CIÊNCIA& TECNOLOGIA
ISSN: 2525-6599
unifev pesquisa
Coordenação de Pesquisa

DIREITO DIGITAL: A ÉTICA E A PRIVACIDADE NO CONTEXTO DIGITAL

Maria Eduarda Briz Bueno[1]
Walter Francisco Sampaio Neto[2]

Resumo:
A crescente coleta e utilização de dados pessoais na era digital levanta questões cruciais sobre a ética e a privacidade. O direito de controlar as informações para uma possível autonomia individual está constantemente desafiado pelo avanço tecnológico e pelos interesses comerciais. Dessa maneira, este estudo busca analisar a relação entre ética e privacidade no contexto dos dados digitais, à luz do ordenamento jurídico brasileiro. O tema é fundamental, uma vez que informações digitais se entrelaçam com a privacidade e personalidade individual, protegidas constitucionalmente. E, para manter a ética na evolução tecnológica e promover uma sociedade civilizada, o Direito Digital emerge como um meio de tutelar a personalidade, segurança e desenvolvimento pessoal e social. O método hipotético-dedutivo se construiu analisando teorias éticas existentes e o desenvolvimento do direito digital em diferentes contextos. Além disso, foi realizada uma revisão da literatura com base em repositórios nacionais, pesquisas em jurisprudências relevantes e análise de leis e regulamentações relacionadas ao tema, proporcionando uma compreensão das nuances digitais. A pesquisa verificou a necessidade de um consentimento informado e granular para o tratamento de dados pessoais. Além disso, destacaram-se os riscos éticos associados ao uso indevido dessas informações e a importância da transparência nas operações de dados. Assim, conclui-se que é essencial estabelecer um equilíbrio entre os avanços tecnológicos e a proteção dos direitos individuais, por meio de implementação de medidas legais e técnicas mais robustas para garantir a privacidade e a segurança dos dados pessoais.

Palavras-chave: direito digital; privacidade; ética digital.

Abstract:
The increasing collection and use of personal data in the digital age raises crucial questions about ethics and privacy. The right to control one's information is fundamental to individual autonomy but is constantly challenged by technological advances and commercial interests. This study seeks to analyze the relationship between ethics and privacy in the context of digital data, in the light of the Brazilian legal system. The topic becomes fundamental, since digital information is intertwined with individual privacy and personality, which are constitutionally protected. And to maintain ethics in technological evolution and promote a civilized society, Digital Law emerges as a means of protecting personality, security and personal and social development. The hypothetical-deductive method was constructed by analyzing existing ethical theories and the development of digital law in different contexts. In addition, a review of existing literature, relevant case law and analysis of laws and regulations related to the topic

[1] Centro Universitário de Votuporanga. Votuporanga, São Paulo, Brasil. Bacharelanda em Direito. Email: mariaeduardabriz@hotmail.com
[2] Centro Universitário de Votuporanga. Votuporanga, São Paulo, Brasil. Pós-graduado em Direito Tributário pela UNIFIA - Centro Universitário Amparense. Pós-graduado em Advocacia do Direito Negocial e Imobiliário pelo EBRADI Centro Universitário Uma. Email: walterneto@fev.edu.br.

was carried out, providing an understanding of digital nuances. The research verified the need for informed and granular consent for the processing of personal data. It also highlights the ethical risks associated with the misuse of this information and the importance of transparency in data operations. Thus, it concludes that it is essential to establish a balance between technological advances and the protection of individual rights, through the implementation of more robust legal and technical measures to guarantee the privacy and security of personal data.

Keywords: digital law; privacy; digital ethics.

INTRODUÇÃO

O avanço da tecnologia digital tem gerado impactos profundos na sociedade, transformando relações interpessoais, econômicas e culturais. Como consequência, a questão de como a privacidade e a ética se manifestam nessas novas relações tornou-se motivo de insônia para aqueles que criticam até mesmo o mínimo de sua existência. Neste momento, em que o compartilhamento de informações pessoais se tornou rotineiro, surgem desafios éticos e jurídicos que necessitam de atenção urgente. Para isso, a problemática foi construída em torno do uso indevido de dados pessoais, amplamente explorados por empresas e governos para fins que, muitas vezes, carecem de transparência e principalmente de consentimento informado.

Com base nessa proposição, este trabalho busca analisar os desdobramentos éticos, jurídicos e sociais relacionados ao tratamento de dados pessoais no contexto da economia digital contemporânea. Com fundamento no direito digital, em sua tutela à privacidade, pretende-se aqui compreender como os dados têm sido utilizados para moldar comportamentos, influenciar decisões e impulsionar o capitalismo de vigilância, em detrimento das liberdades individuais.

Metodologicamente, o trabalho emprega pesquisa bibliográfica e o estudo crítico da legislação brasileira de proteção de dados e do regulamento geral de proteção de dados da união europeia. Esses instrumentos teóricos e legais são comparados e aplicados para avaliar o cenário jurídico, bem como identificar lacunas e limitações na proteção de dados pessoais.

Por fim, apresenta-se o ensaio crítico sobre as implicações éticas, sociais e jurídicas da manipulação dessas informações, culminando em considerações finais que sintetizam os desafios enfrentados pelo direito e pela sociedade diante dessa nova realidade. Esta investigação, portanto, não se propõe apenas a descrever o estado atual da proteção de dados, mas a oferecer reflexões que possam subsidiar soluções mais eficazes e equitativas no enfrentamento dos abusos cometidos pelas corporações e na defesa da privacidade como um

direito inalienável.

1 ORIGEM E MANIPULAÇÃO DE DADOS

A polarização e a manipulação de dados são temas centrais no contexto das mudanças tecnológicas e sociais, uma vez que, "toda mudança tecnológica é uma mudança social, comportamental e, portanto, jurídica" (Peck, 2021, p. 43). Nesse sentido, é evidente que, ao longo do último milênio, as inovações tecnológicas disruptivas provocaram profundas transformações na sociedade, gerando novos modelos de negócios e alterando as dinâmicas econômicas, culturais e sociais.

O pensador Guy Debord, em sua obra mais famosa, A Sociedade do Espetáculo, desenvolve a concepção de que "a busca desenfreada pela acumulação de riqueza se tornou o motor principal da vida social" (Debord, 1997, p. 15). Embora suas reflexões sejam anteriores à ascensão das redes sociais, ele já vislumbrava um cenário atual, no qual a degradação do ser em favor do ter, ou parecer ter, se materializa. Essa dependência de poder econômico e o foco na aparência social revelam uma realidade rasa e alienada, e assim quanto mais a vida se transforma em mercadoria, mais o indivíduo se distancia de si mesmo.

Continua o pensador:

> Aqueles que denunciam o absurdo ou os perigos do incitamento à dissipação na sociedade da abundância econômica, não sabem para que serve a dissipação. Eles acusam de ingratidão, em nome da racionalidade econômica, os bons guardas irracionais sem os quais o poder desta racionalidade econômica se desmoronaria. Boorstin, por exemplo, que descreve em A Imagem o consumo mercantil do espetáculo americano, nunca atinge o conceito de espetáculo, por achar poder deixar a vida privada do lado de fora, em sua noção de 'mercadoria honesta'. Não compreende que a própria mercadoria fez as leis cuja aplicação 'honesta' contamina tanto a realidade da vida privada como a sua conquista ulterior pelo consumo social das imagens (Debord, 1997, p. 119).

O presente trabalho não pretende esgotar o lado filosófico do assunto, mas servir como alerta e desenvolver o tema focando no direito à privacidade, uma vez que, no contexto digital contemporâneo, a troca constante de informações entre os usuários não é tão inofensiva quanto parece. Isso ocorre, porque a revolução digital impõe uma reflexão ética sobre a utilização desses dados, e o direito surge como uma ferramenta essencial para proteger a privacidade dos usuários. Frazão (2020, p. 35) esclarece que os dados são o "novo petróleo", essenciais para a economia moderna. A extração e o uso de dados pessoais tornaram-se o centro do capitalismo

do século XXI, uma nova forma de se tomar decisões a partir da análise de uma imensurável biblioteca construída a partir das informações pessoais da humanidade.

A preocupação com a proteção de dados pessoais acompanha o desenvolvimento da mídia, desde os primeiros questionamentos sobre a inviolabilidade dos dados com a imprensa até o surgimento da internet, quando a liberdade de expressão e a privacidade passaram a coexistir. A recente pandemia de COVID-19 acelerou essa transformação digital, agravando e expondo a vulnerabilidade dos dados pessoais e aumentando a necessidade de regulamentação para prevenir o abuso por parte de empresas privadas (Wolfgang, 2021).

A fim de esclarecimento dos termos apresentados, atenta-se à Lei Geral de Proteção de Dados Pessoais, nº 13.709, de 14 de agosto de 2018:

> O artigo 5º, para os fins dessa lei, considera:
>
> 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;
> [...]
> X - tratamento: 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;
> [...]
> XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada; (Brasil, 2018).

São essas informações, resultantes da conversão de representações binárias de fatos e conceitos, que narram o "ser" de cada usuário em interação com sua máquina, por meio de atividades como curtidas, comentários, histórico de pesquisa, entre muitas outras funções básicas. E, nesse formato de tantos zeros e uns, constitui-se a base essencial para a representação desses dados que formam ou “formarão” a pessoa.

Assim, armazenados em seus servidores, mais uma vez convertidos e transformados em mais capital, permitem, por exemplo, que um navegador exiba páginas da web contendo textos,

imagens e vídeos. E, posteriormente, novos conteúdos aos usuários, com base nos seus perfis infinitamente analisados. Essa nova forma de mercado é como um sistema que visa a prever e a influenciar o comportamento humano para obter lucro, desconsiderando os impactos sociais e éticos (Zuboff, 2018).

A autora afirma que o Big Data envolve uma enorme quantidade de informações que podem ser usadas para monitorar comportamentos individuais e coletivos, além de prever tendências e influenciar decisões. Esse processo é mediado por algoritmos, que moldam nossas percepções e orientam nossas ações, afetando o sucesso econômico de produtos e serviços. (Zuboff, 2018).

2 O CONCEITO DA PRIVACIDADE

A proteção de dados começou a ganhar relevância na década de 1970, com a criação de legislações em países europeus, sendo a Suécia a pioneira ao adotar uma lei de proteção de dados em 1973. Esse movimento se expandiu pela Europa, culminando na implementação da Diretiva 95/46/CE, que estabeleceu um marco legal para a proteção de dados na União Europeia. A introdução do Regulamento Geral de Proteção de Dados foi uma resposta às crescentes preocupações com a privacidade na era digital, refletindo a necessidade de um regulamento mais robusto e flexível diante das novas tecnologias.

No Brasil, antes da criação da Lei Geral de Proteção de Dados, a proteção de dados era fragmentada e regida por normas setoriais, como o Código de Defesa do Consumidor e o Marco Civil da Internet. A LGPD veio para consolidar e modernizar essas normas, estabelecendo um regime unificado que abrange tanto dados pessoais quanto sensíveis, e introduzindo conceitos fundamentais, como a responsabilidade dos controladores de dados e os direitos dos titulares. A implementação da LGPD também está associada à criação da Autoridade Nacional de Proteção de Dados, um passo essencial para regulamentar e fiscalizar a aplicação da lei, garantindo a efetividade da proteção de dados no Brasil.

Mas a ideia de privacidade passou por inúmeras transformações ao longo da história, refletindo diferentes contextos. Mais precisamente a discussão sobre o assunto se popularizou no final do século XIX com o artigo de Samuel D. Warren e Louis D. Brandeis, "The Right to Privacy" (1890), definindo o tema como um direito fundamental, descrito “o direito de ficar sozinho".

O conceito, ainda prepamaturo e individualista na época, surge com a crescente intrusão da imprensa na vida privada, facilitada pelas tecnologias emergentes, exigia proteções legais para a privacidade individual. Eles postularam que as violações de privacidade deveriam ser tratadas de forma análoga às violações de honra e propriedade, elevando assim o status legal da privacidade, sendo crucial sua consagração como direito essencial. Transformando-a em um princípio legal e ético vital que protege os indivíduos contra intrusões em suas vidas pessoais, garantindo sua dignidade e autonomia.

A doutrina destaca a distinção entre o direito à privacidade e o direito ao desenvolvimento individual. Ainda que interconectados dentro do âmbito dos direitos pessoais, a privacidade se foca na defesa contra interferências indevidas no espaço pessoal e nas informações de cada um, o desenvolvimento individual abrange uma perspectiva mais ampla, voltada para a autodeterminação e autonomia. Por sua vez, o direito ao desenvolvimento individual, conforme previsto em legislações atuais como a Lei Geral de Proteção de Dados do Brasil, envolve a liberdade de cada pessoa para moldar sua própria identidade sem interferências indevidas. A lei adota o desenvolvimento da personalidade como princípio fundamental, assegurando não só a proteção de dados, mas também a garantia de escolhas pessoais que contribuam para a formação da identidade e da trajetória individual.

A partir da Segunda Guerra Mundial, a definição de privacidade foi incorporada aos direitos universais, com a Declaração Universal dos Direitos Humanos de 1948 declarando em seu Artigo 12 que “ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência”. (Organização Das Nações Unidas, 1948). Contudo, a Guerra Fria impôs restrições aos direitos individuais, subordinando-os às necessidades estatais.

No Brasil, até 2018, não havia uma legislação específica que tratasse da proteção de dados pessoais. Embora o Marco Civil da Internet tenha representado um avanço significativo ao estabelecer diretrizes para a privacidade *online*, as grandes corporações da economia digital veem o direito à privacidade como um obstáculo à expansão do mercado de dados pessoais, pois limita sua capacidade de coletar e monetizar informações dos usuários. Por outro lado, há aqueles que argumentam que o conceito de privacidade se tornou obsoleto no contexto atual, sugerindo que sua preservação como direito inviabiliza a oferta de produtos e serviços mais personalizados e adaptados às necessidades dos consumidores.

Assim, o debate sobre a privacidade no Brasil revela preocupações éticas e jurídicas, pois os termos de serviço das plataformas digitais muitas vezes protegem apenas os interesses comerciais das empresas, deixando os usuários sem recursos legais para contestar o uso de seus dados.

3 ÉTICA, PRIVACIDADE E O CAPITAL

O conceito de ética, está intrinsecamente ligado às implicações do capitalismo de vigilância e às considerações morais que o cercam. A ética nessa estrutura pode ser entendida como os princípios que regem o comportamento de indivíduos e organizações em relação à coleta, análise e utilização de dados pessoais. Esse acúmulo oculto de dados para os quais os indivíduos contribuem sem saber, levanta questões éticas em relação à transparência e responsabilidade, pois os indivíduos podem não entender completamente como seus dados estão sendo usados ou as consequências de seu uso.

O dilema ético é agravado pelo fato de que esses dados podem ser aproveitados com fins lucrativos desafiando as estruturas éticas, levando a um debate contencioso sobre a legitimidade de tais práticas em uma sociedade democrática. Assim o conceito de ética no contexto digital fica multifacetado, abrangendo questões de consentimento, privacidade, manipulação e o equilíbrio entre benefícios coletivos e direitos individuais.

Jørgensen (2019) critica a hipocrisia dessas grandes plataformas, que proclamam proteger os direitos humanos, mas muitas vezes violam a privacidade dos usuários. A privacidade, segundo Rodotà (2008), não se trata apenas de um simples fornecimento de dados, mas envolve o controle sobre o tratamento dessas informações. A exposição exagerada nas redes sociais contribui para o compartilhamento de informações pessoais, gerando dependência e vulnerabilidade. Comenta o autor:

> Nunca se falou tão eloquentemente em ética para simbolizar a necessidade de aprimoramento dos modos pelos quais os indivíduos se portam numa sociedade marcada pela hipervigilância. A construção dos influxos éticos depende, contudo, de bem mais que a mera reflexão sobre sua necessidade; perpassa, é bem verdade, pela derrubada das barreiras que imantam a cognição dos problemas centrais da sociedade para, em avanço, descortinar horizontes de reflexão e autoaprimoramento (Rozatti, 2020, p. 277).

Ela gera dependência por meio da mercantilização de informações pessoais, da dinâmica relacional entre consumidores e empresas e das compensações que os indivíduos fazem em relação à privacidade por conveniência. Essa dependência não é meramente econômica, mas também social, pois molda comportamentos e expectativas em um mundo movido por dados. As implicações dessa dependência levantam questões importantes sobre autonomia, direitos de privacidade e as considerações éticas que envolvem o uso de dados na sociedade contemporânea.

4 UM PROBLEMA PARA O DIREITO

A proteção da privacidade, entretanto, não é apenas uma questão ética, mas também jurídica. A Constituição Federal de 1988, em seu artigo 5º, inciso X, protege a vida privada e a intimidade, diferenciando-as claramente. A vida privada se refere à maneira como o indivíduo se apresenta à sociedade, enquanto a intimidade diz respeito ao que o indivíduo escolhe manter em segredo. O direito tem a função de regulamentar essas questões, garantindo governança ética e inclusão democrática. A proteção de dados vai além da privacidade individual, afetando a liberdade e coibindo a comercialização indiscriminada de dados pessoais (Frazão, 2020, p. 64).

Nesse sentido, Rodotà (2008) propõe princípios para a proteção de dados pessoais, como a correção na coleta, a exatidão, a finalidade e a publicidade dos dados, além do direito ao esquecimento. A Lei Geral de Proteção de Dados, em particular, estabelece princípios claros sobre a coleta e o tratamento de dados, promovendo a transparência, a segurança e a não discriminação. Embora, represente um avanço significativo na proteção de dados, ela geralmente é considerada insuficiente em várias áreas essenciais.

Uma das principais dúvidas de sua eficácia é sua confiança em princípios e padrões gerais, o que pode levar à ambiguidade na interpretação e aplicação. A Lei Geral de Proteção de Dados é fundamentalmente uma lei baseada em princípios, o que significa que fornece diretrizes amplas em vez de regras específicas, gerando dificuldade em entender como implementá-los de forma eficaz na vida real.

Outra limitação é a dependência da autoridade nacional para impor a conformidade e fornecer orientação. A eficácia da Lei Geral de Proteção de Dados depende da capacidade da autoridade de regular e supervisionar as atividades de processamento de dados. Porém essa

capacidade e recursos da autoridade de monitorar a conformidade de forma adequada e lidar com as violações, sem mecanismos robustos de fiscalização, pode resultar no não cumprimento ou proteção efetiva dos direitos em questão.

Além disso, o método de corregulamentação invocado pelo legislador pode não ser suficiente para lidar com as complexidades da proteção de dados em um cenário digital em rápida evolução. A lei incentiva as organizações a adotarem práticas autorregulatórias, mas essa abordagem pode levar a inconsistências na forma como a proteção de dados é implementada em diferentes setores. A falta de uniformidade pode resultar em níveis variados de proteção para indivíduos, prejudicando a eficácia geral da lei

Mais ainda, a LGPD não aborda totalmente os desafios impostos pelas tecnologias emergentes e pela natureza global dos fluxos de dados. À medida que a tecnologia evolui, surgem novos riscos à privacidade e à segurança de dados, e a lei pode ter dificuldade em acompanhar essas mudanças. A dependência da tecnologia como ferramenta regulatória, embora benéfica, também levanta preocupações sobre sua adequação na abordagem da natureza multifacetada das questões de privacidade.

> A Autoridade Nacional de Proteção de Dados foi criada no Brasil com a responsabilidade de supervisionar e garantir a aplicação da Lei Geral de Proteção de Dados, estabelecida pela Medida Provisória 869/2018. A ANPD tem como funções principais a proteção dos dados pessoais e a promoção da transparência nas práticas de tratamento de dados. Para isso, ela desenvolve diretrizes para a implementação da LGPD, monitora a conformidade das organizações com as normas e aplica sanções em casos de descumprimento. Além disso, a ANPD desempenha um papel educativo, informando os cidadãos sobre seus direitos e a importância da privacidade em um contexto digital. (Frazão, 2020, p. 577)

Entretanto, a autoridade enfrenta desafios relacionados à sua independência, uma vez que sua vinculação ao governo federal gera preocupações sobre a imparcialidade na regulação. A proposta inicial da ANPD previa maior autonomia, mas alterações posteriores levantaram dúvidas sobre sua capacidade de fiscalizar eficazmente o tratamento de dados pessoais, especialmente por órgãos públicos.

Além disso, a ANPD também tem a missão de promover a cooperação internacional, facilitando a transferência de dados entre países e alinhando as práticas brasileiras às normas globais de proteção de dados. Sua eficácia em cumprir esses objetivos será constantemente avaliada, tanto no Brasil quanto no exterior.

5 CENÁRIO JURÍDICO BRASILEIRO ATUAL

O cenário jurídico brasileiro, portanto, reflete uma interação complexa entre a intenção legislativa, a aplicação regulatória e a supervisão judicial. Assim, para compreender como as práticas ocultas de coleta de dados entram em conflito com as legislações, é essencial analisar como o consentimento é abordado por essas legislações, proporcionando um panorama claro dos abusos cometidos por grandes plataformas e empresas de tecnologia em relação aos seus usuários.

Primeiramente, sobre o Regulamento Geral de Proteção de Dados (GDPR) e suas diretrizes referentes ao consentimento. Contextualiza a autora:

> Assim como a Diretiva 95/46 e o Regulamento 2016/679, as Guidelines de nº 5 do European Data Protection Board, de 4 de maio de 2020, estabelecem um ponto de partida para a análise da noção do consentimento no Regulamento Geral de Proteção de Dados da União Europeia, focando nas mudanças dessa concepção a partir do advento do Artigo 29 do Working Party Opinion 15/2011. Segundo as Guidelines, passou a ser obrigação dos controladores de dados a descoberta de novas soluções de operação com observância de parâmetros legais a respeito da proteção de dados pessoais e do interesse dos seus fornecedores. (Silva et al., 2022).

O artigo 6° do Regulamento Geral sobre a Proteção de Dados, constituido pela União Europeia, destaca o consentimento como uma das seis bases legais para o tratamento de dados pessoais, estabelecendo que o processamento de dados é lícito somente se o titular der seu consentimento para finalidades específicas. Conforme o texto da lei:

> Licitude do tratamento. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:
> (a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;
> (b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;
> (c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;
> (d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
> (e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;
> (f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança. (União Europeia, 2016).

Portanto, a liberdade na concessão, a especificidade, a informação adequada e a clareza de sua manifestação explícita por parte do titular são cruciais para a conformidade legal e ética no tratamento de dados pessoais. Essa liberdade no consentimento, está diretamente relacionada à capacidade do titular em exercer controle sobre suas informações pessoais, e se houver imposição, coação ou ameaça de prejuízos desproporcionais o consentimento não será considerado válido.

E, para garantir que o consentimento seja genuinamente livre, ele não pode estar atrelado à aceitação compulsória de termos contratuais ou condições que não sejam essenciais à prestação do serviço. As bases jurídicas do consentimento e de um contrato devem ser tratadas separadamente, evitando assim a limitação da autonomia dos titulares. Por exemplo, um aplicativo de edição de fotos que exige acesso à geolocalização para uso, sem oferecer a opção de recusar tal coleta de dados, viola a liberdade de consentimento, uma vez que a geolocalização não é essencial para a finalidade do serviço (Silva *et al.*, 2022).

Outrossim, insta salientar que, quando um serviço envolve múltiplos processamentos de dados para mais de um fim, há a necessidade de que o titular e eventual fornecedor dos dados possa escolher quais dados ele permite serem processados, em vez de terem de consentir por todo um pacote de dados para diversos propósitos. O consentimento deve ser dado para cada um deles, devendo haver, portanto, granularidade (Silva *et al.*, 2022).

Além de livre, o consentimento deve ser específico, a granularidade é fundamental nesse aspecto, pois impede que os dados sejam utilizados para propósitos distintos daqueles para os quais foram originalmente coletados. Dessa forma, o controlador deve oferecer ao titular diferentes opções para cada finalidade de uso dos dados, detalhadamente os fins para os quais os dados serão tratados, fortalecendo a transparência e evitando a coleta e uso indevidos dessas informações.

Para que o consentimento seja válido, ele deve ser informado. Isso significa que o titular dos dados deve receber informações claras e completas sobre o tratamento a ser realizado. O Regulamento Geral sobre a Proteção de Dados em seu artigo 20, define as informações mínimas que devem ser fornecidas:

> Direito de portabilidade dos dados. O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir, se:

> a) O tratamento se basear no consentimento dado nos termos do artigo 6.o, n.o 1, alínea a), ou do artigo 9.o, n.o 2, alínea a), ou num contrato referido no artigo 6.o, n.o 1, alínea b); e
> b) O tratamento for realizado por meios automatizados.
> Ao exercer o seu direito de portabilidade dos dados nos termos do n.o 1, o titular dos dados tem o direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento, sempre que tal seja tecnicamente possível.
> O exercício do direito a que se refere o n.o 1 do presente artigo aplica-se sem prejuízo do artigo 17.o. Esse direito não se aplica ao tratamento necessário para o exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento.
> O direito a que se refere o n.o 1 não prejudica os direitos e as liberdades de terceiros. Embora o regulamento não especifique a forma pela qual essas informações devem ser apresentadas, elas precisam ser comunicadas de maneira acessível e compreensível para todos os titulares, incluindo grupos com necessidades especiais, como crianças ou pessoas com deficiência. (União Europeia, 2016).

A partir dessa análise, é pertinente aprofundar o debate sobre os desafios práticos da implementação dessas normas. Para isso, abordar as exigências técnicas e organizacionais para o cumprimento das regulamentações e avaliar os impactos dessas obrigações em um ambiente cada vez mais globalizado e automatizado.

6 O CONSENTIMENTO EXPLÍCITO, CLARO E INEQUÍVOCO

Por fim, o consentimento deve ser obtido por meio de um ato positivo claro e inequívoco, sem qualquer ambiguidade. O titular deve manifestar seu consentimento de forma ativa, seja por meio de uma ação física, como clicar em uma opção em um aplicativo, ou por uma declaração escrita. O silêncio ou a falta de manifestação não podem ser interpretados como consentimento.

Para situações em que há um risco elevado de violação de privacidade, como em transferências internacionais de dados ou decisões automatizadas envolvendo *profiling*, o consentimento explícito é indispensável, e a expressão clara dessa autorização deve evitar futuras dúvidas sobre sua validade. Isso pode ser obtido por meio de formulários *online*, assinaturas eletrônicas ou até declarações expressas por escrito.

Quanto à responsabilização dos controladores e processadores de dados, estes devem implementar medidas técnicas e organizacionais adequadas para a proteção dos dados pessoais, conforme detalhado pela legislação. Essa concepção está em consonância com os princípios da minimização de dados e da restrição de finalidades, de modo que apenas os dados necessários para finalidades específicas devem ser processados. A jurisprudência sobre a responsabilidade

no tratamento de dados pessoais reforça ainda mais a ideia de que os controladores de dados devem assegurar conformidade com a LGPD. É o entendimento do Superior Tribunal de Justiça:

> O dever de restituição daquilo que é auferido mediante indevida interferência nos direitos ou bens jurídicos de outra pessoa tem a função de preservar a livre disposição de direitos, nos quais estão inseridos os direitos da personalidade, e de inibir a prática de atos contrários ao ordenamento jurídico. STJ, 3ª T., REsp 1.698.701/RJ, rel. Min. Ricardo Villas Bôas Cueva, DJe 08.10.2018.

Esse conceito leva a conclusões para a responsabilidade civil no tratamento de informações pessoais, mas não especifica de forma clara a natureza dessa responsabilidade. Essa ausência de definição tem gerado interpretações divergentes entre a doutrina, abrindo interpretações para a responsabilidade objetiva, baseada no modelo do Código de Defesa do Consumidor. Por outro lado, que ela deve ser subjetiva, fundamentada em elementos como culpa ou negligência, característica que faria maior sentido com o texto da lei, uma vez que este exemplifica tantas diretrizes a fim de contornar o ilícito.

Entre os mecanismos previstos, destaca-se a possibilidade de inversão do ônus da prova, que favorece os titulares de dados ao facilitar a comprovação de suas alegações em casos de danos causados por práticas inadequadas. Além disso, a norma permite a propositura de ações coletivas de indenização, possibilitando que grupos de indivíduos afetados busquem reparação conjunta, o que fortalece a proteção de direitos e amplia o alcance das garantias previstas. (Frazão, 2020).

Entretanto, apesar de o marco legal fornecer uma base sólida para a responsabilização civil, sua eficácia dependerá do desenvolvimento jurisprudencial e da aplicação prática de suas disposições. Esse processo será crucial para consolidar um cenário equilibrado entre a promoção da inovação tecnológica e a garantia dos direitos fundamentais à privacidade e à proteção de dados pessoais no Brasil.

CONSIDERAÇÕES FINAIS

Embora a LGPD marque um avanço significativo na proteção de dados no Brasil, sua abordagem baseada em princípios, dependência de autoridades reguladoras e desafios para lidar com os avanços tecnológicos contribuem para sua insuficiência. Para que ela seja realmente eficaz, deve existir mais refinamento e adaptação para garantir a proteção abrangente dos dados

pessoais em um ambiente digital cada vez mais complexo.

Entretanto, a proteção de dados não deve ser vista como uma simples questão legislativa, mas como uma necessidade urgente em um mundo digital interconectado. Embora muitas organizações, especialmente as de tecnologia, possuam normas de organização e gestores especializados, nem sempre as práticas estão alinhadas aos preceitos jurídicos e éticos.

Assim, torna-se fundamental fundamental que os titulares dos dados estejam cientes de seus direitos, especialmente no que se refere ao acesso, implicando na responsabilidade do controlador em garantir práticas adequadas no uso desses dados. Isso é particularmente significativo no contexto em que indivíduos expõem dados pessoais de forma inadequada, muitas vezes, devido a autorizações erradas concedidas em plataformas de mídias sociais, onde os usuários frequentemente ignoram o consentimento dado anteriormente.

Além disso, é necessário demonstrar que há uma conexão substancial entre as atividades de processamento e os objetivos específicos para os quais os dados estão sendo coletados, representando um ônus para os controladores de dados no que diz respeito ao cumprimento de suas obrigações legais. Na relação sigilosa de informações, como em requisições médicas, a capacidade consultada legalmente exige não apenas conformidade, mas também o fomento a uma cultura de responsabilidade entre as organizações que processam dados pessoais em suas atividades.

A implementação de mecanismos de controle nas redes sociais, como algoritmos que evitem a criação de "bolhas" e a promoção de desinformação, seria um passo essencial para mitigar os riscos de manipulação de comportamento e assegurar o desenvolvimento pessoal autônomo. Da mesma forma, os usuários devem adotar uma postura mais crítica em relação ao uso dessas plataformas, buscando fontes diversificadas de informação e se familiarizando com as políticas de privacidade, o que fortaleceria a proteção de suas liberdades individuais.

Conclui-se que a transformação do modelo de negócios atual é necessária para garantir um ambiente *online* mais seguro e protegido. O direito à autodeterminação informativa e a proteção dos dados pessoais são essenciais para preservar a privacidade e a dignidade dos indivíduos em um mundo cada vez mais digital. A adaptação da legislação e a implementação de normas eficazes são passos fundamentais para assegurar uma governança digital justa e ética.

REFERÊNCIAS

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 2016. 496 p. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88_Livro_EC91_2016.pdf. Acesso em: 23 nov. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965/2014 (Marco Civil da Internet). **Diário Oficial da União**, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato20152018/2018/lei/l13709.htm. Acesso em: 23 nov. 2024.

BRASIL. Superior Tribunal de Justiça (3. turma). Recurso Especial. Direito Civil. Uso indevido de imagem. Fins Comerciais. Enriquecimento sem causa. art. 884 do Código Civil. Justa Causa. Ausência. Dever de Restituição. Lucro da intervenção. Forma de quantificação. Relator: Ministro Ricardo Villas Bôas Cueva, 02 outubro 2018. Brasília: **Revista do Superior Tribunal de Justiça**. Disponível em: https://scon.stj.jus.br/scon/pesquisar.jsp?b=acor&livre=%28resp.clas.+e+%40num%3d%221698701%22%29+ou+%28resp+adj+%221698701%22%29.suce.&o=jt. acesso em: 23 nov. 2024.

DEBORD, Guy. **A sociedade do espetáculo.** Rio de Janeiro: Contraponto, 1997.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: RT, 2019.

FACCHINI NETO, Egênio; DEMOLINER, Karine Silva. Direito à privacidade na era digital – uma releitura do ART. XII da Declaração Universal dos Direitos Humanos (DUDH) na Sociedade do Espetáculo. **Revista Internacional Consinter de Direito,** Paraná, Brasil, v. 5, n. 9, p. 119–140, 2019. Disponível em: https://doi.org/10.19135/revista.consinter.00009.06. Acesso em: 23 nov. 2024.

FRAZÃO, Ana. Big Data, Plataformas Digitais e Principais impactos sobre o direito da concorrência. In: ROSS, Alec. **The industries of the future**. Nova Iorque: Simon & Schuster, 2016.

ONU - Organização das Nações Unidas. **Declaração Universal dos Direitos Humanos da ONU**. Disponível em :https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 23 nov. 2024.

RODOTÀ, Stefano. **A vida na sociedade da vigilância:** a privacidade hoje. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2019. Disponível em: https://cetic.br/media/docs/publicacoes/2/20200707094721/tic_empresas_2019_livro_eletronico.pdf. Acesso em: 23 nov. 2024.

ROZATTI, João Victor (Coord.). **Fundamentos do Direito Digital.** Uberlândia: LAECC, 2020.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena (coord.). **Lei Geral de Proteção de dados Pessoais:** e suas repercussões no Direito Brasileiro. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

UNIÃO EUROPEIA, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**General Data Protection Regulation**), Art. 6: Lawfulness of processing, 2016a.

WOLFGANG, Hoffmann-Riem. **Teoria Geral do Direito Digital**. São Paulo: Grupo GEN, 2021. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559642267/. Acesso em: 23 nov. 2024.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. São Paulo: Intrínseca, 2021.