FACULDADE DE DIREITO DE VITÓRIA
CURSO DE GRADUAÇÃO EM DIREITO

MIRELA BULOTO DE SOUZA

A VULNERABILIDADE DO CONSUMIDOR NA ERA DIGITAL:
COMERCIALIZAÇÃO DE DADOS PESSOAIS SEM CONSENTIMENTO, À LUZ DO ARTIGO 7º, INCISO I DA LEI GERAL DE PROTEÇÃO DE DADOS

VITÓRIA
2025

MIRELA BULOTO DE SOUZA

A VULNERABILIDADE DO CONSUMIDOR NA ERA DIGITAL:
COMERCIALIZAÇÃO DE DADOS PESSOAIS SEM CONSENTIMENTO, À LUZ DO ARTIGO 7º, INCISO I DA LEI GERAL DE PROTEÇÃO DE DADOS

Trabalho de conclusão de curso apresentado ao Curso de Graduação em Direito da Faculdade de Direito de Vitória-FDV, como requisito para a aprovação na disciplina Projeto de Conclusão de Curso.
Orientador: Prof. Bruno Costa Teixeira.

VITÓRIA
2025

MIRELA BULOTO DE SOUZA

A VULNERABILIDADE DO CONSUMIDOR NA ERA DIGITAL:
COMERCIALIZAÇÃO DE DADOS PESSOAIS SEM CONSENTIMENTO, À LUZ DO ARTIGO 7º, INCISO I DA LEI GERAL DE PROTEÇÃO DE DADOS

Trabalho de conclusão de curso apresentado ao Curso de Graduação em Direito da Faculdade de Direito de Vitória-FDV, como requisito para a aprovação na disciplina Projeto de Conclusão de Curso.
Orientador: Prof. Bruno Costa Teixeira.

.

Aprovada em: XX/XX/XX

COMISSÃO EXAMINADORA:

_____

Prof(a). Dr(a). xxxxxxxxxxx
Orientador(a).
Faculdade de Direito de Vitória

_____

Prof(a). Dr(a). xxxxxxxxxxx
Faculdade de Direito de Vitória

_____

Prof(a). Dr(a). xxxxxxxxxxx
Faculdade de Direito de Vitória

AGRADECIMENTOS

Primeiramente, agradeço a Deus, por me conceder força, serenidade e sabedoria para enfrentar os desafios que surgiram ao longo desta caminhada.

Aos meus pais, Danielle Rodrigues Buloto de Souza e Jefferson Helder de Souza pela dedicação, amor incondicional e por nunca medirem esforços para que eu tivesse acesso à melhor educação possível.

Aos meus irmãos, Jefferson Buloto de Souza e João Pedro Buloto de Souza que são meu maior apoio e motivo de alegria, agradeço por estarem sempre ao meu lado.

À minha tia Rafaela Rodrigues Buloto, verdadeira inspiração como pessoa, profissional, e exemplo constante ao longo dessa jornada.

À minha prima Isabela Buloto Rabelo, pela presença acolhedora e pelas palavras que me acalmaram nos momentos mais desafiadores.

Aos meus amigos, que tornaram essa jornada mais leve e repleta de boas lembranças, minha sincera gratidão pela parceria e companheirismo.

Ao meu orientador, Bruno Costa, pela paciência, orientação e por ter sido fundamental na construção deste trabalho.

À EDV Jr, empresa júnior da FDV, pela contribuição essencial para o meu amadurecimento pessoal e desenvolvimento profissional, bem como pelos valiosos ensinamentos e pelas amizades construídas ao longo dessa jornada.

E, por fim, a todos os professores da FDV, que, com dedicação e compromisso, contribuíram para minha formação.

RESUMO

O presente trabalho analisa a aplicação da Lei Geral de Proteção de Dados Pessoais - LGPD (Lei número 13.709/2018) no contexto das relações de consumo digitais, com enfoque na validade do consentimento e na vulnerabilidade informacional do consumidor diante das práticas de tratamento de dados. O estudo parte da constatação de que a crescente digitalização das relações comerciais intensificou o uso de tecnologias voltadas à coleta e análise de informações pessoais, exigindo uma interpretação integrada entre a LGPD e o Código de Defesa do Consumidor. Busca-se demonstrar que a manipulação algorítmica e a ausência de transparência comprometem a autonomia da vontade do titular, tornando o consentimento inválido quando obtido de forma viciada ou opaca. A partir do método hipotético-dedutivo, o trabalho examina os fundamentos normativos da proteção de dados, os princípios da boa-fé, finalidade e necessidade, bem como o regime de responsabilidade civil dos agentes de tratamento. A análise de casos práticos, como os incidentes envolvendo as empresas Raia Drogasil, Loggi e *23andMe*, evidencia a materialização dos riscos decorrentes do uso indevido de dados pessoais e a importância da conformidade com os dispositivos legais. Conclui-se que a efetividade da proteção de dados pessoais depende não apenas da observância formal das normas, mas do fortalecimento de uma cultura de transparência, responsabilidade e respeito à autodeterminação informativa do consumidor.

Palavras-chave: Lei Geral de Proteção de Dados; Consentimento; Vulnerabilidade do consumidor; Responsabilidade civil; Privacidade digital.

ABSTRACT

This study analyzes the application of the Brazilian General Data Protection Law (Law No. 13.709/2018 – LGPD) within the context of digital consumer relations, focusing on the validity of consent and the informational vulnerability of consumers in data processing practices. This research acknowledges that the increasing digitalization of commercial interactions has intensified the use of technologies aimed at collecting and analyzing personal information, demanding an integrated interpretation between the LGPD and the Consumer Defense Code. The study seeks to demonstrate that algorithmic manipulation and lack of transparency undermine the data subject's autonomy, generating an invalid consent when obtained through deceptive or weak protection means. Using the hypothetical-deductive method, the research studies the normative foundations of data protection, the principles of good faith, purpose, and necessity, as well as the civil liability regime given to data controllers and processors. The analysis of practical cases, such as the incidents involving Raia Drogasil, Loggi, and 23andMe, reveals the materialization of risks coming from the irresponsible usage of personal data and highlights the importance of compliance with legal standards. The study concludes that the effectiveness of personal data protection depends not only on formal adherence to legal norms but also on adopting a culture of transparency, accountability, and respect for the consumer's informational self-determination.

Keywords: Privacy Law; Personal data; Consent; Consumer vulnerability; Civil liability; Digital privacy.

SUMÁRIO

APRESENTAÇÃO

A introdução da internet foi impulsionada pelo fenômeno da globalização, que fez transformações de cunho político, social e econômico, gerou evolução dos meios de transporte e tecnologia no âmbito global (Campos; Canavezes, 2007, online).

Tais acontecimentos, fizeram com que a informação fosse difundida de forma cada vez mais eficaz tendo pontos positivos, como o maior acesso à informação e contato entre pessoas de diversas partes do mundo. No entanto, trouxe novos problemas para o mundo digitalizado, dentre eles, a ausência de limites presentes na internet, como a coleta dos dados pessoais do usuário, surgindo assim, maior vulnerabilidade do consumidor.

A partir da maior exposição da intimidade e privacidade das pessoas no ambiente virtual, os dados pessoais dos usuários são adquiridos em muitos casos por meio do consentimento viciado ou involuntário, sendo necessário o diálogo entre a Lei número 8.078/1990 (Código de Defesa do Consumidor) e Lei número 13.709/2018 (Lei Geral da Proteção de Dados Pessoais - LGPD), para a proteção jurídica efetiva do indivíduo.

O acesso a sites e redes sociais viabiliza o abastecimento e o tráfego de dados pessoais, que foram disponibilizados de forma voluntária ou não pelo usuário. Uma vez coletados e armazenados, esses dados assumem um valor significativo, tendo em vista que permitem mapear preferências pessoais com alto grau de precisão, especialmente quando utilizados por sistemas de inteligência artificial na elaboração de padrões de comportamento e consumo.

Desta forma, a circulação e o aproveitamento de dados passaram a configurar uma nova forma de atividade econômica, tendo como objetivo a centralidade de informação como recurso estratégico. A busca por mecanismos mais eficientes de obtenção e tratamento destes, é considerada como uma nova forma de poder, de modo que as empresas e Estados se dedicam a ampliar sua capacidade de controle informacional, para que detenham benefícios na esfera comercial e organizacional.

Ao ser analisado tal cenário, percebe-se uma correlação entre a falta do acesso à informação aos usuários, o avanço das tecnologias de controle, bem como, a intensa extração de dados pessoais. Desta forma, pode-se afirmar que a base legal do consentimento é legítima para o tratamento de dados pessoais nas práticas de manipulação algorítmica em anúncios direcionados?

A partir do problema de pesquisa exposto acima, este trabalho busca verificar a hipótese de que a manipulação algorítmica em campanhas publicitárias nas redes sociais compromete a validade do consentimento do titular de dados, tornando-o inválido quando obtido de forma induzida, opaca ou sem plena liberdade de escolha**.**

Parte-se da premissa de que, ao direcionar anúncios com base em perfis comportamentais construídos por meio de coleta massiva de dados pessoais, as plataformas digitais violam o princípio da autodeterminação informativa e fragilizam a manifestação de vontade do consumidor, em afronta aos artigos 6º, incisos I e VIII, e 8º da Lei Geral de Proteção de Dados Pessoais (Lei número 13.709/2018**)**, bem como aos princípios da transparência e boa-fé objetiva previstos no Código de Defesa do Consumidor (Lei número 8.078/1990)**.**

Assim, a hipótese central sustenta que o consentimento obtido mediante manipulação algorítmica não pode ser considerado livre, informado e inequívoco, carecendo de validade jurídica.

A Base teórica que norteia este trabalho é constituída, essencialmente, pelos seguintes autores: Laura Schertel Mendes (2020), em sua obra *Autodeterminação informativa: a história de um conceito*, que destaca que o direito à proteção de dados deve ser compreendido como uma projeção do princípio da dignidade da pessoa humana, sendo expressão direta da liberdade individual frente ao poder informacional das corporações. Para a autora, a autodeterminação informativa não se resume ao simples consentimento do titular, mas abrange o efetivo controle sobre a coleta, uso e circulação dos seus dados pessoais, constituindo instrumento de empoderamento do indivíduo no ambiente digital.

Nessa mesma perspectiva, Bruno Ricardo Bioni (2021), em *Proteção de Dados Pessoais: a função e os limites do consentimento*, reforça que o consentimento deve ser interpretado como um dos meios de legitimar o tratamento de dados, mas não o único, pois a proteção informacional deve ser pautada por princípios estruturantes como finalidade, necessidade e transparência.

Já Maria Celina Bodin de Moraes (2019), ao lado de João Quinelato de Queiroz, em *Autodeterminação informativa e responsabilização proativa*, sustenta que a efetividade da tutela de dados pessoais depende da adoção de mecanismos preventivos e de uma responsabilização proativa das empresas, que devem incorporar a ética e a boa-fé nas práticas de tratamento de informações.

Assim, as visões de Mendes, Bioni e Moraes convergem ao compreender a proteção de dados como elemento essencial à dignidade humana e à mitigação da vulnerabilidade do consumidor na sociedade digital.

O método adequado para esse trabalho é o hipotético-dedutivo (Popper, 2014, p. 4). Afinal, parte-se de um problema de pesquisa, “em que medida a manipulação algorítmica em campanhas publicitárias nas redes sociais pode comprometer a validade do consentimento” para, a partir dele, verificar a hipótese no sentido de que de que essas práticas fragilizam a autonomia do titular de dados e tornam o consentimento inválido quando obtido de forma manipulada.

No Capítulo 1, apresenta-se o contexto da sociedade digital e os reflexos das novas tecnologias sobre o comportamento do consumidor, destacando a necessidade de proteção jurídica dos dados pessoais.

O Capítulo 2 aborda o marco normativo da proteção de dados, com ênfase na LGPD e no consentimento como requisito de validade do tratamento, além do dever de transparência nas relações de consumo.

O Capítulo 3 analisa a responsabilidade civil dos agentes de tratamento e a aplicação conjunta da LGPD e do Código de Defesa do Consumidor, ressaltando a vulnerabilidade do consumidor digital.

Por fim, o Capítulo 4 examina casos concretos, como os da Raia Drogasil, Loggi e *23andMe*, evidenciando as consequências jurídicas das violações à proteção de dados e a invalidade do consentimento obtido de forma manipulada.

1 A SOCIEDADE DIGITAL E A VULNERABILIDADE DO CONSUMIDOR NA ERA DOS DADOS

Vivencia-se, na contemporaneidade, o predomínio de um novo paradigma social sustentado a partir da internet, que deixou de ser apenas uma inovação tecnológica para se tornar um meio de comunicação e organização social. Assim como as fábricas e as grandes corporações moldaram a dinâmica econômica e social da era industrial, hoje a rede digital ocupa papel equivalente na configuração das relações humanas, econômicas e culturais (Castells, 2003, p. 287).

Nesse contexto, as organizações empresariais desempenharam papel decisivo na difusão dos ambientes digitais, em que diante das transformações do mercado, as empresas se viram obrigadas a incorporar inovações tecnológicas como forma de otimizar o desempenho, conter despesas e sustentar sua posição competitiva, por meio do direcionamento de suas atividades para o comércio digital, investindo inicialmente em estratégias de publicidade, criando novas formas de aquisição de produtos e serviços pelos consumidores (Rifkin, 2016, p. 25).

Nesse cenário, entre os diversos desafios sociais decorrentes da era da informação, destaca-se a vulnerabilidade do consumidor, uma vez que é nesse ambiente que os dados pessoais passam a ser amplamente coletados e monitorados. Assim, diferentes aspectos da vida do indivíduo acabam sendo influenciados ou determinados por seus comportamentos e padrões de navegação no ambiente digital (Paiva; Lira, 2022, p. 3).

A publicidade constitui um elemento essencial na sociedade de consumo**,** pois tem como principal finalidade informar o consumidor sobre os produtos e serviços ofertados no mercado**,** buscando despertar seu interesse e estimular o ato de consumo (Cavalieri Filho, 2019, p. 157).

Portanto, visando tornar mais homogêneos os processos produtivos e as estratégias de mercado**,** além de minimizar incertezas nas atividades empresariais**,** as empresas passaram a reunir e tratar continuamente vastas quantidades de informações sobre os usuários e seus comportamentos de consumo (Paiva; Lira, 2022, p.10).

O avanço do comércio eletrônico ganhou ainda mais força durante a pandemia de Covid-19. Diante das restrições de circulação e do fechamento temporário das lojas físicas, diversas empresas foram levadas a adaptar seus

modelos de negócio e buscar novas estratégias para garantir sua continuidade no mercado (Santana; Alves, 2025, p.5).

O setor de comércio eletrônico apresentou um crescimento histórico em 2020, impulsionado tanto pelo aumento da demanda durante a pandemia de Covid-19 quanto pela entrada de novas empresas no ambiente digital. A informação foi destacada em levantamento realizado pela Associação Brasileira de Comércio Eletrônico (ABComm) em parceria com a Neotrust (E-commerce Brasil, online, 2021).

Segundo o estudo, as vendas online aumentaram cerca de 68% em relação a 2019, fazendo com que a participação do e-commerce no faturamento do varejo saltasse de aproximadamente 5% no fim de 2019 para mais de 10% em determinados períodos do ano seguinte (E-commerce Brasil, online, 2021).

Dessa forma, o comércio eletrônico deixou de ser apenas uma tendência para se tornar uma necessidade imposta pelas transformações sociais e econômicas contemporâneas**.** O desenvolvimento tecnológico e a ampla conectividade global instauraram novas dinâmicas nas relações de consumo, demandando uma análise cuidadosa acerca da proteção dos direitos do consumidor nesse contexto digital (Santana; Alves, 2025, p. 5).

Atualmente, os dados demonstram que o crescimento do comércio eletrônico não apenas se manteve após o período pandêmico, como também atingiu patamares ainda mais expressivos, de modo que as micro e pequenas empresas do Brasil registraram um aumento expressivo nas vendas realizadas por meio do comércio eletrônico, com alta de cerca de 1.200% entre 2019 e 2024, período em que o faturamento passou de R$ 5 bilhões para R$ 67 bilhões (Brasil, online, 2025).

As informações constam na terceira edição do Painel Nacional de Comércio Eletrônico, elaborado pelo Ministério do Desenvolvimento, Indústria, Comércio e Serviços (MDIC) a partir de dados fornecidos pela Receita Federal, de modo que tal estudo, pela primeira vez, incluiu um recorte voltado ao desempenho das empresas enquadradas no Simples Nacional nas transações virtuais (Brasil, online, 2025).

Os dados indicaram que as empresas de médio e grande porte também ampliaram significativamente sua participação no comércio eletrônico, de modo que o faturamento passou de R$49 bilhões para R$158 bilhões no mesmo período, tendo o crescimento de aproximadamente 220% (Brasil, online, 2025).

Nesse contexto de expansão acelerada do comércio eletrônico, em que cada transação online gera uma vasta quantidade de informações, o uso combinado de múltiplas ferramentas automatizadas permite capturar informações pessoais delicadas dos indivíduos e criar perfis digitais complexos, que acabam servindo de base para decisões em âmbitos econômico, político e social (Mendes, 2008, p. 397)

Contudo, essa prática eleva de forma expressiva o risco de violação da privacidade e da individualidade do consumidor, uma vez que a extração e o uso indevido de dados pessoais podem afetar a percepção do usuário sobre sua própria identidade e sua visão de mundo (Paiva; Lira, 2022, p.10).

A tecnologia exerce influência decisiva no progresso econômico, impulsionando a produção nacional e contribuindo para a ampliação da riqueza dos países, ao mesmo tempo em que precisa ser aplicada de maneira a respeitar e preservar os direitos individuais estabelecidos pela Constituição Federal de 1988 (Fabriz; Martinelli, 2025, p.2).

Além disso, tal conduta representa uma ofensa ao direito fundamental à privacidade, assegurado pelo artigo 5º, inciso X, da Constituição Federal, que garante a inviolabilidade da intimidade, da honra e da imagem das pessoas (Brasil, 1988, online).

Nesse contexto, evidencia-se que os deveres fundamentais não devem ser vistos como limitações a esses direitos, mas como mecanismos que viabilizam sua concretização e asseguram sua plena proteção na prática social e jurídica (Vieria, Pedra, 2013, p. 6).

Os dados pessoais se tornaram essenciais para a economia e, além disso, representam uma base fundamental e um recurso estratégico para diversos modelos de negócios e para a criação de políticas públicas. Dessa forma, tanto a economia quanto a sociedade tornam-se cada vez mais dependentes e condicionadas ao contínuo fluxo dessas informações (Bioni, 2021, p. 107).

Ao considerar a desigualdade existente entre as partes nas relações de consumo e a evidente vulnerabilidade do consumidor, torna-se essencial garantir, tanto no âmbito administrativo quanto judicial**,** a implementação de mecanismos de proteção específicos para aqueles cujos dados pessoais são coletados, processados e transferidos (Mendes, 2008, p. 130).

À medida que os indivíduos se tornam mais imersos em ambientes digitais hiperconectados, a exposição de seus dados pessoais é intensificada, o que por sua

vez, acentua sua vulnerabilidade e a possibilidade de serem submetidos a práticas de manipulação informacional.

Infere-se que tal situação de insegurança do consumidor é agravada pelo crescente assédio de consumo, do desequilíbrio de acesso à informação e da aceitação sem consciência acerca de cláusulas em contratos eletrônicos, sendo intensificado pelo uso inadequado e pela ausência de segurança no tratamento de dados.

Assim, a captação e o direcionamento indevidos de dados sensíveis têm sido utilizados para encontrar perfis de consumidores, sendo estabelecidos padrões estéticos e comportamentais para que ocorra a segmentação do público-alvo. Desse modo, destaca-se a limitação da liberdade de escolha do indivíduo, por esse estar sendo induzido a consumir determinado produto sem consentimento (Verbicaro; Montão, 2022, p.12).

Tal conduta tem influência direta na forma nociva por práticas de assédio mercadológico, atualmente vedado pelo artigo 54- C, inciso VI do Código de Defesa do Consumidor (CDC), que também compromete a privacidade do usuário, pela utilização oculta de determinadas informações pessoais (Verbicaro; Montão, 2022, p.20).

Acerca de tal tema, cabe destacar o documentário “Shoshana Zuboff em Capitalismo de Vigilância” (Duong, 2019, online), em que a autora apresenta o modelo do capitalismo de vigilância como uma nova fase do capitalismo, caracterizada pela apropriação de dados pessoais, fornecidos de forma espontânea pelos usuários, os quais são convertidos em estratégias de alto valor comercial pelas grandes corporações tecnológicas.

O chamado capitalismo de vigilância foi dividido com base em três eixos centrais: (i) as estruturas que sustentam esse novo modelo de produção; (ii) a expansão das dinâmicas digitais para o âmbito da vida real; e (iii) o uso instrumental dos dados como forma de poder e controle (Zuboff, 2019, p. 14- 15).

O conceito procura delinear e compreender as dinâmicas de mercado nas quais o capitalismo se reconfigura ao pressupor que toda ação humana pode ser convertida em dados. Dessa forma, ainda que parte dessas informações seja utilizada para o aperfeiçoamento de serviços, uma parcela significativa é direcionada à exploração de padrões comportamentais pelos detentores dos dados (Fornasier, Knebel, 2020, p.7)

Verbicaro e Montão (2022, p.8), ao analisar o documentário, Zubofff (2019, online) afirmam que a alegação das empresas acerca da coleta de dados tem como objetivo aprimorar os serviços oferecidos. Entretanto, a autora alega que essas informações são utilizadas para identificar padrões de comportamento e prever preferências de grupos específicos.

Esse processo, denominado por ela como “excedente comportamental”, consiste em fluxos de dados com alto potencial preditivo, posteriormente direcionados para estratégias de consumo (Verbicaro; Montão, 2022, p.8).

O sistema do capitalismo de vigilância se faz presente no cotidiano na dimensão coletiva no tratamento de dados pessoais, de modo que inicialmente o foco era no indivíduo, porém os algoritmos atuais buscam compreender padrões de comportamento de grupos e populações, sendo ampliado o impacto social dessas práticas (Zuboff, 2019, online).

Cabe salientar que durante a navegação diária na internet, os usuários fornecem de forma voluntária e involuntária dados pessoais relacionados a preferências, sentimentos e posicionamentos. Esses dados são coletados pelas empresas de tecnologia, processados e transformados em ferramentas de predição comportamental, que são posteriormente comercializadas com o objetivo de influenciar decisões de consumo, muitas vezes sem o consentimento claro do titular (Mena, 2019, online).

Diante desse panorama, torna-se essencial reconhecer que o tratamento das informações pessoais possui uma dimensão social ampla, cujos reflexos extrapolam o âmbito individual. A expansão das práticas de coleta e utilização de dados, que hoje transbordam do espaço virtual para o cotidiano físico, revela um fenômeno que afeta coletivamente a organização das relações sociais e econômicas contemporâneas (Meireles, 2021, p. 2).

A partir da lógica do capitalismo de vigilância, em que os dados pessoais se transformam em insumo estratégico para predição e controle de comportamentos, a utilização de tecnologias aparentemente inofensivas, como a tecnologia conhecida como “cookies”**,** pequenos arquivos presentes na maior parte dos sites da internet. Esses arquivos permitem a construção de bases de dados com o objetivo de otimizar e personalizar a experiência do usuário (Paiva; Lira, 2022, p.11)

Em princípio, o armazenamento do histórico de navegação do usuário tem por finalidade aprimorar a funcionalidade e a experiência nos sites visitados. Todavia,

determinados *cookies* são utilizados para traçar o perfil de consumo do internauta, identificando seus interesses e preferências, a fim de direcionar a anúncios de produtos anteriormente pesquisados ou visualizados (Pinheiro; Bonna, 2020, p.5).

Ao receber uma solicitação de um usuário, o servidor web pode consultar os cookies previamente armazenados, reconhecer as preferências individuais e exibir imediatamente produtos ou conteúdos alinhados aos interesses do usuário (Deitel; Deitel, 2010, p. 971).

A capacidade de retenção de informações na Internet, somada aos mecanismos tecnológicos que permitem associar padrões de comportamento semelhantes, revela-se praticamente inesgotável. Tal característica confere à rede um poder significativo de monitoramento e de interpretação das interações sociais, passível de utilização para múltiplos propósitos (Pinheiro; Bonna, 2020, p.5).

A possibilidade de coleta e processamento de dados pessoais em larga escala tem se ampliado de forma exponencial, sobretudo em razão do avanço das tecnologias de inteligência artificial, que operam por meio de algoritmos complexos e mecanismos de aprendizado automatizado (Mulholland, 2018, p.15).

A consolidação do ambiente digital transformou as relações de consumo, tornando os dados pessoais o principal ativo da economia informacional. Nesse contexto, o consumidor passa a ocupar posição de vulnerabilidade acentuada, pois suas interações e preferências são constantemente monitoradas, registradas e convertidas em valor econômico (Veloso, 2025, p. 3).

Diante desse cenário, a proteção do consumidor digital assume caráter essencial, uma vez que o tratamento de dados extrapola o âmbito individual e afeta coletivamente a sociedade. A coleta massiva de informações, muitas vezes realizada sem transparência ou consentimento efetivo, exige a atuação do Direito como instrumento de equilíbrio e limitação do poder informacional (Veloso, 2025, p. 13).

2 A EVOLUÇÃO DA PROTEÇÃO JURÍDICA DO CONSUMIDOR E O CONSENTIMENTO COMO FUNDAMENTO DA AUTODETERMINAÇÃO INFORMATIVA

A priori, cabe salientar que a Constituição Federal determina que o Estado deve promover a defesa do consumidor, nos termos do artigo 5°, inciso XXXII. A conceituação de consumidor foi determinada pelo CDC, definido por meio do artigo 2, sendo complementado pelos artigos 17 e 29 (Norat, 2012, p.3).

> [...]
> Art. 5º, XXXII CF - o Estado promoverá, na forma da lei, a defesa do consumidor;
> Art. 2° Consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final. Parágrafo único. Equipara-se a consumidor a coletividade de pessoas, ainda que indetermináveis, que haja intervindo nas relações de consumo.
> Art. 17. Para os efeitos desta Seção, equiparam-se aos consumidores todas as vítimas do evento.
> Art. 29. Para os fins deste Capítulo e do seguinte, equiparam-se aos consumidores todas as pessoas, determináveis ou não, expostas às práticas nele previstas.
> [...]

Além da conceituação de consumidor para o CDC, ressalta-se pelo dicionário jurídico da doutrinadora Maria Helena Diniz (1998, p. 818):

> 1. Pessoa física ou jurídica que adquire ou usa produto ou serviço como destinatário final. 2. Coletividade de pessoas que intervêm numa relação de consumo. 3. Aquele que consome. 4. O que compra produtos para uso próprio, sem intenção de revendê-los para obter lucro.

Dessa forma, o consumidor é toda pessoa física ou jurídica que adquire produto ou serviço como destinatário final. A doutrina tem divergências acerca da determinação de quem e em quais circunstâncias é considerado destinatário final, sendo assim dividido em três correntes, a finalista, maximalista e mista.

A corrente finalista defende a tese mais restritiva diante da figura do consumidor, sendo a pessoa física ou jurídica que adquire o produto ou serviço para si ou para outrem de modo que satisfaça sua necessidade privada, não utilizando fins profissionais (Marques; Benjamin, 2009, p. 71).

Acerca da corrente maximalista, esta considera o consumidor no conceito amplo, de modo que o destinatário final é toda pessoa física ou jurídica que retira o

produto ou serviço do mercado, sendo possível utilizá-lo para fins profissionais ou privados (Tartuce; Neves, 2022, p. 81).

A corrente mista, também conceituada como teoria finalista mitigada, contempla como destinatário final aquele que adquire um bem ou serviço com a intenção de consumo próprio ou para exercício de atividade econômica profissional. Ressalta-se a necessidade de comprovar a vulnerabilidade da pessoa física ou jurídica para que seja configurada a relação de consumo (Marques; Benjamin, 2009, p.73).

A atual jurisprudência do Superior Tribunal de Justiça (STJ), firmou posicionamento no sentido de que a teoria finalista deve ser mitigada nos casos em que a pessoa física ou jurídica, mesmo que não for destinatária final do produto, tenha comprovado estado de vulnerabilidade ou hipossuficiência técnica em relação ao fornecedor.

> AGRAVO INTERNO NO AGRAVO EM RECURSO ESPECIAL. CÓDIGO DE DEFESA DO CONSUMIDOR. INVERSÃO. ÔNUS DA PROVA . REQUISITOS. INSTITUIÇÃO FINANCEIRA. PESSOA JURÍDICA. TEORIA FINALISTA . MITIGAÇÃO. VULNERABILIDADE. REEXAME DE PROVAS. 1 . Recurso especial interposto contra acórdão publicado na vigência do Código de Processo Civil de 2015 (Enunciados Administrativos números 2 e 3/STJ). 2. **O Superior Tribunal de Justiça firmou posicionamento no sentido de que a teoria finalista deve ser mitigada nos casos em que a pessoa física ou jurídica, embora não se enquadre nas categorias de fornecedor ou destinatário final do produto, apresenta-se em estado de vulnerabilidade ou hipossuficiência técnica, autorizando a aplicação das normas previstas no Código de Defesa do Consumidor. Precedentes.** 3. Na hipótese, rever o entendimento do tribunal de origem, que, com base nas provas carreadas aos autos, concluiu pela caracterização da vulnerabilidade do adquirente e pelo preenchimento dos requisitos para inversão do ônus da prova, demandaria o reexame de fatos e provas, procedimento inviável em recurso especial, a teor do disposto na Súmula número 7 /STJ. 4. Agravo interno não provido (BRASIL, 2021, online)). [Grifou-se]

No contexto das relações jurídicas, a vulnerabilidade pode ser compreendida como uma condição em que o indivíduo se encontra exposto a riscos estruturais ou à intensa influência de forças de mercado, dificultando o exercício pleno de seus direitos. Essa fragilidade pode se manifestar de maneira contínua ou ocasional, tanto em âmbito individual quanto coletivo, e contribui para a formação de um cenário desigual entre as partes envolvidas (Forcelini; Tonial, 2024, p. 11).

A partir do artigo 4°, inciso I do CDC, entende-se que a presunção de vulnerabilidade orienta a aplicação das normas consumeristas, tendo a finalidade de

reduzir a desigualdade entre consumidor e fornecedor. Para isso, o ordenamento jurídico dispõe de instrumentos capazes de atenuar a posição de desvantagem ocupada pelo consumidor (Silveira, 2022, online).

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

As relações interpessoais na sociedade se transformaram ao longo dos períodos históricos, como ocorreu com as relações de consumo após o surgimento da internet. Nesse novo cenário digital, consolidou-se a prática de comercialização de bens e serviços por meio eletrônico, bem como a intensa circulação de informações em redes sociais (Spagnollo; Tonial, 2023, p. 2).

Ressalta-se que a chamada era da internet gerou mudanças significativas nas formas de interação social, causando impacto direto na dinâmica de consumo. No início tendo sido criada com objetivo de aproximação entre os indivíduos, como forma de superação das barreiras geográficas, a internet passou a ser utilizada como meio estratégico em que empresas e prestadores de serviço utilizam esse ambiente como oportunidade lucrativa de expansão comercial e estímulo ao consumo (Siqueira, 2021, p. 9).

Nesse sentido, ao ser considerado o âmbito digital, as relações de consumo concretizadas por esse meio, agravam a condição de fragilidade do consumidor pelos fatos que fazem parte do comércio eletrônico. Assim, ao serem firmadas transações virtuais, os fornecedores se aproveitam de sua superioridade de domínio técnico para absorver dados pessoais sem consentimento (Azevedo, 2020, p. 36).

No meio digital contemporâneo, ao contrário do consumo convencional que exige o pagamento direto para aquisição de produtos e serviços, a oferta de conteúdos sem custos aparentes é comum. Porém, esse modelo oculta a monetização com base na coleta de dados pessoais, meio pelo qual o consumidor deixa de ser apenas o destinatário da oferta e passa a ser objeto de exploração econômica pelas empresas (Spagnollo; Tonial, 2023, p.17).

Desse modo, infere-se que os consumidores desempenham o papel de mercadoria dentro das plataformas digitais, à medida que seus dados pessoais são coletados, processados e transformados em recursos que são explorados como meio monetário. As informações alimentam o sistema algorítmico, de modo que os conteúdos publicitários são enviados de forma direcionada, sendo moldados e entregues aos usuários conforme seu comportamento, interesse e expectativa (Bioni, 2019, p. 125).

Diante do contexto de coleta massiva e exploração de dados, faz-se necessária a análise jurídica para compreender em que medida o ordenamento brasileiro assegura a proteção do consumidor frente a essas exposições.

No que tange o código civil, o negócio jurídico é definido como manifestação legítima da vontade humana, destinada a produzir efeitos no mundo jurídico (Fiuza, 2004, p. 189).

Por se tratar de um ato de vontade, é indispensável se manifeste de maneira livre, consciente e em conformidade com a lei, para que o negócio seja considerado válido (Marighetto; Silva,2024, online)

Os vícios de consentimento referem-se às situações em que a vontade manifestada pelo agente é alterada por influências externas, de modo que difere da intenção verdadeira que ele teria expressado na ausência dessas circunstâncias, resultando em uma distorção de sua decisão (Pereira, 2007, p. 514).

O primeiro vício de consentimento, se refere ao erro, que ocorre quando o agente baseia sua decisão em uma percepção equivocada sobre fatos, pessoas ou objetos, de modo que sua vontade se forma a partir de informações distorcidas. Essa compreensão incorreta da realidade pode levar à manifestação de consentimento que não refletiria sua intenção genuína, comprometendo, assim, a validade do ato jurídico. (Diniz, 2002, p. 386).

O dolo caracteriza-se por qualquer conduta intencional destinada a enganar o agente que manifesta a vontade, seja por meio de artifícios ou sugestões capazes de criar ou sustentar um equívoco. Inclui-se, ainda, a omissão deliberada de informações relevantes, praticada por quem recebe a declaração ou por terceiros, com o objetivo de levar o declarante a agir sob erro, comprometendo a liberdade e a autenticidade de seu consentimento (Pereira, 2007, p. 526).

A coação se configura quando a vontade de uma pessoa é influenciada por pressões ou ameaças indevidas, de modo a obrigá-la a praticar um ato ou celebrar

um negócio que não faria espontaneamente. Trata-se de um comprometimento da liberdade de decisão, em que a imposição psicológica distorce a manifestação de consentimento, tornando o ato vulnerável à anulação (Gonçalves, 2005, p. 383).

O estado de perigo se caracteriza pela situação de necessidade extrema na qual uma pessoa se vê compelida a assumir obrigações excessivas ou desproporcionais ao celebrar um negócio jurídico. Nessas circunstâncias, a pressão gerada pelo contexto compromete a autonomia da vontade, tornando o consentimento vulnerável e passível de questionamento jurídico (Gonçalves, 2005, p. 392).

A lesão se manifesta quando uma das partes, valendo-se da inexperiência, da necessidade ou da descuidada confiança da outra, obtém vantagens desproporcionais em um negócio jurídico. Nessa hipótese, a parte mais vulnerável assume obrigações excessivas em relação ao benefício que recebe, configurando exploração de sua situação e comprometendo a legitimidade do consentimento (Fiuza, 2004, p. 223).

O Código de Defesa do Consumidor (Lei número 8.078/1990) representou um marco importante ao reforçar a centralidade da informação nas relações de consumo. Diferentemente de um consentimento entendido apenas como ausência de coação, o CDC estabelece que a manifestação de vontade do consumidor deve ser qualificada pela presença de informações claras, completas e acessíveis, justamente em razão da vulnerabilidade que caracteriza essa relação. (Cravo, Joelsons, 2020, p. 6).

O artigo 43 do Código de Defesa do Consumidor antecipou a proteção de dados ao garantir aos consumidores prerrogativas específicas relacionadas a cadastros e bancos de dados. Entre elas, destacam-se o acesso às informações e às respectivas fontes, a obrigatoriedade de comunicação sobre a abertura de registros, a possibilidade de exigir a correção de dados incorretos e o direito de ver excluídas informações negativas após o prazo de cinco anos. Esses mecanismos funcionam como precursores dos direitos posteriormente consagrados na LGPD (Cravo, Joelsons, 2020, p. 8).

Além disso, o artigo 51 do Código de Defesa do Consumidor estabelece a nulidade absoluta das cláusulas contratuais consideradas abusivas, isto é, aquelas que acarretam desequilíbrio excessivo em prejuízo do consumidor ou que se revelem contrárias à boa-fé objetiva. Tal dispositivo tem aplicação direta nos

contratos de adesão, nos quais não raramente se inserem condições pouco transparentes e desvantajosas, circunstâncias que afastam a validade de qualquer consentimento obtido nesses moldes (Cravo; Joelsons, 2020, p.14).

A evolução jurídica do consentimento no Brasil revela uma transição significativa, enquanto o Código Civil adota um modelo reativo, centrado na correção de vícios da vontade, o Código de Defesa do Consumidor inaugura uma postura proativa, ao impor ao fornecedor o dever de prestar informações claras e adequadas, de modo a assegurar que a manifestação do consumidor seja efetivamente livre e consciente (Filho, 2021, p. 9).

O Marco Civil da Internet (Lei número 12.965/2014) foi a primeira norma brasileira a tratar de forma direta o consentimento para o uso de dados pessoais online, estabelecendo a proteção da privacidade como princípio fundamental e definindo direitos e deveres para usuários e provedores de serviços na rede (Reis, 2024, p. 6).

O artigo 7º da referida lei reforçou esses conceitos ao estabelecer requisitos essenciais para a coleta, utilização e armazenamento de dados pessoais, determinando que o consentimento do titular seja livre, expresso e informado, afastando qualquer possibilidade de validade do consentimento tácito ou implícito (Cardoso; Regis, 2024, p.6).

O Marco Civil da Internet introduziu de forma inovadora a exigência de que a cláusula de consentimento para o tratamento de dados fosse apresentada de maneira destacada em relação às demais disposições contratuais, evitando que autorizações fossem ocultadas em termos de serviço longos ou complexos e assegurando ao usuário pleno conhecimento sobre o que estava autorizando (Regis, 2024, p. 6).

Apesar de seu caráter pioneiro, o MCI apresentou limitações. Não houve definição precisa dos conceitos de "livre", "expresso" e "informado", abrindo margem para diferentes interpretações. Além disso, seu escopo se restringia às interações realizadas na internet, sem abordar de forma ampla o tratamento de dados em outros contextos ou detalhar as obrigações dos agentes após a coleta (Cardoso, Regis, 2024, p.12).

Assim, embora tenha preparado o terreno para a proteção de dados no Brasil, carecia da abrangência e do detalhamento que apenas uma lei geral poderia oferecer. Desse modo, o âmbito da proteção de dados é regido pela Lei número

13.709/2018, a Lei Geral de Proteção de Dados (LGPD) que parte da ideia da proteção de dados dos usuários, em que todo dado pessoal é considerado importante.

Tal ideia, consolidada como regra geral, por meio de seu artigo 1° da LGPD, em que o tratamento de dados pessoais, realizado por indivíduos ou entidades, públicas ou privadas, inclusive no âmbito digital, somente é legítimo quando amparado por uma das bases legais previstas em lei (Teffé, Viola, 2020, p. 2).

A LGPD estabelece, entre suas estratégias de proteção, a exigência de bases legais para legitimar o tratamento de dados pessoais. Assim, as hipóteses previstas no artigo 7º, incisos I a X, funcionam como critérios autorizadores, limitando a coleta indiscriminada de informações e fortalecendo o direito do titular à autodeterminação informativa (Cardoso; Regis, 2024, p. 8).

Ressalta-se que o tratamento de dados deverá ser enquadrado em ao menos uma das hipóteses legais previstas, a fim de ser considerado legítimo e lícito (Teffé, Viola, 2020, p.3).

As bases legais previstas no artigo 7º da LGPD constituem pressupostos indispensáveis para a compreensão e conformação do tratamento de dados pessoais, sendo previstas em dez hipóteses legais, todas equivalentes entre si e sem qualquer hierarquia (Fonseca, 2021, p. 4) .

Uma das hipóteses de legitimidade para o tratamento de dados decorre do cumprimento de obrigação legal ou regulatória pelo controlador. Nessa hipótese, a coleta e utilização das informações não dependem da anuência do titular, mas resultam de imposição normativa vinculada ao agente de tratamento (Frazão, 2018, online).

Também se admite o tratamento de dados pessoais para execução de políticas públicas, autorizando que a Administração Pública utilize e compartilhe informações sempre que necessárias para implementação de programas e ações previstos em leis (Scorsim, 2018, online).

No campo científico, a LGPD autoriza a realização de estudos por órgãos de pesquisa, possibilitando o tratamento de dados para fins acadêmicos, científicos ou tecnológicos. Para tanto, exige-se, sempre que viável, a adoção da anonimização, como forma de reduzir riscos de identificação e preservar a privacidade dos titulares (Oliveira, 2018, p. 54).

O tratamento de dados, mostra-se igualmente legítimo quando necessário à execução de contrato ou à realização de procedimentos preliminares relacionados a contrato do qual o titular seja parte, sempre a seu pedido (Oliveira, 2018, p. 54).

Nos casos em que se busca o exercício regular de direitos, incluindo a atuação e defesa em processos judiciais, administrativos e arbitrais, de modo que essa hipótese assegura efetividade do contraditório, ampla defesa e da própria tutela jurisdicional (Frazão, 2018, online).

Situações emergências igualmente justificam o uso de dados, especialmente quando voltadas à proteção da vida ou da integridade física do titular ou de terceiros. Nesses casos, dispensa-se o consentimento, em razão da urgência e da relevância do interesse tutelado (Oliveira, 2018, p. 56).

No âmbito privado, destaca-se ainda o legítimo interesse do controlador, desde que não prevaleçam direitos e liberdades fundamentais do titular, de modo que seja evitada que busca por eficiência empresarial se sobreponha à proteção da privacidade (Souza, 2025, p. 55).

Outra base legal se refere à proteção ao crédito e constitui fundamento específico para o tratamento de dados quando necessário para a realização de atividades de análise de crédito e verificação da capacidade financeira do titular (Oliveira, 2019, p. 61).

O consentimento do titular constitui uma das bases legais centrais da LGPD, sendo a manifestação de vontade do titular, prestada de forma livre e sem ambiguidades, pela qual este autoriza o tratamento de seus dados pessoais. Trata-se de requisito prévio e essencial, que deve ser fornecido de maneira clara, consciente e vinculada a uma finalidade específica, assegurando que o titular tenha plena ciência do uso que será feito de suas informações (Cardoso; Regis, 2024, p. 8).

Destaca-se que a autorização para o tratamento de dados pessoais pelos agentes responsáveis, controlador e operador, decorre do consentimento prestado pelo titular. Tal manifestação deve ser livre, consciente e expressa, além de vinculada a uma finalidade específica, legitimando, assim, a realização de operações como coleta, organização, uso, compartilhamento, reprodução e armazenamento das informações pessoais (Cervelin, 2021, p. 43).

O requisito da liberdade no consentimento exige que a manifestação de vontade do titular seja autônoma e consciente, sem qualquer forma de imposição,

abrangendo apenas os dados estritamente necessários para a finalidade pretendida. Assim, para garantir a efetiva proteção das informações, presume-se que o fornecimento de dados além do autorizado não pode ser exigido como obrigatório (Lugati; Almeida, 2020, p. 17).

Além de livre, o consentimento deve ser informado, garantindo que o titular compreenda plenamente como seus dados serão utilizados. Para isso, é necessário que o tratamento realizado pelo controlador esteja alinhado às finalidades previamente comunicadas, de acordo com o princípio da adequação, e que todas as informações pertinentes sejam apresentadas de forma clara e acessível, atendendo ao princípio da transparência. Dessa forma, o titular tem condições de exercer sua autonomia de maneira consciente e responsável (Lugati; Almeida, 2020, p. 18).

O consentimento deve sempre estar vinculado a finalidades específicas, de modo que o titular saiba exatamente para quais propósitos suas informações estão sendo utilizadas. Conforme previsto no parágrafo 4º do artigo 8º da LGPD e no artigo 11, no caso de dados pessoais sensíveis, cada finalidade exige anuência distinta. Essa exigência assegura que o titular mantenha controle sobre seus dados, podendo decidir livremente sobre cada uso, promovendo transparência e segurança jurídica na relação com o controlador (Teffé Tepedino, 2020, p. 16).

O consentimento deve ser manifestado de forma inequívoca, por meio de uma ação positiva do titular ou de declaração expressa, que, se registrada em contrato, deve estar destacada para evidenciar claramente sua vontade. Ao mesmo tempo, cabe ao controlador demonstrar, por meios idôneos, que a autorização foi obtida de maneira específica e informada para cada finalidade do tratamento. Essa exigência garante que o titular exerça plenamente sua autonomia, permitindo o uso de seus dados pessoais de forma consciente e segura (Teffé Tepedino, 2020, p. 15).

Apesar de o consentimento ocupar posição de destaque no debate sobre proteção de dados, ele não pode ser visto como única solução para legitimar todo e qualquer tratamento de informações pessoais. Em um contexto em que as práticas econômicas são cada vez mais sustentadas por tecnologias complexas e pouco transparentes ao cidadão comum, torna-se difícil exigir que o titular compreenda plenamente o alcance de sua autorização (Souza, 2025, p. 61).

O consentimento, embora esteja associado à autorização do titular e à noção de controle sobre seus dados, não se resume a permitir ou negar o uso das informações, em que no âmbito atual da proteção de dados, essa concepção não

pode ser compreendida de forma restritiva, como se toda e qualquer utilização dependesse apenas de uma autorização expressa (Souza, 2025, p. 61).

Conclui-se, portanto, que o consentimento, embora relevante, não pode ser visto como base única da proteção de dados. A efetividade desse instituto depende da conjugação com outras garantias legais, que assegurem transparência, responsabilidade dos agentes de tratamento e mecanismos reais de proteção aos titulares.

O direito à autodeterminação informativa pode ser entendido como um desdobramento dos direitos à intimidade e à privacidade, voltado a garantir o controle do indivíduo sobre suas próprias informações. A partir dessa perspectiva, busca-se analisá-lo no âmbito da proteção de dados pessoais na sociedade digital e examinar como esse contexto influencia diretamente as formas de expressão humana (Teófilo, 2025, p. 11).

A autodeterminação informacional representa, em sua essência, o poder do indivíduo de gerir seus próprios dados pessoais, podendo escolher de forma autônoma se autoriza ou não a coleta, o uso e o compartilhamento dessas informações. Dessa forma, estabelece-se, como princípio geral, a necessidade de consentimento explícito do titular para qualquer tratamento de seus dados (Martins, 2005, p. 233).

O direito à autodeterminação informativa, ao assegurar ao indivíduo o controle sobre o fornecimento e o uso de seus dados pessoais, também desempenha função protetiva, atuando como uma norma de caráter objetivo no campo das relações privadas. Assim, deve ser observado e aplicado pelos magistrados na análise de casos concretos (Mendes, 2020, p. 14).

A vertente objetiva do direito à autodeterminação informativa impõe não só a obrigação de impedir o acesso indevido de terceiros aos dados pessoais, mas também a de evitar que o tratamento dessas informações se baseie em consentimentos ilusórios ou apenas formais. Desse entendimento decorre a possibilidade de controle judicial específico sobre os contratos que tratam da coleta, uso e gestão de dados pessoais (Mendes, 2020, p. 14).

Dessa forma, observa-se que a proteção do consumidor e a tutela de seus dados pessoais evoluíram significativamente no ordenamento jurídico brasileiro, acompanhando as transformações sociais e tecnológicas.

A partir da Constituição Federal e do Código de Defesa do Consumidor, consolidou-se o reconhecimento da vulnerabilidade como princípio fundamental, ampliado posteriormente pelo Marco Civil da Internet e, de forma mais abrangente, pela Lei Geral de Proteção de Dados (LGPD).

Nesse contexto, o consentimento assume papel central, mas não exclusivo, na legitimação do tratamento de dados, exigindo-se que seja livre, informado e vinculado a finalidades específicas.

Contudo, sua eficácia depende da conjugação com outras garantias legais que assegurem transparência, responsabilidade e efetiva proteção ao titular.

Assim, o direito à autodeterminação informativa emerge como expressão máxima da liberdade individual na sociedade digital, reafirmando o dever do Estado e dos agentes econômicos de respeitar e proteger a privacidade e a dignidade da pessoa humana.

3 OS PRINCÍPIOS FUNDAMENTAIS E O REGIME DE RESPONSABILIDADE CIVIL NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

A Lei número 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), foi instituída com o propósito de garantir a tutela dos direitos fundamentais à liberdade, à privacidade e ao livre desenvolvimento da personalidade da pessoa natural (Brasil, 2025, online).

A legislação regula o tratamento de dados pessoais armazenados em meios físicos ou digitais, aplicando-se a indivíduos e entidades, públicas ou privadas, e compreende diversas operações que podem ocorrer manualmente ou em ambiente eletrônico (Brasil, 2025, online).

A Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece um conjunto de princípios que orientam o tratamento de dados pessoais, com o objetivo de assegurar a proteção integral dos direitos dos titulares (Melo, 2022, p. 20).

Entre esses princípios, destacam-se aqueles que fundamentam a atuação ética e transparente dos agentes de tratamento, garantindo o uso responsável das informações.

O primeiro deles é o princípio da finalidade, previsto no art. 6º, inciso I, da LGPD. Ele determina que o tratamento de dados deve ocorrer para propósitos legítimos, específicos, explícitos e previamente informados ao titular, vedando qualquer utilização posterior que seja incompatível com tais finalidades (Brasil, 2018, online).

O termo “legítimos” relaciona-se à boa-fé e aos bons costumes, evitando usos abusivos dos dados; “específicos” indica a necessidade de objetivos claros e delimitados; e “explícitos” reforça a transparência, afastando ambiguidades (Pestana, 2020, online).

Assim, o princípio assegura que os dados pessoais sejam utilizados apenas conforme autorizado, fortalecendo a privacidade e a autonomia informativa do indivíduo (Oliveira; Pires, 2021, p. 5).

Em continuidade, o princípio da adequação, previsto no art. 6º, inciso II, reforça a coerência entre o tratamento de dados e as finalidades previamente informadas ao titular, devendo existir compatibilidade entre a atividade realizada e o contexto apresentado (Brasil, 2018, online).

Esse princípio exige uma correspondência lógica entre o que foi informado e o que de fato é feito, garantindo transparência e previsibilidade no uso dos dados (Pestana, 2020, online).

Complementarmente, o princípio da necessidade, previsto no art. 6º, inciso III, determina que o tratamento deve se restringir ao mínimo indispensável para alcançar a finalidade pretendida, abrangendo apenas informações pertinentes, proporcionais e não excessivas (Brasil, 2018, online).

Tal princípio possui dupla dimensão: de um lado, impõe maior responsabilidade ao agente que coleta os dados; de outro, veda a obtenção de informações irrelevantes. Dessa forma, a coleta deve ser conduzida com cautela, limitando-se aos dados realmente necessários e evitando qualquer tratamento desproporcional (Lima, 2020, p. 130).

O princípio do livre acesso, previsto no art. 6º, inciso IV, garante ao titular o direito de consultar, de forma gratuita e facilitada, as informações sobre o tratamento de seus dados pessoais, incluindo sua existência, integralidade e duração (Brasil, 2018, online).

Esse princípio promove uma relação mais transparente entre titulares e agentes de tratamento, permitindo que o indivíduo acompanhe o ciclo de vida de suas informações e compreenda como são utilizadas (Oliveira; Pires, 2021, p. 6).

Embora seja classificado formalmente como princípio, o livre acesso também pode ser entendido como uma regra de conduta pautada na boa-fé, impondo o dever de fornecer informações claras e acessíveis (Lima, 2020, p. 131).

Na mesma linha de reforço à clareza e correção das informações, o princípio da qualidade dos dados, previsto no art. 6º, inciso V, exige que os dados pessoais sejam precisos, claros, relevantes e atualizados, de acordo com a finalidade do tratamento (Brasil, 2018, online).

A clareza assegura a compreensão do titular, a relevância limita o uso a informações estritamente necessárias e a atualização mantém os dados condizentes com a realidade do indivíduo (Pestana, 2020, online).

A manutenção desses elementos só se justifica quando há efetiva necessidade, reforçando o equilíbrio entre a proteção dos direitos do titular e o uso responsável das informações (Oliveira; Pires, 2021, p. 7).

O princípio da transparência, previsto no art. 6º, inciso VI, complementa os anteriores ao assegurar ao titular o direito de acesso a informações claras, precisas

e compreensíveis sobre o tratamento de seus dados e sobre os agentes responsáveis, observados os segredos comercial e industrial (Brasil, 2018, online).

A transparência promove a confiança nas relações digitais e garante que o titular saiba como suas informações são coletadas, armazenadas e compartilhadas (Nunes, 2019, online).

Para isso, os dados devem ser verdadeiros, atualizados e compatíveis com a realidade, observando critérios de exatidão e relevância (Nunes, 2019, online).

O princípio da segurança, previsto no art. 6º, inciso VII, impõe aos agentes de tratamento a obrigação de proteger os dados contra acessos não autorizados e contra incidentes como destruição, perda, alteração ou divulgação indevida (Brasil, 2018, online).

Para tanto, devem ser adotadas medidas técnicas e administrativas adequadas que garantam a integridade, confidencialidade e disponibilidade das informações, prevenindo riscos aos direitos dos titulares (Pestana, 2020, online).

De forma complementar, o princípio da prevenção, previsto no art. 6º, inciso VIII, orienta que os agentes de tratamento adotem medidas prévias para evitar danos decorrentes do tratamento de dados pessoais (Brasil, 2018, online).

Trata-se de um princípio que exige atuação proativa das organizações, incentivando a implementação de políticas e mecanismos de segurança que antecipem riscos e reduzam impactos à privacidade. Assim, consolida-se uma cultura preventiva de proteção de dados, pautada na responsabilidade e no cuidado contínuo (Nunes, 2019, online).

No mesmo sentido ético e protetivo, o princípio da não discriminação, previsto no art. 6º, inciso IX, proíbe o tratamento de dados para fins ilícitos ou abusivos de natureza discriminatória (Brasil, 2018, online).

Ainda que a LGPD não detalhe todas as práticas abusivas, entende-se que qualquer tratamento contrário aos direitos fundamentais ou aos princípios da lei configura violação. Dessa forma, o princípio reafirma o compromisso com a igualdade, a integridade e o respeito à dignidade humana (Oliveira; Pires, 2021, p. 9).

Por fim, o princípio da responsabilização e da prestação de contas, previsto no art. 6º, inciso X, impõe aos agentes de tratamento o dever de comprovar a adoção de medidas eficazes voltadas ao cumprimento da LGPD (Brasil, 2018, online).

Esse princípio ultrapassa a simples observância formal da lei, exigindo dos controladores e operadores uma postura ativa e transparente de conformidade, por meio da implementação de mecanismos técnicos, administrativos e organizacionais que assegurem a efetividade da proteção de dados (Nunes, 2019, online).

Outrossim, no que tange ao *caput* do artigo 6, cabe destacar o conceito de boa-fé objetiva, tendo seu propósito de atuar conforme os padrões de honestidade e retidão socialmente aceitos, os quais asseguram a confiança recíproca indispensável à convivência social e ao adequado funcionamento das relações econômicas e contratuais e se manifesta, de forma contínua e atemporal (Cordeiro, 2017, p. 1280).

É possível identificar dois efeitos fundamentais da boa-fé no contexto da Lei Geral de Proteção de Dados, o primeiro diz respeito à sua natureza normativa, que lhe atribui força jurídica própria; o segundo refere-se à sua função de assegurar a confiança recíproca entre os participantes da relação de tratamento, com especial proteção ao titular dos dados (Toniazzo, 2022, p.57).

A boa-fé apresenta distintas acepções no âmbito jurídico. Em determinadas situações, assume natureza subjetiva, vinculada ao estado psicológico do sujeito e ao seu grau de conhecimento sobre certas circunstâncias, em outras, manifesta-se sob a forma objetiva, traduzindo-se em um padrão ético de conduta que impõe aos indivíduos o dever de agir com lealdade, honestidade e cooperação nas relações jurídicas, podendo ainda repercutir na aquisição de direitos, como o de perceber frutos (Silva; Clovis, 2006. p. 33).

Pode-se compreender a boa-fé como um verdadeiro parâmetro normativo de conduta, destinado a orientar o comportamento ético, leal e confiável das partes nas relações jurídicas. Agir de acordo com a boa-fé implica observar a probidade, a correção e a lealdade que devem reger os vínculos negociais (Garcia, 2011. p. 50).

Na perspectiva da Lei Geral de Proteção de Dados, o princípio da boa-fé objetiva funciona como diretriz fundamental de comportamento, exigindo que as partes envolvidas no tratamento de dados ajam com integridade, transparência e respeito mútuo. Esse princípio reforça a dimensão preventiva da norma, integrando-se às medidas voltadas à salvaguarda da privacidade e à proteção dos dados pessoais desde a fase de concepção das atividades até sua implementação efetiva (Tepedino, Teffé, 2019, p. 300).

Um dos meios de promover maior transparência no fluxo informacional e mitigar as assimetrias existentes nas relações de tratamento de dados pessoais consiste na adoção da metodologia denominada privacy *by design*. Esse conceito traduz a premissa de que a proteção de dados deve ser incorporada desde a fase de concepção de produtos, serviços ou sistemas**,** de modo que as soluções tecnológicas empregadas já contenham mecanismos voltados ao controle, à segurança e à preservação das informações pessoais (Bioni, 2021, p.170).

Trata-se da incorporação, desde a fase de desenvolvimento de produtos, serviços e sistemas, de medidas preventivas voltadas à proteção da privacidade e à minimização dos riscos de violação de dados pessoais (Toniazzo, 2022, p.100).

Tal metodologia se fundamenta na constatação de que a simples aplicação de normas legais não é suficiente para garantir a proteção efetiva da privacidade. Para ser realmente eficaz, a salvaguarda dos dados pessoais deve estar integrada aos processos e à cultura operacional das organizações, tornando-se parte intrínseca das decisões e fluxos internos, e não apenas uma exigência imposta externamente pela legislação (Bodanese, Vieira, 2021, p. 267).

O conceito de dado pessoal abrange qualquer informação que identifique ou torne possível identificar uma pessoa natural (artigo 5º, I, LGPD). Já os dados pessoais sensíveis dizem respeito a informações sobre origem racial ou étnica, crença religiosa, opinião política, filiação a sindicato ou entidade de caráter religioso, filosófico ou político, além de dados relativos à saúde, vida sexual, características genéticas ou biométricas vinculadas a um indivíduo (artigo 5º, II, LGPD) (Brasil, 2018, online).

Diante dessas premissas, os dados sensíveis podem ser definidos como uma categoria específica de dados pessoais, caracterizada pelo maior potencial de exposição a situações de vulnerabilidade ou discriminação (Bioni, 2018, p. 84).

Os dados sensíveis recebem essa qualificação não apenas em razão de seu caráter intimamente ligado à esfera pessoal do indivíduo, mas sobretudo em função da forma como são utilizados e das finalidades que orientam seu tratamento, as quais podem ensejar práticas discriminatórias ou usos indevidos (Mulholland, 2020 p. 3).

Da mesma forma, um dado aparentemente comum pode adquirir caráter sensível quando analisado com o uso de tecnologias avançadas, como o *big data*, sendo o tratamento de grandes volumes de dados por meio de técnicas

computacionais, capazes de cruzar diversas informações e extrair previsões sobre comportamentos ou eventos futuros (Bioni, 2018, p. 84).

O acesso a essas informações permite que instituições públicas e privadas classifiquem indivíduos segundo padrões de hábitos e comportamentos, potencializando a ocorrência de discriminações relevantes, sobretudo quando estão envolvidos dados pessoais sensíveis (Bodin; Teffé, 2016, p. 21).

A responsabilidade torna-se mais evidente, em razão da legislação estabelecer que tanto o controlador, responsável pelas decisões relacionadas ao tratamento dos dados, quanto o operador, que realiza o tratamento em nome do controlador, podem ser responsabilizados (Gondim, 2021, p. 6).

A responsabilidade decorre do exercício da atividade de tratamento de dados que infrinja a legislação de proteção de dados. Ao empregar essa expressão, o legislador reconhece que o regime jurídico de proteção de dados constitui um verdadeiro microssistema normativo, composto por diversas leis interligadas, tendo a LGPD como seu núcleo fundamental (Capanema, 2020, p.3).

Entretanto, a responsabilidade civil prevista na LGPD não decorre exclusivamente da violação do microssistema jurídico de proteção de dados. A correta interpretação deve considerar o artigo 42, *caput***,** em conjunto com o art. 44, parágrafo único, pois é dessa leitura sistemática que se extrai o verdadeiro alcance das hipóteses de responsabilização previstas na legislação (Capanema, 2020, p. 3).

Por sua vez, o art. 46 determina que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas apropriadas, com a finalidade de assegurar a proteção dos dados pessoais sob sua guarda (Brasil, 2018, online).

O art. 42 limita a responsabilidade civil ao controlador ou ao operador. O uso da conjunção alternativa “ou” indica que a responsabilização recai sobre um ou outro desses agentes, evidenciando a existência de uma alternância entre eles (Capanema, 2020, p. 3).

O § 1º do art. 42 constitui uma exceção à regra de alternância prevista no caput, ao admitir a responsabilidade solidária em situações específicas, com o propósito de garantir a efetiva reparação ao titular dos dados (Brasil, 2018, online).

Conforme o inciso I, o operador será responsabilizado solidariamente em duas circunstâncias: quando descumprir a legislação de proteção de dados ou quando deixar de observar as instruções lícitas do controlador, equiparando-se, nesse caso, ao próprio controlador (Tasso, 2020, p. 8).

Já o inciso II prevê a solidariedade entre controladores que participem diretamente do tratamento de dados, isto é, que tomem decisões conjuntas que resultem em violação às normas do microssistema de proteção de dados ou às regras técnicas pertinentes (Tasso, 2020, p. 8).

Por fim, essas hipóteses de solidariedade não se aplicam quando estiverem presentes as excludentes de responsabilidade previstas no art. 43 da LGPD (Tasso, 2020, p.12).

A LGPD não prevê expressamente a responsabilidade civil do encarregado, porém ela pode ocorrer em situações específicas, como por exemplo, quando essa função é desempenhada por pessoa natural ou jurídica independente do controlador e do operador, especialmente no âmbito de relações de consumo (Capanema, 2020, p. 4).

Nesses casos, por integrar a cadeia de fornecimento**,** o encarregado pode ser responsabilizado solidariamente pelos danos eventualmente causados ao titular dos dados (Capanema, 2020, p. 4).

O regime de responsabilidade civil estabelecido pela LGPD é uniforme, abrangendo todos os tipos de dados. Isso porque os danos decorrentes de sua violação, sejam patrimoniais ou morais, individuais ou coletivos, não se alteram conforme a classificação dos dados, exigindo reparação integral. Dessa forma, não há fundamento para adotar regimes distintos entre dados sensíveis e dados comuns (Mulholland, 2020 p. 11).

Quanto a essa questão, observa-se divergência na doutrina sobre o tipo de responsabilidade aplicável. Nos artigos 42 a 45, a LGPD disciplina a responsabilidade civil dos agentes de tratamento de dados pessoais, suscitando debate acerca da natureza da obrigação de indenizar: se de caráter subjetivo, fundamentada na culpa do agente, ou objetiva, baseada no risco da atividade exercida (Mulholland, 2020, p. 11).

Na primeira visão, entende que foi adotada a teoria subjetiva da responsabilidade civil, exigindo a comprovação da culpa do agente de tratamento no momento do dano (Guedes; Meireles, 2019, p. 231).

Essa culpa pode se manifestar, por um lado, pela omissão na implementação de medidas de segurança adequadas ao tratamento de dados, isto é, quando não se proporciona a proteção que o titular tem direito de esperar e, por outro, pelo

descumprimento das obrigações previstas na legislação, configurando violação das normas de proteção de dados pessoais (Guedes; Meireles, 2019, p. 231).

Em posição diversa, ressalta-se a teoria ativa ou proativa da responsabilidade civil, que propõe uma visão positiva da responsabilidade, na qual os agentes de tratamento de dados devem adotar medidas que previnam danos, tornando a obrigação de indenizar uma exceção (Moraes; Queiroz, 2019, p. 118).

Destaca-se que os dados pessoais, por integrarem a esfera do direito à privacidade, exigem que sua coleta e tratamento sejam precedidos de medidas de proteção eficazes e rigorosas, com atenção especial aos dados sensíveis, considerados essenciais à preservação da dignidade humana (Moraes; Queiroz, 2019, p. 119).

Por outro lado, outra visão se refere a de que a atividade de tratamento de dados envolve um risco inerente, dada a significativa potencialidade de dano em caso de violação, considerando a natureza personalíssima e fundamental desses direitos (Doneda; Mendes, 2018, p. 479).

A LGPD tem como um dos seus objetivos centrais, a redução ao máximo dos riscos de prejuízo aos titulares de dados. Nesse sentido, a responsabilidade dos agentes de tratamento deve ser analisada considerando a própria atividade, que a lei restringe às hipóteses previstas legalmente (artigo 7º, LGPD) e exige que envolvam apenas os dados essenciais, respeitando o princípio da finalidade (artigo 6º, III, LGPD) e evitando práticas inadequadas ou desproporcionais em relação à finalidade do tratamento (Doneda; Mendes, 2018, p. 479).

Diante das divergências doutrinárias apresentadas, conclui-se que o artigo 42 da LGPD adota a responsabilidade civil objetiva, impondo a obrigação de indenizar independentemente da comprovação de culpa do agente de tratamento. Essa interpretação se justifica pelo reconhecimento de que o tratamento de dados constitui uma atividade que, por sua própria natureza, envolve riscos aos direitos dos titulares (Mulholland, 2020 p. 15).

A recente decisão do Superior Tribunal de Justiça, proferida no Recurso Especial número 2.201.694/SP (Brasil, 2025, online), consolidou importante precedente sobre a responsabilidade civil no tratamento indevido de dados pessoais.

> CIVIL, CONSUMIDOR E PROCESSUAL CIVIL. RECURSO ESPECIAL. AÇÃO DE OBRIGAÇÃO DE FAZER C/C INDENIZAÇÃO POR DANOS MORAIS. TEMA 710 E SÚMULA 550 DO STJ. DISTINÇÃO. BANCO DE

> DADOS. DISPONIBILIZAÇÃO DOS DADOS DO CADASTRADO. HIPÓTESES PREVISTAS NA LEI número 12.414/2011. TERCEIROS CONSULENTES. RESTRIÇÃO LEGAL. DISPONIBILIZAÇÃO INDEVIDA. DANO MORAL PRESUMIDO. RESPONSABILIDADE OBJETIVA DO GESTOR DE BANCO DE DADOS. CONFIGURAÇÃO. 1. Ação de obrigação de fazer c/c compensação de danos morais. 2. No particular, não se aplicam o Tema 710/STJ e a Súmula 550/STJ, que tratam especificamente do credit scoring, ficando expressamente consignado que essa prática "não constitui banco de dados", sendo este regulamentado pela Lei número 12.414/2011. 3. O gestor de banco de dados regido pela Lei número 12.414/2011 somente pode disponibilizar a terceiros consulentes o score de crédito, desnecessário o consentimento prévio; e o histórico de crédito, mediante prévia autorização específica do cadastrado (art. 4º, IV). Por outro lado, as informações cadastrais e de adimplemento armazenadas somente podem ser compartilhadas com outros bancos de dados (art. 4º, III). Precedentes. 4. O gestor de banco de dados que disponibiliza para terceiros consulentes o acesso aos dados do cadastrado que somente poderiam ser compartilhados entre bancos de dados (como as informações cadastrais e de adimplemento) deve responder objetivamente pelos danos morais causados ao cadastrado, que são presumidos, diante da forte sensação de insegurança por ele experimentada. Precedentes. 5. Recurso especial conhecido e provido (Brasil, 2025, online).

O caso envolveu a divulgação de informações cadastrais de consumidores por empresa gestora de banco de dados, sem o consentimento do titular, a terceiros consulentes (Lobo; Aloiai, 2025, online).

A Terceira Turma, por maioria, reconheceu a ocorrência de dano moral presumido (in re ipsa) e afirmou a responsabilidade objetiva do gestor do banco de dados, considerando que a disponibilização indevida de dados pessoais gera, por si só, violação aos direitos da personalidade e ao direito fundamental à privacidade (Brasil, 2025, online).

Tal entendimento reforça a diretriz de que o tratamento de dados pessoais deve observar rigorosamente os limites legais estabelecidos pela LGPD, especialmente os artigos 42 e 43, que impõem ao agente de tratamento o dever de reparar o dano decorrente de violação às normas de proteção de dados (Federighi; Preta; 2025, online).

A Corte reconheceu que o gestor de banco de dados regido pela Lei número 12.414/2011 somente pode compartilhar determinadas informações, como o histórico de crédito mediante autorização expressa do titular, sendo vedada a disponibilização a terceiros consulentes de dados cadastrais e de adimplemento (Brasil, 2025, online).

O descumprimento desse dever configura ato ilícito e enseja a obrigação de indenizar, independentemente da demonstração de culpa, em razão do risco inerente à atividade desempenhada (Lobo; Aloiai, 2025, online).

Nesse contexto, a decisão reafirma a aplicação da teoria do risco e a adoção da responsabilidade civil objetiva como mecanismo de proteção efetiva dos titulares de dados (Federighi; Preta. 2025, online).

A presunção de dano moral, reconhecida pelo STJ, decorre da própria sensação de insegurança e vulnerabilidade experimentada pelo indivíduo diante da exposição indevida de suas informações pessoais, evidenciando a gravidade da violação e a necessidade de tutela integral da dignidade informacional (Brasil, 2025, online).

Dessa forma, conclui-se que a LGPD representa um marco essencial na consolidação do direito fundamental à privacidade e à proteção de dados no Brasil, ao instituir um sistema normativo coerente e abrangente voltado à tutela da dignidade informacional.

A legislação estabelece princípios e deveres que orientam o tratamento de dados pessoais, reforçando a necessidade de transparência, segurança e responsabilidade dos agentes envolvidos.

No âmbito da responsabilidade civil**,** verifica-se que o legislador optou por um modelo objetivo, pautado na teoria do risco, de modo a assegurar a reparação integral dos danos causados aos titulares, independentemente da demonstração de culpa.

A recente decisão do Superior Tribunal de Justiça, ao reconhecer a responsabilidade objetiva e o dano moral presumido decorrente do tratamento indevido de dados pessoais, consolida a aplicação prática dos fundamentos da LGPD e reforça o compromisso do ordenamento jurídico brasileiro com a efetividade da proteção de dados.

Assim, a norma não apenas impõe obrigações técnicas e administrativas aos agentes de tratamento, mas também promove uma mudança de paradigma, deslocando o foco para uma atuação preventiva e ética.

4 ANÁLISE DE CASOS CONCRETOS DE VIOLAÇÃO À PROTEÇÃO DE DADOS PESSOAIS NAS RELAÇÕES DE CONSUMO

O presente capítulo tem como finalidade examinar casos concretos que evidenciam situações de tratamento indevido de dados pessoais no contexto das relações de consumo, a fim de demonstrar, de forma prática, como as violações à legislação de proteção de dados se manifestam.

A análise desses casos permite a compreensão da importância do consentimento como elemento central da legitimidade no tratamento de dados pessoais, conforme previsto no artigo 7°, inciso I, da Lei Geral de Proteção de Dados - LGPD, que estabelece que o consentimento do titular é requisito essencial para a coleta, o armazenamento e a utilização de suas informações (Teffé, 2020, p. 5).

Dessa forma, cabe demonstrar que a inobservância dessa exigência legal compromete a privacidade individual e as relações de consumo por meio da tecnologia (Segundo; Couto, 2022, p. 7).

Quando o consentimento do consumidor é suprimido, obtido de forma viciada ou manipulado por práticas pouco transparentes, a vulnerabilidade do titular de dados é acentuada (Segundo; Couto, 2022, p. 14).

Tal situação revela um cenário em que o indivíduo perde o controle sobre suas próprias informações, tornando-se mero objeto de estratégias comerciais e tecnologias voltadas à coleta e a monetização de dados. (Mendes, 2020, p. 11).

O caso envolvendo a empresa Raia Drogasil S/A, analisado pelo Procon-MG e pelo Ministério Público de Minas Gerais, ganhou destaque nacional por evidenciar práticas abusivas relacionadas à coleta e ao tratamento de dados pessoais de consumidores sem o devido consentimento (G1, online, 2024).

A empresa, responsável por uma das maiores redes de farmácias do país, foi autuada por solicitar o número do Cadastro de Pessoa Física - CPF dos clientes tanto no balcão de atendimento quanto no momento do pagamento, independentemente de finalidade clara ou da concordância expressa do titular (MINAS GERAIS, 2024, online).

Segundo o entendimento dos órgãos fiscalizadores, a conduta configurou coleta de dados sem base legal válida, uma vez que os consumidores não eram devidamente informados sobre o uso e a destinação dessas informações.

O Procon-MG, vinculado ao Ministério Público de Minas Gerais, considerou que a prática violava o direito à privacidade e à transparência, impondo à empresa uma multa administrativa de R$ 8.497.500,00 (G1, 2024, online).

O promotor citou como exemplo, o caso de um consumidor que compre medicamentos para tratar a pressão arterial de seu pai ou outra doença. Em eventual vazamento dessas informações, os registros de compra poderiam ser utilizados de forma indevida, como por exemplo, por operadoras de planos de saúde para negar cobertura alegando doença preexistente não declarada, ou por seguradoras para recusar a contratação ou o pagamento de indenizações pelo mesmo motivo (MINAS GERAIS, 2024, online).

A autuação da Raia Drogasil teve fundamento em diversos dispositivos legais que tutelam o direito à proteção de dados e a defesa do consumidor. Primeiramente, o artigo 43, §2º, do Código de Defesa do Consumidor (CDC) veda a manutenção e o compartilhamento de informações pessoais sem a ciência e o consentimento do titular, o que reforça o dever de transparência nas relações de consumo (MINAS GERAIS, 2024, online).

Além disso, o artigo 13, inciso XIII, do Decreto Federal número 2.181/97, que regulamenta as sanções administrativas aplicáveis às práticas abusivas também foi violado, pois proíbe a coleta de dados do consumidor para finalidades diversas da prestação do serviço contratado (MINAS GERAIS, 2024, online).

No âmbito da Lei Geral de Proteção de Dados Pessoais (LGPD), o caso envolveu o descumprimento do artigo 7º, inciso I, que estabelece o consentimento do titular como a principal base legal para o tratamento de dados, e do artigo 11, incisos I e II, alíneas “a” e “g”, que impõem condições específicas para o tratamento de dados sensíveis, especialmente em situações que envolvem informações sobre saúde e hábitos de consumo farmacêutico (MINAS GERAIS, 2024, online).

Dessa forma, a conduta da empresa violou os princípios da transparência e da finalidade, além de contrariar o dever de obtenção de consentimento livre, informado e inequívoco (MINAS GERAIS, 2024, online).

A sanção aplicada pelo Procon-MG configurou responsabilidade administrativa pela infração à legislação consumerista e de proteção de dados, reafirmando a importância da conformidade corporativa e do respeito aos direitos fundamentais do consumidor digital (MINAS GERAIS, 2024, online).

Sob a perspectiva da LGPD, o caso da Raia Drogasil evidencia a ausência de base legal legítima para o tratamento de dados pessoais, uma vez que o simples fornecimento do CPF não era essencial para a concretização da relação de consumo.

A prática, portanto, extrapolou os limites da necessidade e da finalidade, princípios basilares da legislação. Ainda que a empresa alegasse coletar o dado com a intenção de oferecer benefícios em programas de fidelidade, tal argumento não se sustenta juridicamente sem a manifestação de consentimento expresso do consumidor (Teffé, 2020, p. 4).

O caso envolvendo a transportadora *Loggi* ilustra de forma contundente os riscos decorrentes do vazamento de dados pessoais no ambiente digital e as consequências diretas sobre a segurança e a confiança dos consumidores (G1, 2025, online).

Centenas de clientes da empresa foram vítimas de uma tentativa de golpe em larga escala, na qual criminosos utilizaram informações pessoais reais, como nome, endereço de entrega e telefone, para aplicar fraudes por meio do aplicativo WhatsApp[1]**.**

O golpe era conduzido por indivíduos que se apresentavam como representantes de uma suposta empresa denominada "*Red Strike*"**,** que alegava atuar em parceria com a Loggi (Souza, 2025, online).

As vítimas recebiam mensagens informando que suas encomendas estavam retidas e que a liberação só ocorreria mediante o pagamento de uma taxa adicional. Para tornar a fraude mais convincente, os golpistas enviavam um link falso que direcionava a vítima a um site visualmente idêntico ao da transportadora, solicitando o pagamento de valores simbólicos, geralmente via Pix[2] ou boleto bancário (G1, 2025, online).

A sofisticação do golpe estava justamente no uso de dados reais dos consumidores, o que aumentava a credibilidade da fraude e a probabilidade de sucesso (Souza, 2025, online).

Ainda que não tenha sido comprovado oficialmente o momento ou a origem exata do vazamento, o episódio demonstrou que informações pessoais sob responsabilidade de empresas de logística podem ser exploradas por terceiros

[1] Disponível em: https://whatsapp.com. Acesso em: 9 nov. 2025.
[2] Sistema de pagamento instantâneo desenvolvido e mantido pelo Banco Central do Brasil.

mal-intencionados, revelando a fragilidade da proteção de dados no comércio eletrônico e na cadeia de entregas (Souza, 2025, online).

Sob o ponto de vista jurídico, o caso Loggi se relaciona diretamente com o dever de segurança previsto no artigo 46 da LGPD, que impõe aos controladores e operadores a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (Brasil, 2018, online).

No contexto da empresa de transporte *Loggi*, observa-se a presença de diferentes agentes de tratamento, a empresa atua como controladora dos dados de seus clientes, enquanto outras empresas contratadas, como operadores logísticos, transportadoras terceirizadas ou plataformas tecnológicas, podem ser enquadradas como operadores. Já os criminosos que praticaram a fraude são classificados como terceiros não autorizados, que se beneficiaram da vulnerabilidade do sistema (Filho, 2021, p. 3).

O vazamento de dados da 23andMe, empresa norte-americana especializada em testes genéticos, ocorreu em outubro de 2023 e representou uma grave violação de segurança digital. *Cracker* obtiveram acesso a informações pessoais de milhões de usuários, alcançando aproximadamente 6,9 milhões de contas (BBC, 2024, online).

Entre os dados expostos estavam nome, foto de perfil, data de nascimento, localização e informações genéticas que revelavam ancestralidade e vínculos de parentesco (British Broadcasting Corporation, 2024, online).

O ataque teve caráter direcionado, sendo conduzido por um invasor que se identificou como “Golem”, o qual alegou ter obtido perfis de pessoas com ascendência judaica asquenaze, oriundas da Europa Central e Oriental (Kleeman, 2024, online).

Esses dados foram posteriormente colocados à venda em fóruns virtuais de cibercriminosos, contendo agrupamentos étnicos, haplogrupos, estimativas de origem, características fenotípicas, fotografias e perfis genéticos brutos. A comercialização seguia uma tabela de preços que variava de US$ 1 mil por 100 perfis a US$ 100 mil por 100 mil perfis, revelando a mercantilização de informações altamente sensíveis (British Broadcasting Corporation, 2024, online).

O incidente impactou potencialmente 14 milhões de pessoas que haviam submetido seu DNA para análise genética, muitas das quais não compreendiam

plenamente os riscos de privacidade e segurança associados a esse tipo de serviço (Kleeman, 2024, online).

O episódio evidenciou a vulnerabilidade do consumidor diante de empresas que tratam dados sensíveis em larga escala, especialmente quando essas informações são utilizadas para fins discriminatórios ou comerciais, sem o consentimento expresso do titular.

Em decorrência do vazamento, a empresa celebrou um acordo judicial de US$ 30 milhões (cerca de R$ 165 milhões) para indenizar os consumidores afetados, configurando uma das maiores compensações já pagas por incidente de segurança envolvendo dados genéticos (British Broadcasting Corporation, 2024, online).

Considerando o contexto jurídico dos Estados Unidos, onde o caso se originou, difere significativamente dos sistemas de proteção europeus e brasileiros. Enquanto o GDPR e a LGPD (Lei número 13.709/2018) estruturam microssistemas abrangentes de proteção de dados, o modelo norte-americano é fragmentado, com normas setoriais que carecem de uniformidade, o que favorece lacunas e inconsistências exploradas pelo mercado (Colzanni; Rosa, 2025, online).

Nesse cenário, a LGPD aplica-se também às vítimas brasileiras eventualmente atingidas, conforme prevê o artigo 3º, que estabelece a aplicabilidade extraterritorial da norma. Assim, ainda que a 23andMe tenha sede nos Estados Unidos, o tratamento de dados genéticos de titulares localizados no Brasil, seja pela coleta direta de amostras, seja pelo uso da plataforma digital, submete a empresa às disposições da legislação brasileira (Brasil, 2018, online).

Como controladora de dados, a empresa deveria ter observado os princípios da finalidade, segurança e prevenção (artigo 6º, LGPD) e adotado medidas técnicas e administrativas eficazes para evitar o acesso não autorizado (Brasil, 2018, online).

Além disso, os dados genéticos expostos são dados sensíveis, conforme o artigo 11**,** exigindo consentimento explícito e limites claros de uso. A falha na proteção dessas informações revela deficiências na transparência e na segurança, contrariando os fundamentos da LGPD (Castells, 1999, p. 21).

De igual modo, o artigo 48 impõe a comunicação imediata à ANPD e aos titulares em casos de incidentes de segurança com risco relevante — exigência que, diante da dimensão do vazamento, possivelmente não foi devidamente observada (Paganella, 2021, p. 225).

Assim, a exposição dos dados genéticos de cidadãos brasileiros configura violação direta à LGPD, gerando responsabilidade civil pelos danos materiais e morais sofridos, artigo 42 (Brasil, 2018, online).

Portanto, o caso da 23andMe reforça a necessidade de efetividade transnacional da LGPD e da cooperação internacional em matéria de proteção de dados pessoais, especialmente quando envolvem informações genéticas de alta sensibilidade (Colzanni; Rosa, 2025, online).

Diante das análises apresentadas, é possível concluir que os casos estudados, Raia Drogasil**,** Loggi e 23andMe, ilustram de forma concreta as múltiplas dimensões da violação à proteção de dados pessoais no contexto das relações de consumo, revelando tanto falhas estruturais de governança quanto práticas que afrontam os princípios fundamentais da Lei Geral de Proteção de Dados (LGPD)**.**

Em todos os exemplos, observa-se o comprometimento da privacidade, a ausência de consentimento válido e a insuficiência das medidas de segurança**,** fatores que acentuam a vulnerabilidade do consumidor digital e demonstram a urgência de uma cultura de conformidade e responsabilidade corporativa**.**

Assim, a consolidação de uma proteção de dados efetiva e humanizada é condição indispensável para o fortalecimento da confiança nas relações de consumo digitais e para a preservação dos direitos fundamentais à privacidade e à autodeterminação informativa no ambiente tecnológico contemporâneo.

CONSIDERAÇÕES FINAIS

Diante do exposto, conclui-se que o tratamento de dados pessoais no ambiente digital impõe desafios significativos à efetividade dos direitos fundamentais à privacidade e à autodeterminação informativa. A crescente utilização de algoritmos e técnicas de direcionamento comportamental nas relações de consumo evidencia a necessidade de um controle mais rigoroso sobre a coleta, o uso e o compartilhamento de informações pessoais.

Verifica-se que o consentimento, embora consagrado pela Lei Geral de Proteção de Dados Pessoais (Lei número 13.709/2018) como uma das principais bases legais para o tratamento de dados, pode se tornar inválido quando obtido por meios manipulativos, opacos ou desproporcionais. Nessas circunstâncias, o titular deixa de exercer uma manifestação livre e esclarecida de vontade, o que compromete a legitimidade do tratamento e viola os princípios da transparência, finalidade e boa-fé previstos no artigo 6º da LGPD.

A análise desenvolvida demonstra que a vulnerabilidade informacional do consumidor digital exige a adoção de medidas preventivas e corretivas por parte dos agentes de tratamento, de modo a assegurar que o consentimento seja realmente uma expressão da autonomia do titular, e não resultado de práticas persuasivas que deturpam sua capacidade decisória. O cumprimento efetivo da legislação demanda, portanto, a integração entre a LGPD e o Código de Defesa do Consumidor, reforçando a responsabilidade objetiva dos controladores e operadores diante de falhas na segurança ou no uso indevido de dados.

Conclui-se, ainda, que a consolidação de uma cultura de proteção de dados depende da internalização dos princípios da ética digital e da responsabilidade social no âmbito corporativo. A conformidade não deve ser tratada como mera obrigação legal, mas como instrumento essencial de tutela da dignidade da pessoa humana e da confiança nas relações digitais.

Em suma, a proteção de dados pessoais representa um dos maiores desafios jurídicos da era tecnológica e deve ser compreendida como um dever permanente do Estado, do mercado e da sociedade. O fortalecimento das práticas de transparência, segurança e governança informacional é condição indispensável para assegurar a efetividade dos direitos fundamentais e a preservação da liberdade individual em um cenário cada vez mais orientado por dados e algoritmos.

REFERÊNCIAS

AZEVEDO, Anna Karoline Carneiro Nery. Comércio Eletrônico: a vulnerabilidade agravada do consumidor virtual e sua proteção no Brasil. *In:* CALADO, Vinícius de Negreiros *et al* (orgs.) **Temas de Direito do Consumidor**: estudos em homenagem aos 30 anos do CDC. Recife, 2020. E-book.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 1. ed. Rio de Janeiro: Forense, 2019.
_____. **Proteção de dados pessoais**: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

BODANESE, Andréa; VIEIRA, Thyessa Junqueira Gervásio. A segurança dos dados: o conteúdo do
dever e os efeitos dos incidentes de segurança.

BRASIL. Constituição (1988). **Constituição** da República Federativa do Brasil. Brasília, DF.
_____. **Lei número 13.707**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2020.
_____. **Lei número 8.078**, de 11 de setembro de 1990. Dispões sobre a proteção do consumidor e dá outras providências. Brasília, DF: Diário Oficial da União, 1990.

BRASIL. Vendas de pequenas empresas pela internet crescem 1.200% desde a pandemia, mostra painel do MDIC. **Portal Gov Br**. 2025. Disponível em: https://www.gov.br/mdic/pt-br/assuntos/noticias/2025/junho/vendas-de-pequenas-empresas-pela-internet-crescem-1-200-desde-a-pandemia-mostra-painel-do-mdic . Acesso em: 22 out. 2025

CAMPOS, Luís; CANAVEZES, Sara. **Introdução à globalização**. 2007. Disponível em: https://dspace.uevora.pt/rdpc/bitstream/10174/2468/1/Introdu%C3%A7%C3%A3o%20%C3%A0%20Globaliza%C3%A7%C3%A3o.pdf?msclkid=8915f5a9b55b11ec891fbc0906e51459. Acesso em: 30 out 2025.

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. **Cadernos Jurídicos, São Paulo, ano**, v. 21, p. 163-170, 2020. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_6_a_responsabilidade_civil.pdf. Acesso em: 30 out 2025.

CARDOSO, Caroline DE MELO; RÉGIS, Jonathan Cardoso. Direito Comparado: LGPD e o Marco Civil da Internet. **Revista de Direito**, v. 16, n. 1, p. 1-23, 2024. Disponível em: file:///C:/Users/mirel/Downloads/Dialnet-DireitoComparado-10189444%20(2).pdf. Acesso em: 30 out 2025.

CASTELLS, M. A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade. Trad. Maria Luiz X. de A. Borges. Rio de Janeiro: Jorge Zahar, 2003.

_____. A era da informação: economia, sociedade e cultura. São Paulo: Paz e Terra, 1999.

CAVALIERI FILHO, Sérgio. **Programa de direito do consumidor**. 5. ed. São Paulo: Atlas, 2019.

CERVELIN, Pietro Dalla Costa. Da conceituação do Controlador e Operador na Lei Geral de Proteção de Dados. 2021. Disponível em: https://lume.ufrgs.br/handle/10183/238084. Acesso em: 30 out 2025.

COLZANI, Ana Luiza. ROSA, Alexandre Morais. DNA em leilão: caso 23andMe e a mercantilização da privacidade. **Conjur**. Disponível em: https://www.conjur.com.br/2025-set-05/dna-em-leilao-caso-23andme-e-a-mercantilizacao-da-privacidade/. Acesso em:04 dnov. 2025.

COMÉRCIO eletrônico tem salto em 2020 e dobra participação no varejo brasileiro. **E-commerce Brasil**. 2021. Disponível em: https://www.ecommercebrasil.com.br/noticias/comercio-eletronico-salto-2020-varejo. Acesso em: 22 out. 2025

COMO criminosos podem se aproveitar de testes de DNA para roubar dados genéticos. **The British Broadcasting Corporation**. Disponível em: https://www.bbc.com/portuguese/articles/c72062jqxvxo. Acesso em: 30 out.2025.

CORDEIRO, António Menezes. **Da boa fé no Direito Civil**. São Paulo: Almedina, 2017.

CRAVO, Daniela Copetti; JOELSONS, Marcela. A importância do CDC no tratamento de dados pessoais de consumidores no contexto da pandemia e de vacatio legis da LGPD. **Revista de Direito do Consumidor**, v. 131, p. 111-145, 2020. Disponível em:https://www.researchgate.net/profile/Marcela-Joelsons-2/publication/352131773_A_IMPORTANCIA_DO_CDC_NO_TRATAMENTO_DE_DADOS_PESSOAIS_DE_CONSUMIDORES_NO_CONTEXTO_DE_PANDEMIA_E_DE_VACATIO_LEGIS_DA_LGPD/links/60ba40cd299bf10dff96e2d3/A-IMPORTANCIA-DO-CDC-NO-TRATAMENTO-DE-DADOS-PESSOAIS-DE-CONSUMIDORES-NO-CONTEXTO-DE-PANDEMIA-E-DE-VACATIO-LEGIS-DA-LGPD.pdf. Acesso em: 30 out. 2025.

DEITEL, P.; DEITEL, H. **Java - como programar.** 8ª ed. São Paulo: Pearson Prentice Hall, 2010. Disponível em: https://www.kufunda.net/publicdocs/Java%20Como%20Programar%20(Paul%20Deitel%20Harvey%20Deitel)%20(z-lib.org).pdf. Acesso em: 30 out 2025.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro –** Teoria Geral do Direito Civil. São Paulo: Saraiva, 2002, p. 386

DINIZ, Maria Helena**. Dicionário jurídico**. São Paulo: Saraiva, 1998. Volume 1.

BRASIL. Disponibilizaçãoindevida de informações pessoais em banco de dados gera dano moral presumido. **Superior Tribunal de Justiça**. Disponível em:

https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2025/05092025-Disponibilizacao-indevida-de-informacoes-pessoais-em-banco-de-dados-gera-dano-moral-presumido.aspx. Acesso em: 30 out. 2025.

DUONG, R. (2019). **Shoshana Zuboff em Capitalismo de Vigilância.** [Video]. Canal VPRO Documentary. 20 dez.. 50 min. https://www.youtube.com/watch?v=hIXhnWUmMvw&t=37s. Acesso em: 30 out. 2025.

É #FAKE mensagem de WhatsApp que se passa por Loggi e Jadlog e cobra “taxa” para liberar encomenda; trata-se de golpe. **G1**. Disponível em https://g1.globo.com/fato-ou-fake/noticia/2025/08/19/e-fake-mensagem-de-whatsapp-que-se-passa-por-loggi-e-jadlog-e-cobra-taxa-para-liberar-encomenda-trata-se-de-golpe.ghtml. Acesso em: 30 out. 2025.

FABRIZ, Daury César; MARTINELLI, Claudio. O avanço da tecnologia no mercado de trabalho: uma releitura do direito fundamental à proteção contra a automação. **Utopía y praxis latinoamericana: revista internacional de filosofía iberoamericana y teoría social,** v. 30, n. 110, p. 9, 2025. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=10276749 .Acesso em: 30 out. 2025.

FEDERIGHI. Preta. Virada na jurisprudência de responsabilidade em proteção de dados?. **JOTA**. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/virada-na-jurisprudencia-de-responsabilidade-em-protecao-de-dados. Acesso em: 30 out. 2025.

FILHO, Adalberto Simão. Limites e contornos da responsabilidade civil dos agentes de tratamento de dados: diálogo entre o CDC e a LGPD. **Revista IBERC**, v. 4, n. 3, p. 38-52, 2021. Disponível em ;https://revistaiberc.responsabilidadecivil.org/iberc/article/view/185. Acesso em: 30 out 2025.

FIUZA, César. **Direito Civil -** Curso Completo. Belo Horizonte: Del Rey, 2004.

FONSECA, Edson Pires. Lei Geral de Proteção de Dados Pessoais - LGPD. JUSPODIVM, 2021.São Paulo.

FORCELINI, L. S., & TONIAL, N. R. G. (2024). A influência dos algoritmos na personalização do consumo: os novos tipos de vulnerabilidade do consumidor e os desafios na regulamentação do comércio eletrônico. **Revista de Direito**, Globalização e Responsabilidade nas Relações de Consumo, v. 10, n. 1, 2024. Disponível em: https://www.indexlaw.org/index.php/revistadgrc/article/view/10520. Acesso em:30 out. 2025.

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. **Revista Direito e Práxis**, v. 12, n. 2, p. 1002-1033, 2021. Disponível em: https://dspace.almg.gov.br/handle/11037/41817. Acesso em:30 out. 2025.

FRAZÃO, Ana.Nova LGPD: as demais hipóteses de tratamento de dados pessoais. JOTA. 2018. Disponível em < https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-as-demais-hipoteses-de-tratamento-de-dados-pessoais. Acesso em: 30 out. 2025

GARCIA, Ricardo Lupion. **Boa-fé objetiva nos contratos empresariais: contornos dogmáticos dos deveres de conduta**. Porto Alegre: Livraria do Advogado. 2011.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro**. São Paulo: Saraiva, 2005.

GONDIM, Glenda Gonçalves. A responsabilidade civil no uso indevido dos dados pessoais. **Revista IBERC**, v. 4, n. 1, p. 19-34, 2021. Disponível em: https://revistaiberc.responsabilidadecivil.org/iberc/article/view/140. Acesso em: 30 out 2025.

LEI Geral de Proteção de Dados Pessoais (LGPD). **GOV**. Disponível em: https://www.gov.br/esporte/pt-br/acesso-a-informacao/lgpd. Acesso em: 30 out. 2025.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau. Término do tratamento de dados. *In*: Tepedino, Gustavo; Frazão, Ana; Oliva, Milena Donato. **Lei Geral de Proteção de Dados Pessoais**. São Paulo: Editora Revista dos Tribunais. 2019.

KLEEMAN, Jenny. Como criminosos podem se aproveitar de testes de DNA para roubar dados genéticos. Disponível em https://www.bbc.com/portuguese/articles/c72062jqxvxo. Acesso em: 03 nov. 2025.

LIMA, Cíntia Rosa Pereira. Comentários à Lei Geral de Proteção de Dados. São Paulo: Grupo Almedina (Portugal), 2020.
LOBO, Arthur Mendes. Aloia Myreilla. Decisão do STJ sobre dano moral em proteção de dados afeta crédito. Disponível em: https://www.conjur.com.br/2025-set-16/decisao-do-stj-sobre-dano-moral-em-protecao-de-dados-afeta-credito/>.Acesso em: 30 out. 2025

LUGATI, Lys Nunes; DE ALMEIDA, Juliana Evangelista. Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. **Revista de Direito**, v. 12, n. 2, p. 1-33, 2020.Disponível em: file:///C:/Users/mirel/Downloads/Dialnet-DaEvolucaoDasLegislacoesSobreProtecaoDeDados-8112951%20(4).pdf. Acesso em: 30 out. 2025

MARQUES, Claudia Lima in BENJAMIN, Antônio Herman V. Manual de direito do consumidor. 2. ed. rev. atual. e ampl., São Paulo: Revista dos Tribunais, 2009.

MARTINS, Leonardo. Introdução à jurisprudência do Tribunal Constitucional Federal Alemão. *In:* MARTINS, Leonardo (Org.). **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Tradução de Beatriz Henning et al. Prefácio de Jan Woischnik. Montevidéu: Fundação Konrad Adenauer, 2005. p. 233-

245. Disponível em: https://www.mpf.mp.br/atuacao-tematica/sci/jurisprudencias-e-pareceres/jurisprudencias/docs-jurisprudencias/50_anos_dejurisprudencia_do_tribunal_constitucional_federal_alemao.pdf#page=33. Acesso em: 30 out 2025

MARIGHETTO,Andrea. SILVA, Franciso de Assis. Manifestação da vontade no negócio jurídico deve ser livre e incondicionada. **CONJUR**. Disponível em: https://www.conjur.com.br/2024-mar-05/manifestacao-da-vontade-no-negocio-juridico-deve-ser-livre-e-incondicionada/. Acesso em: 30 out. 2025.

MEIRELES, Adriana Veloso. Algoritmos e autonomia: relações de poder e resistência no capitalismo de vigilância. **Opinião Pública**, v. 27, n. 1, p. 28-50, 2021.Disponível em: https://www.researchgate.net/publication/352147462_Algoritmos_e_autonomia_relacoes_de_poder_e_resistencia_no_capitalismo_de_vigilancia. Acesso em: 30 out 2025.

MELO, Ruy Ovídio Perrelli. **Percepção dos Usuários sobre a LGPD: Bases Legais, Princípios e Direitos dos Titulares**. 2022. Tese de Doutorado. UNIVERSIDADE FEDERAL DE PERNAMBUCO.Disponível em: https://www.cin.ufpe.br/~jffv/docs/TG_Ruy_Ovidio.pdf. Acesso em: 30 out 2025

MENA,, Isabela. **Verbete Draft: o que é capitalismo de vigilância**. Projeto draft 2019. Disponível em: https://www.projetodraft.com/verbete-draft-o-que-e-capitalismo-de-vigilancia.Acesso em: 30 out. 2025.

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Revista Pensar,** Fortaleza, v. 25, n. 4, p. 1-18, 2020.Acesso em: https://ojs.unifor.br/rpen/article/view/10828. Disponível em: 30 out 2025.

MENDES, Laura Schertel. Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo. 2008, 158 f. Dissertação (Mestrado em Direito) – Faculdade de Direito da Universidade de Brasília, Brasília, 2008. Disponível em: https://ojs.unifor.br/rpen/article/view/10828. Acesso em: 30 out 2025.

MENDES, Laura Schertel; DONEDA, D. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018), o novo paradigma da proteção de dados no Brasil. **Revista de Direito do Consumidor**, v. 120, p. 555, 2018. Acesso em: https://www.academia.edu/42740879/Coment%C3%A1rio_%C3%A0_nova_Lei_de_Prote%C3%A7%C3%A3o_de_Dados_lei_13_709_2018_o_novo_paradigma_da_prote%C3%A7%C3%A3o_de_dados_no_brasil. Disponível em: 30 out 2025.

MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **REI-Revista Estudos Institucionais**, v. 6, n. 2, p. 507-533, 2020.Disponível em: https://www.estudosinstitucionais.com/REI/article/view/521. Acesso em: 30 out 2025.

MENKE, Fabiano (org.). **Lei Geral de Proteção de Dados:** aspectos relevantes. Indaiatuba-SP: Editora Foco, 2021. Disponível em: https://bdjur.stj.jus.br/server/api/core/bitstreams/9a589202-53c2-43d5-923d-93ea976997dc/content. Acesso em: 30 out 2025.
MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGDP. IN: Cadernos Adenauer, volume 3, 2019. Disponível em: https://pt.scribd.com/document/514222045/Autodeterminacao-Informativa-e-Responsabilizacao-Proativa-Maria-Celina-e-Joao-Quinelato. Acesso em: 30 out 2025.

MINAS GERAIS. **PROCON-MG multa rede de farmácias por exigir CPF de consumidor**. Disponível em: https://www.mpmg.mp.br/portal/menu/comunicacao/noticias/procon-mg-multa-rede-de-farmacias-por-exigir-cpf-do-consumidor.shtml>.Acesso em: 30 out. 2025

MINAS GERAIS. RAIA DROGRASIL é multada em mais de R$8 milhões pelo Procon de MG por exigir CPF de consumidores. MPMG. Disponível em: https://g1.globo.com/mg/minas-gerais/noticia/2024/12/16/procon-mg-multa-raia-drogasil-em-mais-de-r-8-milhoes-por-exigir-cpf-de-clientes.ghtml. Acesso em: 30 out. 2025

MORAES, Maria Celina Bodin de; TEFFÉ, Chiara. Redes sociais virtuais, privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. **Revista Pensar**, v. 22, n. 1, 2017. Disponível em: https://ojs.unifor.br/rpen/article/view/6272. Acesso em: 30 out 2025.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, v. 19, n. 3, p. 159-180, 2018. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603. Acesso em 30 out 2025.

MULHOLLAND, Caitlin. Responsabilidade civil por danos causados pela violação de dados sensíveis e a Lei Geral de Proteção de Dados Pessoais (lei 13.709/2018). *In*: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (coords.). **Responsabilidade civil e novas tecnologias**. Indaiatuba, SP**:** Editora Foco, 2020.

NORAT, Markus Samuel Leite**.** O conceito de consumidor no direito: uma comparação entre as teorias finalista, maximalista e mista. **Cognitio Juris**, v.2, n. 4, p.80-95, 2012.

NUNES, Natalia. 10 princípios da LGPD para o tratamento de dados pessoais. Disponível em https://www.jusbrasil.com.br/artigos/10-principios-da-lgpd-para-o-tratamento-de-dados-pessoais/698194397. .Acesso em: 30 out. 2025.

OLIVEIRA, Ana Carolina Rios; DA CRUZ FERREIRA, Henrique; PIRES, Fernanda Ivo. Princípios da Lei Geral de Proteção de Dados (LGPD). **Seara Jurídica**, v. 1, n.

19, p. 1-12, 2021. Disponível em: https://publicacoes.unijorge.com.br/searajuridica/article/view/431. Acesso em 30 out 2025.

OLIVEIRA, Guilherme Henrique Gualtieri. As bases legais para o tratamento de dados pessoais: muito além do consentimento. **Lei Geral de Proteção de Dados: uma análise preliminar da Lei**, v. 13, p. 45-63, 2018.Disponível em: https://www.researchgate.net/profile/Bernardo-Grossi-2/publication/345774449_Lei_Geral_de_Protecao_de_Dados_uma_analise_preliminar_da_Lei_1370918_e_da_experiencia_de_sua_implantacao_no_contexto_empresarial/links/5fad7a6aa6fdcc9389acd493/Lei-Geral-de-Protecao-de-Dados-uma-analise-preliminar-da-Lei-13709-18-e-da-experiencia-de-sua-implantacao-no-contexto-empresarial.pdf. Acesso em: 30 out 2025.

PAGANELLA, Victoria Dickow. Responsabilidade Civil na Lei Geral de Proteção de Dados: uma análise do nexo de imputação. In: DRESCH, Rafael de Freitas Valle;

PAIVA, Carolina Andrade; BEZERRA, Úrsula; LIRA, Silva. Análise jurídica da proteção de dados pessoais na esfera do comércio digital. **Revista de Estudos Jurídicos do UNI-RN**, n. 6, p. 322-351, 2022.Disponível em: https://revistas.unirn.edu.br/index.php/revistajuridica/article/view/837. Acesso em 30 out 2025.

PEREIRA, Caio Mário da Silva. **Instituições de Direito Civil**. Rio de Janeiro: Forense, 2007. Disponível em: https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:livro:2017;001085986. Acesso em: 30 out 2025.

PESTANA, Marcio. Os princípios no tratamento de dados na LGPD (Lei Geral da Proteção de Dados Pessoais). **Conjur**, mai. 2020. Disponível em: https://www.conjur.com.br/2020-mai-25/marcio-pestana-principios-tratamento-dados-lgpd. Acesso em: 30 out. 2025

PINHEIRO, Victor Sales; BONNA, Alexandre Pereira. Sociedade da informação e direito à privacidade no Marco Civil da Internet: fundamentação filosófica do Estado de Direito. **Revista de Direitos e Garantias Fundamentais**, v. 21, n. 3, p. 365-394, 2020. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1555. Acesso em: 30 out 2025.

POPPER, Karl R. **A lógica da pesquisa científica**. São Paulo: Unesp, 2014. Disponível em: https://ocondedemontecristo.wordpress.com/wp-content/uploads/2011/05/popper-karl-a-logica-da-pesquisa-cientifica.pdf. Acesso em: 30 out de 2025.

REIS, Icaro Gabriel da Cunha. Entre inovação e privacidade:: a LGPD como baluarte dos direitos fundamentais na era tecnocientífica brasileira. **Revista Científica da Academia Brasileira de Direito Civil**, v. 5, p. 79-109, 2024.Disponível em:ABDC+-+revista+-+2+Artigo (5).pdf . Acesso em: 30 out 2025.

RIFKIN, Jeremy. **Sociedade com custo marginal zero:** a internet das coisas, os bens comuns colaborativos e o eclipse do capitalismo. São Paulo: MBooks, 2016

SANTANA, Vithorya Kellen Fonseca; ALVES, Israel Andrade. Direito do Consumidor nas Compras pela Internet. **Revista JRG de Estudos Acadêmicos**, v. 8, n. 18, p. e082144-e082144, 2025. Disponível em: https://revistajrg.com/index.php/jrg/article/view/2144. Acesso em: 30 out 2025.

SEGUNDO, Elpídio Paiva Luz; COUTO, Eliane Lopes. A Proteção de Dados e a Hipervulnerabilidade do Consumidor sob a Perspectiva do Consentimento e Privacidade na Internet. **Revista Jurídica Cesumar-Mestrado**, v. 22, n. 3, p. 551-566, 2022.Acesso em: https://periodicos.unicesumar.edu.br/index.php/revjuridica/article/view/11114. Disponível em: 30 out 2025

SILVA, Clóvis V. do Couto e. A obrigação como processo. Rio de Janeiro: FGV
SILVA, Rosana Oliveira da et al. Uma discussão necessária sobre a vulnerabilidade do consumidor: avanços, lacunas e novas perspectivas. **Cadernos EBAPE. BR**, v. 19, p. 83-95, 2021. Disponível em: https://www.researchgate.net/publication/350083231_Uma_discussao_necessaria_sobre_a_vulnerabilidade_do_consumidor_avancos_lacunas_e_novas_perspectivas. Acesso em: 30 out 2025.

SILVEIRA, Neli Alessandro Medeiros. O princípio da vulnerabilidade perante o Código de Defesa do Consumidor. Jusbrasil. Disponível em: https://www.jusbrasil.com.br/artigos/o-principio-da-vulnerabilidade-perante-o-codigo-de-defesa-do-consumidor/1577310506. Acesso em: 30 out. 2025

SIQUEIRA, Oniye Nashara et al. A (hiper) vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD. **Revista Eletrônica Pesquiseduca**, v. 13, n. 29, p. 236-255, 2021. Disponível em: https://periodicos.unisantos.br/pesquiseduca/article/view/1029. Acesso em: 30 out 2025.

SOUZA, Déborah Barreto. **O Art 2° do Código de Defesa do Consumidor e as regras de hermenêutica jurídica.** Âmbito jurídico,01/07/2010. Disponível em: https://ambitojuridico.com.br/o-art-2-do-codigo-de-defesa-do-consumidor-e-as-regras-de-hermeneutica-juridica/ . Acesso em: 30 out. 2025

SOUZA, Felipe Gabriades de. **O mito da supremacia do consentimento:** o mecanismo de pluralidade de bases legais da LGPD. 2025. Disponível em: https://repositorio.fgv.br/server/api/core/bitstreams/974095fa-1383-44c1-9158-a631a53a90c9/content. Acesso em: 30 out 2025.

SOUZA, Thais. Golpe da transportadora Loggi. Davi. Disponível em: https://www.davi.com.br/seguranca-digital-144/golpe-da-transportadora-loggi/. Acesso em: 30 out. 2025.

SPAGNOLLO, LETICIA; TONIAL, Nadya Regina Gusella. O papel do algoritmo como influenciador na sociedade de consumo e a (hiper) vulnerabilidade do consumidor. **Revista de Direito, Globalização e Responsabilidade nas Relações de Consumo,** v. 9, n. 1, p. 76–95-76–95, 2023. Disponível em: https://www.indexlaw.org/index.php/revistadgrc/article/view/9708. Acesso em: 30 out 2025.

(**STJ** - AgInt no AREsp: 1856105 RJ 2021/0073793-9, Data de Julgamento: 02/05/2022, T3 - TERCEIRA TURMA, Data de Publicação: DJe 05/05/2022). Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/1523582379/inteiro-teor-1523582407. Acesso em: 30 out 2025.

(**STJ** - REsp: 2201694 - SP (2025/0081134-2), Data de Julgamento: 05/08/2025, T3 - TERCEIRA TURMA, Data de Publicação: DJe 15/08/2025). Disponível em: https://processo.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202500811342&dt_publicacao=15/08/2025. Acesso em: 30 out 2025.

TARTUCE, F; NEVES, D. A. A. **Manual de Direito do Consumidor**. 11. ed. Rio de Janeiro: Método, 2022.

TASSO, Fernando Antonio. A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor. **Cadernos Jurídicos, São Paulo, ano**, v. 21, p. 97-115, 2020
.

TEFFÉ, Chiara Antonia Spadaccini; TEPEDINO, Gustavo. O consentimento na circulação de dados pessoais. **Revista Brasileira de Direito Civil**, v. 25, n. 03, p. 83-83, 2020. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/521. Acesso em: 30 out 2025.

TEFFÉ, Chiara Spadaccini; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica. com**, v. 9, n. 1, p. 1-38, 2020.Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/510. Acesso em 30 out 2025.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 281-318. p. 300. Disponível em:521-Texto do Artigo-2027-1918-10-20201117 (4).pdf. Acesso em: 30 out 2025.

TONIAZZO, Daniela Wendt. O consentimento na Lei geral de proteção de dados e o problema da assimetria informacional: soluções a partir da cláusula geral da boa-fé

objetiva. 2022. **Dissertação de Mestrado**. Pontifícia Universidade Católica do Rio Grande do Sul.Disponível em: https://repositorio.pucrs.br/dspace/handle/10923/24466?locale=pt_BR. Acesso em: 30 out 2025.

VELLOSO, Larissa Cimarelli. A vulnerabilidade do consumidor nas relações de consumo mediadas por inteligência artificial. **REVISTA FOCO**, v. 18, n. 6, p. e8723-e8723, 2025.Disponível em: https://ojs.focopublicacoes.com.br/foco/article/view/8723. Acesso em: 30 out 2025.

VERBICARO, Dennis et al. O consumidor digital: vulnerabilidade algorítmica ao empoderamento. **FURB Revista jurídica**. v. 26. 2022. Disponível em: leonardorocha,+Gerente+da+revista,+e9910 (8).pdf. Acesso em 30 out 2025.

VIEIRA, Pedro Gallo; PEDRA, Adriano Sant'Ana. O rol de deveres fundamentais na Constituição como numerus apertus. **Derecho y Cambio Social**, v. 10, n. 31, 2013. Disponível em: file:///C:/Users/mirel/Downloads/O+ROL+DE+DEVERES+FUNDAMENTAIS+NA+CONSTITUI%C3%87%C3%83O%20(1).pdf. Acesso em: 30 out 2025.

ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância: A Luta por um Futuro Humano na Nova Fronteira do Poder**. Nova York: PublicAffairs, 2019.

ZUBOFF, Shoshana. The age of surveillance capitalism: The fight for a human future at the new frontier of power. Londres: Profile Books, 2019.