

NAVEGANDO PELA PRIVACIDADE DIGITAL: COOKIES E LGPD NA PROTEÇÃO DA PRIVACIDADE ONLINE

NAVIGATING DIGITAL PRIVACY: COOKIES AND LGPD IN PROTECTING ONLINE PRIVACY

DOI: 10.16891/2317-434X.v14.e1.a2026.id2364

Recebido em: 30.09.2024 | Aceito em: 04.08.2025

**Ana Paula dos Santos Silva^{a*}, Áquila Raquel de Sousa Matos Reis^a,
Luana Brandão Ribeiro^a**

Faculdade Anhanguera de Imperatriz, Imperatriz – MA, Brasil^a
***E-mail: paulaana.santossilva20@gmail.com**

RESUMO

O artigo aborda a evolução dos cookies, desde sua criação nos anos 1990 por Lou Montulli, engenheiro da Netscape. Inicialmente concebidos para facilitar a navegação na web, os cookies se tornaram essenciais na personalização e aprimoramento da experiência do usuário online. No entanto, com o avanço tecnológico, surgiram preocupações com a privacidade e segurança dos dados pessoais, levando à criação da Lei Geral de Proteção de Dados (LGPD) em 2018. O artigo enfatiza a importância de compreender a relação entre aceitar os cookies e proteger dados pessoais, ressaltando a falta de compreensão por parte dos usuários sobre as implicações dos cookies na privacidade. A pesquisa empregou uma abordagem abrangente, incluindo métodos qualitativos e pesquisa bibliográfica. O texto explora os princípios fundamentais da LGPD para o tratamento de dados pessoais, destacando a necessidade de transparência, segurança e responsabilidade na coleta e uso de dados. Além disso, sublinha a importância de equilibrar a inovação tecnológica com a proteção dos direitos dos cidadãos na era digital, promovendo uma cultura de transparência e confiança. Enfatiza também que a proteção de dados é uma responsabilidade ética e legal das empresas e organizações, e destaca a conscientização sobre o uso de cookies como um elemento crucial para uma internet mais transparente e ética.

Palavras-chave: Cookies de Navegadores. LGPD. Dados Pessoais. Privacidade.

ABSTRACT

The article discusses the evolution of cookies, since their creation in the 1990s by Lou Montulli, an engineer at Netscape. Initially designed to facilitate web browsing, cookies have become essential in personalizing and improving the online user experience. However, with technological advancement, concerns arose about the privacy and security of personal data, leading to the creation of the General Data Protection Law (LGPD) in 2018. The article emphasizes the importance of understanding the relationship between accepting cookies and protecting personal data, highlighting the lack of understanding on the part of users about the privacy implications of cookies. The research employed a comprehensive approach, including quantitative methods and detailed literature search. The text explores the fundamental principles of the LGPD for the processing of personal data, highlighting the need for transparency, security and responsibility in the collection and use of data. Furthermore, it highlights the importance of balancing technological innovation with the protection of citizens' rights in the digital age, promoting a culture of transparency and trust. It also emphasizes that data protection is an ethical and legal responsibility of companies and organizations, and highlights awareness of the use of cookies as a crucial element for a more transparent and ethical internet.

Keywords: Browser Cookies. LGPD. Personal data. Privacy.

INTRODUÇÃO

Os cookies, pequenos arquivos de texto usados em navegação na web, surgiram na década de 1990, época em que a internet ainda estava em seus estágios de desenvolvimento. Foi nesse contexto que o engenheiro Lou Montulli, enquanto trabalhava na Netscape Communications, criou os cookies com o propósito de resolver um problema específico. Naquela época, os navegadores da “web” ainda não dispunham de uma maneira eficiente de armazenar informações dos visitantes. Por isso, as pessoas precisavam inserir repetidamente dados, como, por exemplo, nome de usuário e senha, toda vez que interagiam com um site.

Essa inovação se mostrou incrivelmente útil e logo foi incorporada por outros navegadores e sistemas. Se, a princípio, sua função era apenas facilitar o uso dos sites, permitindo o registro de preferências como o idioma e itens no carrinho de compras, atualmente, os cookies são parte essencial da navegação online, viabilizando a personalização, a autenticação e outras funcionalidades que aprimoram a interação do usuário com as plataformas.

Dessa maneira, observa-se como uma pequena inovação técnica foi capaz de acompanhar a rápida evolução digital e se tornar fundamental na experiência online dos usuários. No entanto, à medida que os cookies evoluíram, também surgiram preocupações sobre privacidade e a segurança dos dados pessoais. É nesse contexto que surge a Lei Geral de Proteção de Dados (LGPD), criada em 2018, a qual representa um marco histórico para a proteção da privacidade no Brasil, definindo diretrizes claras para o uso responsável de dados pessoais em um mundo digital cada vez mais complexo.

Assim, neste artigo será abordado o delicado limiar entre aceitar os cookies e a proteção de dados pessoais, analisando como a LGPD influencia e orienta essa relação. Afinal, o ato aparentemente simples de consentir o uso de cookies pode ter implicações profundas na segurança dos dados de cada usuário.

METODOLOGIA

Para o estudo, empregamos uma abordagem metodológica abrangente que integrou métodos qualitativos e pesquisa bibliográfica. Desta forma, a aplicação da metodologia indutiva possibilitou o

entendimento de que a maioria das pessoas não possui uma compreensão completa das implicações que os cookies podem ter sobre sua privacidade.

A pesquisa bibliográfica, por sua vez, proporcionou a este artigo um embasamento teórico sólido para o desenvolvimento do estudo, contribuindo para uma compreensão mais ampla do assunto e das questões envolvidas. Assim, a combinação dessas abordagens metodológicas ofereceu uma visão fundamentada sobre o impacto dos cookies na privacidade dos usuários.

RESULTADOS E DISCUSSÃO

A análise evidencia que, no contexto tecnológico, os cookies atuam como instrumentos estratégicos para personalização da experiência online, viabilizando que os sites colem e processem informações relacionadas às preferências, histórico de navegação e configurações dos usuários.

Inicialmente voltados apenas para otimizar a usabilidade, os cookies evoluíram para possibilitar a criação de perfis altamente individualizados, tornando a experiência de navegação mais envolvente e direcionada. Conforme observa Lessig (2006, p. 07; 48), eles foram indispensáveis para o avanço da internet, especialmente no âmbito comercial.

Entretanto, com o crescimento da internet, essa prática passou a ser um mecanismo de rastreamento intensivo, o que suscitou preocupações relativas à privacidade. Dessa forma, gigantes tecnológicos como Google, Facebook e Amazon passaram a coletar dados sensíveis em larga escala, acumulando, assim, enormes volumes de informações pessoais. Como consequência, esse cenário redefiniu a publicidade online e alterou a forma como as empresas enxergam os consumidores.

É neste cenário que a Lei Geral de Proteção de Dados (LGPD), inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, emerge como instrumento legal estruturado para enfrentar os desafios da privacidade e da proteção de dados no ambiente digital brasileiro.

DA Europa ao Brasil: lições do regulamento geral sobre a proteção de dados da União Europeia (GDPR).

Com o crescimento das preocupações globais

relacionadas à proteção de dados pessoais, diversos países passaram a adotar normas específicas para regulamentar o uso dessas informações, especialmente no ambiente digital. Nesse viés, o GDPR destacou-se como uma das normas mais abrangentes e influentes, servindo como modelo para outras legislações ao redor do mundo, inclusive para a LGPD.

Em termos de fundamentos, GDPR e LGPD compartilham princípios fundamentais, como a finalidade, a necessidade, a transparência e a segurança e têm como objetivo central garantir os direitos dos titulares de dados frente ao avanço tecnológico e à crescente digitalização das relações. No entanto, apesar das semelhanças, existem diferenças significativas quanto à forma de aplicação, à estrutura institucional e ao rigor das sanções previstas.

Enquanto o GDPR possui um alcance supranacional, aplicável de forma uniforme em todos os Estados-membros da União Europeia, a LGPD foi construída com base nas particularidades do sistema

jurídico brasileiro. Além disso, a LGPD introduziu a Autoridade Nacional de Proteção de Dados (ANPD) como órgão responsável pela fiscalização e regulação da lei no Brasil, papel desempenhado, no âmbito europeu, por autoridades nacionais de proteção de dados em cada país, supervisionadas por um órgão central, o Comitê Europeu de Proteção de Dados (CEPD).

Outra diferença importante está no regime de punições adotado em caso de descumprimento. O GDPR é amplamente reconhecido por sua severidade, prevendo penalidades que podem atingir até 20 milhões de euros ou 4% do faturamento anual global da organização, conforme dispõe o Art. 83, §5 (UNIÃO EUROPEIA, 2016). A LGPD, por sua vez, estabelece sanções mais brandas, limitando a multa a até 2% do faturamento da empresa no Brasil, com teto de R\$ 50 milhões por infração, conforme o Art. 52, inciso II (BRASIL, 2018).

Para ilustrar essas diferenças e semelhanças de forma clara, apresente-se a seguir uma tabela comparativa:

Tabela 1. Comparativo entre LGPD e GDPR.

Aspecto	GDPR	LGPD
Princípios Compartilhados	Finalidade, necessidade, transparência, segurança	Finalidade, necessidade, transparência, segurança
Alcance	Uniforme na União Europeia	Baseado no sistema jurídico brasileiro
Multas	Até 20 milhões de euros ou 4% do faturamento global	Até 2% do faturamento no Brasil, com teto de R\$ 50 milhões por infração
Órgão Fiscalizador	Autoridades nacionais supervisionadas pelo CEPD	Autoridade Nacional de Proteção de Dados (ANPD)
Extraterritorialidade	Sim, aplica-se a empresas globais que tratam dados de cidadãos europeus	Sim, aplica-se a empresas globais que tratam dados de brasileiros

Fonte: Adaptado de INSTITUTO CÁTEDRA (“GDPR: o que é e qual a diferença em relação à LGPD?”, agosto 2021). Disponível em: idcatedra.com.br/2021/08/gdpr-o-que-e-e-qual-a-diferenca-em-relacao-a-lgpd/. Acesso em: 18 ago. 2025.

Essas distinções mostram que, embora caminhem na mesma direção, cada uma trilha um caminho próprio. É importante destacar que a extraterritorialidade é um ponto-chave nessa discussão. O GDPR aplica-se não apenas a empresas sediadas na União Europeia, mas também a qualquer organização, em qualquer parte do mundo, que ofereça serviços a cidadãos europeus (UNIÃO EUROPEIA, 2016, Art. 3º). Isso significa que, sim, uma empresa pode ser responsabilizada pelo GDPR mesmo sem ter presença física na Europa.

Um caso emblemático foi o da Clearview, empresa norte-americana especializada em reconhecimento facial, que coletou imagens públicas, incluindo fotos de cidadãos europeus. O problema? Essa

coleta foi feita sem o consentimento dos titulares. Mesmo estando fora da União Europeia, a empresa foi alvo da autoridade italiana de proteção de dados, país integrante do bloco europeu, que aplicou uma multa de 20 milhões de euros e ordenou a exclusão imediata dos dados dos cidadãos italianos (EDRi, 2022).

Esse caso deixa claro que se uma organização oferece serviços ou trata dados de pessoas localizadas na União Europeia, ela pode ser responsabilizada, independentemente de onde esteja sediada. Da mesma forma, a LGPD também prevê aplicação extraterritorial, podendo responsabilizar empresas fora do Brasil quando processam dados de indivíduos brasileiros (LGPD, 2018, Art. 3º).

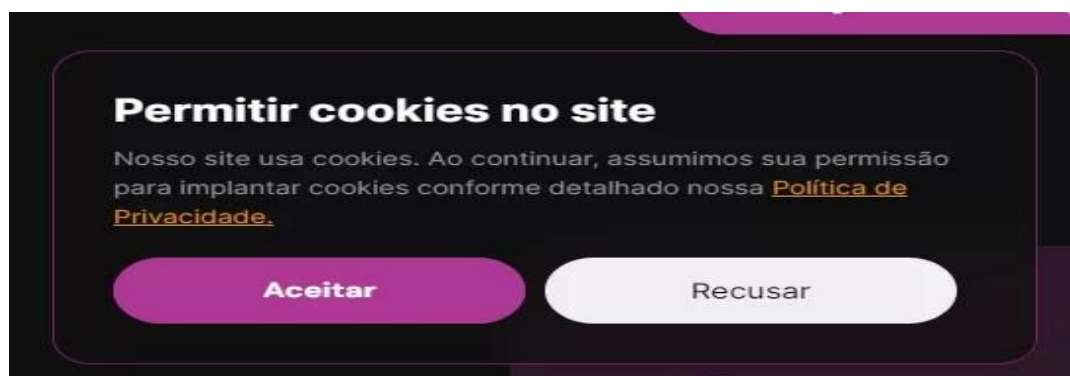
Nesse contexto, é evidente que os fluxos de dados atravessam fronteiras em questão de segundos, e garantir a privacidade dos usuários tornou-se um dos pilares fundamentais para a confiança nas relações internacionais. Para o Brasil, adotar modelos internacionais como o europeu vai além do simples alinhamento normativo, é uma estratégia para fortalecer sua atuação em um ecossistema digital mais seguro e comprometido com a proteção dos direitos fundamentais.

Cookies: aliados ou vilões da privacidade? Avaliando o risco e proteção de dados pessoais

A partir da compreensão das normas e da experiência europeia, percebe-se que os cookies se tornam um exemplo emblemático de como a tecnologia pode beneficiar ou prejudicar a privacidade dos usuários.

Assim, ao visitar um site pela primeira vez, é comum se deparar com uma notificação ou janela pop-up exibindo a seguinte mensagem: “O nosso site utiliza cookies para melhorar a navegação”. Essa declaração é emplamente difundida na web e desempenha um papel crucial na experiência online, registrando os sites visitados pelos usuários e até mesmo os formulários já preenchidos (Figura 1).

Figura 1. Notificação de uso de cookies no site H2K.



Fonte: EDUARDA, Maria. H2K, 2023. Disponível em: <https://h2k.com.br/blog/cookies-de-sites-tudo-que-voce-precisa-saber/>. Acesso em: 11 ago. 2025.

Os cookies desempenham um papel fundamental na melhoria da experiência de navegação, tornando-a mais atrativa e dinâmica. De acordo com Rohr (2010):

O cookie é um recurso básico da web. Ele é criado quando um site solicita ao navegador que uma informação seja armazenada. Por exemplo, quando você faz login em um site, o site pede que o navegador armazene um código. Toda vez que você visitar outra página naquele site, o navegador enviará o código. O site estará preparado para saber que o internauta com aquele código é você e o manterá logado no sistema. É por esse motivo que o chamado roubo de cookies é problematizado. Se um site tem alguma brecha que permite o roubo dos cookies, o código armazenado pode ser injetado no navegador do criminoso, que irá acessar a página como se fosse você. Por motivo de segurança, cada site só pode

ter os próprios cookies, ou seja, a Globo.com só pode ler os cookies criados por sites dela mesma. É preciso um falha de segurança nos sites para permitir a leitura dos cookies.

Desse modo, se um site adota essa prática para coletar e armazenar informações e padrões de uso, é fundamental estar atento. Afinal, no contexto atual da crescente interconexão digital, a coleta de dados por meio de cookies tornou-se uma prática corriqueira na maioria dos sites. Contudo, a amplitude dessas ações suscita preocupações em relação à privacidade e à proteção dos dados pessoais dos usuários. Segundo os preceitos da Constituição de 1988, a dignidade da pessoa humana é um dos fundamentos primordiais da República Federativa do Brasil (Art. 1º, inciso III), evidenciando a importância da proteção dos direitos individuais. Além disso, o inciso X do Artigo 5º da Constituição estabelece:

“São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização por dano material ou moral decorrente de sua violação”.

Por conseguinte, a norma constitucional concede status de direitos fundamentais ao sigilo de dados e à inviolabilidade da intimidade e da vida privada. Desse modo, à medida que a sociedade se depara com as complexidades da tecnologia da informação, a proteção dos dados pessoais surge como uma exigência essencial, respaldada pela própria Constituição Brasileira desde 1988.

Diante desse contexto, é essencial ressaltar que os cookies em si não representam uma ameaça. Os dados armazenados nos cookies dos navegadores são acessíveis pelo próprio usuário. Contudo, uma questão crucial reside na maneira como as empresas os utilizam. Em alguns casos, ocorre um mau uso desses dados, como evidenciado na primeira ação civil pública com base na LGPD, instaurada pelo Ministério Público do Distrito Federal e Territórios. Esta ação buscava impedir que uma empresa comercializasse um banco de dados contendo informações de aproximadamente 500 mil pessoas de São Paulo, sem obter o consentimento para a coleta (BRASIL, 2020). A ação foi indeferida por falta de interesse processual, uma vez que o portal da empresa foi retirado do ar, pressupondo uma adequação aos requisitos legais de proteção de dados pessoais (VITAL, 2020).

Esse fato destacou a importância de regular e fiscalizar rigorosamente o uso de dados por parte das empresas. Tal vigilância é essencial para garantir um tratamento ético e responsável por essas informações. Consequentemente, as regulamentações estipulam que as empresas expliquem detalhadamente o propósito de cada cookie a ser armazenado pelo site, como a informação será utilizada e, em seguida, solicitará a permissão do usuário para sua utilização. Por isso, ao acessar um site, é provável que você se depare com um aviso sobre cookies. Uma forma de garantir a proteção dos seus dados ao aceitar os cookies é sempre ler minuciosamente os termos e as políticas de privacidade contidas nesses avisos. Essa prática torna-se fundamental para garantir que seus dados sejam manipulados de acordo com suas preferências e com a transparência, fortalecendo a proteção de sua

privacidade enquanto navega na internet.

Dessa forma, para a geração de leads, é essencial identificar e fundamentar-se em uma base legal que justifique o uso de dados pessoais. Esta abordagem é fundamental para garantir que toda a obtenção e uso de informações ocorram em conformidade com as diretrizes e disposições estabelecidas pela LGPD. Diante dos riscos e benefícios dos cookies, a conformidade com a LGPD exige práticas transparentes e responsáveis.

Orientações práticas para o uso responsável de cookies: garantindo conformidade e transparência nas empresas

A Lei Geral de Proteção de Dados (LGPD), em seu artigo 5º, define dados pessoais como informações relacionadas a uma pessoa identificada ou identificável, como nome, número de identificação, dados de localização, endereço de IP. Contudo, nem todos os dados coletados por cookies são considerados pessoais. Uma simples visita a um site, por exemplo, não constitui dado pessoal. Entretanto, ao fornecer informações pessoais, como um e-mail, esses dados podem ser armazenados por um cookie, e nesse caso, passam a ser considerados pessoais.

A LGPD exige transparência e justificativa clara no uso de cookies, reforçando os direitos dos consumidores e impondo às empresas a obrigação de tratar informações de forma ética. Trata-se de um arcabouço legal que coloca o consumidor no centro, exigindo clareza sobre o tratamento de dados pessoais.

Carvalho e Ferreira (2018) reforçam essa perspectiva ao afirmar que:

A defesa do consumidor e a proteção de dados pessoais visam proteger o cidadão de um desequilíbrio de poderes que possa afetar a tomada de uma decisão livre, autônoma e informada. Enquanto a defesa do consumidor busca reequilibrar a relação entre consumidor e fornecedor no mercado de bens e consumo, a proteção de dados diz respeito ao reequilíbrio entre controlador dos dados pessoais e o titular, que muitas vezes desconhece como se dá o tratamento de dados, suas finalidades ou os seus possíveis riscos.

Dessa maneira, o consentimento do usuário torna-

se elemento essencial para reequilibrar a relação com os controladores de dados, como sites e plataformas digitais, haja vista que frequentemente o usuário se depara com pop-ups solicitando permissão para o uso de cookies, e a decisão de consentir ou não afeta diretamente a forma como seus dados serão tratados.

Por isso, torna-se crucial a leitura atenta desses avisos, pois o consentimento transparente, respaldado em termos de uso claros e compreensíveis, com opções explícitas ao final, como "Eu aceito", "Concordo" ou "Autorizo", representa a permissão concedida pelo usuário ao site para realizar o tratamento de seus dados. Esse momento de decisão não deve ser subestimado, já que, uma vez aceito, influencia diretamente a forma como as informações pessoais serão coletadas, armazenadas e utilizadas durante uma interação online.

Nesse contexto, o artigo 6º da LGPD, em seus incisos I a X, estabelece princípios fundamentais que devem nortear a utilização de cookies, tais como a finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas no tratamento de informações pessoais.

Portanto, dando início ao princípio da finalidade, este estabelece que o tratamento de dados pessoais deve ter um propósito legítimo, específico e informado ao titular dos dados, visando garantir que as informações sejam coletadas e utilizadas de maneira transparente e alinhada com as expectativas do titular. Isso evita a manipulação ou uso indevido dos dados para propósitos não autorizados.

Por outro lado, o princípio da adequação, enfatiza que o tratamento dos dados deve ser compatível com as finalidades informadas ao titular, significa dizer que as práticas de coleta e uso devem ser apropriadas e proporcionais à finalidade original, sem extrapolar ou desviar do que foi informado ao titular.

Ao se falar do princípio da necessidade, o tratamento de dados deve ser limitado ao mínimo necessário para alcançar a finalidade desejada, isso significa que apenas as informações essenciais para cumprir o propósito informado devem ser coletadas, evitando a coleta excessiva ou irrelevante de dados.

No que se refere ao princípio do livre acesso, este garante ao titular o direito de consultar de forma fácil e gratuita como seus dados estão sendo tratados, incluindo

informações sobre a forma e duração do tratamento, bem como o acesso aos dados pessoais na sua totalidade.

No que tange o princípio da qualidade dos dados, este assegura que os dados pessoais sejam precisos, claros, relevantes e estejam atualizados de acordo com a necessidade e finalidade do tratamento. Isso garante que as informações utilizadas sejam confiáveis e estejam devidamente atualizadas.

Já o princípio da transparência, requer que os titulares de dados recebam informações claras, precisas e facilmente acessíveis sobre o tratamento de seus dados pessoais, incluindo que são os responsáveis pelo tratamento e como podem ser contatados.

O princípio da segurança, exige a implementação de medidas técnicas e administrativas para proteger os dados pessoais contra acesso não autorizado, bem como contra situações acidentais e procedimentos que visam proteger os dados contra potenciais riscos.

No que diz respeito ao princípio da prevenção, este envolve a adoção de medidas para evitar a ocorrência de danos em virtude do tratamento de dados pessoais. Isso inclui a implementação de práticas de segurança e procedimentos que visam proteger os dados contra potenciais riscos.

O princípio da não discriminação, proíbe o tratamento de dados pessoais para fins discriminatórios ou abusivos, garantindo que as informações não sejam utilizadas de forma injusta ou prejudicial para os titulares.

Por fim, o princípio da responsabilização e prestação de contas, este último que exige que os agentes de tratamento de dados demonstrem a adoção de medidas eficazes para cumprir as normas de proteção de dados pessoais e eficácia dessas medidas.

Nessa seara, esses princípios fornecem a base ética e legal para o tratamento de dados pessoais, sendo fundamentais para que empresas utilizem cookies de maneira responsável. Sua observância assegura não apenas o cumprimento da lei, mas também a construção de uma internet mais segura, transparente e confiável.

Construindo uma internet segura e confiável: equilibrando privacidade, proteção de dados e conscientização do uso de cookies

Com esses princípios orientando o uso ético de dados, a construção de uma internet segura e confiável

exige equilibrar privacidade, proteção de dados e educação digital da sociedade. Em uma era em constante evolução, a criação de uma rede confiável transcende a simples adoção de medidas de segurança cibernética robustas. Envolve também a preservação da privacidade, a proteção das informações pessoais dos usuários e a promoção da transparência quanto às tecnologias de rastreamento, incluindo os cookies.

A privacidade online não é apenas uma conveniência, mas sim um direito resguardado pela Constituição Federal do Brasil, um direito fundamental estabelecido no artigo 5º, inciso X 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;

XII - e 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;

O artigo 5º, inciso X da Carta Magna estabelece de forma explícita a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas. Essa salvaguarda constitucional assegura que nenhum indivíduo ou entidade pode invadir ou violar esses aspectos essenciais da dignidade humana sem o devido consentimento ou sem a base legal apropriada. Além disso, o inciso XII, do mesmo artigo, consagra o princípio do sigilo das comunicações, a inviolabilidade desse sigilo é uma garantia fundamental para a preservação da privacidade dos cidadãos. Desse modo, é possível observarmos que ambos os incisos enfatizam a importância da privacidade e da proteção dos dados pessoais. Garantem que as informações íntimas e privadas dos cidadãos sejam preservadas e não sejam violadas sem o devido respaldo legal.

No contexto digital, a utilização de cookies desempenha um papel crucial na experiência do usuário e

na personalização de conteúdo. No entanto, é imperativo que o uso de cookies esteja alinhado com os princípios constitucionais da inviolabilidade da privacidade. Além disso, são essenciais políticas claras de privacidade e a observância dos princípios da Lei Geral de Proteção de Dados (LGPD), passos que são cruciais nessa direção.

Assim, destaca-se a importância de equilibrar a inovação tecnológica com a proteção dos direitos fundamentais dos cidadãos na era digital. Ao fazê-lo, não apenas preservando a integridade e a dignidade dos indivíduos, mas também fortalecendo os alicerces de uma sociedade digital ética, transparente e justa.

Paralelamente, a proteção de dados assume relevância ainda maior no mundo digital. Com a crescente digitalização e armazenamento de informações, a proteção de dados tornou-se uma preocupação crucial.

É válido mencionar um episódio que serviu como um despertar global para a crítica importância da proteção de dados na era digital, o escândalo de Cambridge Analytica em 2018, incidente que expôs informações de milhões de usuários do Facebook, dados que foram acessados e utilizados para influenciar campanhas políticas. Esse episódio não apenas ilustrou a vulnerabilidade dos dados na internet, mas também destacou a necessidade urgente de regulamentações e práticas mais rigorosas de proteção de dados.

Com o advento de leis como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia, governos e organizações têm trabalhado para estabelecer diretrizes claras para a coleta, armazenamento e uso de informações pessoais. Desse modo, é importante frisar que a proteção de dados não é mais uma mera consideração técnica, mas uma responsabilidade ética e legal que recai sobre empresas e organizações que lidam com informações pessoais, trazendo a promoção de uma cultura de transparência e confiança com os usuários.

Assim, o escândalo da Cambridge Analytica é um lembrete contundente de que a proteção de dados não é uma questão trivial, mas sim um pilar fundamental da segurança digital e da integridade dos direitos individuais. É um chamado para a colaboração global entre usuários, empresas e reguladores para garantir que os dados sejam tratados com o máximo de responsabilidade e respeito na era da informação.

Outro ponto relevante é a alfabetização digital do

usuário, que envolve não apenas compreender o funcionamento dos cookies, mas também avaliar os riscos e benefícios do compartilhamento de informações na internet. Como já destacado ao longo deste trabalho, os cookies, quando empregados de forma adequada, podem aprimorar a experiência do usuário, tornando-a mais personalizada e eficiente. Contudo, é essencial que os indivíduos estejam conscientes e detenham controle sobre os dados que decidem disponibilizar no ambiente digital.

Portanto, a construção de uma internet segura e confiável não é uma tarefa unilateral. Requer a colaboração ativa de organizações, usuários e legisladores. Ao equilibrar a privacidade, a proteção de dados e a educação digital da sociedade, podemos criar um ambiente digital mais responsável, transparente e confiável, que beneficie a todos os participantes da rede global.

CONCLUSÃO

Diante de todas as informações repassadas no presente artigo, conclui-se que com o avanço da tecnologia, surgiram desafios significativos relacionados à privacidade e segurança dos dados pessoais, levando à promulgação da Lei Geral de Proteção de Dados (LGPD) em 2020 no Brasil. Além disso, evidencia-se que compreender a importância dos cookies na navegação online é crucial para uma experiência digital mais segura e personalizada. A falta de conhecimento sobre esses

pequenos arquivos de texto pode resultar em sérias desvantagens para os usuários, desde a perda de controle sobre a privacidade até uma experiência de navegação menos eficiente.

AGRADECIMENTOS

Agradecemos primeiramente a Deus, cuja infinita graça nos permitiu alcançar este objetivo, iluminando nossos caminhos e fortalecendo nossa fé. Manifestamos também nossa profunda gratidão aos nossos pais, pelo apoio incondicional, amor e incentivo em cada etapa dessa caminhada.

Ressaltamos ainda que este trabalho foi desenvolvido em coautoria com a Professora e Advogada Luana Brandão Ribeiro, pós-graduada em Direito Processual Civil e Direito Público, cuja experiência e comprometimento foram fundamentais não apenas para a construção deste artigo, mas também para nosso crescimento profissional. Registrar essa parceria é, ao mesmo tempo, uma honra e um motivo de sincera gratidão.

Por fim, gostaríamos de registrar nosso especial agradecimento ao Dr. Gabriel Arride Costa, especialista em Inteligência Artificial, que gentilmente se mostrou solícito ao compartilhar artigos e notícias que serviram de base relevante para a construção deste trabalho.

REFERÊNCIAS

ANDRADE, Gabriel. LGPD: **Entenda Como Cookies Participam Da Coleta de Dados. Comunique-se**. 2021. Disponível em: <https://www.comunique-se.com.br/blog/lgpd-os-impactos-dos-cookies/>. Acessado em 25/09/2023.

BRASIL. Autoridade Nacional de Proteção de Dados – ANPD. Institucional. Disponível em: <https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional>. Acesso em: 05 ago. 2025.

BRASIL. **Constituição da República Federativa do Brasil, 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 09/09/2023.

BRASIL. **Lei no 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 01/10/2023.

BRASIL. Ministério Público do Distrito Federal e Territórios. **MPDFT ajuíza 1ª ação civil pública com base na LGPD**. MPDFT, Brasília, 22 set. 2020b. Disponível em: <https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2020/12384-mpdft-ajuiza-1-acao-civil-publica-com-base-na-lgpd>. Acesso em: 28/10/2023.

CARVALHO, Diógenes Faria de; FERREIRA, Vitor Hugo do Amaral. **Defesa do consumidor ganha com a nova lei de proteção de dados pessoais**. 15 de agosto de 2018. Disponível em:

<<https://www.conjur.com.br/2018-ago-15/garantias-consumo-defesa-consumidor-ganha-lei-protacao-dados>>. Acesso em: 29/10/2023.

CÁTEDRA, Instituto. *GDPR: o que é e qual a diferença em relação à LGPD?* 2021. Disponível em: <https://idcatedra.com.br/2021/08/gdpr-o-que-e-e-qual-a-diferenca-em-relacao-a-lgpd/>. Acesso em: 18 ago. 2025.

CONSELHO EUROPEU DE PROTEÇÃO DE DADOS (EDPB). *About EDPB*. [s.d.]. Disponível em: <https://edpb.europa.eu/about-edpb/about-edpb>. Acesso em: 6 ago. 2025.

DONDA, Daniel. **GUIA PRÁTICO DE IMPLEMENTAÇÃO DE IMPLEMENTAÇÃO DA LGPD: Conheça estratégias e soluções para adequar sua empresa em conformidade com a lei**. São Paulo: Editora Labrador, 2020.

EDRi – EUROPEAN DIGITAL RIGHTS. Autoridade italiana aplica multa à Clearview AI por monitoramento e tratamento ilegal de dados biométricos de cidadãos italianos. 2022. Disponível em: <https://edri.org/our-work/italian-dpa-fines-clearview-ai-for-illegally-monitoring-and-processing-biometric-data-of-italian-citizens/>. Acesso em: 08 ago. 2025.

LESSIG, Lawrence. *Code* (version 2.0), Nova Iorque: Basic Books, 2006. ISBN-10: 0-465-03914-6. ISBN-13: 978-0-465-03914-2

MOZILLA. MDN web docs. **Cookies HTTP**. Disponível em: <<https://developer.mozilla.org/pt-BR/docs/Web/HTTP/Cookies>>. Acesso em 02/10/2023.

REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS (GDPR). *GDPR-info.eu*, [s.d.]. Disponível em: <https://gdpr-info.eu/>. Acesso em: 6 ago. 2025.

ROHR, Altieres. **'Cookie eterno' pode rastrear internauta e é impossível de apagar**. 2010 Disponível em:

<<https://g1.globo.com/tecnologia/noticia/2010/10/cookie-eterno-pode-rastrear-internauta-e-e-impossivel-de-apagar.html#:~:text=Alguns%20chamam%20os%20cookies%20marcados,deles%20%C3%A9%20ainda%20mais%20perigoso>>. Acesso em: 29/10/2023.

SALESFORCE. **Desvendando os cookies: uma receita para transformar a experiência on-line**. Disponível em: <<https://www.salesforce.com/br/quarta-revolucao-industrial/o-que-sao-cookies/>>. Acesso em 28/10/2023.

UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho*, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados – GDPR). *Jornal Oficial da União Europeia*, L 119, p. 1–88, 4 maio 2016.

VERRUMO, Marcel. **O que são cookies? Super Interessante**. Disponível em:

<<https://super.abril.com.br/tecnologia/o-que-sao-cookies/#:~:text=Provavelmente%20nada.,pessoa%20de%20um%20determinado%20tipo%E2%80%9D.&text=E%20%C3%A9%20exatamente%20essa%20a,um%20pequeno%20arquivo%20de%20texto>>. Acesso em 10/10/2023.