REVISTA

DOI: 10.56119/rcabdc.v7.105

V.7, 2026, ISSN 2318-602X
p.39-59
https://abdc.emnuvens.com.br/abdc

ARTIGO

A ilusão da privacidade a eficácia a LGPD na era da hipervigilância digital

The illusion of privacy: the effectiveness of the LGPD in the era of digital hyper-surveillance

Kayke Guimarães Salviano de Oliveira
Orcid: 0009-0009-5239-4500

Resumo

Este tema é cada vez mais conhecido e estudado por estudantes de Direito. A escolha do assunto surgiu de um número crescente de questionamentos e comparações entre a legislação vigente e a realidade da aplicação das normas. Temos a LGPD (Lei Geral de Proteção de Dados); no entanto, ela enfrenta limitações quanto à sua implementação efetiva. Muitas vezes, os cidadãos não se dão conta de que empresas e sites coletam e compartilham dados com terceiros, o que resulta na disseminação de informações. A LGPD realmente protege o público ou serve apenas como uma barreira superficial e inadequada diante da complexidade do problema?

Palavras-chave: LGPD; Privacidade; Proteção de dados; Hipervigilância digital

CC BY

Abstract

This topic is becoming increasingly well-known and studied by law students. The choice of this subject stemmed from a growing number of questions and comparisons between established law and the reality of how regulations are applied. We have the LGPD (General Data Protection Law); however, it faces limitations regarding its effective implementation. Citizens often fail to realize that companies and websites collect and share their data with third parties, leading to the widespread dissemination of personal and sensitive information. Does the LGPD truly protect the public, or does it merely serve as a superficial and inadequate barrier in the face of the problem's complexity?

Keywords: LGPD; Privacy; Data protection; Digital hyper-surveillance; Consent.

Introdução

Com o avanço constante da tecnologia e a ampliação do uso da internet nas atividades cotidianas, a circulação de dados pessoais tornou-se cada vez mais intensa. Informações como nome, localização, hábitos de consumo, preferências e até dados considerados sensíveis passaram a ser coletados por empresas, aplicativos e plataformas digitais de maneira contínua, muitas vezes sem que os próprios usuários tenham plena consciência disso. Nesse cenário, o Direito Digital ganha destaque como uma área contemporânea do Direito, voltada à regulamentação das relações no ambiente virtual e à proteção dos direitos fundamentais diante das transformações tecnológicas.

A escolha do presente tema surgiu a partir da observação da realidade atual e dos inúmeros questionamentos relacionados à efetividade da proteção de dados no Brasil. Embora exista a Lei Geral de Proteção de Dados Pessoais, criada com o objetivo de assegurar maior segurança e privacidade aos cidadãos, ainda é possível perceber diversas falhas quanto à sua aplicação prática e fiscalização. Muitas empresas

realizam a coleta e o compartilhamento de informações pessoais de forma ampla, enquanto grande parte da população sequer compreende a dimensão da utilização de seus próprios dados no ambiente digital.

Além disso, o aumento expressivo de golpes virtuais e vazamentos de informações demonstra que os dados pessoais têm se tornado um dos principais alvos de práticas ilícitas. Neste contexto, Bioni (2021) destaca que a proteção de dados pessoais busca reduzir os riscos decorrentes do tratamento massivo de informações, preservando a autodeterminação informativa do titular. Em muitos casos, os indivíduos somente percebem a exposição de suas informações após sofrerem prejuízos financeiros ou terem sua privacidade violada.

Surgem, então, importantes questionamentos: o Estado tem conseguido cumprir seu dever constitucional de garantir o direito à privacidade? A legislação atual acompanha, de fato, a velocidade da evolução tecnológica? E, principalmente, a LGPD possui efetividade suficiente para garantir a proteção dos dados pessoais na atual sociedade marcada pela hipervigilância digital?

Partem-se da hipótese de que a LGPD representa um grande avanço na titularidade dos dados pessoais. No entanto, possui limitações efetivas diante de modelos econômicos de plataformas digitais e da coleta massiva de informações. A relevância desta pesquisa está justamente na necessidade de aprofundar a discussão sobre a proteção de dados pessoais e os limites da atuação estatal frente aos desafios tecnológicos atuais. Trata-se de um tema cada vez mais presente na vida da sociedade, mas que ainda necessita de maior debate acadêmico, especialmente no campo jurídico.

Assim, um dos principais objetivos é analisar a efetividade da LGPD e compreender até que ponto a legislação brasileira consegue assegurar, na prática, a proteção dos dados pessoais e do direito fundamental à privacidade.

1. Surgimento e ampliação da LGPD

A Lei Geral de Proteção de Dados foi sancionada em 2018, mas entrou em vigor em 2020. Trata-se de uma legislação relativamente "nova", porém considerada um marco muito importante para o ramo do Direito.

Com a expansão contínua das tecnologias da informação, tornam-se cada vez mais frequentes os casos de vazamento de dados e de utilização indevida de informações pessoais, evidenciando a necessidade de mecanismos jurídicos capazes de garantir a privacidade e a segurança dos titulares.

O desenvolvimento das tecnologias digitais transformou os dados pessoais em um ativo econômico estratégico para empresas e organizações, tornando necessária a criação de instrumentos normativos destinados a limitar o tratamento indiscriminado dessas informações (Doneda, 2019).

Nesse cenário, foi promulgada a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), com o objetivo de estabelecer princípios, direitos e deveres relacionados ao tratamento de dados pessoais, buscando assegurar maior proteção à privacidade e à autodeterminação informativa dos titulares.

O avanço das tecnologias da informação e a intensificação do tratamento de dados pessoais no ambiente digital evidenciaram a necessidade de uma tutela jurídica mais robusta, culminando no reconhecimento da proteção de dados pessoais como direito fundamental, por meio da Emenda Constitucional nº 115/2022, que inseriu o inciso LXXIX no art. 5º da Constituição Federal, assegurando, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

Por outro lado, a LGPD também tem gerado grandes questionamentos na sociedade, especialmente quanto à sua efetividade diante das grandes empresas que realizam o tratamento de dados pessoais. Assim, questiona-se até que ponto os cidadãos estariam realmente protegidos. Portanto, a LGPD surgiu da necessidade de garantir maior proteção aos cidadãos brasileiros, independentemente das limitações territo-

riais, seguindo os princípios estabelecidos pela Constituição Federal, que dispõe o seguinte: "São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação" (Art. 5º, X, da CF).

A Lei Geral de Proteção de Dados (LGPD) é necessária para compreender que essa legislação tem como principal objetivo limitar o acesso irrestrito de empresas e instituições públicas aos dados de pessoas físicas.

A LGPD sofreu grande influência do GDPR (General Data Protection Regulation ou, em português, RGPD – Regulamento Geral sobre a Proteção de Dados), que é originário da Europa e foi criado antes da lei de dados brasileira; entretanto, as duas criações foram bem próximas.

Sob esta ótica, a LGPD adotou estrutura semelhante à do GDPR, com adaptações à realidade brasileira, pois ela se aplica a qualquer pessoa jurídica ou física, pública ou privada, independente do país ou da sede; por outro lado, o GDPR aplica-se exclusivamente a pessoas vinculadas ao mercado europeu.

A criação da Lei Geral de Proteção de Dados representou uma importante resposta do ordenamento jurídico brasileiro às transformações promovidas pela sociedade digital. Ao estabelecer normas para o tratamento de dados pessoais e assegurar direitos aos seus titulares, a legislação buscou equilibrar o avanço tecnológico com a proteção da privacidade e da dignidade da pessoa humana.

Apesar de representar um significativo avanço legislativo, a efetividade da LGPD ainda enfrenta desafios decorrentes da constante evolução tecnológica e da crescente exploração econômica dos dados pessoais.

2.Dados pessoais

Inicialmente, cabe definir o que se entende por dado pessoal. De forma simplificada, dados pessoais são quaisquer informações relacionadas a uma pessoa natural

identificada ou identificável. Conforme definido pelo artigo da LGPD: "Para os fins desta Lei, considera-se: dado pessoal: informação relacionada a pessoa natural identificada ou identificável" (Art. 5º, inciso I, da LGPD).

A identificabilidade refere-se à possibilidade de reconhecimento do titular por meios indiretos, como o cruzamento de bancos de dados, no qual informações aparentemente isoladas, quando combinadas por algoritmos ou ferramentas de busca, permitem a identificação precisa do indivíduo. Conforme Danilo Doneda, a proteção de dados pessoais está diretamente ligada ao controle do indivíduo sobre suas próprias informações, especialmente diante da ampliação dos mecanismos tecnológicos de coleta e tratamento de dados (Doneda, 2019, p. 35).

Nesse caso, a Lei Geral de Proteção de Dados (LGPD) busca regular o tratamento dessas informações, estabelecendo limites e diretrizes para reduzir os riscos inerentes à exposição de dados. Todavia, na era da hiperconectividade, em que o fluxo informacional é intenso e contínuo, questiona-se a real eficácia dessa proteção, uma vez que qualquer indivíduo conectado pode ter seus dados coletados, correlacionados e potencialmente manipulados. Conforme Duque e Araujo (2020), os indivíduos produzem continuamente uma grande quantidade de dados pessoais, tanto em ambientes físicos quanto virtuais, e a exposição irresponsável ou o tratamento inadequado dessas informações pode resultar em incidentes de segurança e graves ilícitos cibernéticos.

Assim, o tratamento massivo e o cruzamento de dados pessoais evidenciam a violação do princípio da transparência, previsto no art. 6º, VI, da LGPD, pois o titular frequentemente não possui informações claras, precisas e acessíveis sobre a forma como seus dados são coletados, utilizados e compartilhados por terceiros.

2.1 Classificação dos dados pessoais

Costuma-se pensar em dados apenas como informações numéricas ou pessoais; contudo, os dados abrangem uma lógica muito mais ampla, pois são quaisquer ele-

mentos que possuem uma informação atribuída a algo, levando em consideração desde a cor de um objeto ou a sua quantidade até mesmo um apelido que lhe seja atribuído em uma roda de amigos.

Todavia, dentro da ideia de dados, ocorre uma classificação. O primeiro tipo, e o mais comum de ser ouvido em empresas e em grupos sociais, são os dados sensíveis, que consistem em informações sobre etnia, visão política, vida sexual e impressões digitais, revelando características profundas dos titulares.

Os dados sensíveis são frequentemente confundidos com os dados pessoais, que englobam o CPF, endereço, IP e e-mail. Também possuímos os dados anonimizados, que são aqueles que passam por um processo de dessocialização direta ou indireta do seu titular; nesses casos, não se aplica a LGPD, a menos que esse processo seja revertido.

2.2 Tratamento dos dados pessoais e seus riscos

Trazendo essa problemática para a atualidade, percebe-se que os indivíduos compartilham seus dados pessoais de maneira contínua no ambiente digital, seja por meio de redes sociais, formulários eletrônicos ou das próprias interações cotidianas realizadas na internet. Essa superexposição informacional contribui para a disseminação massiva de dados, ampliando a vulnerabilidade dos usuários diante de práticas fraudulentas e mecanismos de vigilância digital.

A concentração de informações nas mãos de grandes plataformas e agentes econômicos possibilita não apenas a exploração comercial dos dados, mas também a potencial influência sobre comportamentos sociais, culturais e políticos. Nesse contexto, Byung-Chul Han destaca que **"**cada clique, cada busca e cada comunicação alimentam um sistema de vigilância digital" (Han, 2018, p. 17), demonstrando como a constante exposição de informações pessoais fortalece mecanismos de monitoramento e influência social.

Dentro desse panorama, infelizmente toda essa situação contribui para o alarmante cenário de crimes cibernéticos. Segundo levantamento realizado pela Serasa Experian, 51% dos brasileiros foram vítimas de algum tipo de fraude no último ano,

sendo que 54,2% dessas vítimas sofreram perdas financeiros (o correto é financeiras). Diante desse cenário, torna-se necessário discutir de que maneira é possível reduzir o avanço dessas práticas. Portanto, onde se encontram os órgãos responsáveis pela proteção dos dados? Até que ponto, de fato, nossos dados estão protegidos? Se é que de fato estamos protegidos.

A LGPD não protege apenas os dados "parados" ou "armazenados"; ela se estende a todo o tratamento de dados, que inclui desde a coleta até o armazenamento e o compartilhamento, processo também conhecido como o "Ciclo de Vida do Dado".

Qualquer operação realizada com dados pessoais — como acesso, utilização, processamento, transmissão ou eliminação — está sujeita às disposições da lei, exigindo que as organizações adotem medidas de segurança, transparência e finalidade adequada em todas as etapas, garantindo a proteção contínua das informações do titular. Com base no art. 5º, X, da LGPD:

> tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

2.3 Responsabilidade jurídica e fiscalização

No desenvolvimento desse tratamento, destacam-se etapas centrais que evidenciam riscos específicos. A coleta de dados, por exemplo, pode ocorrer de forma excessiva, em violação ao princípio da necessidade. O compartilhamento, por sua vez, envolve o risco de utilização indevida por terceiros mal-intencionados. Já o armazenamento mostra-se atualmente especialmente sensível diante da recorrência de vazamentos de dados, frequentemente explorados para práticas ilícitas e estratégias de manipulação no contexto comercial.

As consequências jurídicas que decorrem do vazamento de dados podem obrigar o controlador ou operador a indenizar o titular pelo dano sofrido. A LGPD estabelece,

no art. 42, que o controlador ou o operador que causar dano patrimonial, moral, individual ou coletivo em razão do tratamento de dados de maneira irregular responderá por ele. Também se estende às sanções administrativas aplicadas pela ANPD, como, por exemplo, multas simples de até 2% do faturamento da empresa, limitadas a R$ 50 milhões por infração, previstas no art. 52 da LGPD.

Em suma, a eliminação dos dados configura-se como a etapa final do ciclo de vida do dado, tendo por finalidade evitar a retenção desnecessária de informações e, consequentemente, reduzir os riscos associados a incidentes de segurança.

Tal procedimento encontra fundamento na Lei Geral de Proteção de Dados, que estabelece o término do tratamento e disciplina as hipóteses de eliminação ou conservação dos dados pessoais, observados os princípios da necessidade e da finalidade (arts. 6º, III, 15 e 16 da Lei nº 13.709/2018).

Nesse quadro, compete à Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública responsável por zelar pela proteção de dados pessoais, fiscalizar, regulamentar e assegurar o cumprimento da Lei Geral de Proteção de Dados.

A atuação da ANPD mostra-se essencial para a efetividade da legislação, na medida em que lhe incumbe orientar os agentes de tratamento, aplicar sanções administrativas e promover a cultura de proteção de dados no país.

Nesse sentido, Bruno Bioni sustenta que a efetividade da proteção de dados depende não apenas da existência de normas jurídicas, mas também da atuação institucional dos órgãos responsáveis por sua fiscalização e concretização (BIONI, 2024).

No entanto, a LGPD apresenta importantes mecanismos normativos, encontrando-se, contudo, parcialmente efetiva, pois, para que se complete de maneira sólida, é necessário que a sua aplicabilidade caminhe junto com aquilo que é apresentado em sua teoria. Conforme Assis e Diniz (2025), a existência de regulamentação formal não é, por si só, suficiente para garantir uma proteção efetiva, uma vez que falhas na execução das medidas previstas podem comprometer a salvaguarda dos direitos dos titulares.

2.4 Comercialização dos dados pessoais

Um dos principais tópicos dentro deste artigo é a comercialização de dados dos usuários entre empresas que detêm o monopólio de desenvolvimentos lucrativos. Na visão geral dessas empresas, não há interesse em dados "brutos"; o real objetivo é o que se pode produzir com a manipulação dessas informações.

Conforme destaca Lanier (2018): "As empresas de tecnologia não comercializam apenas serviços, mas utilizam os dados dos usuários como matéria-prima para a construção de modelos de negócios altamente lucrativos." A partir do momento em que o cidadão adentra as redes de comunicação, existem comunidades e camadas específicas de ideias padronizadas, regras ou incentivos que o fazem permanecer dentro dos sites.

É exatamente nesse momento que as empresas atuam: esses dados são transformados em insights estratégicos (compreensões aprofundadas baseadas em dados) que revelam os padrões comportamentais de determinadas comunidades ou indivíduos, descobrindo oportunidades ocultas e transformando "números" em direção para negócios, orientando decisões e incentivando determinadas compras com base em emoções e pesquisas recentes.

"Os dados pessoais tornaram-se um ativo econômico de grande valor, sendo coletados, processados e comercializados por plataformas digitais para fins de publicidade e previsão comportamental." (ZUBOFF, 2020).

De certa forma, essa estratégia possui seus benefícios, pois pode, consequentemente, desestimular comportamentos ou ideias de cunho infracional. Porém, majoritariamente, não é isso que de fato acontece. Esses dados são obtidos e vendidos de maneiras que direcionam e selecionam os maiores compradores em "potencial", muitas vezes sem que os usuários percebam que determinadas empresas e instituições se beneficiam dessas informações, utilizando-as para criar e personalizar anúncios direcionados aos interesses e ao comportamento de cada indivíduo.

Um exemplo prático é o de um cidadão que pretende começar a praticar exercícios e faz uma pesquisa por "academias de ginástica" ou "roupas para prática de exercício"; ao acessar outro site de pesquisa, serão apresentados a ele anúncios de suplementos para melhorar sua performance na academia.

Conforme observa Pariser (2012), os algoritmos de personalização tendem a criar "bolhas de filtros", nas quais os indivíduos passam a receber predominantemente conteúdos compatíveis com seus interesses e crenças anteriores, reduzindo o contato com perspectivas divergentes.

A partir dessa premissa, todos os que possuem ponto de acesso à internet por aparelhos de comunicação móveis estão à mercê do vazamento e da manipulação de seus dados sensíveis, pois a todo momento estamos "conectados" a outras pessoas e empresas, compartilhando nossas informações por meio de dados.

3. Impactos e desafios da efetividade da Lei Geral de Proteção De Dados

A Lei Geral de Proteção de Dados apresenta-se como um elemento transversal de proteção ao direito à privacidade no meio digital, atribuindo deveres ao Estado e aos agentes que realizam o tratamento de dados pessoais.

Contudo, na atual realidade de hipervigilância digital, sua eficácia enfrenta limites, o que contribui para a sensação de uma privacidade apenas superficial. Conforme argumenta Stefano Rodotà, "a proteção de dados tornou-se uma das questões centrais da liberdade na sociedade contemporânea" (Rodotá, 2008, p. 15).

A intensa concentração de dados por empresas e por plataformas governamentais reforça esse cenário, pois, embora existam normas voltadas à proteção do titular, o tratamento massivo de informações ocorre de forma contínua. Nesse contexto, os crimes cibernéticos evidenciam a fragilidade da proteção prometida, uma vez que dados sensíveis permanecem suscetíveis a acessos indevidos e fraudes.

Um grande exemplo seria a fraude envolvendo o INEP em 2024, que ilustra essa realidade. Apesar da existência de mecanismos legais de proteção, aproximadamente 35 mil candidatos tiveram seus dados comprometidos, com prejuízo estimado em 3 milhões de reais (Couto; Maia, 2025).

O episódio demonstra que, mesmo sob a vigência da LGPD, a garantia da privacidade nem sempre se concretiza de forma efetiva. O caso evidencia que a existência formal de mecanismos de proteção não impede, por si só, a exposição massiva de dados, reforçando a percepção de que a privacidade, embora juridicamente assegurada, mostra-se vulnerável na prática.

Em um ambiente marcado pela ampla circulação de informações em plataformas digitais, como WhatsApp e Facebook, percebe-se que a proteção de dados enfrenta desafios práticos. Assim, a LGPD, embora represente um avanço normativo relevante, mostra-se limitada diante da dinâmica de vigilância constante, reforçando a ideia de que a privacidade, na era digital, pode assumir contornos mais ilusórios do que reais.

3.1 A assimetria informacional como obstáculo a efetividade da LGPD

Destaca-se que, a partir do momento em que o indivíduo não tem conhecimento de que seus dados pessoais estão sendo tratados por terceiros ou circulando de forma difusa em ambientes digitais, torna-se significativamente comprometida a efetivação da tutela jurídica prevista na Lei Geral de Proteção de Dados, em desacordo com o disposto no art. 6º, VI, da Lei nº 13.709/2018, que estabelece a "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento".

A ausência de ciência sobre a violação dificulta a adoção de medidas pelo titular, reduzindo a incidência de denúncias e, consequentemente, a atuação repressiva e corretiva dos mecanismos de responsabilização, o que evidencia um dos principais desafios à eficácia da LGPD na era da hipervigilância digital. Segundo Toniazzo

(2022, p. 67), o ambiente digital dificulta significativamente a manifestação voluntária de vontade, especialmente em razão do cenário de grande assimetria informacional presente nas relações de tratamento de dados.

3.2Hipervigilância e influência comportamental

Fica evidente que a concentração de grandes volumes de dados pessoais nas mãos de terceiros ou de empresas pode ser utilizada para influenciar e incentivar determinados grupos sociais a adotarem condutas que favorecem os agentes, tanto sob o aspecto econômico quanto social. Isso acaba por gerar, de maneira indireta, um processo de manipulação social em massa. Nesse sentido, Byung-Chul Han afirma que "o poder inteligente lê e avalia nossos pensamentos conscientes e inconscientes", utilizando-se dos dados para influenciar comportamentos de maneira silenciosa e eficiente (Han, 2018, p. 23).

Tal realidade ecoa a crítica política presente no livro A Revolução dos Bichos, de George Orwell, ao destacar que "todos os animais são iguais, mas alguns animais são mais iguais que os outros", evidenciando que, embora haja um discurso formal de igualdade e proteção, determinados agentes concentram privilégios e poder decisório.

3.3 Os desafios da implementação da LGPD

Um dos principais desafios da efetividade da Lei Geral de Proteção de Dados (LGPD) na atualidade encontra-se na insuficiente maturidade organizacional de empresas e instituições quanto à sua implementação.

Em muitos casos, a adequação à legislação é tratada de forma superficial ou meramente formal, sem a construção de uma cultura interna de proteção de dados. Embora grandes corporações invistam em estruturas robustas de segurança da informação, incluindo criptografia e protocolos avançados de proteção, essa realidade não se reflete de maneira homogênea em empresas de médio e pequeno porte.

A ausência de conhecimento técnico, aliada à percepção da adequação como um custo ou ônus operacional adicional, resulta na negligência de práticas essenciais de segurança.

Tal cenário contribui diretamente para a ampliação dos riscos de incidentes e vazamentos de dados, evidenciando uma fragilidade estrutural que compromete a eficácia prática da LGPD no contexto da hipervigilância digital. Conforme Bioni (2024), a efetividade da LGPD depende não apenas da existência de normas jurídicas, mas também da implementação de uma cultura organizacional voltada à governança e à proteção de dados pessoais.

Percebe-se que a Lei Geral de Proteção de Dados representa um importante avanço na proteção da privacidade e dos dados pessoais. Entretanto, os desafios relacionados à hipervigilância digital, à falta de transparência no tratamento das informações e às dificuldades de implementação da própria legislação demonstram que a proteção prevista na lei nem sempre se concretiza na prática. Nesse sentido, Assis e Diniz (2025) evidenciam que, embora existam previsões normativas relacionadas à proteção de dados, persistem lacunas na execução das práticas previstas, comprometendo a transparência, a governança e a proteção dos direitos dos titulares. Assim, a LGPD, apesar de seu avanço normativo, mostra-se insuficiente para romper com essa lógica estrutural, contribuindo para a manutenção de uma privacidade mais aparente do que efetiva.

Nesse contexto, cabe indagar se o consentimento aplicado cumpre a função de garantir a autonomia do titular dos dados ou se representa apenas uma formalidade para legitimar o tratamento dessas informações.

4. O consentimento na Lei Geral de Proteção de Dados

O consentimento constitui um dos principais fundamentos utilizados para legitimar o tratamento de dados pessoais no ambiente digital. Entretanto, diante da crescente massificação da coleta de informações, questiona-se se esse consentimento

realmente representa uma manifestação livre, informada e consciente da vontade do titular dos dados. Pois, a partir de qual premissa se pode deduzir que o consentimento expresso do cidadão se perfaz pleno e eficaz sobre os seus dados exibidos dentro de um site ou aplicativo?

O consentimento do usuário no ambiente digital costuma se manifestar por meio da aceitação das diretrizes estabelecidas pelos próprios sites, especialmente no que se refere às políticas de privacidade e ao uso de cookies.

Esses cookies são pequenos arquivos de texto enviados ao navegador do usuário durante as suas visitas a sites de seu interesse, com a finalidade de registrar determinadas informações relacionadas à sua interação com a plataforma. Nos termos do art. 5º, XII, da Lei nº 13.709/2018, o consentimento consiste na "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".

Em termos práticos, sua utilização permite o armazenamento de preferências do usuário, como dados de login, idioma selecionado e itens inseridos em carrinhos de compra, contribuindo para uma navegação mais eficiente e personalizada. Por essa razão, podem ser compreendidos como mecanismos de armazenamento temporário de dados, essenciais para o funcionamento adequado de diversos serviços digitais.

Do ponto de vista jurídico, a utilização de cookies, sobretudo quando envolver dados pessoais, deve observar os requisitos de validade do consentimento, que precisa ser livre, informado e inequívoco. Além disso, impõe-se ao fornecedor o dever de transparência quanto à forma de coleta, uso e eventual compartilhamento dessas informações, em conformidade com a legislação de proteção de dados.

Esse mecanismo de armazenamento utilizado pelos sites revela-se eficiente para o reconhecimento do usuário durante a navegação, permitindo a identificação de preferências e a personalização da experiência digital. No entanto, sua utilização ocorre, muitas vezes, de maneira excessiva, sem que haja garantias claras de que os dados coletados serão automaticamente eliminados após determinado período.

Conforme Shoshana Zuboff, os dados pessoais passaram a ser utilizados como matéria-prima de um modelo econômico baseado na vigilância e na previsão comportamental dos indivíduos (ZUBOFF, 2021, p. 18).

Em diversos casos, a exclusão dessas informações depende de uma atuação ativa do próprio usuário, que precisa realizar a remoção manual dos dados armazenados em seu navegador. Tal cenário contribui para a concentração de informações nas mãos dos responsáveis pelas plataformas digitais, possibilitando o monitoramento contínuo do comportamento do usuário.

Como consequência, abre-se espaço para o rastreamento do dispositivo e, potencialmente, do próprio indivíduo, o que pode gerar riscos à privacidade. Nesse sentido, Byung-Chul Han afirma que "o Big Data possibilita um conhecimento integral da dinâmica inerente à sociedade da comunicação" (HAN, 2018, p. 11), evidenciando como o armazenamento massivo de dados amplia os mecanismos de vigilância e controle digital, o que reforça a importância de instrumentos jurídicos capazes de limitar práticas abusivas de coleta e utilização de dados, garantindo maior segurança e efetividade ao direito fundamental à privacidade.

4.1 A necessidade de aceitação dos termos de uso

A necessidade de aceitação dos termos de uso constitui um dos principais fatores que colocam em discussão a validade do consentimento no ambiente digital. A exigência de aderir aos termos do site que o usuário acessa ou deseja utilizar — seja para fins intelectuais, de entretenimento ou recreativos — faz com que tais termos sejam utilizados pelas plataformas para que a coleta e o armazenamento dos dados de cada indivíduo ocorram de forma "legal". Segundo Bioni (2021), a prática de aceitar termos de uso extensos e complexos faz com que o consentimento do usuário seja frequentemente apenas formal, sem que exista efetiva compreensão sobre o tratamento de seus dados.

Portanto, trata-se de termos que são clicados sem a devida atenção ao seu conteúdo. Os próprios usuários não possuem o hábito de ler o que de fato está escrito, além de

esbarrarem na complexidade linguística. Esse tipo de abordagem gramatical cria uma barreira invisível nos textos, sendo utilizada para desestimular a leitura por pessoas mais leigas.

Outro pilar dentro da complexidade do texto é o seu tamanho, pois o usuário que acessa a plataforma deseja desenvolver suas atividades de forma rápida e "fácil", sem a necessidade de interpretações complexas ou de despender horas apenas para ler os termos. Conforme demonstram McDonald e Cranor (2008), a leitura integral das políticas de privacidade demandaria centenas de horas por ano de um usuário comum, evidenciando a inviabilidade prática de um consentimento plenamente informado.

4.2 O consentimento como fundamento da exploração econômica dos dados

São esses termos que proporcionam uma base legítima para que empresas, principalmente aquelas voltadas ao setor comercial, realizem o tratamento de dados pessoais de forma ampla e juridicamente amparada. Um dos principais exemplos são as plataformas de pwublicidade digital, que utilizam dados, comportamentos e outras informações capazes de identificar interesses, muitas vezes implícitos, de seus usuários.

Com base nesses dados, é possível direcionar anúncios para determinados grupos sociais, econômicos e comportamentais, aumentando a efetividade das campanhas publicitárias. Dessa forma, as informações obtidas por meio do consentimento conferido nos termos de uso passam a integrar um modelo de exploração econômica dos dados pessoais, permitindo sua utilização em larga escala para fins comerciais (ZUBOFF, 2021; BIONI, 2021).

4.3 O consentimento forçado

Outro aspecto determinante para este debate é a obrigatoriedade de aceitar os termos de uso para acessar determinadas plataformas e serviços digitais. Em muitos casos, o usuário só consegue utilizar as funcionalidades oferecidas após concordar

com os termos estabelecidos pela plataforma, sendo impedido de prosseguir caso não manifeste seu consentimento.

Essa prática faz com que a liberdade de escolha do titular seja significativamente reduzida, uma vez que a necessidade de acesso ao serviço acaba condicionando o fornecimento de seus dados pessoais. Nesses casos, o consentimento deixa de representar uma manifestação plenamente livre da vontade do usuário, aproximando-se de um consentimento imposto pelas circunstâncias, o que compromete sua efetiva validade como fundamento para o tratamento de dados pessoais (BIONI, 2021; BRASIL, 2018).

Entretanto, um dos principais fatores que fragilizam a validade desse consentimento é justamente a complexidade dos termos de uso. Embora a LGPD exija que o consentimento seja livre, informado e inequívoco, a realidade demonstra que tais requisitos dificilmente são observados no ambiente digital.

A necessidade de acesso a determinados serviços, aliada à complexidade dos termos de uso e à impossibilidade prática de leitura integral dessas políticas, faz com que o consentimento seja frequentemente manifestado sem a efetiva compreensão de suas consequências.

Assim, o que a legislação apresenta como manifestação livre da vontade do titular acaba se convertendo, em muitos casos, em um requisito meramente formal para viabilizar o tratamento de dados pessoais.

Verifica-se que o consentimento, embora previsto pela LGPD como uma das principais bases legais para o tratamento de dados pessoais, nem sempre representa uma manifestação autêntica da vontade do titular.

As limitações impostas pela complexidade dos termos de uso, pela dependência dos serviços digitais e pela assimetria informacional evidenciam que esse mecanismo frequentemente atua apenas como instrumento formal de legitimação do tratamento de dados, sem assegurar o efetivo controle do indivíduo sobre suas informações pessoais.

Considerações finais

Ao longo da pesquisa, foi possível analisar que a Lei Geral de Proteção de Dados (LGPD) constitui um marco importante na sociedade contemporânea. Quando analisada em sua estrutura normativa, a legislação apresenta mecanismos destinados à proteção de dados pessoais e da privacidade; contudo, se por um lado o texto se mostra completo em sua forma prescritiva, por outro apresenta falhas evidentes em sua aplicabilidade prática.

Além disso, é evidente que este direito é uma garantia constitucional e um direito fundamental, reconhecido expressamente na Carta Magna. Esse reconhecimento demonstra a grande importância atribuída à proteção de informações pessoais no ordenamento jurídico.

Verificou-se, ainda, que a LGPD ainda não alcança plena efetividade diante dos desafios da era da hipervigilância digital. Parte-se da premissa de que o consentimento pode ser formalmente válido, mas materialmente limitado, seja pela complexidade estrutural e linguística dos textos longos, ocasionando uma ilusão de privacidade no âmbito digital, seja pelas dificuldades do titular em compreender ou controlar o fluxo de seus dados. Além disso, a imposição da aceitação como condição de uso de determinados sistemas restringe a liberdade de escolha do usuário.

Essas limitações impostas por determinados sites e sistemas acabam dificultando o cumprimento da função social prevista na LGPD, criando uma barreira de obrigatoriedade indireta. Desse modo, confirma-se que o consentimento funciona muitas vezes mais como uma formalidade legal do que como uma verdadeira manifestação de vontade.

Ocasionalmente, o usuário perde parcialmente o controle sobre os seus próprios dados, sobretudo quando aceita os termos que conferem às plataformas uma base legal de acesso aos serviços. Como resultado, o titular permanece exposto diariamente a diferentes formas de coleta e manuseio de suas informações no âmbito digital.

A Lei Geral de Proteção de Dados demonstra um avanço importante para os mecanismos de proteção; porém, a existência dessa estrutura não sustenta, sozinha, a sua efetividade, especificamente diante das diferentes formas de obtenção do consentimento no ambiente digital. Observa-se, portanto, uma distância entre a proteção assegurada ao titular e a sua capacidade real de compreensão. É nessa lacuna entre a formalidade do consentimento e o controle prático e efetivo que se sustenta a ideia da "ilusão da privacidade".

Referências

ASSIS, Thamirys Moreira de Sousa; DINIZ, Fernanda Paula. *A LGPD no Poder Público Municipal e a efetividade das práticas adotadas:* estudo de caso da Prefeitura Municipal de Carangola-MG. Cadernos da Escola do Legislativo, 2025. DOI: https://doi.org/10.62551/2595-4539.2025.538. Disponível em: https://cadernosdolegislativo.almg.gov.br/cadernos-ele/article/view/538. Acesso em: 12 abr 2026.

BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2024.

BRASIL. *Lei nº 13.709*, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago 2018.

COUTO, Camille; MAIA, Elijonas. Operação mira golpe do falso site do Enem; mais de 35 mil foram vítimas. CNN Brasil, 2025. Disponível em: https://www.cnnbrasil.com.br/nacional/sudeste/rj/operacao-mira-golpe-do-falso-site-do-enem-mais-de-35-mil-foram-vitimas/. Acesso em: 20 mai 2026.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Revista dos Tribunais, 2019

DUQUE, Rafaela Gonçalves; ARAÚJO, Luiz Felipe de Medeiros. *Proteção de dados pessoais:* impactos e desafios na sociedade da informação. Revista do Poder Judiciário do Estado do Rio Grande do Norte, v. 1, n. 1, 2020. Disponível em: https://revista.tjrn.jus.br/repojurn/article/view/23. Acesso em: 01 ago 2026.

HAN, Byung-Chul. *Psicopolítica:* o neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte: Âyiné, 2018.

LANIER, Jaron. *Dez argumentos para você deletar agora suas redes sociais*. Rio de Janeiro: Intrínseca, 2018.

MCDONALD, Aleecia M.; CRANOR, Lorrie Faith. *The cost of reading privacy policies.* A Journal of Law and Policy for the Information Society, v. 4, n. 3, 2008.

ORWELL, George. *A revolução dos bichos*: um conto de fadas. Tradução de Heitor Aquino Ferreira. São Paulo: Companhia das Letras, 2007.

PARISER, Eli. *O filtro invisível*: o que a internet está escondendo de você. Tradução de Diego Alfaro. Rio de Janeiro: Zahar, 2012.

RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Rio de Janeiro: Renovar, 2008.

SERASA EXPERIAN. Mais da metade dos brasileiros já foi vítima de fraude e 20% deles perderam até R$ 5 mil, revela estudo inédito da Serasa Experian. 25 mar. 2025. Disponível em: https://www.serasaexperian.com.br/sala-de-imprensa/prevencao-a-fraude/mais-da-metade-dos-brasileiros-ja-foi-vitima-de-fraude-e-20-deles-perderam-ate-rdollar-5-mil-revela-estudo-inedito-da-serasa-experian/. Acesso em: 24 ago 2026.

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 (Mestrado em Direito) – Escola de Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2022. Disponível em:* https://repositorio.pucrs.br/dspace/handle/10923/24466. Acesso em: 20 mai 2026.

ZUBOFF, Shoshana. A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2020.

Qualificação

Kayke Guimarães Salviano de Oliveira - ORCID: 0009-0009-5239-4500
Graduanda em Direito pela Pontifícia Universidade Católica de Goiás (PUC Goiás)
Lattes: http://lattes.cnpq.br/8759958888300499
Email: kaykeguimaraes04@gmail.com