**UNIVERSIDADE ESTADUAL DA PARAÍBA**
**CAMPUS III**
**CENTRO DE HUMANIDADES**
**DEPARTAMENTO DE DIREITO**
**CURSO DE DIREITO**

**EDUARDO VIEIRA DA ROCHA GOUVEIA**

# O USO DE DADOS E INFORMAÇÕES DOS CONSUMIDORES PARA RASTREAR SUAS PREFERÊNCIAS DE CONSUMO

**GUARABIRA – PB**
**2025**

EDUARDO VIEIRA DA ROCHA GOUVEIA

# O USO DE DADOS E INFORMAÇÕES DOS CONSUMIDORES PARA RASTREAR SUAS PREFERÊNCIAS DE CONSUMO

Trabalho de Conclusão de Curso (Artigo) apresentado à Coordenação do Curso de Direito da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de Bacharel em Direito.

**Área de concentração:** Direito do Consumidor.

**Orientadora:** Profa. Ma. Crizeuda Farias da Silva Dias.

**GUARABIRA-PB**
**2025**

G719u Gouveia, Eduardo Vieira da Rocha.
O uso de dados e informações dos consumidores para rastrear suas preferências de consumo [manuscrito] / Eduardo Vieira da Rocha Gouveia. - 2025.
27 f.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Estadual da Paraíba, Centro de Humanidades, 2025.

"Orientação : Prof. Ma. Crizeuda Farias da Silva Dias, Departamento de Ciências Jurídicas - CH".

1. Dados. 2. Direito. 3. Consumo. 4. Internet. I. Título

21. ed. CDD 342.2

Elaborada por Maria Suzana Diniz da Silva - CRB - 15/873 BSC3

EDUARDO VIEIRA DA ROCHA GOUVEIA

# O USO DE DADOS E INFORMAÇÕES DOS CONSUMIDORES PARA RASTREAR SUAS PREFERÊNCIAS DE CONSUMO

Trabalho de Conclusão de Curso apresentado à Coordenação do Curso de Direito da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de Bacharel em Direito

Aprovada em: 30/05/2025.

BANCA EXAMINADORA

Documento assinado eletronicamente por:

- **Alex Taveira dos Santos** (***.526.184-**), em **05/06/2025 17:49:00** com chave **8220a7ba424e11f086a006adb0a3afce**.
- **Crizeuda Farias da Silva Dias** (***.943.474-**), em **06/06/2025 15:55:54** com chave **df8e6040430711f09d131a7cc27eb1f9**.
- **Valter Henrique Pereira Junior** (***.822.054-**), em **05/06/2025 18:21:01** com chave **fafa92c8425211f09a351a7cc27eb1f9**.

Documento emitido pelo SUAP. Para comprovar sua autenticidade, faça a leitura do QrCode ao lado ou acesse https://suap.uepb.edu.br/comum/autenticar_documento/ e informe os dados a seguir.
**Tipo de Documento:** Folha de Aprovação do Projeto Final
**Data da Emissão:** 06/06/2025
**Código de Autenticação:** d03540

**SUMÁRIO**


| | | |
|---|---|---|
| **1** | **INTRODUÇÃO** ..... | 5 |
| **2** | **DADO SENSÍVEL E DADO PESSOAL** ..... | 6 |
| **3** | **PUBLICIDADE PERSONALIZADA E COLETA DE DADOS** ..... | 9 |
| **4** | **REGULAÇÃO JURÍDICA** ..... | 12 |
| **5** | **CONSIDERAÇÕES FINAIS** ..... | 19 |
| | **REFERÊNCIAS** ..... | 20 |

# O USO DE DADOS E INFORMAÇÕES DOS CONSUMIDORES PARA RASTREAR SUAS PREFERÊNCIAS DE CONSUMO

## THE USE OF CONSUMER DATA AND INFORMATION TO TRACK THEIR CONSUMPTION PREFERENCES

Eduardo Vieira da Rocha Gouveia[*]


## RESUMO

O presente trabalho examina o uso de dados e informações pessoais de consumidores como instrumento de rastreamento de preferências de consumo em ambientes digitais. Parte-se da constatação de que o avanço das tecnologias de informação e comunicação permitiu a intensificação da coleta automatizada de dados por empresas privadas, com fins publicitários e comerciais. Utilizando metodologia qualitativa, com base em pesquisa bibliográfica e documental, a análise recai sobre o ordenamento jurídico brasileiro, com foco na Constituição Federal, no Código de Defesa do Consumidor, no Marco Civil da Internet e na Lei Geral de Proteção de Dados Pessoais (LGPD). A investigação aborda o tratamento de dados pessoais, dados sensíveis e dados anonimizados, além da aplicação de mecanismos de segurança da informação voltados à preservação da privacidade dos titulares. Demonstra-se que, embora existam mecanismos legais de controle e responsabilização, persistem lacunas normativas e desafios relacionados à eficácia prática das garantias previstas. Conclui-se que a proteção jurídica do consumidor no cenário digital exige não apenas atualização legislativa, mas também fiscalização contínua e educação informacional da sociedade.


**Palavras-chave:** dados; direito; consumo; internet.


## ABSTRACT

This study examines the use of consumers' personal data and information as a tool to track consumption preferences in digital environments. It starts from the premise that advances in information and communication technologies have intensified the automated collection of data by private companies for advertising and commercial purposes. Adopting a qualitative methodology, based on bibliographic and documental research, the analysis focuses on the Brazilian legal system, especially the Federal Constitution, the Consumer Protection Code, the Civil Rights Framework for the Internet, and the General Data Protection Law (LGPD). The study addresses the processing of personal data, sensitive data, and anonymized data, as well as the application of information security mechanisms aimed at preserving the privacy of data subjects. It demonstrates that, although legal mechanisms for control and accountability exist, regulatory gaps and challenges regarding the practical effectiveness of these guarantees remain. It concludes that legal protection of consumers in the digital context requires not only updated legislation but also continuous oversight and public education on data rights.


[*] Graduando em Direito pela Universidade Estadual da Paraíba (UEPB). E-mail: eduardo.gouveia@aluno.uepb.edu.br.

**Keywords**: data; law; consumption; internet.

## 1 INTRODUÇÃO

Hodiernamente, com o avanço da tecnologia, a explosão das redes sociais e o surgimento de novas modalidades de consumo através da internet, as empresas procuram cada vez mais maneiras de identificar os gostos e preferências dos consumidores, objetivando cercá-los com uma publicidade direcionada ao seu perfil de tal modo que a resistência em adquirir produtos e serviços seja vencida.

Assim, o consumidor ao navegar na internet, pesquisar sobre suas necessidades, visitar sites de compras ou simplesmente interagir com os seus seguidores, expõe seus dados pessoais e preferências de consumo, possibilitando que empresas especializadas em análise e captação de dados, como *Palantir Technologies, Microsoft Azure Data & AI* e *Semantix*, captem os seus dados sensíveis e pessoais e os compartilhem com empresas de diferentes ramos comerciais para diversas finalidades.

Essa perspectiva de captação e uso de dados dos consumidores brasileiros os expõe de forma ilegal e os coloca em situação de vulnerabilidade, afrontando sobremaneira a proteção estabelecida no art. 5º, inciso XXXII, da Constituição Federal de 1988. Nesse sentido, o Poder Legislativo brasileiro tem elaborado leis que buscam oferecer uma maior proteção ao consumidor em face da captação indevida de seus dados pessoais pelas empresas para serem usados no direcionamento de propagandas e publicidade em ambiente virtual. De início, é necessário evidenciar que o presente estudo aborda a problemática dos avanços tecnológicos e a insegurança dos dados sensíveis referentes às preferências de consumo dos usuários.

A pesquisa será conduzida por meio de uma análise da proteção à privacidade do consumidor, da defesa Ordem Econômica em face da busca desenfreada por lucros das empresas, que não cumprem a legislação consumerista e da insuficiência da atual legislação regulamentadora, que não contempla efetivamente a proteção constitucional direcionada ao consumidor no art. 5º, inciso XXXII da Constituição Federal de 1988. Para isso, será utilizada uma abordagem qualitativa, por meio de pesquisa bibliográfica e documental, analisando doutrinas e legislações pertinentes ao tema, permitindo uma avaliação crítica. No decorrer da pesquisa, abordará detalhadamente sobre o conceito de dados e a efetividade das normas supracitadas frente ao uso de dados e informações dos consumidores para rastrear suas preferências de consumo.

É certo que os avanços tecnológicos possibilitaram práticas comerciais inimagináveis em um passado recente. Isso porque a comunicação rápida, o acesso às notícias de forma instantânea e a compra de produtos de diferentes categorias através de aparelhos eletrônicos como o celular, poderiam ser ações inalcançáveis mesmo para o indivíduo de maior posição social do século passado. Entretanto, hoje é impensável viver sem tais facilidades.

Sob uma perspectiva crítica, observa-se que os grandes fornecedores, apesar de fomentarem milhares de empregos, dependem intensamente da venda de seus produtos para se manterem. Na busca por um aumento de suas receitas recorrem a diversas estratégias de marketing, muitas vezes agressivas e manipuladoras, como os Pop-ups, que são janelas que se abrem automaticamente no navegador de forma

excessiva para exibir promoções ou compartilhar conteúdos, visando alcançar o consumidor final a qualquer custo, sem considerar os impactos de suas práticas.

Nessa tendência, o uso irrestrito do algoritmo, mecanismo utilizado para filtrar informações dos usuários de plataformas de redes sociais, sites de pesquisas ou por histórico de navegação, coleta informações sobre preferências de consumo e através da análise de dados durante a navegação na rede e estabelece um perfil de consumo. Algoritmos como esses são transmitidos com o objetivo de moldar o comportamento e as preferências dos usuários enquanto navegam no ambiente digital, bem como para predizer suas necessidades e ações futuras.

O Direito, de modo geral, atua a partir das informações disponíveis, tanto para sustentar quanto para contrariar argumentos. Contudo, em determinadas situações, o Direito não consegue acompanhar os avanços tecnológicos e a mudança dos costumes da sociedade, tornando-se ineficiente perante o desconforto do indivíduo. Nessa perspectiva de fragilidade do direito, situa-se a proteção dos dados do consumidor, frente a atuação das empresas através dos meios digitais, a qual está gradativamente mais invasiva, captando dados sigilosos e sensíveis dos usuários da rede de computadores, a fim de ofertar produtos moldados pelo interesse do usuário.

Apesar disso, o ordenamento jurídico brasileiro vigente dispõe de normas que regulam o e-commerce (termo em inglês que significa comércio eletrônico, referindo-se as transações feitas pela internet), a privacidade digital dos consumidores e a atuação das empresas, sendo elas: Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei n.º 13.709/2018, Código de Defesa do Consumidor (CDC) - Lei n.º 8.078/1990, Marco Civil da Internet - Lei n.º 12.965/2014 e a própria Constituição Federal de 1988.

## 2 DADO SENSÍVEL E DADO PESSOAL

Dado é toda informação que pode ser associada a algo ou alguém. Podendo ser um telefone, local ou característica que, quando analisados e combinados adquirem grande valor, revelando informações importantes. São elementos fundamentais que formam a base da percepção e do conhecimento do indivíduo, pois, ao serem processados e contextualizados fornecem elementos que ajudam no direcionamento e na tomada de decisões. A Lei Geral de Proteção de Dados (LGPD) classifica as informações em três categorias principais: dado pessoal, dado sensível e dado anonimizado.

Para a legislação, dado pessoal é conceituado como qualquer informação relacionada à pessoa natural identificada ou identificável. Exemplificam-se dados cadastrais como: nome, Cadastro de Pessoa Física (CPF), Registro Geral (RG), data de nascimento, endereço e telefone. No ambiente virtual, esses dados cadastrais podem ser: endereço de e-mail, Internet Protocol (IP) de acesso e geolocalização. Os dados pessoais sensíveis são aqueles aos quais a LGPD conferiu uma proteção ainda maior, por estarem diretamente relacionados aos aspectos mais íntimos da personalidade de um indivíduo (Brasil, 2022).

O artigo 5º da LGPD apresenta um rol de situações que caracterizam um dado sensível, alguns dos quais serão analisados durante o presente capítulo. Verifica-se a seguir:

> II – dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (Brasil, 2018, art. 5º, inciso II).

O tratamento adequado dos dados de origem étnica e racial é essencial para fomentar a inclusão social e garantir a igualdade de oportunidades, bem como têm em comum o fato de fazerem menção a uma noção mais ampla, a de “origem”, e, de participarem de um jogo em que são potenciadores de fenômenos discriminatórios (Matos, 2019). Em ambientes institucionais, tais informações podem ser utilizadas para avaliar a eficácia de políticas de ações afirmativas e programas de diversidade, assim como demanda a Lei n.º 14.553/2023, a qual exige que empregadores coletem informações sobre a origem étnica e racial de seus funcionários para promover a igualdade no mercado de trabalho (Brasil, 2023). Em contrapartida, se esses dados forem usados de forma inadequada, podem aumentar preconceitos e a discriminação.

Quanto aos dados de convicção religiosa, trata-se de informações já protegidas pela Constituição Federal, que garante a inviolabilidade da liberdade de consciência e de crença, assegurando o livre exercício dos cultos religiosos e a proteção dos locais de culto e suas liturgias (Brasil, 1988). A Lei Geral de Proteção de Dados (LGPD), por sua vez, regula o tratamento dessas informações, protegendo a privacidade dos fiéis, garantindo que não sejam utilizadas de maneira indevida, seja para influenciar preferências no ambiente externo ou até mesmo dentro dos próprios locais de culto. Determinadas igrejas possuem o funcionamento baseado em campanhas de arrecadação de fundos e realização de atividades religiosas remuneradas, o que envolve a utilização de dados pessoais sensíveis dos fiéis para a organização e gestão dessas iniciativas. Segundo Zuffo:

> Ao menos desde o início de 2019, algumas igrejas têm utilizado câmeras de reconhecimento facial para traçar o perfil do fiel, obtendo relatórios sobre a assiduidade de seu público e o humor durante os cultos, visando aumentar o engajamento em relação às atividades religiosas, dentre outras questões. Há duas empresas especializadas no setor religioso no Brasil (Igreja Mobile e Kuzzma), ambas apresentadas durante a 15ª Expo Cristã realizada em São Paulo, em 2019. A empresa brasileira, Igreja Mobile, desenvolveu os serviços para atender a demanda específica de religiosos nesse sentido, e realiza diversos tratamentos, além dos atrelados aos dados religiosos e biométricos dos fiéis, prometendo a entrega de relatórios de número de pessoas classificadas por gênero (Zuffo, 2021).

Outro ponto de extrema relevância é quanto aos estigmas e preconceitos que um indivíduo pode enfrentar por seguir determinada religião. Apesar de ser tipificado criminalmente pelo Código Penal, a discriminação em razão da opção religiosa ainda é comum no Brasil. Dessa forma, o tratamento correto por parte do detentor desses dados pessoais sensíveis se torna essencial, pois assegura a proteção da identidade e a prevenção dessa discriminação.

No tocante aos dados pessoais sensíveis vinculados à opinião política, o processamento adequado desses dados tornou-se ainda mais crucial, especialmente nas eleições presidenciais de 2022, marcada pela intensa disseminação de fake news. O uso indevido dessas informações revelou-se um fator preocupante, permitindo que publicações falsas e conteúdos manipulados fossem direcionados estrategicamente aos eleitores, influenciando sua intenção de voto. Além disso, o uso de dados sobre opinião política também pôde resultar em práticas abusivas, como direcionamento de propaganda eleitoral sem autorização, manipulação de perfis eleitorais e até mesmo tentativas de ameaças ou intimidações de eleitores por parte das milícias digitais.

Nessa perspectiva, o Tribunal Superior Eleitoral promulgou a Resolução n.º 23.650 de 2021, a qual institui a Política Geral de Privacidade e Proteção de Dados

Pessoais no âmbito da Justiça Eleitoral, inserindo dispositivos destinados a diminuir riscos relacionados ao uso indevido dessas informações no processo eleitoral.

Outros dados de extrema relevância mencionados no texto legal são aqueles relacionados à saúde ou à vida sexual, possivelmente os dados mais íntimos e sensíveis de um indivíduo. A legislação brasileira, portanto, reconheceu o caráter sensível dos dados pessoais relativos à saúde, bem como a necessidade de exigir um nível maior de proteção no seu tratamento (Figueiredo *et al*., 2023). Através desses dados, é possível identificar doenças, dietas terapêuticas, além do uso de medicamentos e tratamentos médicos. Logo, deve-se reafirmar que se trata de dados com elevado potencial discriminatório, cuja utilização pode ensejar consequências especialmente lesivas. (Figueiredo *et al*., 2023).

Com o objetivo de fortalecer a proteção dos dados relacionados à saúde, em 2021, o então Ministro de Estado da Saúde, Marcelo Queiroga, promoveu a atualização da Política Nacional de Informação e Informática em Saúde (PNIIS), incorporando novos dispositivos voltados à segurança da informação garantindo maior controle no uso das informações de saúde dos cidadãos. Essa portaria é fundamentada em diversos princípios essenciais, entre eles:

Art. 2º São princípios da PNIIS:

> I - promoção da universalidade, integralidade e equidade na atenção e proteção à saúde, direcionada à continuidade do cuidado individual e coletivo por meio dos processos de coleta, gestão, produção e disseminação dos dados e informação em saúde;
> II - fomento à gestão e à produção dos dados e informação em saúde, como elementos capazes de gerar conhecimento, na totalidade das ações de atenção, gestão, auditoria, pesquisa, controle e participação social, de modo a fundamentar ações de vigilância em saúde e formulação de políticas públicas;
> III - democratização dos dados e informação em saúde como dever das entidades no âmbito do SUS;
> IV - promoção do acesso aberto aos dados e à informação em saúde como direito do cidadão;
> V - descentralização dos processos de produção e disseminação dos dados e da informação em saúde, para atender às necessidades de compartilhamento de dados e às especificidades regionais e locais;
> VI - preservação da autenticidade, da integridade, rastreabilidade e da qualidade da informação em saúde, observado o disposto na Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados;
> VII - confidencialidade, privacidade, proteção de dados e segurança da informação de saúde pessoal como direito de todo indivíduo (Brasil, 2021, art. 2º).

Consideram-se dados anonimizados aqueles que, após serem submetidos a procedimentos, mediante a utilização de meios técnicos razoáveis e disponíveis no momento de seu tratamento (Brasil, 2018), perdem qualquer vínculo com a pessoa a quem originalmente pertenciam, impedindo sua identificação. Através de técnicas, um conjunto de dados original é transformado em um novo conjunto, por meio de alterações. As principais são: supressão, generalização e randomização (Barreto; Henrique, 2021). Essa conceituação visa garantir que, uma vez anonimizado, o dado não esteja mais sujeito às regras da lei, já que não representa mais risco à privacidade do indivíduo.

A supressão está relacionada com a remoção total de uma parte dos dados sensíveis ou pessoais, impossibilitando a identificação do indivíduo. Na prática, pode funcionar da seguinte maneira: dentre vários dados, a remoção do nome completo e

o CPF de um conjunto de informações, antes de disponibilizá-la para pesquisadores. Observa-se como vantagem a facilidade de implementar e a eficácia na remoção dos dados. Analogamente, nota-se como desvantagem a perda de qualquer valor estatístico ou analítico dos dados (Ferreira *et al*., 2022). Mesmo que outros dados permaneçam no conjunto, a retirada desses elementos impede que a pessoa seja identificada, garantindo um grau adequado de anonimização.

A generalização caracteriza-se na substituição de referências específicas por uma informação mais ampla do indivíduo. Um exemplo dessa técnica é trocar a idade exata por um intervalo etário, o que dificulta a identificação direta da pessoa, mas ainda preserva o valor informativo daquele dado. Nesse sentido, ainda que os valores originais apresentem significativas variações entre si, a generalização é eficaz, já que, de certa forma, os valores acabam sendo padronizados (Paiva, 2021).

Por fim, a randomização consiste na modificação dos dados por meio da introdução de elementos aleatórios, de modo a distorcer ou misturar as informações originais. Essa técnica tem como objetivo dificultar ao máximo que os dados sejam ligados a uma pessoa em particular, mesmo com métodos de reidentificação. Paiva também ressalta que:

> Ainda que um conjunto de dados anonimizado guarde sempre um risco residual de reidentificar os titulares das informações, o risco de danos em caso de eventual vazamento ou acesso indevido à base de dados é consideravelmente reduzido se comparado a uma base de dados em "estado bruto (Paiva, 2021, p. 73).

Dessa forma, as informações úteis são mantidas para fins de análise, ao mesmo tempo em que se impede que esses dados sejam ligados com precisão a alguém.

Com base no que foi exposto, foi possível compreender a relevância dos dados e a forma como são organizados. Além disso, ficou evidente que, apesar dos diversos dispositivos legais que asseguram a proteção dos dados previstos na legislação, estes continuam sendo frequentemente violados ou utilizados para fins diversos, evidenciando a necessidade de regulamentações complementares por parte de outros órgãos. Diante disso, torna-se necessário uma análise mais aprofundada sobre como essas informações vêm sendo utilizadas. Será pertinente analisar, mais adiante, o papel estratégico que os dados assumem nos processos de personalização de conteúdo.

## 3 PUBLICIDADE PERSONALIZADA E COLETA DE DADOS

Os padrões consumeristas se formam a partir da Primeira Revolução Industrial, no século XVIII, na qual houve a expansão do comércio e a mecanização dos processos produtivos possibilitou maior produtividade e, consequentemente, o aumento dos lucros (Rocha; Lima; Waldman, 2020). Já no século XIX, com a Segunda Revolução Industrial, quando a partir dessa data não só a oferta de alimentos cresceu, como todo o mercado de bens de consumo para os pobres começou a se transformar com multiplicação de lojas varejistas (sobretudo cadeias de lojas) (Hobsbawn, 2000).

Esta mesma revolução ficou marcada pelo modelo de produção de Henry Ford, o Fordismo, que defendia a produção de itens em série, possibilitando a venda de produtos em massa a preços mais baixos, já que esse modelo de produção de produtos barateava os custos de mão de obra, tornando-os acessíveis a uma maior

parte da população que não tinha como adquiri-los.

Posteriormente, em meados da década de 1970, com a Terceira Revolução Industrial, surge a internet para remodelar os meios de consumo. Para Milton Santos:

> (...) o mundo está marcado por novos signos, como: a multinacionalização das firmas e a internacionalização da produção e do produto; a generalização do fenômeno do crédito, que reforça as características da economização da vida social; os novos papéis do Estado em uma sociedade e uma economia mundializadas; o frenesi de uma circulação tornada fator essencial da acumulação; a grande revolução da informação que liga instantaneamente os lugares, graças aos progressos da informática (Santos, 2020, p.84).

Nessa referida era da revolução digital, as empresas de vendas on-line utilizam diversos artifícios com o objetivo de transformar os dados e informações dos consumidores em vendas lucrativas, adaptadas às suas preferências. Esse procedimento é possibilitado pelo uso de Cookies, geomarketing, Big Data, entre outras ferramentas eficazes para a coleta de dados dos consumidores. Esses recursos permitem uma análise detalhada do comportamento on-line dos usuários. Verifica-se mais detalhadamente como cada um desses elementos desempenha um papel crucial na coleta e análise de dados digitais.

Os Cookies são fragmentos de arquivos, cuja função principal é registrar as preferências do usuário enquanto ele navega no site. Em grande parte, os cookies salvam informações pessoais, como o histórico da pessoa, e-mail, senhas e outros dados para serem usados durante sua experiência (Costa, 2022).

De maneira geral, essa ferramenta pode ser classificada em duas categorias: Cookies de sessão e Cookies persistentes. O primeiro é temporário, sendo deletado automaticamente da máquina quando o utilizador fecha o site. Como exemplo, pode-se citar o carrinho de compras de uma loja virtual, que armazena temporariamente os itens selecionados, permitindo que o comprador volte e finalize a compra em outro momento. Enquanto o segundo pode ser prejudicial devido a sua duração previamente determinada, permanecendo armazenado por anos até que o usuário decida deletá-lo, o que, na maioria das vezes, não acontece devido à falta de conhecimento. As empresas que usam Cookies defendem que estes ajudam a aprimorar os sites, melhorando a experiência do usuário durante a navegação.

Ainda sobre os cookies, a Lei Geral de Proteção de Dados Pessoais (LGPD) exige que os sites informem com clareza e precisão sobre a coleta e o uso de dados dos usuários, utilizando avisos e solicitações de consentimento. Observa-se:

> Art. 7° O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I – mediante o fornecimento de consentimento pelo titular;
> II – para o cumprimento de obrigação legal ou regulatória pelo controlador; (Brasil, 2018, art. 7º).

Dessa forma, com a regulamentação do uso dos dados relacionados aos Cookies, o usuário conta com proteção legal contra a divulgação indevida de suas informações pelos sites e empresas de e-commerce.

O sistema de geomarketing consiste na captação de dados de clientes através da sua localização geográfica. Essa modalidade está vinculada ao número de IP (*Internet Protocol*), que atua como uma identidade virtual única do dispositivo.

Embora o rastreamento de IP permita identificar a rede à qual o dispositivo está conectado, ele não oferece uma localização precisa. Para obter a localização exata

do usuário, as empresas de marketplace utilizam o GPS (*Global Positioning System*), o qual nos últimos tempos, é uma das principais ferramentas para oferta de serviços e geomarketing como é o caso dos aplicativos *Waze, Uber, CittaMobi* e *iFood* (Santana *et al*., 2020).

Para fornecer a localização, basta que o usuário se conecte a uma rede Wi-Fi ou dados móveis. Após isso, as plataformas digitais circundantes ao consumidor têm acesso às suas preferências de consumo, podendo, assim, influenciá-lo.

Atualmente, os GPS utilizam satélites que orbitam a Terra, estações no solo e antenas de celular para dispor de localização precisa. É possível citar diferentes tipos: SBAS (*Satellite-Based Augmentation System*) é manuseado na aviação, DGPS (*Differential Global Positioning System*) é utilizado na agricultura e navegação marítima, enquanto o GNSS (*Global Navigation Satellite System*) consiste no sistema de navegação que está presente em celulares, carros e *smartwatches*.

Cumpre esclarecer que o geomarketing conta com técnicas de captação que permitem o uso de dados e informações dos consumidores em tempo real, para dividir o público com base em sua localização geográfica. Já o Geofence pode ser conceituada como um perímetro virtualmente definido ao redor de um certo ponto no globo terrestre, uma espécie de “cerca virtual” (Maia; Paulino, 2020).

Em síntese, ao entrar nessa área delimitada, o consumidor pode receber uma notificação ou publicidade específica programada pela Geofence. Similarmente, há também os Beacons, que são mecanismos cuja sua inteligência interna permite que armazenem informações e disseminem esse conteúdo conforme os usuários se aproximam do dispositivo (Bandeira, 2018).

Essa vigilância geográfica reduz a espontaneidade das escolhas dos consumidores, uma vez que potenciais compradores são monitorados e constantemente direcionados a estabelecimentos locais ou plataformas de marketplace específicas, com base em suas atividades e localização.

Big Data consiste no que há de mais tecnológico quando se diz respeito à captação e direcionamento de dados em alta velocidade. É um conjunto de métodos e técnicas usados para o processamento em grande escala desses dados. A principal fonte de big data é a Internet: toda a pegada digital dos utilizadores é convertível em informação (Costa, 2021). Com o uso do Big Data, é possível interpretar fenômenos relevantes e a personalização de ofertas de produtos, por meio do uso de dados e informações dos usuários frequentemente disponibilizados de forma consciente pelos usuários nas redes sociais ou coletadas automaticamente durante a navegação em ambientes digitais.

A estrutura conceitual desse modelo apoia-se em três pilares fundamentais: volume, velocidade e variedade.

O primeiro pilar está ligado com a grande quantidade de informações geradas de forma contínua por diversas fontes. Com os avanços tecnológicos, praticamente todos os dispositivos do cotidiano emitem registros de dados. Em razão desse grandioso crescimento, tornou-se necessário a adoção de uma tecnologia capaz de suportar e processar esse volume elevado de informações.

Enquanto o segundo destaca a rapidez com que esses dados são processados, exigindo mais sistemas capazes de operar em tempo real. Observa-se uma relação de interdependência entre o avanço dos dispositivos tecnológicos e a necessidade de aprimoramento dos mecanismos de processamento de dados. À medida que os dispositivos se tornam mais sofisticados, cresce proporcionalmente a demanda por sistemas que assegurem agilidade.

Por último, mas não menos importante, o terceiro pilar está ligado à diversidade

de fontes e formatos de dados. Esses conteúdos podem ser disponibilizados em vários formatos, abrangendo textos, imagens, áudios e vídeos. Essa diversidade acaba implicando na necessidade de métodos versáteis para tratar e extrair valor desses conteúdos. Essa variedade de formatos exige uma categorização baseada na forma como os dados são organizados, resultando em três grupos distintos: estruturados, não estruturados e semiestruturados.

Os dados estruturados, como o próprio nome sugere, são caracterizados por sua organização rígida, o que facilita significativamente seu processamento. Normalmente, são encontrados em bancos de dados relacionais, organizados com informações distribuídas em linhas e colunas. Entre os exemplos mais comuns, destacam-se dados cadastrais, planilhas eletrônicas e demais registros organizados de forma sistemática.

Diferentemente do primeiro, os dados não estruturados não se organizam em linhas e colunas, o que lhes atribui um formato mais variável, dificultando a sua organização e demandando ferramentas tecnológicas mais avançadas. Os exemplos de dados não estruturados podem incluir vídeos, imagens, áudios e outros conteúdos.

Os dados semiestruturados representam um ponto intermediário entre os estruturados e os não estruturados. Embora não sigam o formato tradicional de tabelas, apresentam certo grau de organização, podendo ser identificados por etiquetas que facilitam sua interpretação. Esses dados são comumente e-mails ou arquivos compactados.

Do ponto de vista mercadológico, a utilização de Big Data torna as preferências de consumo cada vez mais previsíveis, permitindo que as empresas observem os comportamentos e personalizem ofertas com maior precisão por meio da análise dos dados dos consumidores. No entanto, essa capacidade de previsão também levanta importantes discussões sobre os limites da coleta e do uso de dados pessoais, especialmente no que se refere à autonomia do consumidor e à transparência nas decisões. A esse respeito, Bauman observa:

> O capitalismo não entregou bens às pessoas, as pessoas foram crescentemente entregues aos bens; o que quer dizer o próprio caráter e sensibilidade das pessoas foi reelaborado, reformulado de tal forma que elas se agrupam aproximadamente...com as mercadorias, experiências e sensações, cuja a venda é o que dá forma e significado à suas vidas (Bauman, 2002, p. 100).

Fica claro, portanto, que o uso dos dados influencia diretamente a forma como se consome e se relaciona com o mundo. Foi possível observar, em diversas situações, que empresas ultrapassaram os limites éticos e legais no tratamento dessas informações, explorando dados pessoais de maneira excessiva ou sem o devido consentimento, evidenciando a importância de uma legislação adequada com sanções eficazes para coibir abusos.

## 4 REGULAÇÃO JURÍDICA

Quando se busca entender a evolução das normas que regulam o uso de dados e informações dos consumidores no Brasil, é inevitável começar pela Carta Constitucional de 1988. Foi ela que estabeleceu as bases para a proteção dos direitos fundamentais relacionados à privacidade e ao tratamento de dados pessoais. Em especial, destaca-se o artigo 5º, inciso XXXII, que reafirma a importância da defesa do consumidor como um direito essencial a ser promovido pelo Estado.

Para Pinto, os direitos fundamentais são aqueles que:

> [...] são os direitos do homem jurídico, institucionalizados e amparados objetivamente em determinada ordem jurídica concreta, ou seja, os direitos fundamentais são os direitos do homem, garantidos e limitados espaço temporalmente, o que implica no reconhecimento de que enquanto os direitos do homem são decorrentes da própria natureza humana, possuindo, destarte, caráter inviolável, intemporal e universal, os direitos fundamentais são os direitos vigentes numa específica ordem jurídica (Pinto, 2009, p.127).

A Constituição Federal reflete os anseios do povo, ela é um pilar essencial para garantir a dignidade humana, protegendo as liberdades individuais e promovendo a justiça social, sendo indispensável para a construção de uma sociedade pautada nos princípios da justiça e da igualdade. A Constituição formal, por conta de sua própria natureza, além de fixar diretrizes e impor limites, é resultado da positivação de uma ordem de valores que uma determinada sociedade entende ser importante para si (Pretto, 2007).

O artigo 5°, inciso X, da Constituição Federal de 1988, institui que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, garantindo, ainda, o direito à indenização por danos materiais ou morais decorrentes de sua violação (Brasil, 1988). Assim, para o constituinte, a proteção da intimidade e da vida privada dos consumidores é reconhecida como um direito fundamental que deve ser garantido e respeitado.

Ainda no mesmo artigo 5°, especificamente no inciso XII, estabelece-se a inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, visando proteger contra práticas ilícitas de espionagem e impedir a intromissão indevida de terceiros em questões privadas (Brasil, 1988). Todavia, o próprio texto do inciso prevê uma exceção, autorizando a quebra do sigilo das comunicações telefônicas por ordem judicial, desde que vinculada a casos de investigação criminal ou instrução processual penal.

A legislação específica que regulamenta a quebra de sigilo das comunicações telefônicas é a Lei n.º 9.296/1996. Esta lei regulamenta as interceptações de comunicações telefônicas e telemáticas, estabelecendo as condições para a realização dessa medida. A lei institui que, em qualquer hipótese, deve ser descrita com clareza a situação objeto da investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada (Brasil, 1996). Além disso, a lei proíbe a interceptação de comunicações telefônicas por terceiros quando não houver indícios razoáveis da autoria ou participação em infração penal, a prova puder ser feita por outros meios disponíveis e o fato investigado constituir infração penal punida, no máximo, com pena de detenção (Brasil, 1996). Conclui-se que a captação de informações dos consumidores é matéria relevante para o direito, devendo ser respeitada a privacidade.

A Emenda Constitucional n.º 115, de 2022, introduziu de forma expressa o direito à proteção dos dados pessoais, inclusive nos meios digitais (Brasil, 1988) no catálogo de direitos e garantias fundamentais previsto no artigo 5º da Constituição Federal de 1988. Ao reconhecer a importância da preservação da privacidade e do controle sobre as informações pessoais, a emenda contribui para a construção de uma sociedade mais justa e consciente no âmbito da gestão de dados (Laerte; Rocha, 2024). Tal inclusão evidencia a relevância atribuída pelo legislador brasileiro à proteção dos dados pessoais digitais, conferindo o mesmo status jurídico dos demais direitos fundamentais.

Avançando com as legislações específicas, encontra-se a Lei n.º 8.078/1990, o Código de Defesa do Consumidor, também contemplada no artigo 5º, inciso XXXII, artigo 170, inciso V da Constituição Federal de 1988. Conforme o legislador constitucional, o Estado promoverá, na forma da lei, a defesa do consumidor (Brasil, 1988), cuja finalidade é estabelecer princípios garantidores e regular as relações de consumo.

O Capítulo I do Código de Defesa do Consumidor estabelece definições para as relações de consumo no Brasil, buscando criar um equilíbrio entre as partes envolvidas. O conceito de consumidor abrange tanto pessoas físicas quanto jurídicas que adquirem ou utilizam produtos, ou serviços com o intuito de atender as suas necessidades. Por outro lado, o fornecedor é identificado como qualquer pessoa, seja física ou jurídica, que se ocupa da produção, distribuição ou comercialização de produtos e serviços, sendo, portanto, o responsável por colocá-los no mercado. A definição de produto é ampla, abrangendo bens tanto materiais quanto imateriais, móveis ou imóveis, enquanto serviço se refere a qualquer atividade disponibilizada ao público mediante pagamento, incluindo serviços bancários, financeiros e securitários (Brasil, 1990).

O Capítulo III dispõe acerca dos direitos básicos do consumidor:

> Art. 6º. São direitos básicos do consumidor:
> [...].
> II - a educação e divulgação sobre o consumo adequado dos produtos e serviços, asseguradas a liberdade de escolha e a igualdade nas contratações;
> III - a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem;
> IV - a proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, bem como contra práticas e cláusulas abusivas ou impostas no fornecimento de produtos e serviços (Brasil, 1990).

Pode-se notar que o consumidor está revestido de direitos fundamentais que garantem sua liberdade de escolha entre os produtos e serviços disponíveis no mercado, além de ter o direito a informação clara sobre os detalhes e características das mercadorias que adquire.

É absolutamente vedado o uso de métodos coercitivos e desleais para influenciar ou manipular as escolhas do consumidor. A liberdade de escolha deve ser preservada, garantindo uma decisão consciente, livre de manipulações e participações externas indevidas, para escolhas de produtos e serviços. Seguindo adiante, o ordenamento jurídico brasileiro dispõe do Marco Civil da Internet, instituído pela Lei n.º 12.965/2014. A referida Lei foi o resultado de constantes discussões entre a sociedade civil organizada e os poderes legislativo e executivo (Carvalho, 2017). Antes da criação de uma regulamentação específica, não existiam leis que disciplinassem de forma direta o uso da internet. Esse vazio legal gerava insegurança jurídica.

Sob essa análise, disserta Resende:

> A regulamentação da Internet exigia, desta forma, a elaboração de normas sobre o próprio funcionamento da rede, estabelecendo claramente quais os direitos e deveres dos seus usuários e das empresas provedoras da conexão, bem como as providências essenciais à identificação dos autores das condutas ali praticadas, sejam legais ou não (Resende, 2016, p. 67).

O Marco Civil da Internet surge como um marco regulatório fundamental para a utilização da rede de internet no Brasil, dispondo de um conjunto de normas essenciais que buscam organizar e disciplinar o funcionamento do *cyberspace*. Além de reafirmar a proteção dos direitos dos usuários, essa legislação também reforça a segurança nas relações de consumo realizadas on-line, algo cada vez mais necessário para a época, diante da forte digitalização do comércio. Seus princípios norteadores estão dispostos no artigo 3º, verifica-se:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> IV - preservação e garantia da neutralidade de rede;
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII - preservação da natureza participativa da rede;
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei (Brasil, 2014, art. 3º).

Outro aspecto significativo é que o parágrafo único do artigo em questão estabelece que os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados a matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte (Brasil, 2014). Os princípios mencionados pelo artigo 3º demonstram que a lei opera em harmonia com as demais leis do sistema jurídico, admitindo outros previstos na Constituição Brasileira, no Código Civil, ou em outros ramos do direito nacional, ou internacional.

O Capítulo II do Código de Defesa do Consumidor é responsável por abordar os direitos e garantias dos usuários, destacando que a internet desempenha um papel essencial como promotora do exercício da cidadania. Por meio dele, é possível garantir o acesso à informação, a liberdade de expressão e a privacidade.

Nesse sentido, o artigo 8º do Marco Civil da Internet designa o seguinte:

> Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.
> Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no caput, tais como aquelas que:
> I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou
> II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil (Brasil, 2014, art. 8º).

Portanto, ficou evidente que o Marco Civil da Internet atende aos anseios da sociedade, considerando que esta participou ativamente do seu processo de formulação. É importante destacar, ainda, que até a promulgação dessa lei, não havia regulamentações brasileiras específicas para o uso da Internet. Além disto, o MCI tem sido considerado uma verdadeira “Constituição da Internet”, pois traça diretrizes e normas fundamentais em relação à rede no Estado brasileiro (Resende, 2016).

Dando sequência, cumpre mencionar a Lei Geral de Proteção de Dados, a Lei

n.º 13.709/2018. A promulgação da LGPD representou um marco normativo ao preencher uma lacuna legislativa no ordenamento jurídico brasileiro, que até então carecia de uma regulamentação específica e abrangente sobre o tema. Esse dispositivo legal é prudente ao tratar em sua íntegra da preservação de dados pessoais, com procedimentos necessários em plena era digital, onde dados pessoais são tratados como valorosas mercadorias (Almeida; Soares, 2022).

A sanção da Lei Geral de Proteção de Dados Pessoais (LGPD) em 2018 foi precedida por um processo extenso de debates, iniciado ainda em 2010 com o anteprojeto elaborado pelo Ministério da Justiça. Ao longo de aproximadamente oito anos, a proposta foi submetida a consultas públicas, especialmente nos anos de 2010 e 2015, recebendo cerca de duas mil contribuições da sociedade civil, especialistas, órgãos do governo e empresas em um processo participativo (Mendes; Doneda, 2018).

A LGPD define os agentes responsáveis pelo uso e tratamento de dados pessoais, classificando-os de acordo com suas funções e responsabilidades. O controlador decide os métodos de coleta, armazenamento e compartilhamento dos dados, o operador realiza o tratamento dos dados em nome do controlador e o titular de dados é a quem os dados se referem.

Sob essa ótica, Danilo Doneda, um dos principais entusiastas e formuladores da LGPD, adverte:

> O tratamento de dados pessoais, em particular por processos automatizados, é, no entanto, uma atividade de risco. Risco que se concretiza na possibilidade de exposição e utilização indevida ou abusiva de dados pessoais, na eventualidade desses dados não serem corretos e representarem erroneamente seu titular, em sua utilização por terceiros sem o conhecimento deste, somente para citar algumas hipóteses reais (Doneda, 2011, p. XX).

O Capítulo I é responsável por estabelecer diretrizes para o funcionamento da regulação jurídica da proteção de dados no Brasil. Nele, encontram-se conceitos que servem de base para toda a aplicação lei. Logo no art. 1º, a lei delimita seu objetivo: proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018). Também é possível encontrar fundamentos que norteiam a interpretação e aplicação da LGPD.

Em seguida, o Capítulo II da referida legislação fala especificamente acerca das circunstâncias em que os dados pessoais podem ser utilizados pelo controlador e operador. É possível verificar:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo

> ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (Brasil, 2018, art. 7º).

Nesse sentido, Laura Mendes, também autora do Anteprojeto da LGPD, destaca:

> Um dos pressupostos fundamentais da LGPD é que o tratamento de dados só poderá ser realizado se existir uma base normativa que o autorize. Somente será legítimo o tratamento que se enquadre em ao menos uma de onze hipóteses, como o consentimento do próprio titular. Para que o consentimento seja considerado válido, ele deve ser livre, informado, inequívoco e com uma finalidade determinada (Mendes, 2019, p. XX).

Convém enfatizar que o titular dos dados pessoais possui o direito de acessar, retificar, excluir e solicitar a portabilidade dos seus dados, que são armazenados pelos controladores. Além disso, a legislação vigente garante que o titular seja informado sobre qualquer compartilhamento realizado com entidades públicas e privadas, assegurando maior transparência com o usuário.

Avançando no tema, um embate doutrinário gira em torno da definição quanto à natureza da responsabilidade civil prevista na Lei Geral de Proteção de Dados Pessoais. Parcela da doutrina indica que a LGPD adota a responsabilidade subjetiva, pois a lei não utiliza expressões como “Independentemente de culpa” ou “independentemente da existência da culpa” (Bessa; Almeida, 2023). Por outro lado, a letra da lei estabelece que, o agente que em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo (Brasil, 2018). Logo, a redação da lei não exige comprovação de culpa, o que indica a adoção da responsabilidade objetiva. Portanto, a interpretação correta é no sentido de que houve adoção do regime da responsabilidade objetiva nos casos que envolvam danos decorrentes do tratamento de dados pessoais no âmbito da LGPD (Bessa; Almeida, 2023).

A Autoridade Nacional de Proteção Dados (ANPD) é o órgão central responsável por regular a Lei Geral de Proteção de Dados. Entre suas atribuições, destaca-se a responsabilidade de editar normas complementares, orientar os agentes de tratamento quanto às melhores práticas, analisar denúncias, aplicar sanções administrativas e promover a cooperação com autoridades internacionais.

Dando continuidade à análise, apresentam-se jurisprudências relevantes que tratam sobre a proteção de dados pessoais dos consumidores, destacando o entendimento dos tribunais quanto aos limites e responsabilidades no tratamento dessas informações. Controle esse que se revelou necessário diante do crescente uso de dispositivos e plataformas digitais pela população brasileira, bem como das recorrentes violações às normas vigentes por parte de grandes empresas responsáveis pelo tratamento de dados.

Um caso emblemático é o Recurso Especial n.º 1.316.921/RJ, em que o

Superior Tribunal de Justiça analisou a responsabilidade do Google pela permanência de conteúdo ofensivo à Xuxa Meneghel na rede social. A relatora do caso, Ministra Nancy Andrighi, votou no sentido de reconhecer a responsabilidade civil do Google após a notificação do conteúdo ilícito, com base na proteção da dignidade da pessoa humana e dos direitos da personalidade:

> CIVIL. CONSTITUCIONAL. INTERNET. GOOGLE. RESPONSABILIDADE CIVIL. PUBLICAÇÃO ANÔNIMA. ORKUT. IMPOSSIBILIDADE DE EXIGÊNCIA PRÉVIA DE CENSURA PELO PROVEDOR. RESPONSABILIDADE APÓS A CIÊNCIA DO CONTEÚDO ILÍCITO. DIGNIDADE DA PESSOA HUMANA. DIREITO À IMAGEM. DANO MORAL CONFIGURADO. CASO CONCRETO. AUSÊNCIA DE COMPROVAÇÃO DA CIÊNCIA INEQUÍVOCA.
> Não se pode permitir que, sob o manto da neutralidade da rede, os provedores de internet se isentem de adotar providências mínimas para impedir a continuidade da ofensa à dignidade da pessoa humana, sobretudo quando são devidamente notificados da existência de conteúdo manifestamente ilícito (STJ, EDcl no REsp 1.316.921, Rel. Min. Nancy Andrighi, 2013).

Outro caso de relevante importância é a Ação Civil Pública ajuizada pelo Ministério Público Federal e pelo Instituto Brasileiro de Defesa do Consumidor (IDEC) em face do WhatsApp e da Autoridade Nacional de Proteção de Dados (ANPD), na qual se discute a legalidade da nova política de privacidade. Os autores alegam que o compartilhamento de dados com outras empresas foi imposto sem o devido consentimento específico:

> DADOS PESSOAIS. PROTEÇÃO À PRIVACIDADE. CONSUMO DIGITAL. APLICAÇÃO DA LGPD. CONSENTIMENTO INFORMADO. VIOLAÇÃO DE DIREITOS FUNDAMENTAIS.
> A nova política de privacidade do WhatsApp obrigou os usuários a aceitarem, de forma imposta e sem possibilidade real de escolha, o compartilhamento de seus dados com outras empresas do Grupo Meta, sob pena de perda do acesso ao serviço. Tal conduta afronta os princípios da autodeterminação informativa, da boa-fé e da transparência, bem como caracteriza prática abusiva nos termos do art. 6º, IV e VI, do CDC e dos arts. 6º, 7º e 8º da LGPD (MPF e IDEC, Ação Civil Pública ajuizada em 30 de janeiro de 2024, Processo nº 5011257-66.2024.4.03.6100 – Justiça Federal de São Paulo).

A seguir, serão apresentadas algumas ações em que a legislação mostrou resultados eficientes, com a atuação do Judiciário e de órgãos responsáveis pela fiscalização. Tais episódios envolvem empresas de grande porte, evidenciando que, apesar dos desafios de fiscalização e aplicação, o ordenamento jurídico brasileiro tem sido capaz de impor sanções relevantes em comportamentos que vão contra o que está previsto na LGPD e nas demais normas.

Uma decisão bastante polêmica foi a suspensão do aplicativo de mensagens Telegram, determinada pelo ministro Alexandre de Moraes, do Supremo Tribunal Federal, no âmbito do Inquérito n.º 4.781/DF. Um dos fundamentos para a medida foi o descumprimento do artigo 10 do Marco Civil da Internet, que exige a existência de um representante legal no país para responder judicialmente por demandas relacionadas ao tratamento de dados. Apesar das polêmicas, a decisão evidenciou aplicabilidade das legislações específicas voltadas à regulação digital no Brasil:

> MEDIDA CAUTELAR. SUSPENSÃO DE APLICATIVO DE MENSAGENS. DESCUMPRIMENTO DE ORDEM JUDICIAL. INOBSERVÂNCIA DO MARCO CIVIL DA INTERNET. AUSÊNCIA DE REPRESENTANTE LEGAL

> NO PAÍS. PROTEÇÃO DE DADOS E RESPONSABILIZAÇÃO. DECISÃO MANTIDA.
> A plataforma TELEGRAM, em todas essas oportunidades, deixou de atender ao comando judicial, em total desprezo à JUSTIÇA BRASILEIRA.
> O desrespeito à legislação brasileira e o reiterado descumprimento de inúmeras decisões judiciais pelo TELEGRAM, – empresa que opera no território brasileiro, sem indicar seu representante – inclusive emanadas do SUPREMO TRIBUNAL FEDERAL – é circunstância completamente incompatível com a ordem constitucional vigente, além de contrariar expressamente dispositivo legal (art. 10, § 1º, da Lei 12.965/14). (STF, PET 9935/DF, Rel. Min. Alexandre de Moraes, decisão monocrática, DJe 18/03/2022).

Para finalizar, o desembargador Sandoval Oliveira, do Tribunal de Justiça do Distrito Federal e Territórios, manteve os termos da sentença de primeiro grau que determinou à empresa Serasa S.A. a interrupção da comercialização de dados pessoais por meio dos serviços “Lista Online” e “Prospecção de Clientes”. A decisão teve como fundamento a violação das normas previstas na Lei Geral de Proteção de Dados Pessoais:

> APELAÇÃO. AÇÃO CIVIL PÚBLICA. PRELIMINAR DE NEGATIVA DE PRESTAÇÃO JURISDICIONAL. REJEITADA. COMERCIALIZAÇÃO DE PRODUTOS E FERRAMENTAS DE TRATAMENTO DE DADOS PESSOAIS. PROTEÇÃO DOS DIREITOS DO CONSUMIDOR. INOBSERVÂNCIA DA LEGISLAÇÃO DE REGÊNCIA.
> O consumidor precisa ter a exata noção acerca de quais dados pessoais foram utilizados no tratamento, como foram coletados, a forma de processamento e qual a política de compartilhamento, especialmente porque elementos socioeconômicos e comportamentais estão intrinsecamente vinculados à esfera da privacidade e, como tal, reclamam proteção (art. 2º, inciso I, Lei nº 13.709/2018). Não são elementos ou comportamentos plenamente acessíveis ao público ou suscetíveis de serem conhecidos por todos, em absoluto. (TJDFT, Apelação Cível nº 0736634-81.2020.8.07.0001, Rel. Des. Sandoval Oliveira, Acórdão nº 1397176).

Com base em tudo o que foi exposto, é possível perceber que o Brasil conta com um conjunto importante de leis voltadas à proteção dos dados e direitos dos consumidores. Essas normas representam um avanço relevante, especialmente diante das transformações trazidas pela era digital. Apesar dos avanços, ainda existem muitos desafios, pois a aplicação das leis nem sempre funciona como deveria, seja por falhas na fiscalização, demora nos processos ou dificuldade em acompanhar o ritmo acelerado das inovações tecnológicas.

## 5 CONSIDERAÇÕES FINAIS

Diante do exposto, é possível afirmar que o ordenamento jurídico brasileiro conta com diversas normas que convergem para um objetivo comum: a proteção do usuário no ambiente digital. Essas legislações asseguram direitos constitucionais fundamentais, como a intimidade, a vida privada, a honra e a imagem. Ademais, é responsabilidade do Estado assegurar uma navegação segura na internet, preservando não apenas a privacidade, mas também a integridade dos dados pessoais dos consumidores.

A Constituição Federal, o Código de Defesa do Consumidor, a Lei de

Interceptações Telefônicas, o Marco Civil da Internet e a Lei Geral de Proteção de Dados são exemplos de legislações que asseguram o bem-estar digital dos consumidores, fiscalizando as relações consumeristas para evitar irregularidades das plataformas de e-commerce.

A efetividade das normas depende, também da compreensão dos cidadãos sobre seus direitos, o que ainda é insuficiente no Brasil, seja pela ausência de políticas públicas educativas voltadas a proteção de dados, seja pela complexidade técnica do tema, que dificulta o exercício consciente dos direitos normatizados pela legislação vigente.

Conclui-se igualmente que a promulgação tardia das leis que protegem os direitos dos consumidores no cyberspace também pode ser um fator crucial para o aumento da vulnerabilidade dos usuários em ambientes digitais. Isso é especialmente relevante quando se observa que a primeira legislação específica sobre o tema, o Marco Civil da Internet, foi sancionada apenas em 2014, e a Lei Geral de Proteção de Dados, foi sancionada somente em 2018.

Ainda assim, o mercado continua a utilizar diversos mecanismos e estratégias, sejam elas lícitas ou não, com o propósito de coletar os dados e informações dos consumidores para fins de rastrear suas preferências de consumo. A análise comportamental, direcionamento de publicidade e aumento das vendas é um ciclo cada vez mais presente nas políticas das empresas.

Cabe ao Direito estabelecer os limites para a utilização de dados pessoais, especialmente quando esse uso visa apenas ao aumento do lucro das grandes corporações, sem o devido respeito à privacidade dos consumidores. Essa regulação é essencial para assegurar o equilíbrio entre inovação tecnológica e a proteção dos direitos fundamentais.

## REFERÊNCIAS

ALMEIDA, Silvia do Carmo Dias de; SOARES, Túlio Augusto. Os impactos da lei geral de proteção de dados - LGPD no cenário digital. **Perspectivas em Ciência da Informação**, v. 27, n. 3, p. 26-45, 2022. Disponível em: https://www.scielo.br/j/pci/a/tb9czy3W9RtzgbWWxHTXkCc/#ModalHowcite. Acesso em: 16 nov. 2024.

BANDEIRA, Camila. **A tecnologia beacon e como estes dispositivos podem facilitar a vida dos clientes**. Trabalho de Conclusão de Curso (Pós-graduação em Marketing Digital) Centro Universitário de Brasília, Instituto CEUB de Pesquisa e Desenvolvimento – ICPD, Brasília, 2018. Disponível em: https://repositorio.uniceub.br/jspui/bitstream/235/12287/1/51400146.pdf. Acesso em: 1 nov. de 2024.

BARRETO, Fabíola Gonçalves; HENRIQUE, Fabricio Gustavo. Lei geral de proteção de dados e a aplicabilidade na anonimização. **IV Workshop de Tecnologia da Fatec Ribeirão Preto**, v. 1, n. 4, dez. 2021. Disponível em: http://www.fatecrp.edu.br/WorkTec/edicoes/2021-2/trabalhos/IV-Worktec-LEI_GERAL_DE_PROTEC%CC%A7A%CC%83O_DE_DADOS_E_A_APLICABILIDADE_NA_ANONIMIZAC%CC%A7A%CC%83O.pdf. Acesso em: 22 out. 2024.

BAUMAN, Zygmunt. **Modernidade Líquida**. Rio de Janeiro: Zahar, 2001.

BESSA, Leonardo Roscoe; ALMEIDA, Mário Henrique Silveira de. A vulnerabilidade do titular de dados e a responsabilidade civil na lei geral de proteção de dados – LGPD. **Civilistica**, Rio de Janeiro, v. 12, n. 2, p. 1–23, 2023. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/926. Acesso em: 22 abr. 2025.

BRASIL. Constituição Federal. **Constituição da República Federativa do Brasil de 1988**. Diário Oficial da União: Brasília, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 14 out. 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União: Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 3 maio 2025.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União: Brasília, DF, 12 set. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 3 maio 2025.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Regula a interceptação de comunicações telefônicas e outras providências. Diário Oficial da União: seção 1, Brasília, DF, 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 3 maio 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União:* Brasília, DF, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 3 maio 2025.

BRASIL. **Lei nº 14.553, de 20 de abril de 2023**. Altera os arts. 39 e 49 da Lei nº 12.288, de 20 de julho de 2010 (Estatuto da Igualdade Racial), para determinar procedimentos e critérios de coleta de informações relativas à distribuição dos segmentos étnicos e raciais no mercado de trabalho. Diário Oficial da União, Brasília, DF, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/l14553.htm. Acesso em: 3 maio 2025.

BRASIL. Ministério da Saúde. **Portaria GM/MS nº 1.768, de 30 de julho de 2021**. Altera o Anexo XLII da Portaria de Consolidação GM/MS nº 2, de 28 de setembro de 2017, para dispor sobre a Política Nacional de Informação e Informática em Saúde (PNIIS). *Diário Oficial da União,* Brasília, DF, 2021. Disponível em: https://bvsms.saude.gov.br/bvs/saudelegis/gm/2021/prt1768_02_08_2021.html. Acesso em: 3 maio 2025.

BRASIL. Ministério dos Transportes. Perguntas e respostas sob aspectos da LGPD. **Gov.br**, 2022. Disponível em: https://www.gov.br/transportes/pt-

br/ouvidoria/perguntas-e-respostas-sob-aspectos-da-lgpd#R2.2. Acesso em: 2 maio 2025.

BRASIL. Ministério Público Federal. Ação civil pública proposta pelo MPF e IDEC contra WhatsApp e ANPD. **Portal do Ministério Público Federal, 2024.** Disponível em: https://www.mpf.mp.br/sp/sala-de-imprensa/noticias-sp/docs/2024-acp-mpf-e-idec-x- whatsapp-e-anpd.pdf. Acesso em: 24 abril 2025

BRASIL. Superior Tribunal de Justiça. **Embargos de Declaração no Recurso Especial nº 1.316.921**. Relatora: Ministra Nancy Andrighi. 2013. Disponível em: https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ATC?seq=28224920&tipo=51&nr. Acesso em: 3 maio 2025.

BRASIL. Supremo Tribunal Federal. **Petição nº 9935/DF**. Relator: Ministro Alexandre de Moraes. Decisão monocrática. 2022. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/DespachoTelegram1.pdf. Acesso em: 6 maio 2025.

BRASIL. Tribunal de Justiça do Distrito Federal e dos Territórios. **Apelação Cível nº 0736634-81.2020.8.07.0001.** Relator: Desembargador Sandoval Oliveira. Acórdão nº 1397176. 2022. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/noticias/2021/julho/lgpd-justica-determina-que-serasa-deixe-de-comercializar-dados-pessoais. Acesso em: 6 maio 2025.

CARVALHO, Patrícia Heloisa de. O “Marco Civil da Internet”: uma análise sobre a constitucionalidade do artigo 19. **Revista da Faculdade de Direito do Sul de Minas**, Pouso Alegre, v. 33, n. 2, p. 228-244, 2017. Disponível em: https://www.fdsm.edu.br/adm/artigos/6917c36392274c9b6393c7f7a7bddbd1.pdf. Acesso em: 12 novembro 2024.

COSTA, Inês da Silva. A proteção da pessoa na era dos big data: a opacidade do algoritmo e as decisões automatizadas. **Revista Electrónica de Direito**, Porto, Portugal, v. 24, n. 1, fev. 2021. Disponível em: https://cij.up.pt/pt/red/edicoes-anteriores/2021-nordm-1/a-protecao-da-pessoa-na- era-dos-big-data-a-opacidade-do-algoritmo-e-as-decisoes-automatizadas/. Acesso em: 11 out. 2024.

COSTA, Vitor. **Cookies e a violação de direitos fundamentais no meio digital**. Centro Universitário Antônio Eufrásio de Toledo, v. 18, n. 18, 2022. Disponível em: http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/viewFile/9480/67651367. Acesso em: 11 out. de 2024.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. espaço jurídico: **Journal of Law**, [s.l.], v. 12, n. 2, p. 91-108, 2011. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=4555153. Acesso em: 22 abr. 2025.

FERREIRA, Juliano Rodrigues; *et al*. Mitigação dos riscos à privacidade através da anonimização de dados. **Revista Ibérica de Sistemas e Tecnologias de Informação**, 2022. Disponível em: https://www.researchgate.net/publication/363107109_Mitigacao_dos_Riscos_a_Priva

cidade_atraves_da_Anonimizacao_de_Dados. Acesso em: 09 out. 2025.

FIGUEIREDO, Virna de Barros Nunes; VARELLA, Marcelo Dias. Dimensões da privacidade das informações em saúde no Brasil. **Revista Brasileira de Direitos Fundamentais & Justiça**, v. 17, n. 47, 2023.Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/1203. Acesso em: 09 out. 2024.

HOBSBAWM, Eric. **Da revolução inglesa ao imperialismo**. Rio de Janeiro: Forense Universitária, 2000.

LEARTE, Bruno Emanuel Setubal; ROCHA, Walerya Reis da Silva. Proteção de dados pessoais como direito fundamental no Brasil: aspectos e reflexos da Emenda Constitucional 115/2022. **Migalhas**, 2024. Disponível em: https://www.migalhas.com.br/depeso/400183/protecao-de-dados-pessoais-como-direito-fundamental-no-brasil. Acesso em: 03 jun. 2025.

MAIA, Tiago Dias; PAULINO, Galtiênio da Cruz. A quebra de sigilo de dados baseada em coordenadas geográficas e o princípio da proporcionalidade. **Escola Superior do Ministério Público da União**, [S.L.], 2020. Disponível em: https://escola.mpu.mp.br/publicacoesepesquisas/nao-periodicos/obras-avulsas/e-books-esmpu/direitos-fundamentais-em-processo-2013-estudos-em-comemoracao-aos-20-anos-da-escola-superior-do-ministerio-publico-da-uniao/44_a-quebra-de-sigilo-de-dados.pdf. Acesso em: 1 nov. de 2024.

MATOS, Adriana Lima de. **A legitimidade da recolha e processamento de dados relativos à raça e à origem étnica**: impactos na esfera privada dos indivíduos e no combate à discriminação. Dissertação (Mestrado em Ciências Jurídico-Políticas) Universidade do Porto, Porto, 2019.

MENDES, Laura Schertel; DONEDA, Danilo. 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**, São Paulo, v. 120, p. 555–587, nov./dez., 2018. Disponível em: https://d1wqtxts1xzle7.cloudfront.net/62959269/2018_Comentario_-_Laura_Mendes_-_RDC_120_220200414-30823-utejkp-libre.pdf. Acesso em: 22 abr. 2025.

MENDES, Laura Schertel. Privacidade e dados pessoais. proteção de dados pessoais: fundamento, conceitos e modelo de aplicação. **Panorama Setorial da Internet**, 2019. Disponível em: https://cetic.br/media/docs/publicacoes/6/15122520190717-panorama_setorial_ano-xi_n_2_privacidade_e_dados_pessoais.pdf. Acesso em: 23 abr. 2025.

PAIVA, Eduarda Beutinger. **A reversibilidade do processo de anonimização e as suas repercussões no regime de proteção de datos pessoais**. 2021. 87 f. Monografia (Graduação em Direito). Faculdade de Direito – Universidade Federal do Rio Grande do Sul, Porto Alegre, 2021. Disponível em: https://lume.ufrgs.br/handle/10183/236499. Acesso em: 10 out. 2025.

PINTO, Alexandre Guimarães Gavião. Direitos fundamentais: legítimas prerrogativas

de liberdade, igualdade e dignidade. **Revista da EMERJ**, v. 12, n. 46, 2009. Disponível em: https://www.emerj.tjrj.jus.br/revistaemerj_online/edicoes/revista46/Revista46_126.pdf . Acesso em: 11 novembro de 2024.

PRETTO, Ana Lucia. Jurisdição constitucional na Constituição Federal de 1988: entre ativismo e auto-contenção. **Revista Direitos Fundamentais & Democracia**, [S. l.], v. 2, n. 2, 2007. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/108. Acesso em: 11 novembro de 2024.

RESENDE, Mariana Junqueira Bezerra. **Cidadania na sociedade da informação**: a internet como instrumento para efetivação de direitos fundamentais. Dissertação (Mestrado em Direito) – Universidade de Ribeirão Preto, Ribeirão Preto, 2016.

ROCHA, Bruno Augusto Barros; LIMA, Fernando Rister de Sousa; WALDMAN, Ricardo Libel. Mudanças no papel do indivíduo pós- revolução industrial e o mercado de trabalho na sociedade da informação. **Revista Pensamento Jurídico**, São Paulo, Brasil, v. 14, n. 1, 2020. Disponível em: https://ojs.unialfa.com.br/index.php/pensamentojuridico/article/view/419. Acesso em: 10 out. 2024.

SANTANA, John Kennedy Ribeiro de; *et al*. Precisão de GPS em smartphones: uma ferramenta para pesquisas acadêmicas e trabalhos de campo. **Revista de Geografia - PPGEO - UFJF**, [S.L.], v. 9, n. 2, p. 255-267, 2020. Disponível em: https://periodicos.ufjf.br/index.php/geografia/article/view/30154/20362. Acesso em: 14 out. de 2024.

SANTOS, Milton. A revolução tecnológica e o território: realidades e perspectivas. **Caderno Prudentino de Geografia**, [S. l.], v. 1, n. 27, p. 83–94, 2020. Disponível em: https://revista.fct.unesp.br/index.php/cpg/article/view/7378. Acesso em: 10 out. 2024.

ZUFFO, Milena Maltese. A LGPD e o tratamento de dados de fiéis religiosos. **Law Innovation**, 2021. Disponível em: https://lawinnovation.com.br/a-lgpd-e-o-tratamento-de-dados-de-fieis-religiosos/. Acesso em: 07 out. 2024.

## AGRADECIMENTOS

Agradeço a Deus, por Sua presença constante em minha vida, pelo cuidado, proteção e discernimento concedidos ao longo desta jornada.

Aos meus pais, Marcelo e Eunaliana, agradeço por todo amor, incentivo e por serem meu alicerce em todas as fases da vida.

Aos meus irmãos, Marcelo Filho e Liana, agradeço por me darem suporte contínuo.

À minha namorada, Raissa, sou grato pelo carinho, compreensão e presença constante ao meu lado.

À minha orientadora, Crizeuda Farias, expresso minha sincera gratidão pela

orientação dedicada, pelos ensinamentos transmitidos e pelo apoio essencial durante todo o desenvolvimento deste trabalho.