao passo que aquele que não se conecta às redes caminha para uma espécie de “morte social”. Atualmente, quase todas as pessoas desejam estar conectadas e desfrutando dos benefícios fornecidos pelos serviços e produtos digitais. (MENEZES; COLAÇO, 2017, p. 2320)

Há muito tempo que o campo da ciência jurídica tem se preocupado com as relações desiguais de poder. Isso é evidente no campo do direito do trabalho, no qual o poder econômico do empregador resulta em uma disparidade de forças em relação ao trabalhador. Ultimamente, é possível verificar que o mesmo ocorre no âmbito da privacidade digital. (BIONI, 2020, p. 219)

Apesar de os termos de privacidade destes serviços afirmarem que os usuários têm controle sobre suas informações, como decidir quem pode acessar suas postagens e saber quando é mencionado em publicações de terceiros, percebe-se que ainda há uma lacuna em relação ao tratamento dos dados pessoais e seu compartilhamento com empresas parceiras. (MENEZES; COLAÇO, 2017, p. 2321)

Para SEBASTIÃO (2022, p. 113), devido à cultura brasileira, em uma relação contratual “[...] não é comum que os direitos e deveres [...] sejam questionados já no momento do consentimento, e um dos motivos é a falta de uma leitura atenta antes de expressar concordância [...]”.

Para o pesquisador, isto ocorre com a política de privacidade, documento digital geralmente ignorado pelos indivíduos antes de consentirem com seus termos. Em alguns casos, verifica-se que nem é realizada a coleta do consentimento do usuário antes do início do tratamento de seus dados pessoais. (Ibid., p. 113-114)

O aplicativo de comunicação *WhatsApp* teve sua política de privacidade atualizada em janeiro de 2021 (ANPD, 2022b, n.p.). Em nota, a Autoridade Nacional de Proteção de Dados concluiu que haviam “[...] alterações necessárias para que a política se torne mais clara e transparente para o usuário.” (ANPD, 2022b, n.p.)

Consoante nota do mesmo órgão, os usuários do aplicativo foram notificados pela *WhatsApp Inc.* sobre alterações em sua política de privacidade, mais

precisamente, sobre o compartilhamento de metadados entre o aplicativo e a rede social *Facebook*. (ANPD, 2021, p. 01)

> O compartilhamento de dados pessoais de usuários do WhatsApp com o Facebook não é totalmente uma novidade, posto que o compartilhamento de metadados já ocorria entre as empresas do grupo desde 2016. Segundo a empresa, a alteração da sua política visa atualizar a linguagem para melhorar a legibilidade, introduzir uma formatação mais clara e adicionar alguns exemplos mais atualizados dos produtos e funcionalidades implementados desde a época. (ANPD, 2021, p. 01).

De acordo com o relatório, a nova política de privacidade removeu a restrição de compartilhamento de dados entre as empresas pertencentes à então *Facebook* (ANPD, 2021, p. 10). Desta forma, a empresa agora poderia utilizar dados dos usuários do *WhatsApp* para enviar anúncios personalizados na rede social *Facebook*.

Entre esses dados, estão elencados: dados da conta, mensagens, contatos, suporte ao cliente, dados de uso e registro, dados sobre transações, dados sobre dispositivos e conexões, dados de localização, cookies, dados de status, dados divulgados por terceiros, prestadores de serviços terceirizados e servicos de terceiro (ANPD, 2021, p. 10). A Autoridade Nacional de Proteção de Dados chegou à conclusão de que esta atualização:

> [...] deixa em aberto se o Facebook é capaz ou não de usar as mensagens do WhatsApp para quaisquer motivos. Se o conteúdo das mensagens pode ser acessado pelo Facebook para fins que não estão claros, pode haver um prejuízo à legítima expectativa dos titulares dos dados pessoais, que acreditam que o conteúdo das mensagens nunca é acessado. (ANPD, 2021, p. 13).

Além disso, a notificação emitida pela empresa não fazia referência aos direitos previstos no artigo 18 da Lei Geral de Proteção de Dados, quais sejam: anonimização e bloqueio, revogação do consentimento e informação sobre a possibilidade de não o fornecer. (ANPD, 2021, p. 30)

> Sobre o tema, é importante notar que a necessidade de menção explícita aos direitos previstos no art. 18 da LGPD não pode ser entendida corno uma exigência abstrata de reprodução literal do dispositivo da lei. De forma diversa, o controlador deve privilegiar a utilização de linguagem simples, com informações claras, precisas e facilmente acessíveis, que assegurem ou que, conforme o contexto, sejam adequadas e suficientes para a

> compreensão do usuário, tal como ocorre no presente caso. (ANPD, 2021, p.30).

Com esta observação, é importante ressaltar que em resposta, a *WhatsApp Inc.* disse que “[...] atualmente não se utiliza do consentimento como base legal para tratar dados pessoais no Brasil” (ANPD, 2021, p.30), fator que restringe a aplicação dos direitos relativos ao consentimento.

O caso evidenciado retro deixa explícita a banalização do consentimento, em especial por um grande conglomerado como o *Facebook*, atualmente *META*. No entanto, também se pode citar como exemplos de preocupação com cláusulas abusivas na política de privacidade as práticas dos aplicativos *FaceApp* e *TikTok*, que utilizaram dados pessoais de seus usuários além da finalidade dos referidos aplicativos sem seu consentimento. (SEBASTIÃO, 2022, p. 115)

Neste diapasão, é válido lembrar que a disposição sobre o consentimento do usuário em relação aos documentos digitais, como a política de privacidade, é fundamental e deve ser obtido pelo controlador antes do tratamento dos dados, consoante a Lei Geral de Proteção de Dados (SEBASTIÃO, 2022, p. 114).

Como discutido anteriormente, o consentimento deve ser obtido por meio de uma manifestação livre, informada, inequívoca, eficiente, acessível e atrelada à finalidade (BRASIL, 2018). Além disso, o consentimento deve ser específico quando se tratar de dados pessoais de crianças e adolescentes, e o titular deve ser informado sobre a possibilidade de não fornecer consentimento, bem como as consequências da negativa e da revogação do consentimento. (BRASIL, 2018, artigo 8º, § 5º)

Verifica-se que a política de privacidade dos mais diversos produtos e serviços pode conter cláusulas abusivas que não estejam de acordo com a legislação vigente. Essas cláusulas são geralmente definidas pela violação de direitos ou pela criação de desvantagem excessiva entre as partes, e são formuladas com base na desigualdade de poder entre elas. (SEBASTIÃO, 2022, p. 114)

> Evidentemente, os Intermediários de Internet são estruturas dotadas de grande poder sobre os indivíduos e se apresentam como verdadeiras infraestruturas de serviços considerados essenciais. Os gigantes da Internet, por sua dimensão e oferta de serviços em grande escala, tornaram-se indispensáveis ao cotidiano do homem contemporâneo. O Google é uma ferramenta indispensável para busca de dados; a Amazon

> tornou-se a empresa mais valiosa do mundo e exerce um papel fundamental no setor de vendas a varejo; e o Facebook tornou-se imprescindível para o fluxo de informações e comunicação entre pessoas. À medida em que estas plataformas são mais utilizadas, elas se tornam mais fundamentais para o acesso à informação, podendo-se afirmar que parte da vida econômica, social e cultural dos indivíduos flui por meio dos serviços oferecidos por estas empresas. (CARNEIRO, 2020, n.p.).

As cláusulas podem ser consideradas abusivas quando criadas com o objetivo de se aproveitar da boa-fé do usuário, especialmente em contratos de adesão, em que o fornecedor pode se aproveitar do desejo, da necessidade ou mesmo da falta de instrução e informação clara ao usuário para tornar mais vantajoso aderir ao serviço. Corriqueiramente, documentos eletrônicos apresentam termos técnicos em excesso e concedem acesso ilimitado aos dados pessoais, sem respeitar os direitos do usuário. (SEBASTIÃO, 2022, p. 114)

A despersonalização do contratante é uma constante na sociedade da informação, onde a distribuição de bens e serviços é feita de "[...] maneira padronizada e impessoal através de práticas, tais como, as condições gerais de contrato [...]". (LIMA, 2014, p. 06)

É normal nos depararmos com formulários de consentimento ao navegarmos pela *internet*. Esse contrato de adesão virtual é chamado de *click-wrap*, e nele o fornecedor unilateralmente institui cláusulas, notificando o usuário a fim de conseguir a manifestação do consentimento deste. Nestes casos, o consentimento é demonstrado por via de condutas sociais típicas do meio digital, como por um mero clique. (LIMA, 2014, p. 08)

O consentimento nos contratos deste tipo é manifestado quando o usuário clica em uma determinada parte referente à expressão de anuência, como "eu aceito" ou "eu concordo". (CARNEIRO, 2020, n.p.)

> A partir deste instante, em linha com o princípio do Direito Civil de que o contrato se torna lei entre as partes (pacta sunt servanda), o usuário-adquirente está obrigado às cláusulas contratuais, com as quais concordou expressamente. Esta concordância expressa, contudo, não significa a impossibilidade de se anular o contrato ou algumas de suas cláusulas. O acordo poderá ser anulado nos casos de vício no consentimento, ou seja, naquelas hipóteses nas quais a concordância com os Termos de Uso tenha se dado por erro, dolo ou coação, ou estado de necessidade.10 Também será possível declarar nulas cláusulas consideradas abusivas, conforme o art. 51 do CDC, como, dentre outras, cláusulas de isenção de responsabilidade, arbitragem compulsória e aquelas que possibilitem a alteração unilateral do contrato pelo fornecedor sem garantir esta opção para o usuário. (CARNEIRO, 2020, n.p.).

No entanto, a leitura de políticas de privacidade é demorada e, via de regra, improvável. Conforme aponta CARNEIRO (2020, n.p., apud MCDONALD; CRANOR, 2008, n.p.), um estudo da Universidade Carnegie Mellon concluiu que seria necessário a um usuário reservar oito horas diárias para ler somente as políticas de privacidade de uma média de 1.462 páginas visitadas em um ano.

> Em 2007, um estudo monitorou mais de 48.000 indivíduos que visitaram a página de um serviço e os resultados mostraram que os Termos de Uso foram acessados por menos de 0,2% dos visitantes e, entre os que visitaram, o tempo médio gasto visualizando o contrato foi de 30 segundos (Bakos, Marotta-Wurgler, & Trossen, 2014). Num ambiente virtual marcado pela troca rápida de informações, a leitura dos Termos de Uso se torna dispendiosa e enfadonha, consumindo o tempo produtivo dos usuários. (CARNEIRO, 2020, n.p.)

Levando em consideração que os termos de uso e políticas de privacidade são longos, complexos e às vezes de difícil acesso, empresas podem incluir cláusulas prejudiciais sem o conhecimento do usuário, como no caso a seguir:

> Em uma brincadeira no dia 1º de abril de 2010, a loja de jogos online Gamestation.co.uk incluiu uma disposição nos seus Termos de Uso estabelecendo a transferência da alma do usuário para a empresa. No total, 7.500 usuários não clicaram na opção de “cancelar transferência de alma” disponibilizada pelo site. Por outro lado, algumas empresas já deram prêmios para os primeiros usuários que lessem os Termos de Uso. Em 2019, a empresa de seguros SquareMouth lançou uma campanha secreta chamada It Pays to Read para disseminar a importância da leitura dos Termos de Uso. A companhia pagou um prêmio de 10 mil dólares para a primeira cliente que leu todos os Termos de Uso. (CARNEIRO, 2020, n.p.).

Consoante LIMA (2014, p. 12), “[...] embora exista o dever de ler os termos de um contrato, sendo imperiosa a manutenção deste ônus, há um abuso por parte dos fornecedores [...]”, pois direta ou indiretamente induzem os usuários a não lerem os contratos.

Desta forma, inobstante o ordenamento jurídico disponha em contrário a estas práticas, na realidade fática a proteção do consumidor fica debilitada. LIMA (2014, p. 18) estabelece como possíveis alternativas para a resolução deste problema:

> [...] considerar uma cláusula abusiva no contexto acima descrito (art. 51 do CDC); pressionar o mercado (os fornecedores que operam online) a estabelecerem cláusulas equitativas e que estejam de acordo com a justa expectativa do consumidor diante da relação jurídica em concreto; e, por fim, a adoção de algumas ferramentas tecnológicas, tais como, ter que

> descer até ao final a barra de rolagem para poder finalizar a adesão; aparecer um pop up ou outra ferramenta mais eficaz de avisos (warnings) com os termos que fogem à justa expectativa do consumidor; clicar ao lado de cada cláusula manifestando sua expressa anuência.

Portanto, ante todo o exposto, verifica-se a existência de um abuso de direito por parte dos fornecedores, cujos compactuam com a formalização de contratos e licenças que desestimulam sua leitura à íntegra, porém, as cláusulas restritivas de direito são inseridas neste amontoado de expressões jurídicas. No entanto, LIMA (2014, p. 19) aduz que "[...] a ficção de que houve uma anuência à integralidade do contrato impõe que o usuário se sujeite à restrição com a qual ele 'concordou'."

Seguindo este raciocínio, caso "[...] os tribunais validarem estas cláusulas inseridas em contratos e licenças de uso desta forma, irão consagrar o que se denomina 'ditadura dos contratos de adesão eletrônicos'." (Ibid., 2014, p. 19)

CONSIDERAÇÕES FINAIS

A pletora de produtos e serviços disponibilizados com a evolução dos computadores e da *internet* permitiu que as pessoas fizessem mais com menos recursos e tempo. A digitalização de vários âmbitos do cotidiano, como o comércio e até mesmo a vida social, gerou impactos que provavelmente alteraram a história da humanidade para sempre. Atualmente, é impensável viver em sociedade sem estar atrelado à *internet*, computadores e redes sociais.

Mas como qualquer tecnologia que promova um progresso súbito, a formação da chamada sociedade da informação também trouxe consigo algumas mazelas. Uma delas é o risco que a tecnologia impõe à privacidade, um direito fundamental conforme a Constituição Federal.

Na era digital, conforme exposto ao longo da pesquisa, empresas que oferecem produtos e serviços virtuais possuem grande poder em suas mãos. Aqueles que detém dados podem utilizá-los para os mais variados fins, inclusive alheios ao consentimento de usuários.

Inobstante a legislação dite que o consentimento deve ser adquirido mediante exposição do termos com transparência, de forma clara e inequívoca, essa não é uma realidade.

Redes sociais e aplicativos como o *Facebook*, *WhatsApp*, *TikTok* e *FaceApp* coletam dados de seus usuários e os utilizam como bem entender para personalização de anúncios.

Essas práticas ocorrem geralmente sem o conhecimento do usuário, que inobstante tenha consentido em tese, dificilmente tenha lido a política de privacidade e termos de uso do produto ou serviço, ao passo que as empresas parecem não se importar com a legibilidade desses documentos.

Como foi verificado, há a ocorrência de uma relação assimétrica entre o titular dos dados e o controlador. Normalmente, o titular não dispõe dos meios necessários para realizar o efetivo controle de seus dados, tornando sua privacidade suscetível às vontades das grandes empresas que os coletam.

No Brasil, foi recentemente promulgada a Lei Geral de Proteção de Dados, a qual aborda a proteção de dados no contexto público e privado nacional e internacional.

O Estado se demonstra ávido em realizar a efetivação da referida lei, ao passo que a Autoridade Nacional de Proteção de Dados mantém vigilância constante à atualização e implementação de políticas de privacidade das redes sociais e outras empresas.

No entanto, observou-se que os elementos instituídos pela Lei Geral de Proteção de Dados ainda não são universalmente aplicados e respeitados, ao passo que empresas oferecem produtos e serviços mediante condições que se aproveitam da natureza humana, colhendo o alegado consentimento do usuário na promessa de benefícios imediatos.

O indivíduo, refém da digitalização e constrangido a utilizar tais produtos e serviços, sem escapatória acaba por aceitar quaisquer condições, se tornando ele mesmo um produto em prejuízo de seus direitos fundamentais, efetivando a banalização do consentimento.

REFERÊNCIAS

ANPD. **Tratamento de dados pessoais pelo Poder Público**. 2022a. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 08 out. 2022.

ANPD. **ANPD conclui a análise de adequação da nova Política de Privacidade do WhatsApp à LGPD**. 2022b. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-conclui-a-analise-de-adequacao-da-nova-politica-de-privacidade-do-aplicativo-a-lgpd. Acesso em 11 mai. 2023.

ANPD. **Nota técnica n.º 02/2021/CGTP/ANPD**. 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/NotaTecnicaANPDWhatsapp_ocr.pdf. Acesso em: 11 mai. 2023.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro : Forense, 2019.
BRASIL. **Constituição Federal de 1988**. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 06 out. 2022.

BRASIL. **Lei Geral de Proteção de Dados**. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 06 out. 2022.

BUCHAIN, Luiz Carlos. **Proteção de dados:** legítimo interesse e consentimento. Revista da Faculdade de Direito da UFRGS, Porto Alegre, n. 45, p. 103-127, abr. 2021. Disponível em: Acesso em: 02 mai. 2023.

CARNEIRO, Ramon Mariano. **"Li e aceito":** violações a direitos fundamentais nos termos de uso das plataformas digitais. 2020. Disponível em: https://revista.internetlab.org.br/li-e-aceitoviolacoes-a-direitos-fundamentais-nos-termos-de-uso-das-plataformas-digitais/. Acesso em: 11 mai. 2023.

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. – São Paulo : Thomson Reuters Brasil, 2020.

FORNASIER, Mateus de Oliveira; KNEBEL, Norberto Milton Paiva. **O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados na Lei Geral de Proteção de Dados**. Rev. Direito e Práx., Rio de Janeiro, Vol. 12, n. 2, 2021, p. 1002-1033. Disponível em: https://www.scielo.br/j/rdp/a/hTqmGJVy7FP5PWq4Z7RsbCG/?format=html&lang=pt#. Acesso em: 17 abr. 2023

LEWIS, Paul; HILDER, Paul. ***Leaked:*** *Cambridge Analytica's blueprint for Trump victory*. The Guardian. 2018. Disponível em: https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory. Acesso em: 02 set. 2022.

LIMA, Cíntia Rosa Pereira de Lima. **O ônus de ler o contrato no contexto da "ditadura" dos contratos de adesão eletrônicos**. 2014. Disponível em: https://edisciplinas.usp.br/mod/resource/view.php?id=3200521&forceview=1. Acesso em: 11 mai. 2023.

MA, Alexandra; GILBERT, Ben. ***Facebook understood how dangerous the Trump-linked data firm Cambridge Analytica could be much earlier than it previously said. Here's everything that's happened up until now***. Business Insider, 2019. Disponível em: https://www.businessinsider.com/cambridge-analytica-a-guide-to-the-trump-linked-data-firm-that-harvested-50-million-facebook-profiles-2018-3#where-did-it-come-from-3. Acesso em: 02 set. 2022.

MALDONADO, V. N.; BLUM, R. N. **LGPD:** Lei Geral de Proteção de Dados comentada. 2ª ed. – São Paulo : Thomson Reuters Brasil, 2020.

MENEZES, J. B. de; COLAÇO, H. S. **Facebook como o novo Big Brother:** uma abertura para a responsabilização civil por violação à autodeterminação informativa. Quaestio Iuris. vol. 10, nº. 04, Rio de Janeiro, 2017. Disponível em: https://www.e-publicacoes.uerj.br/index.php/quaestioiuris/article/view/22579. Acesso em: 02 mai. 2023

META. ***An Update on Our Plans to Restrict Data Access on Facebook***. 2018. Disponível em: https://about.fb.com/news/2018/04/restricting-data-access/. Acesso em: 02 set. 2022.

MJSP. **Facebook é condenado a pagar R$ 6,6 mi por vazar dados de usuários**. 2022. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/facebook-e-condenado-a-pagar-r-6-6-mi-por-vazar-dados-de-usuarios. Acesso em 06 out. 2022.

MULHOLLAND, Caitlin Sampaio. **Dados pessoais sensíveis e a tutela de direitos fundamentais:** uma análise à luz da Lei Geral de Proteção de Dados. Revista De Direitos E Garantias Fundamentais, 19(3), 2018, p. 159–180. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603. Acesso em: 15 abr. 2023.

PIURCOSKY, Fabrício Pelloso; et al. **A Lei Geral de Proteção de Dados Pessoais em empresas brasileiras:** uma análise de múltiplos casos. Suma de Negocios, vol. 10, núm. 23, 2019, Julho-Dezembro, p. 89-99 Fundación Universitaria Konrad Lorenz. Disponível em: https://www.redalyc.org/journal/6099/609964312002/609964312002.pdf. Acesso em: 17 abr. 2023

SEBASTIÃO, M. P. D. A. **Proteção aos dados do usuário de serviços digitais pela LGPD e as cláusulas abusivas na política de privacidade**. Cadernos Jurídicos Da Faculdade De Direito De Sorocaba, 3(1), p. 107–120. 2022. Disponível em: https://www.fadi.br/revista/index.php/cadernosjuridicos/article/view/92. Acesso em: 11 mai. 2023.

SHARMA, Sanjay. ***Data privacy and GDPR handbook***. Hoboken, New Jersey : John Wiley & Sons, Inc., 2020.

SILVA, S. A. A. da; CARDOSO, A. M. P.; PINHEIRO, M. M. K. **Lei Geral de Proteção de Dados e Consentimento:** uma análise da política de dados do Facebook. 2021. Disponível em: http://hdl.handle.net/20.500.11959/brapci/192786. Acesso em: 25 abr. 2023.

TEFFÉ, C. S. DE; VIOLA, M. **Tratamento de dados pessoais na LGPD:** estudo sobre as bases legais. Civilistica.com, v. 9, n. 1, p. 1-38, 9 de maio de 2020. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/510. Acesso em: 20 abr. 2023.

ANEXOS

RELATÓRIO DE VERIFICAÇÃO DE PLÁGIO

DISCENTE: Nathan Igor Dias Furlan

CURSO: Direito

DATA DE ANÁLISE: 15.05.2023

RESULTADO DA ANÁLISE

Estatísticas

Suspeitas na Internet: **4,47%**
Percentual do texto com expressões localizadas na internet ⚠

Suspeitas confirmadas: **3,87**%
Confirmada existência dos trechos suspeitos nos endereços encontrados ⚠

Texto analisado: **93,88%**
Percentual do texto efetivamente analisado (frases curtas, caracteres especiais, texto quebrado não são analisados).

Sucesso da análise: **100%**
Percentual das pesquisas com sucesso, indica a qualidade da análise, quanto maior, melhor.

Analisado por Plagius - Detector de Plágio 2.8.5
segunda-feira, 15 de maio de 2023 10:21

PARECER FINAL

Declaro para devidos fins, que o trabalho do discente **NATHAN IGOR DIAS FURLAN**, n. de matrícula **36881**, do curso de Direito, foi aprovado na verificação de plágio, com porcentagem conferida em 4,47%. Devendo o aluno fazer as correções necessárias.

Assinado digitalmente por: Herta Maria de A?ucena do Nascimento Soeiro
Razão: Faculdade de Educação e Meio Ambiente - FAEMA

(assinado eletronicamente)
HERTA MARIA DE AÇUCENA DO N. SOEIRO
Bibliotecária CRB 1114/11
Biblioteca Central Júlio Bordignon
Centro Universitário FAEMA – UNIFAEMA