CENTRO UNIVERSITÁRIO DE VOTUPORANGA – UNIFEV
CURSO DE DIREITO

ANA CLARA DA SILVA

ALÉM DO CLIQUE: OS DESAFIOS DA LGPD NA GARANTIA DA PRIVACIDADE E SEGURANÇA DOS DADOS EM REDES SOCIAIS

VOTUPORANGA
2025

ANA CLARA DA SILVA

ALÉM DO CLIQUE: OS DESAFIOS DA LGPD NA GARANTIA DA PRIVACIDADE E SEGURANÇA DOS DADOS EM REDES SOCIAIS

Trabalho de Curso apresentado à Unifev – Centro Universitário de Votuporanga – para a obtenção do grau de Bacharel em Direito, sob a orientação do professor Esp. Bruno Henrique Procópio Silva.

VOTUPORANGA

2025

Silva, Ana Clara da.

Além do clique: os desafios da LGPD na garantia da privacidade e segurança dos dados em redes sociais. / Ana Clara da Silva. - Votuporanga. Ed. do Autor, 2025.

25 p., 30cm.

Trabalho de Conclusão de Curso (Graduação - Bacharelado) - UNIFEV - Centro Universitário de Votuporanga, Curso de Direito, 2025.

Orientador: Prof. Esp. Bruno Henrique Procópio Silva.

1.Dados Pessoais. 2. LGPD. 3. Política de Privacidade. 4. Redes Sociais. 5. Titulares de Dados. I. Título.

Sistema de geração automática de fichas catalográficas da Unifev.

Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

Bibliotecária Responsável: Marcia Faria Cavalcante - CRB-8/ 10706

ALÉM DO CLIQUE: OS DESAFIOS DA LGPD NA GARANTIA DA PRIVACIDADE E SEGURANÇA DOS DADOS EM REDES SOCIAIS

Ana Clara da Silva[1]

Resumo:
Através do expressivo crescimento do ambiente digital e das redes sociais, marcado pela crescente coleta de dados pessoais e informações utilizadas para fins comerciais, publicitários e tecnológicos, desencadearam-se preocupações quanto à privacidade e à proteção das informações pessoais. Esse cenário resultou no presente estudo, que teve como objetivo observar a aplicabilidade das disposições da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), investigando a aplicação da LGPD, principalmente em plataformas como Instagram, Facebook e X (antigo Twitter), bem como identificar falhas em sua implementação, além de propor medidas para aprimorar a transparência e a segurança das informações tratadas por essas empresas. A justificativa do trabalho baseou-se na crescente relevância do tema para a sociedade, considerando que a compreensão crítica da proteção de dados é essencial para promover a conscientização sobre os riscos da exposição de informações e fortalecer a autonomia dos usuários diante das plataformas digitais. Adotou-se o método hipotético-dedutivo, além dos métodos histórico, comparativo e monográfico, com abordagem qualitativa, não empírica, bibliográfica, doutrinária e jurisprudencial, analisando obras de autores especializados, a própria legislação e decisões da Agência Nacional de Proteção de Dados (ANPD). Constatou-se que as plataformas não aplicam integralmente a LGPD, sobretudo no que se refere ao consentimento livre e informado, frequentemente substituído por aceites automáticos de "termos de uso" pouco claros. Conclui-se que há necessidade de maior fiscalização e transparência, bem como do aprimoramento das políticas de privacidade, a fim de assegurar efetivamente o direito fundamental à proteção de dados pessoais.

Palavras-chave: dados pessoais; LGPD; política de privacidade; redes sociais; titulares de dados.

Abstract
Through the significant growth of the digital environment and social networks, marked by the increasing collection of personal data and information used for commercial, advertising, and technological purposes, concerns have arisen regarding privacy and the protection of personal information. This scenario led to the present study, which aimed to observe the applicability of the provisions of the General Data Protection Law (Law No. 13,709/2018), investigating the implementation of the LGPD, particularly on platforms such as Instagram, Facebook, and X (formerly Twitter), as well as identifying flaws in its enforcement and proposing measures to enhance the transparency and security of the information processed by these companies. The justification for this research lies in the growing relevance of the topic to society, considering that a critical understanding of data protection is essential to raise awareness of the risks associated with information exposure and to strengthen users' autonomy in relation to digital platforms. The hypothetical-deductive method was adopted, along with historical, comparative, and monographic methods, using a qualitative, non-empirical, bibliographic, doctrinal, and jurisprudential approach. Works by specialized authors, relevant legislation, and decisions from

[1] Centro Universitário de Votuporanga (Unifev). Votuporanga, São Paulo, Brasil. Bacharelado em Direito. Email: anaclarafranhan@gmail.com.

the National Data Protection Authority (ANPD) were analyzed. It was found that the platforms do not fully comply with the LGPD, especially regarding free and informed consent, which is often replaced by automatic acceptance of unclear "terms of use". It is concluded that greater oversight and transparency are needed, as well as the improvement of privacy policies, in order to effectively ensure the fundamental right to the protection of personal data.

Keywords: personal data; LGPD; privacy policy; social networks; data subjects.

INTRODUÇÃO

O crescimento do ambiente digital e das redes sociais caracterizou-se como um dos fenômenos mais marcantes e significativos nos últimos tempos, transformando as relações sociais, econômicas e políticas. As plataformas digitais tornaram-se espaços centrais de interação e de circulação de informações. Nesse contexto, os dados pessoais passaram a representar um dos recursos mais valiosos da economia, no qual as informações coletadas dos usuários foram amplamente utilizadas para fins comerciais, publicitários e tecnológicos. Entretanto, essa crescente coleta e tratamento massivo de dados levantaram preocupações significativas quanto à privacidade e à proteção das informações pessoais, especialmente diante das práticas adotadas por grandes empresas do setor tecnológico.

O estudo teve como problema central compreender em que medida as redes sociais observaram e aplicaram as disposições da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), investigando os impactos na proteção da privacidade dos titulares de dados. Partiu-se da hipótese de que as principais plataformas como o Instagram, Facebook e X (antigo Twitter) não cumpriram integralmente os preceitos da LGPD, sobretudo no que se referiu à obtenção do consentimento livre, informado e inequívoco previsto nos artigos 7º e 8º da referida lei. Observou-se que, em muitos casos, os usuários aceitaram os "termos de uso" sem plena compreensão de seu conteúdo, em razão da linguagem técnica e ambígua, configurando um consentimento meramente formal e simbólico.

O objetivo geral consistiu em analisar a aplicação da LGPD no contexto das redes sociais, verificando se as plataformas respeitaram os direitos dos titulares de dados e identificando falhas em sua implementação. A pesquisa buscou, ainda, propor medidas de aprimoramento capazes de reforçar a transparência e a segurança das informações tratadas por tais empresas. Entre as etapas do estudo, foram identificados os tipos de dados coletados, examinadas as políticas de privacidade e analisados os potenciais impactos jurídicos e sociais da coleta indevida de informações, bem como as sanções previstas em caso de descumprimento da legislação.

A justificativa do trabalho baseou-se na relevância crescente do tema para a sociedade, uma vez que a vida digital se tornou indispensável no cotidiano e a proteção de dados pessoais passou a constituir um direito fundamental. Buscou-se, fomentar a conscientização sobre os riscos associados à exposição excessiva de dados e o empoderamento dos usuários diante das práticas das grandes plataformas.

Metodologicamente, a pesquisa utilizou o método hipotético-dedutivo, partindo de conceitos gerais sobre privacidade e proteção de dados para chegar a conclusões específicas sobre sua aplicação no ambiente digital. Empregaram-se, ainda, os métodos histórico, comparativo e monográfico, com abordagem qualitativa, não empírica, bibliográfica, doutrinária e jurisprudencial. Foram analisadas obras de autores como Danilo Donda, Flavio Tartuce e Patricia Peck, além da própria legislação e de decisões da Agência Nacional de Proteção de Dados (ANPD).

1 FUNDAMENTOS TEÓRICOS E LEGAIS DA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

1.1 O direito à privacidade no contexto digital

Para entender como o direito à privacidade se consolidou nos tempos atuais, é preciso revisitar sua trajetória ao longo da história. É necessário voltar à Constituição de 1824, conhecida como Constituição do Império. Foi nessa época que surgiu, de forma embrionária, o direito à privacidade.

Os maiores exemplos disso são o "segredo da carta" e a "inviolabilidade da casa". Nessa época, a privacidade era vista de forma concreta e material, tanto é que o "segredo da carta" se referia à proteção do "documento físico", como, por exemplo o papel e o envelope, não necessariamente ao que está escrita na carta. Ou seja, na Constituição do Império, a proteção visava a proteção física dos espaços e objetos.

Em 1890, nos Estados Unidos, o direito à privacidade era conhecido como “Direito a intimidade”, refletindo uma preocupação com a proteção da vida privada contra interferências indevidas. Foi nessa época que o direito à privacidade passou a ser teorizado como um direito fundamental, muito por conta do artigo publicado na revista de Direito de Harvard por Warren e Brandeis, que definiam privacidade como:

> [...] "right to be let alone" em tradução direta “direito de ser deixado em paz”. O direito à privacidade era visto como um direito de ser deixado em paz, de longe da curiosidade alheia. Até que ponto a lei é necessária para garantir aos indivíduos que desejam transmitir sua mensagem, seus pensamentos, sentimentos e emoções aos outros (Warren; Brandeis, 1890, p. 2).

Neste mesmo sentido, preceitua Donda:

> A moderna doutrina do direito à privacidade, cujo início podemos considerar como sendo o famoso artigo de Brandeis e Warren, The right to privacy, apresenta uma clara linha evolutiva. Em seus primórdios, marcada por um individualismo exacerbado e até egoísta, portava a feição do direito a ser deixado só. A esse período remonta o paradigma da privacidade como uma zero-relationship, pelo qual representaria, no limite, a ausência de comunicação entre uma pessoa e as demais. Essa concepção foi o marco inicial posteriormente temperado por uma crescente consciência de que a privacidade seria um aspecto fundamental da realização da pessoa e do desenvolvimento da sua personalidade (Donda, 2020, p. 31-32).

Com o passar do tempo, principalmente no século XX, com os avanços da tecnologia - especialmente as de registros, como câmeras, televisão, rádio -, intensificou-se a necessidade de proteger não só os espaços e objetos físicos, mas também a honra, a imagem e a dignidade da pessoa. Com consequência disso, foi necessário debater sobre direitos de privacidade mais amplos.

A conquista significativa ocorreu com a promulgação da Constituição Federal de 1988, que reconheceu o direito à privacidade como um direito fundamental, previsto no Artigo 5º, incisos X, XI e XII:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no país a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> X – São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> XI – a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;
> XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (Brasil, 1988).

Assim, é garantida às pessoas a inviolabilidade da intimidade, da vida privada, da honra e da imagem, assegurando o direito à indenização por danos decorrentes de sua violação. A partir daí, a privacidade passou a ser reconhecida como um direito da personalidade, inato, inalienável e irrenunciável.

1.2 A proteção de dados pessoais como direito fundamental

Em agosto de 2018, foi promulgada a Lei nº 13.709, intitulada Lei Geral de Proteção de Dados (LGPD), e, em fevereiro de 2022, houve uma Emenda Constitucional nº 115, que incluiu a proteção de dados pessoais entre os direitos e garantias fundamentais, inserindo o inciso LXXIX ao artigo 5º da Constituição Federal de 1988:

> Art. 5º. [...]
> [...]
> LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais (Brasil, 1988).

Com o grande aumento no uso da internet, das redes sociais e dos sistemas digitais de coleta de dados, novos desafios surgiram. Segundo o Instituto Brasileiro de Geografia e Estatística (IBGE):

> [...] 70,5% dos domicílios estavam conectados à rede em 2017. Em 92,7% das residências, pelo menos um morador possuía telefone celular, enquanto o telefone fixo era encontrado em apenas 32,1% (Agência Senado, 2020, p. 1).

No mesmo sentido, de acordo com dados e projeções de uma pesquisa feita pela companhia NordVPN (2022), a população mundial passa em média 41 anos de suas vidas conectadas na internet, o que representa 54% da expectativa média de vida da população, ou seja, a população passa mais da metade de suas vidas conectadas na internet. Em relação aos brasileiros, eles passam em média semanalmente, assistindo 12 horas de vídeos no Youtube e 11 horas conectadas em redes sociais sendo a maior parte delas no WhatsApp, Facebook e Instagram.

A privacidade deixou de ser apenas uma questão de proteção física ou moral e passou a envolver o controle sobre dados pessoais. Por conta disso, foi sancionada a LGPD, que estabelece regras claras sobre o tratamento de dados pessoais por empresas e instituições, exigindo consentimento, transparência e segurança, além de criar mecanismos de fiscalização e penalização.

A LGPD foi inspirada na *General Data Protection Regulation* (GDPR), da União Europeia. O debate sobre a GDPR teve início em 2012, foi publicada em 2016 e entrou em vigor em maio de 2018. A GDPR se consolidou como principal marco regulatório internacional

sobre o tema, inspirando diversas outras legislações ao redor do mundo, além da própria LGPD.

Nesse sentido, destaca Donda (2020) que a Lei Geral de Proteção de Dados (LGPD) foi inspirada no Regulamento Geral de Proteção de Dados (GDPR), que embora tenha parecido coincidência a aprovação da LGPD no Congresso Nacional pouco tempo depois da entrada em vigor da GDPR na União Europeia, na verdade foi consequência de sua inspiração. A LGPD possui muitos valores e princípios em sintonia com a GDPR, ambas as legislações possuem uma estrutura ampla e horizontal, com foco à proteção dos direitos individuais e fiscalizadas por uma autoridade.

A GDPR se baseia em princípios como: licitude, lealdade, transparência, limitação das finalidades, minimização dos dados, exatidão, limitação da conservação, integridade e confiabilidade e responsabilidade.

1.3. Análise da Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018)

A LGPD tem como objetivo a proteção dos direitos fundamentais de liberdade e privacidade, sendo reconhecida como um marco jurídico no Brasil. É a lei que disciplina todo o tratamento de dados pessoais, como a coleta, uso, compartilhamento e armazenamento dos dados pessoais. Ela é aplicada para dados pessoais físicos e digitais, sendo válida tanto para empresas quanto para órgãos públicos. Assim dispõe seu artigo 1º:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018).

É importante destacar a aplicação territorial da lei, sendo uma lei com alcance extraterritorial, segundo Donda (2020), a LGPD é aplicada em qualquer país, desde que a coleta do dado pessoal tenha sido realizada no Brasil, mesmo que a sede da empresa esteja em território estrangeiro. A Meta, por exemplo, possui sede na Califórnia, nos Estados Unidos, mas está sujeita à LGPD, pois coleta dados pessoais no Brasil.

Em certas situações, a LGPD não se aplica, como, por exemplo, na coleta e no tratamento de dados pessoais por pessoa natural e para fins particulares ou jornalísticos. As situações de inaplicabilidade se encontram em seu artigo 4º:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> I - realizado por pessoa natural para fins exclusivamente particulares e não

> econômicos;
> II - realizado para fins exclusivamente:
> a) jornalístico e artísticos; ou
> b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
> III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais; ou
> IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei (Brasil, 2018).

É importante contextualizar a diferença entre dado pessoal e dado pessoal sensível. Segundo Donda (2020), dado pessoal é qualquer dado que possa identificar um indivíduo, informações como: CPF, RH, CNH, nome e sobrenome. Dados pessoais sensíveis são aqueles que requerem maior cuidado em seu tratamento pois são informações que podem causar atos discriminatórios, são dados referentes à: 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.

A LGPD estabelece 10 (dez) princípios fundamentais que devem orientar qualquer atividade de tratamento de dado pessoal, segundo Donda:

> a) Finalidade: A realização do tratamento para propósitos legítimos, específicos, explícitos, e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.
> b) Necessidade: Limitação do tratamento ao mínimo necessário para realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em reação às finalidades do tratamento de dados.
> c) Adequação: Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento:
> d)Livre Acesso: garantia aos titulares de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integridade de seus dados pessoais.
> e) Qualidade dos dados: garantia aos titulares de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.
> f) Transparência: Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.
> g) Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.
> h) Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.
> i) Não discriminação: Impossibilidade de realização do tratamento para fins discriminatórios, ilícitos ou abusivos.
> j) Responsabilização e prestação de contas: Demonstração pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e inclusive da eficácia dessas medidas (Donda, 2020,

p.22).

Na LGPD existem os agentes de tratamento de dados, que são os responsáveis pelo correto tratamento de dados pessoais do titular. O titular, segundo a LGPD em seu artigo 5º, inciso V é a pessoa natural a quem se referem os dados pessoais que são objetos de tratamento. Entre os agentes de tratamento, estão o controlador e o operador. A LGPD em seu artigo 5º, inciso VI, define o controlador como a pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais. Já o operador a LGPD define em seu artigo 5º, inciso VII como sendo a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Com essas definições, para exemplificar na prática essa relação de controlador e operador considere o seguinte exemplo: o titular de dados realiza seu cadastro na plataforma do Instagram. O Instagram neste caso atua como controlador das informações pessoais. O Instagram sozinho não consegue garantir a segurança desses dados, o Instagram então contrata uma empresa terceirizada, que assume o papel de operador. Nesse cenário, o operador somente pode tratar os dados conforme as instruções expressas do controlador, ou seja, o Instagram. Ele não possui autonomia para decidir sobre a finalidade ou forma de tratamento dos dados, devendo seguir rigorosamente os limites estabelecidos pelo controlador (Brasil, 2018).

Também é importante destacar o papel do encarregado de proteção de dados, que é a "ponte" entre o controlador, titular de dados e a Agência Nacional de Proteção de Dados (ANPD), que pode ser tanto uma pessoa física quanto jurídica. É o encarregado que será responsável por receber reclamações e solicitações dos titulares dos dados, atender comunicações da ANPD, orientar colaboradores e prestadores sobre a LGPD, além de desempenhar outras tarefas designadas pelo controlador ou pela legislação.

Importante destacar a ANPD, que teve uma medida provisória (nº 1.317, de 17 de setembro de 2025) que alterou a Lei nº 13.709, de 14 de agosto de 2018, para tratar da ANPD, que anteriormente era chamada de Autoridade Nacional de Proteção de Dados. Segue nova redação da lei com a medida provisória:

> Art. 55-A. Fica criada a Agência Nacional de Proteção de Dados – ANPD, autarquia de natureza especial vinculada ao Ministério da Justiça e Segurança Pública, dotada de autonomia funcional, técnica, decisória, administrativa e financeira, com patrimônio próprio e com sede e foro no Distrito Federal (Brasil, 2025).

Com essa nova medida provisória, a ANPD, além de zelar pela proteção de dados

pessoais com a responsabilidade de orientar, regulamentar e fiscalizar o cumprimento da LGPD, aplicando sanções em caso de não conformidade, também foi designada para ser responsável pela nova Lei nº 15.211, de 17 de setembro de 2025 - Estatuto Digital da Criança e do Adolescente.

2 FUNDAMENTOS TEÓRICOS E LEGAIS DA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

2.1 O modelo de negócios das redes sociais e a coleta de dados pessoais

O Instagram, Facebook e X (antigo Twitter) são aplicativos de interação social e consumo de conteúdo. Embora pareçam aplicativos gratuitos, a monetização desses aplicativos está concentrada na coleta e no tratamento intensivo de dados pessoais. Essa monetização fica explícita na própria política de privacidade da Meta, empresa responsável pelo Instagram, Facebook e Threads:

> Compartilhamos informações sobre você com fornecedores de marketing. Por exemplo, compartilhamos o seu identificador de dispositivo ou outros identificadores com fornecedores de marketing. Assim, eles nos ajudam a exibir anúncios mais pertinentes aos seus interesses. Os fornecedores de marketing apoiam nossos esforços de marketing e de publicidade da seguinte maneira: veiculando nossos anúncios na internet, inclusive em dispositivos móveis, desktop e TVs conectadas; rastreando e categorizando sua atividade online e em apps para celular; fornecendo informações sobre os seus interesses e as interações que você tem com a comunidade e a publicidade. Esses fornecedores de marketing nos ajudam a entender quem pode achar nossa publicidade mais relevante para os próprios interesses e qual dos nossos produtos pode interessar a você. É possível usar essas informações para personalizar quais anúncios mostramos para você. Os fornecedores de marketing também usam essas informações para mensurar a resposta aos nossos esforços de marketing e a eficácia da nossa publicidade (Meta, 2025, p. 6).

A mesma coisa corre com a plataforma X (antigo Twitter):

> Com anunciantes. A receita publicitária permite-nos fornecer nossos produtos e serviços. Os anunciantes podem ter informações sobre o nosso engajamento com seus anúncios dentro ou fora do X. Por exemplo, se você clicar em um link ou anúncio externo em nossos serviços, aquele anunciante ou operador do website poderá descobrir que você veio do X, juntamente com outras informações associadas ao anúncio no qual você clicou, tais como características do público que se pretende atingir e outros identificadores gerados pelo X para aquele anúncio. Eles também podem coletar outras informações pessoais suas, tais como identificadores de cookies, ou seu endereço de IP (X Corp., 2025, p. 8).

Nesse sentido, para Silveira, Avelino e Souza (2016), os dados pessoais se tornaram

uma mercadoria com a finalidade exclusiva de compra e venda. Este mercado é regrado pela necessidade que algumas empresas e órgãos públicos possuem em determinadas informações pessoais.

Assim, nas redes sociais, o conteúdo postado pelos usuários não é o que realmente tem valor comercial. As empresas pagam as redes sociais para que seus anúncios cheguem a usuários com perfis e interesses semelhantes, informações que são obtidas a partir do comportamento de cada pessoa dentro da plataforma. Por isso, o usuário acaba se tornando o verdadeiro produto dessas plataformas.

Os principais tipos de dados coletados pelas plataformas Instagram, Facebook e X, podem ser enquadrados como: dados cadastrais, comportamentais, de localização, de interação e sensíveis. É importante contextualizar o que significa cada um deles e o que cada política de privacidade informa que é coletado. As informações as seguir foram coletadas diretamente da política de privacidade da Meta (Facebook e Instagram) e do X.

Dados cadastrais são informações fornecidas diretamente pelo usuário no momento da criação da conta. A Meta coleta endereço de e-mail, telefone ou idade (Meta, 2025). O X coleta nome de exibição, nome de usuário, e-mail ou telefone, data de nascimento, idioma e dados profissionais (X Corp, 2025).

Dados comportamentais são ações realizadas pelo usuário dentro da plataforma, como tempo de permanência, cliques em anúncios, curtidas, comentários e compartilhamentos. A Meta coleta o conteúdo criado pelo usuário, como posts, comentários ou áudios; as mensagens enviadas e recebidas, incluindo o conteúdo; as hashtags usadas; o horário, a frequência e a duração das atividades. Inclusive, identifica o que o usuário está fazendo no dispositivo, como, por exemplo, se o aplicativo está em primeiro plano ou o se mouse está se movendo (Meta, 2025). O X coleta dados sobre o conteúdo criado, postado ou recebido, como tweets, mensagens diretas, curtidas, retweets e respostas. Também coleta informações sobre interações com anúncios e links (X Corp, 2025).

Dados de localização são coletados por meio de GPS e endereços IP. Essa coleta pode ser contínua, mesmo com o aplicativo em segundo plano. A Meta coleta informações relacionadas à localização mesmo se os serviços de localização estão desativados nas configurações do dispositivo. Isso inclui o uso de endereços de IP para estimar a localização geral, sinais de Bluetooth, pontos de acesso de Wi-Fi nas imediações, beacons e torres de antena de celular (Meta, 2025). O X coleta informações de localização aproximada, como endereço de IP ou configurações de dispositivo. Também pode coletar a localização exata caso o usuário

deixe ativada a função. Podem armazenar locais usados anteriormente para personalização de anúncios e conteúdo (X Corp, 2025).

Dados de interação são aqueles em que o usuário interage com outros perfis, como frequência de mensagens trocadas, com quem mais interage, quais contas visita com maior frequência. A Meta coleta informações sobre amigos, seguidores, grupos, contas, páginas do Facebook e outros usuários e comunidades com quem o usuário tem conexão ou interage. Coleta também informações dos contatos, incluindo nome e endereço de e-mail ou telefone, caso o usuário carregue ou importe de um dispositivo (Meta, 2025). O X coleta informações sobre mensagens diretas, seguidores, contas que o usuário segue, curtidas, retweets, contatos importados e outras conexões sociais (X Corp, 2025).

Dados sensíveis são informações sobre origem racial ou étnica, opiniões políticas, convicções religiosas, dados de saúde e vida sexual podem ser inferidos e utilizados, direta ou indiretamente, no perfilamento algorítmico. Nas plataformas da Meta, o usuário pode optar por fornecer informações sobre sua religião, sua orientação sexual, suas preferências políticas, sua saúde, sua origem racial ou étnica, suas crenças filosóficas ou sua filiação sindical (Meta, 2025). O X pode coletar informações biométricas (com consentimento) para segurança, proteção e identificação. Em alguns países, podem ser coletados dados exigidos por lei (X Corp).

A abrangência da coleta é, portanto, bastante significativa, indo muito além dos dados fornecidos conscientemente pelo usuário.

2.2 Análise crítica das políticas de privacidade

A LGPD (Lei nº 13.709/2018) estabelece como um dos princípios fundamentais a transparência e clareza das informações:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; (Brasil, 2018).

Em primeiro lugar, nota-se que a Meta utiliza uma única política para todos seus produtos, como: Facebook; Messenger; Instagram, incluindo apps como Edits, Threads e Boomerang; Produtos da Meta Platforms Technologies, como o Meta Horizon Worlds ou o Meta Quest; e Dispositivos da marca Meta Portal. Essa forma de englobar várias plataformas em uma só política causa ambiguidade e confusão no usuário/titular de dados, pois diversas

plataformas se valem da mesma política de privacidade, dificultando o entendimento sobre quais informações são coletadas e tratadas em cada produto, fragilizando a transparência exigida pela LGPD (Meta, 2025).

A transparência na política de privacidade da Meta fica visivelmente comprometida ao comparar o cadastro em duas plataformas que são propriedades da Meta, o Facebook e o Instagram. Ao se cadastrar no Facebook, é solicitado ao titular de dados as seguintes informações: nome e sobrenome, data de nascimento, gênero e telefone celular ou e-mail. Já ao se cadastrar no Instagram é solicitado: nome completo, número de celular ou e-mail e nome de usuário. Na política de privacidade, é informado a coleta dos seguintes dados pessoais: "As informações que você nos fornece ao se cadastrar nos nossos Produtos e criar um perfil, como endereço de e-mail, telefone ou idade" (Meta, 2025).

Apesar dessa diferença clara na coleta de informações, a política de privacidade da Meta, que é unificada para ambos os serviços, não especifica de forma transparente quais dados são coletados em cada plataforma, tampouco esclarece a finalidade ou a necessidade da coleta de determinados dados, como o gênero, exigido apenas no Facebook.

Analisando a política do X no momento do cadastro, torna-se ainda mais evidente a falta de transparência da Meta. Isso porque, no X, todas as informações solicitadas ao usuário são descritas com clareza e exatidão, em conformidade com o que é efetivamente requerido no momento do cadastro, como previsto em sua política:

> Informações que você nos fornece.
> Contas Pessoais. Se você criar uma conta, deve fornecer-nos algumas informações para que possamos prestar-lhe nossos serviços. Isto inclui um nome de exibição (por exemplo, "Criadores"); um nome de usuário (por exemplo, @XCreators); uma senha; um endereço de e-mail ou número de telefone; uma data de nascimento; seu idioma de exibição; e informações de login único de terceiros (se você escolher este método de login). Você também pode optar por compartilhar sua localização em seu perfil e nos posts, e carregar sua lista de contatos no X para ajudar a encontrar pessoas que você possa conhecer. Suas informações de perfil, que incluem seu nome de apresentação e nome de usuário, são sempre públicas, mas você pode usar ou seu nome verdadeiro ou um pseudônimo (X Corp, 2025, p. 2-3).

Contudo, ao aprofundar a análise, observa-se que o X não segue integralmente os requisitos da LGPD. Isso ocorre porque, durante o cadastro, caixas de seleção (*checkboxes*) destinadas à autorização para o envio de comunicações, como e-mails promocionais, já vêm previamente marcadas:

> A. Permitir o compartilhamento de informações adicionais com parceiros de negócios

> O X sempre compartilha informações com parceiros de negócios para gerenciar e melhorar seus produtos. Quando essa opção é ativada, o X pode compartilhar mais informações com esses parceiros para oferecer suporte ao gerenciamento dos negócios do X, inclusive tornar as atividades de marketing do X em outros sites e aplicativos mais relevantes para você.
> B. Tenha mais do X
> Receba e-mails sobre sua atividade no X e recomendações (X Corp, 2025, p. 7).

Essa prática compromete a validade do consentimento, uma vez que a LGPD exige manifestação livre, informada e inequívoca do titular. Assim, ao induzir o usuário a consentir sem uma escolha ativa, o X incorre em desconformidade com a legislação de proteção de dados, conforme destaca Mendes (2014) o consentimento realizado pelo indivíduo precisa ser fruto de uma manifestação livre, específica e informada, necessitando de uma ação do titular. O Titular não pode ser induzido em seu consentimento, por isso checkboxes não podem estar previamente selecionados, pois induz o titular a aceitar de forma involuntária, não estando essa prática em conformidade com a lei geral de proteção de dados.

Retornando à política da Meta, observa-se que o conteúdo presente em sua política de privacidade é excessivamente genérico, acabando por suscitar mais dúvidas ao titular de dados do que propriamente oferecer respostas claras, como se vê:

> Também coletamos as informações dos seus contatos, incluindo nome e endereço de email ou telefone, caso você as carregue ou importe de um dispositivo, como ao sincronizar uma agenda de contatos. Se você não usa os Produtos da Meta ou os usa sem uma conta, **suas informações ainda podem ser coletadas**. Saiba mais sobre como a Meta usa as informações de contato carregadas pelos titulares das contas (Meta, 2025, p. 3-4).

No trecho, há inúmeras inconformidades com a LGPD. A LGPD estabelece, no art. 7º, que, para o tratamento de dado pessoal, é necessário possuir uma base legal específica, como o consentimento, a execução de contrato ou o cumprimento de obrigação legal. Destaca Donda (2020, p. 23) que "Qualquer tratamento sem alguma das bases legais é ilícito". No caso em análise, a Meta passa a coletar informações de terceiros que não são usuários dos serviços, baseando-se apenas na ação de um usuário que sincroniza sua agenda e de terceiros que não são usuários da plataforma. Isso significa que o consentimento de um indivíduo é estendido indevidamente a seus contatos, o que contraria a LGPD, uma vez que ninguém pode consentir em nome de outra pessoa.

Além disso, a redação utilizada pela Meta compromete novamente o princípio da transparência, visto que não deixa claro quais dados são coletados de não usuários, para quais finalidades, por quanto tempo serão armazenados e com quem poderão ser compartilhados.

Em análise ao direito dos titulares, que é obrigação legal do controlador de dados:

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> I - confirmação da existência de tratamento;
> II - acesso aos dados;
> III - correção de dados incompletos, inexatos ou desatualizados;
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019) Vigência
> VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
> VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei (Brasil, 2018).

Para verificar o efetivo cumprimento dessa obrigação legal, optou-se por realizar um estudo de caso prático. Foram abertas duas solicitações: uma direcionada ao Instagram e outra ao Facebook, ambas relacionadas ao direito de "acesso aos dados", ou seja, a identificação de quais dados pessoais essas plataformas tratam. A primeira solicitação de titular foi encaminhada ao Instagram (Solicitações de direitos de privacidade #1364788232314125), cuja resposta foi recebida dentro do prazo legal de até 15 (quinze) dias, contados a partir da data do requerimento. Ocorre, contudo, que a resposta fornecida foi genérica e automática, apenas replicando o conteúdo já disponível na própria política de privacidade. Segue, na íntegra, a resposta encaminhada pelo Instagram:

> Olá,
> Agradecemos o contato para saber quais são os tipos de informações que coletamos. As informações coletadas e tratadas sobre você dependem do seu uso dos nossos Produtos. Por exemplo, coletamos informações diferentes se você vende móveis no Marketplace ou publica um reels no Instagram. Quando você usa nossos Produtos, coletamos algumas informações sobre você, mesmo que não tenha uma conta.
> Você pode optar por fornecer informações sobre sua religião, sua orientação sexual, suas preferências políticas, sua saúde, sua origem racial ou étnica, suas crenças filosóficas ou sua filiação sindical. Dependendo das leis de sua jurisdição, esses e outros tipos de informações podem ter proteções especiais.
> Estas são as informações que coletamos:
> - Sua atividade e as informações que você fornece: https://privacycenter.instagram.com/policy/?subpage=subpage-1.1
> - Os amigos, os seguidores e outras conexões: https://privacycenter.instagram.com/policy/?subpage=subpage-1.3
> - Informações de apps, navegadores e dispositivos: https://privacycenter.instagram.com/policy/?subpage=subpage-1.4

> - Informações de Parceiros, de fornecedores e de outros terceiros: https://privacycenter.instagram.com/policy/?subpage=subpage-1.5
>
> Para saber mais sobre as informações que coletamos, consulte a Política de Privacidade: https://privacycenter.instagram.com/policy
> Caso tenha qualquer outra pergunta, responda a este email.
> Atenciosamente,
> Operações de Privacidade (Meta, 2025).

A segunda solicitação de titular foi encaminhada ao Facebook (Solicitações de direitos de privacidade #1131212258509250), cuja resposta também foi recebida dentro do prazo legal de até 15 (quinze) dias, contados a partir da data do requerimento. Entretanto, assim como ocorreu no caso do Instagram, a resposta do Facebook apresentou os mesmos problemas: foi igualmente genérica e automatizada, limitando-se a reproduzir informações já constantes em sua política de privacidade, sem fornecer efetivamente os dados pessoais tratados:

> Olá,
> Agradecemos o contato para saber quais são os tipos de informações que coletamos.
> As informações coletadas e tratadas sobre você dependem do seu uso dos nossos Produtos. Por exemplo, coletamos informações diferentes se você vende móveis no Marketplace ou publica um vídeo do Reels no Instagram. Quando você usa nossos Produtos, coletamos algumas informações sobre você, mesmo que não tenha uma conta.
> Estas são as informações que coletamos:
> - Sua atividade e as informações que você fornece: https://www.facebook.com/privacy/policy?subpage=1.subpage.1-YourActivityAndInformation
> - Os amigos, os seguidores e outras conexões: https://www.facebook.com/privacy/policy?subpage=1.subpage.2-FriendsFollowersAndOther
> - Informações de apps, navegadores e dispositivos: https://www.facebook.com/privacy/policy?subpage=1.subpage.3-AppBrowserAndDevice
> - Informações de Parceiros, fornecedores e terceiros: https://www.facebook.com/privacy/policy?subpage=1.subpage.4-InformationFromPartnersVendors
>
> Para saber mais sobre as informações que coletamos, consulte a Política de Privacidade:
> https://www.facebook.com/privacy/policy?section_id=1-WhatInformationDoWe
> Caso tenha qualquer outra pergunta, responda a este email.
> Atenciosamente,
> Operações de Privacidade (Meta, 2025).

A análise da resposta encaminhada pela Meta evidencia que, embora exista a formalidade de atendimento às solicitações do titular, o conteúdo fornecido não cumpre integralmente as exigências da LGPD. A resposta automática, genérica e desprovida de clareza contraria diretamente os princípios da transparência e da boa-fé previstos no art. 6º da lei, uma vez que não oferece ao titular informações suficientes para compreender o tratamento de seus

dados nem para exercer de forma efetiva seus direitos.

3 IMPACTOS, SANÇÕES E PROPOSTAS PARA O REFORÇO DA PROTEÇÃO DE DADOS NAS REDES SOCIAIS

3.1 Consequências da coleta indevida e do tratamento irregular de dados

A coleta inadequada e o tratamento irregular de dados pessoais em redes sociais configuram uma ameaça ao direito fundamental à privacidade, gerando repercussões que ultrapassam o âmbito jurídico e alcançam dimensões sociais mais amplas. Sob a perspectiva legal, a Lei Geral de Proteção de Dados Pessoais (LGPD), em seu artigo 42, estabelece que o controlador ou o operador que, no exercício de atividades de tratamento de dados pessoais, causar dano patrimonial, moral, individual ou coletivo a outrem, em violação às disposições da legislação de proteção de dados, tem o dever de repará-lo. Desse modo, os titulares de dados afetados dispõem de respaldo jurídico para pleitear a reparação de danos materiais e morais na esfera cível, em decorrência da responsabilidade civil resultante do ato ilícito. A responsabilidade civil é prevista no Código Civil, em seus artigos 186, 187 e 927, que discorrem sobre a obrigação de reparar o dano, por todos aqueles que violarem o dever jurídico por meio de ato ilícito, sendo hoje em dia aplicável a responsabilidade das redes sociais para seus usuários.

De acordo com Assis (2020), nas redes sociais a responsabilidade civil tem como objetivo a proteção dos direitos fundamentos, como a honra, a imagem e a privacidade, responsabilizando aqueles que violarem a lei por prejuízo causados a outros indivíduos. Para Tartuce (2020), no que se diz respeito a responsabilidade civil no âmbito das redes sociais, tanto os autores quanto as plataformas podem ser responsabilizadas por seus atos ilícitos.

Dessa forma, ações realizadas no Facebook, Instagram ou X (antigo Twitter), como a coleta de informações de contatos de terceiros sem consentimento, falha na proteção de dados pessoais, coleta de dados pessoais e/ou sensíveis sem uma transparência clara de sua necessidade e finalidade, ou o compartilhamento de dados com parceiros comerciais sem transparência, configuram potenciais violações da LGPD, sujeitando as empresas a sanções administrativas, multas e responsabilização civil.

Há precedentes sobre o assunto:

> RECURSO INOMINADO. RESIDUAL. AÇÃO DE OBRIGAÇÃO DE FAZER C/C INDENIZAÇÃO POR DANO MORAL. INVASÃO DE PERFIL NA REDE SOCIAL INSTAGRAM. UTILIZAÇÃO PARA GOLPES. MANUTENÇÃO DA OBRIGAÇÃO DE FAZER. DESNECESSIDADE DE QUE A USUÁRIA FORNEÇA NOVO E-MAIL PARA O CUMPRIMENTO DA MEDIDA IMPOSTA. DANO MORAL. TRATAMENTO INADEQUADO DE DADOS PESSOAIS. RESPONSABILIDADE DOS AGENTES DE TRATAMENTO. LGPD. VAZAMENTO E EMPREGO DOS DADOS POR GOLPISTAS. PREJUÍZO CONCRETO. VIOLAÇÃO A DIREITO DA PERSONALIDADE. DIREITOS FUNDAMENTAIS À PROTEÇÃO DE DADOS E À PRIVACIDADE. RESPONSABILIDADE CIVIL CONFIGURADA. PEDIDO DE MINORAÇÃO DO QUANTUM INDENIZATÓRIO ACOLHIDO. SENTENÇA PARCIALMENTE REFORMADA. RECURSO INOMINADO CONHECIDO E PARCIALMENTE PROVIDO. (TJ-PR, 0009486-75.2021.8.16.0026, 2ª Turma Recursal, julgado em 02 de junho de 2023).

Esse precedente trata da responsabilidade civil decorrente de falha na proteção de dados pessoais, reconhecendo o dever de indenizar por dano moral em razão da violação aos direitos da personalidade da autora, vítima de golpe. A decisão fundamenta-se nos arts. 44 e 46 da Lei nº 13.709/2018 (LGPD), que impõem aos agentes de tratamento a adoção de medidas técnicas e administrativas adequadas para proteger os dados pessoais contra acessos não autorizados, perdas ou tratamentos ilícitos. O tribunal destacou que a omissão na adoção dessas medidas configura violação à segurança da informação, atraindo a responsabilidade do controlador ou do operador pelos danos causados. Além disso, o acórdão ressalta que a proteção de dados pessoais é direito fundamental (art. 5º, LXXIX, da Constituição Federal), diretamente relacionado à liberdade, à privacidade e ao livre desenvolvimento da personalidade.

A Meta enfrenta diversas consequências por conta da prática de tratamento indevido no tratamento de dados pessoais. O primeiro escândalo foi o caso Cambridge Analytica - assessoria britânica que trabalhou para a campanha eleitoral do presidente americano, Donald Trump- ocorrido em 2018, quando milhões de dados de usuários do Facebook foram coletados sem consentimento para a criação de perfis com a finalidade de realizar propaganda política. Esse caso demonstra como uso indevido de informações pode resultar em manipulação de comportamentos políticos e sociais.

Em 2021 o Facebook foi novamente alvo de vazamento massivo de dados, que expôs informações de cerca de 530 milhões de usuários, incluindo nomes, números de telefone e endereço de e-mail, gerando riscos de fraude de identidade, *phishing* e extorsão digital. Sobre o *phishing*, de acordo com o relatório Spam e *phishing*, baseado em tentativas de acesso a páginas fraudulentas, os brasileiros são os que mais sofrem tentativas de *phishing*, encontrando-se com 20% a mais se comparado com a média mundial de 13%. Para Assiolini (2020), o que pode explicar essa diferença é pelos brasileiros terem mais dificuldades de identificar tentativas

de golpes.

Em outro caso de vazamento de dados, ocorrido em 2018 e 2019, o Tribunal de Justiça de Minas Gerais (TJMG) decidiu que a Meta, empresa controladora do Facebook, Instagram e WhatsApp, deveria pagar indenizações aos usuários afetados por vazamentos de dados. A Meta foi condenada a pagar R$ 40 milhões por danos morais coletivos, além de R$ 10 mil para cada usuário afetado.

Esses casos demonstram as consequências reais que podem ocorrer com pessoas que têm seus dados pessoais coletados e/ou vazados indevidamente. Os ricos extrapolam a questão financeira ou moral, atingindo também questões sociais e políticas. Nesse sentido, Mendes (2018) explica que quando um indivíduo não tem mais a capacidade de saber o que e quem sabe sobre eles, se tem um grande problema, pois macula a liberdade individual e a sociedade deixa de ser justa e transparente, sendo violado o direito à autodeterminação.

As redes sociais ao utilizarem dados comportamentais dos usuários para criar perfis, conseguem antever o que os usuários consomem, em quem votam e até como se sentem. Dessa forma, as redes sociais conseguem realizar publicidade direcionada e até manipular informações que os usuários vão receber.

3.2 Atuação da ANPD e medidas para o aprimoramento da privacidade e proteção de dados

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) estabeleceu sanções administrativas aos agentes de tratamento de dados que não cumprirem com a LGPD. As sanções estão previstas em seu artigo 52 (Brasil, 2018), e visam garantir a efetividade da lei e a responsabilização daqueles que desrespeitam suas disposições.

As sanções previstas são: advertência, com indicação de prazo para adoção de medidas corretivas; multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; multa diária, observado o limite total de R$ 50.000.000,00 (cinquenta milhões de reais); publicização da infração, após devidamente apurada e confirmada a sua ocorrência; bloqueio dos dados pessoais a que se refere a infração até a sua regularização; eliminação dos dados pessoais a que se refere a infração; suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da

atividade de tratamento pelo controlador; suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período e a proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados (Brasil, 2018).

As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa e analisará os critérios previstos no parágrafo primeiro do artigo 52 que são: a gravidade e a natureza das infrações e dos direitos pessoais afetados; a boa-fé do infrator; a vantagem auferida ou pretendida pelo infrator; a condição econômica do infrator; a reincidência; o grau do dano; a cooperação do infrator; a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados; a adoção de política de boas práticas e governança; a pronta adoção de medidas corretivas; e a proporcionalidade entre a gravidade da falta e a intensidade da sanção (Brasil, 2018).

Desde o início de suas atividades, em 2021, a ANPD tem passado por um processo contínuo de aperfeiçoamento, o que reflete sua evolução enquanto órgão responsável pela implementação e fiscalização da LGPD. Isso explica o aumento progressivo do número de fiscalizações e ações regulatórias com o passar dos anos, conforme apurado por Causin:

> Em um mês, autoridade brasileira de dados abre mais investigações contra empresas do que em quatro anos. Em outubro de 2024, um caso considerado "extraordinário" pela própria entidade levou à abertura de um número inédito de fiscalizações, mais do que o apurado em quatro anos de existência da autarquia. Nas duas primeiras semanas de outubro, a ANPD deu início a 21 processos de apuração de incidentes de segurança, que se somaram a outros dez procedimentos abertos desde janeiro deste ano. Ao todo, são 31 abertos em 2024. Entre 2021 e 2023, foram apenas 15 procedimentos ao todo, metade do número registrado nos últimos dez meses (Causin, 2024, p. 1).

Em 2025, a ANPD foi transformada em agência, reforçando sua independência administrativa e técnica. Segundo o balanço de 4 anos divulgados pela ANPD, seu quadro funcional entre 2021 e 2024, cresceu significativamente, passando de 50 servidores para 141 servidores. Importante destacar a atuação da ANPD:

> A ANDP exerce sua função fiscalizatória por meio de ações de monitoramento, orientação, prevenção e repressão. O monitoramento tem caráter proativo, permitindo identificar práticas irregulares e riscos potenciais, além de subsidiar futuras ações fiscalizatórias. Essa atuação preventiva visa garantir a conformidade dos agentes de tratamento com a LGPD e promover um ambiente mais seguro para o uso de dados pessoais no Brasil. A ANPD também recebe requerimentos da sociedade, divididos em dois tipos: petições de titular, que permitem ao indivíduo reclamar diretamente contra controladores em casos de violação de direitos, e denúncias, que podem ser

> apresentadas por qualquer pessoa para comunicar supostas infrações à legislação de proteção de dados (ANPD, 2024, p. 24).

Uma das principais fiscalizações da ANPD ocorreu em 2024, quando emitiu uma Medida Preventiva (PROCESSO Nº 00261.004509/2024-36) determinando a imediata suspensão, no Brasil, da vigência política de privacidade da Meta, que autorizava o uso de dados pessoais publicados em suas plataformas para fins de treinamento de sistemas de inteligência artificial (IA):

> 1. GRUPO META. ALTERAÇÃO NA POLÍTICA DE PRIVACIDADE. TRATAMENTO DE DADOS PESSOAIS COM A FINALIDADE DE TREINAMENTO DE SISTEMAS DE INTELIGÊNCIA ARTIFICIAL GENERATIVA.
> 2. DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS. INDÍCIOS DE: (I) AUSÊNCIA DE HIPÓTESE LEGAL APROPRIADA PARA A REALIZAÇÃO DO TRATAMENTO; (II) FALTA DE TRANSPARÊNCIA NA DIVULGAÇÃO DAS NOVAS INFORMAÇÕES AOS TITULARES; (III) LIMITAÇÃO AO EXERCÍCIO DE DIREITOS; E (IV) TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES SEM AS DEVIDAS SALVAGUARDAS.
> 3. RISCO IMINENTE DE DANO GRAVE E IRREPARÁVEL OU DE DIFÍCIL REPARAÇÃO.
> 4. MEDIDA PREVENTIVA PARA DETERMINAR, ATÉ ULTERIOR DECISÃO DESTA AUTORIDADE, A IMEDIATA SUSPENSÃO NO BRASIL: (I) DA VIGÊNCIA DA NOVA POLÍTICA DE PRIVACIDADE DA EMPRESA, NO QUE TOCA À PARTE RELATIVA AO USO DE DADOS PESSOAIS PARA FINS DE TREINAMENTO DE SISTEMAS DE IA GENERATIVA; E (II) DO TRATAMENTO DE DADOS PESSOAIS DOS TITULARES PARA ESSA FINALIDADE EM TODOS OS "PRODUTOS DA META", INCLUSIVE DE PESSOAS NÃO USUÁRIAS DE SUAS PLATAFORMAS, SOB PENA DE MULTA DIÁRIA DE R$ 50.000,00 (CINQUENTA MIL REAIS) POR DIA DE DESCUMPRIMENTO (ANPD, 2024, p. 1 e 2).

É evidente que a ANPD é um órgão novo e está em constante evolução. Tem se observado um aumento bastante significativo em suas fiscalizações e orientações legais, bem como no recebimento de petições legais, demonstrando evolução na privacidade e proteção de dados no Brasil. Em relatório divulgado pela ANPD, em janeiro de 2024 foram recebidas 32 solicitações de petições de titulares e em julho foram recebidas 148 solicitações de titulares. A ANPD destaca:

> A partir de julho, observou-se um aumento significativo no número de petições enviadas à Autoridade Nacional de Proteção de Dados (ANPD), resultado direto da implementação de uma nova funcionalidade lançada em parceria com o Ministério da Gestão e da Inovação em Serviços Públicos (MGI). Esse novo serviço, permite que titulares de dados pessoais enviem petições e denúncias de violações à Lei Geral de Proteção de Dados (LGPD) por meio de uma plataforma moderna e acessível no portal GOV.BR. A introdução dessa ferramenta representou um avanço importante no processo de modernização dos serviços prestados pela ANPD, ampliando a

> acessibilidade e facilitando o exercício dos direitos dos titulares de dados. O aumento nas petições a partir de julho demonstra a eficácia e a adesão positiva à nova plataforma, que simplificou a interação dos cidadãos com a ANPD (ANPD, 2024, p. 25).

Contudo, o fortalecimento da proteção de dados no Brasil não pode se limitar apenas ao trabalho realizado pela ANPD. Ele exige, igualmente, a consolidação de uma cultura social que valorize a privacidade, alcançando empresas e os próprios titulares de dados pessoais. Para isso, é fundamental que os indivíduos tenham clareza sobre os seus direitos.

As políticas de privacidade possuem como público-alvo o usuário. Dessa forma, em sua elaboração, é necessário que não apresentem uma linguagem excessivamente técnica, afinal, é preciso levar em consideração que o usuário pode não ter conhecimento de linguagem jurídica e formal. Portanto, é imprescindível que a política de privacidade seja clara, transparente e acessível. O importante é que o usuário compreenda todo o ciclo de tratamento de dados que será realizado, entendendo informações como: quais dados são coletados, para quais finalidades, com quem são compartilhados e qual é o período de retenção desses dados.

Por conta disso, destaca-se a necessidade de investimento em educação digital, para que se tenha uma sociedade participativa e crítica quanto ao tratamento de seus dados pessoais, compreendendo seus direitos e os valores que seus dados possuem.

CONSIDERAÇÕES FINAIS

O presente trabalho objetivou a análise da aplicação da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) no ambiente das redes sociais, realizando uma análise nas plataformas como o Instagram, Facebook e X (antigo Twitter) observando as diretrizes legais direcionadas à privacidade e proteção dos dados de seus usuários. A pesquisa teve como base o questionamento sobre os desafios da proteção dos dados pessoais, especialmente em um cenário dominado por práticas de coleta de dados em larga escala, perfis comportamentais e políticas de privacidade complexas e pouco claras.

Com base no estudo teórico e nas análises práticas realizadas, houve a confirmação da hipótese de que as principais redes sociais não cumprem integralmente as regras da LGPD. As investigações demonstraram que a maior parte das plataformas adotam práticas de consentimento superficiais e automatizadas, nas quais o titular de dados aceita termos extensos e ambíguos sem a efetiva compreensão de seu conteúdo. Em muitos casos, o consentimento foi reduzido a uma formalidade burocrática, desprovida de valor real quanto à vontade informada

do usuário. Além disso, verificou-se o uso de caixas de seleção pré-marcadas, estratégias que induzem o usuário à aceitação, violando princípios da liberdade e da autodeterminação informativa e a base legal do consentimento.

Ademais, foi também observado a falta de clareza e objetividade nas políticas de privacidade das plataformas analisadas. A unificação de políticas de privacidade para diferentes produtos, como ocorre no caso da Meta (controladora do Facebook e do Instagram), que dificulta a compreensão das finalidades e do alcance da coleta de dados, fragilizando o princípio da transparência previsto no artigo 6º, VI da LGPD. Observou-se também que a resposta das empresas às solicitações dos titulares foi padronizada e automática, sem fornecer informações completas sobre os dados efetivamente tratados, o que demonstra um atendimento meramente formal aos direitos previstos na legislação.

Esses resultados evidenciaram que a adequação das redes sociais à LGPD ainda é preambular e majoritariamente simbólica, concentrando-se mais em ajustes redacionais das políticas do que em mudanças estruturais nas práticas de tratamento de dados. Cenário esse, em que reforçou a constatação de que a proteção da privacidade nas plataformas digitais permanece fragilizada, uma vez que o usuário, mesmo amparado pela lei, continua sem acesso fácil, claro e compreensível às informações que lhe dizem respeito.

Constatou-se que o tratamento inadequado de dados pessoais gera relevantes repercussões sociais e econômicas. O uso indevido dessas informações possibilita a elaboração de perfis detalhados, que são capazes de influenciar preferências individuais, padrões de consumo e até mesmo decisões de cunho político. Reiterados episódios de vazamentos e escândalos envolvendo a empresa Meta demonstram que a manipulação de dados pessoais pode comprometer diretamente a liberdade individual e a integridade democrática. As consequências dessas práticas vão além dos danos morais e materiais, atingindo valores essenciais como a dignidade, a confiança e a autonomia informacional dos cidadãos.

No âmbito institucional, o estudo evidenciou a relevância da atuação da Agência Nacional de Proteção de Dados (ANPD) na consolidação de uma cultura de privacidade no Brasil. Desde sua criação, a ANPD tem aprimorado sua capacidade técnica e fiscalizatória, implementando medidas preventivas e sancionatórias voltadas a empresas que descumprirem os princípios estabelecidos pela LGPD. Episódios recentes, como a suspensão da política de privacidade da empresa Meta em 2024, demonstraram um avanço efetivo em sua atuação.

É de suma importância a conscientização e do empoderamento dos usuários frente à coleta e ao tratamento de suas informações. Tornou-se evidente que o simples cumprimento

formal da lei não é suficiente para garantir a efetiva proteção de dados; é indispensável que os titulares compreendam seus direitos, saibam como exercê-los e exijam transparência das empresas.

A efetividade da LGPD dependerá não apenas de sua aplicação legal, mas da consolidação de uma cultura de respeito à privacidade e à proteção de dados pessoais. Embora avanços significativos tenham ocorrido, a construção de um ambiente digital ético, seguro e transparente depende do contínuo engajamento do Estado, das empresas e da sociedade. Apenas por meio deste esforço coletivo será possível transformar o direito à privacidade em uma realidade concreta, garantindo que o ambiente digital evolua em conformidade com os valores democráticos e os direitos fundamentais.

REFERÊNCIAS

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS. **ANPD determina suspensão cautelar do tratamento de dados pessoais para treinamento da IA da Meta**. Publicado em 02/07/2024 06h54 Atualizado em 02/07/2024 08h34. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-cautelar-do-tratamento-de-dados-pessoais-para-treinamento-da-ia-da-meta Acesso em: 5 out. 2025.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS. **Balanço 4 anos ANPD**. Novembro 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/anpd-balanco-4-anos.pdf Acesso em: 10 out. 2025.

AGÊNCIA SENADO. **Lei Geral de Proteção de Dados entra em vigor**. Senado Notícias. 18/09/2020, 16h09. 18/09/2020. Disponível em: https://www12.senado.leg.br/noticias/materias/2020/09/18/lei-geral-de-protecao-de-dados-entra-em-vigor Acesso em: 11 set. 2025.

ASSIS, Gustavo; ANDRADE, Renata; CARVALHO, Samara. **Responsabilidade civil no ambiente virtual**. Revista Brasileira de Direito Civil, Rio de Janeiro, v. 21, n. 1, p. 99-124, jan.-mar. 2020. Disponível em: https://unisecal.edu.br/wp-content/uploads/2023/08/ALINE-DO-CARMO-PAZ-DIAS.pdf Acesso em: 11 set. 2025

ASSOLINI, F. **Um em cada cinco brasileiros sofreu tentativa do golpe de "pescaria digital" em 2020.** Disponível em: https://febrabantech.febraban.org.br/temas/seguranca/um-em-cada-cincobrasileiros-sofreu-tentativa-do-golpe-de-pescaria-digital-em-2020 Acesso em: 05 mar. 2023.
BARBOSA, M. C. A. Responsabilidade civil e a internet. In: MIRANDA, A. (Coord.). Tratado de Direito Privado. São Paulo: Thomson Reuters Brasil, 2019.

BARROS, S. **Responsabilidade civil por danos morais na internet.** Rio de Janeiro: Forense, 2017.

BIONI, B. R. **Proteção de dados pessoais: a função e os limites do consentimento.** Rio de Janeiro: Forense, 2019.

BRASIL. **Facebook condenado por vazamento de dados: quem tem direito e como pedir indenização?** Disponível em: https://www.jusbrasil.com.br/artigos/facebook-condenado-por-vazamento-de-dados-quem-tem-direito-e-como-pedir-indenizacao/1941248694 Acesso em: 5 out. 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: seção 1, Brasília, DF, 15 ago. 2018.

BRASIL. **Medida Provisória nº 1.317, de 17 de setembro de 2025**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para tratar da Agência Nacional de Proteção de Dados, a Lei nº 10.871, de 20 de maio de 2004, para criar a Carreira de Regulação e Fiscalização de Proteção de Dados, transforma cargos no âmbito do Poder Executivo federal, e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, 17 set. 2025.

DO CARMO, A.; DIAS, P.; ZENARDI, R. **A responsabilidade civil no âmbito das redes sociais.** Unisecal, 2023. Disponível em: https://unisecal.edu.br/wp-content/uploads/2023/08/ALINE-DO-CARMO-PAZ-DIAS.pdf Acesso em: 10 out, 2025.

DONDA, D. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

DONDA, D. **Guia prático de implementação da LGPD.** 1. ed. São Paulo: Editora Labrador, 2020.

GIARA, M. **A coleta de dados pessoais pelas redes sociais digitais com impactos sobre a privacidade.** 2024. 75 f. Monografia (Bacharelado em Biblioteconomia) — Departamento de Ciências da Informação, Centro de Humanidades, Universidade Federal do Ceará, Fortaleza, 2024.

GLOBO. **Facebook atribui vazamento de dados de 530 milhões de usuários a "raspagem".** Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/04/07/facebook-atribui-vazamento-de-dados-de-530-milhoes-de-dados-a-raspagem.ghtml Acesso em: 2 out. 2025.

GOVERNO DO PARANÁ. **Manual de implementação da LGPD.** Disponível em: https://www.cge.pr.gov.br/sites/default/arquivos_restritos/files/documento/2021-06/manual_implementacao_lgpd.pdf Acesso em: 30 set. 2025.

GOVERNO FEDERAL. **Governo Federal estrutura ANPD para assumir competências do ECA Digital.** Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/governo-federal-estrutura-anpd-para-assumir-competencias-do-eca-digital Acesso em: 14 out. 2025.
GOVERNO FEDERAL. Proteção de dados pessoais agora é um direito fundamental. Disponível em: https://www.gov.br/anpd/pt-br/protecao-de-dados-pessoais-agora-e-um-direito-fundamental Acesso em: 11 set. 2025.

MENDES, L. S. F. **Habeas data e autodeterminação informativa: os dois lados da mesma**

moeda. Direitos Fundamentais & Justiça, Belo Horizonte, ano 12, n. 39, p. 185–216, 2018.

META PLATFORMS, Inc. **Política de privacidade** [Internet]. Em vigor em 17 de julho de 2025 |São Paulo: Meta Platforms, Inc., [s.d.]. Disponível em: https://www.facebook.com/privacy/policy/?locale=pt_BR Acesso em: 07 nov. 2025.

NALIN, C. **Oito em cada dez brasileiros que conhecem a LGPD acreditam que seus dados estão seguros, diz pesquisa**. Disponível em: https://epocanegocios.globo.com/tecnologia/noticia/2024/10/oito-em-cada-dez-brasileiros-que-conhecem-a-lgpd-acreditam-que-seus-dados-estao-seguros-diz-pesquisa.ghtml Acesso em: 11 set. 2025.

O GLOBO. **Em um mês, autoridade brasileira de dados abre mais investigações contra empresas do que em quatro anos**. Disponível em: https://oglobo.globo.com/economia/noticia/2024/10/25/em-um-mes-autoridade-brasileira-de-dados-abre-mais-investigacoes-contra-empresas-do-que-em-quatro-anos.ghtml Acesso em: 10 out. 2025.

O GLOBO. **Justiça condena Meta a pagar indenização por vazamento de dados no Facebook, Instagram e WhatsApp**. Disponível em: https://oglobo.globo.com/economia/noticia/2025/06/16/justica-condena-meta-a-pagar-indenizacao-por-vazamento-de-dados-no-facebook-instagram-e-whatsapp.ghtml Acesso em: 2 out. 2025.

PINHEIRO, P. P. **Proteção de dados pessoais – comentários à Lei n. 13.709/2018 (LGPD).** São Paulo: Saraiva Educação, 2018.

SILVEIRA, Sergio Amadeu; AVELINO, Rodolfo; SOUZA, Joyce. **A privacidade e o mercado de dados pessoais**. Liinc em Revista. v. 12 n. 2 (2016): Privacidade e vigilância nos meios digitais. São Paulo: LIINC, 2016. Disponível em: http://revista.ibict.br/liinc/article/view/3719 Acesso em: 11 set. 2025.

TARTUCE, F. **Direito Civil: Responsabilidade Civil.** 16. ed. rev., atual. e ampl. Rio de Janeiro: Forense; São Paulo: Método, 2020.

TECHTUDO. **Brasileiros passam mais da metade de suas vidas na Internet, estima pesquisa.** Disponível em: https://www.techtudo.com.br/noticias/2022/05/brasileiros-passam-mais-da-metade-de-suas-vidas-na-internet-estima-pesquisa.ghtml Acesso em: 11 set. 2025.

TRIBUNAL DE JUSTIÇA PARANÁ. Processo nº 0009486-75.2021.8.16.0026, Campo Largo. Relator: Maurício Pereira Doutor. Julgado em: 2 jun. 2023. 2ª Turma Recursal. Publicado em: 7 jun. 2023.

TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO (TRT4). **Manual de implementação da LGPD: estudos sobre a Lei Geral de Proteção de Dados**. Disponível em: https://www.trt4.jus.br/portais/media/1063693/E-book-EstudosLGPD-Edjud4.pdf Acesso em: 30 set. 2025.

MAIA, C. Y. M.; LUZ, M. Ad. da S.; LUZ, M. S. (Org.). **Diálogos científicos em direito: produções acadêmicas** 2021.2. V. I. Cabedelo, PB: Centro Universitário Uniesp, 2022.

WARREN, S. D.; BRANDEIS, L. D. **O direito à privacidade. Revista de Direito de Harvard.** Vol. IV 15 de dezembro de 1890 Nº 5. Disponível em: https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html Acesso em: 30 set. 2025.

X CORP. **Política de Privacidade do X** [Internet]. [s.l.]. Em vigor: 28 de julho de 2025. Disponível em: https://x.com/pt/privacy Acesso em: 07 nov. 2025

ZANINI, L. E. de A. **O surgimento e o desenvolvimento do right of privacy nos Estados Unidos**. Revista Eletrônica da Faculdade de Direito de Franca, v. 9, n. 2, 2014. Disponível em: https://www.ajufe.org.br/images/bkp/ajufe/arquivos/downloads/leonardo-estevam-de-assis-zanini-o-surgimento-e-o-desenvolvimento-do-right-of-privacy-nos-estados-unidos-2661518.pdf Acesso em: 30 set. 2025.