

A proteção da privacidade no ciberespaço: desafios e impactos da Lei Geral de Proteção de Dados no Brasil

Privacy protection in cyberspace: challenges and impacts of the General Data Protection Law in Brazil

JÚLIA MARQUES SANTOS 

Universidade Tiradentes (UNIT), Brasil

RESUMO: Este artigo analisa a eficácia da Lei Geral de Proteção de Dados (LGPD) na garantia do direito à privacidade no ciberespaço. O objetivo é investigar se a legislação brasileira atual é suficiente para enfrentar os desafios impostos pela digitalização acelerada e pela crescente coleta de dados pessoais. Adota-se metodologia qualitativa, com abordagem descritiva, por meio de revisão bibliográfica, análise normativa comparativa e estudo de casos de vazamentos de dados. Os resultados demonstram que, embora a LGPD represente um avanço significativo na proteção de dados, ainda enfrenta barreiras práticas, como a falta de conhecimento da população sobre seus direitos, dificuldades técnicas para implementação por empresas, e limitações estruturais na atuação da Autoridade Nacional de Proteção de Dados (ANPD). A pesquisa destaca ainda a importância da educação digital e da cooperação internacional como estratégias complementares à legislação. Conclui-se que a LGPD é uma ferramenta essencial, mas demanda atualização constante, fortalecimento institucional e políticas públicas integradas para garantir, de forma eficaz, a privacidade e a segurança no ambiente digital.

PALAVRAS-CHAVE: CIBERESPAÇO; DIREITOS FUNDAMENTAIS; LEI GERAL DE PROTEÇÃO DE DADOS; PRIVACIDADE; SEGURANÇA DA INFORMAÇÃO.

ABSTRACT: This article analyzes the effectiveness of the General Data Protection Law (LGPD) in ensuring the right to privacy in cyberspace. The objective is to investigate whether current Brazilian legislation is sufficient to address the challenges posed by rapid digitalization and the growing collection of personal data. A qualitative and descriptive methodology is used, through bibliographic review, comparative normative analysis, and case studies of data breaches. The results show that although the LGPD represents significant progress in data protection, it still faces practical barriers, such as the population's lack of awareness about their rights, technical challenges for companies, and structural limitations in the performance of the National Data Protection Authority (ANPD). The study also highlights the importance of digital education and international cooperation as strategies to complement the legislation. It concludes that the LGPD is an essential tool but requires constant updates, institutional strengthening, and integrated public policies to effectively ensure privacy and security in the digital environment.

KEYWORDS: CYBERSPACE; FUNDAMENTAL RIGHTS; GENERAL DATA PROTECTION LAW; PRIVACY; INFORMATION SECURITY.

1 Introdução

O direito à privacidade é um dos pilares fundamentais da dignidade humana, assegurado pela Constituição Federal Brasileira nos incisos X, XI e XII do artigo 5º. Esse direito abrange a proteção dos dados e informações pessoais, garantindo a cada indivíduo o poder de decidir, de forma livre e consciente, o que deve ser compartilhado ou resguardado em sua vida privada e profissional. No contexto do ciberespaço, proteger a privacidade tornou-se um dos grandes desafios da era digital.

A Lei Geral de Proteção de Dados (LGPD), sancionada em 2018, surge como resposta aos inúmeros desafios impostos pela “terra sem lei” da Internet. Como um marco regulatório, a LGPD não apenas assegura direitos fundamentais e estabelece critérios claros para o manejo de dados, mas também impõe sanções em casos de descumprimento, buscando criar um ambiente digital mais seguro, ético e transparente. Antes de sua promulgação, dispositivos legais, como o Código de Defesa do Consumidor e a própria Constituição Federal, já abordavam aspectos da privacidade e proteção de dados. Contudo, foi com a LGPD que o Brasil instituiu uma legislação específica e abrangente sobre o tema, alinhada às demandas tecnológicas e sociais contemporâneas.

Apesar de sua relevância, a implementação da LGPD ainda enfrenta obstáculos significativos. Vazamentos de dados, fraudes cibernéticas e roubo de identidade são problemas persistentes que afetam tanto indivíduos quanto organizações. No âmbito corporativo, a exposição de informações sensíveis pode minar a credibilidade de empresas e instituições, prejudicando sua reputação e relação com clientes. Além disso, no setor público, falhas na proteção de dados podem comprometer a administração pública brasileira, expondo sistemas governamentais e fragilizando a segurança nacional. Nesse sentido, a promulgação, em 2023, da primeira política nacional de segurança cibernética do Brasil é um passo importante, mas ainda insuficiente diante da complexidade dos desafios impostos pelo ciberespaço.

Esta pesquisa analisa a eficácia da LGPD na proteção de dados pessoais no Brasil, investigando se o marco regulatório é suficiente para enfrentar os desafios da era digital. A problemática centra-se na necessidade de avaliar até que ponto a LGPD, isoladamente, pode assegurar a privacidade e a segurança no ambiente virtual, bem como propor soluções para sua aplicação prática.

O objetivo geral é avaliar a eficácia da LGPD como instrumento de proteção da privacidade no ciberespaço, considerando suas limitações e potencialidades. Os objetivos específicos incluem: explorar os fundamentos jurídicos e históricos da LGPD e seu papel na proteção da privacidade; identificar desafios práticos enfrentados por empresas, indivíduos e instituições públicas na aplicação da lei; comparar a LGPD a marcos regulatórios internacionais, como o GDPR da União Europeia e propor medidas complementares para aprimorar a eficácia da LGPD, incluindo estratégias de educação, transparência corporativa e governança em cibersegurança.

A pesquisa adota uma metodologia qualitativa e descritiva, com base em revisão bibliográfica de artigos acadêmicos, análise de legislações nacionais e internacionais, e estudo de casos de vazamento de dados. Também se considera uma abordagem comparativa para identificar boas práticas internacionais que possam ser adaptadas ao contexto brasileiro.

Este trabalho está estruturado em três seções principais. A primeira aborda os fundamentos teóricos do direito à privacidade e a evolução histórica da proteção de dados, contextualizando o surgimento da LGPD. A segunda explora os aspectos normativos e práticos da LGPD, com ênfase nas obrigações impostas às empresas, nos direitos dos titulares de dados e no papel da Autoridade Nacional de Proteção de Dados (ANPD). A terceira analisa criticamente a eficácia da LGPD, destacando desafios na sua aplicação e propondo medidas que possam fortalecer a proteção de dados no Brasil, especialmente no contexto de um modelo eficaz de governança em cibersegurança.

Dessa forma, espera-se que este estudo

contribua para o debate sobre a proteção de dados no Brasil, não apenas como uma análise teórica, mas como uma proposta prática que reforce a aplicação da LGPD e amplie a conscientização sobre o direito à privacidade. Em um mundo cada vez mais conectado, garantir a segurança e a confidencialidade das informações é fundamental para preservar a dignidade humana e fortalecer a confiança no ambiente digital.

2 O ciberespaço e seus impactos na privacidade

Surgindo a partir da interconexão das redes digitais, abrindo um universo de informações, o Ciberespaço faz parte das tecnologias digitais, permitindo o vínculo entre pessoas, quer elas estejam próximas ou, até mesmo, em outro continente. Essa é uma das grandes reformas que o Ciberespaço proporcionou: uma mudança significativa para a humanidade, criando uma rede global, aproximando e interconectando pessoas e possibilitando uma maior transmissão de conhecimento e informação, em várias áreas da sociedade, transformando a distância, que antes era um obstáculo, para um fato insignificante, trazendo um novo conceito e uma nova relação entre a tecnologia e a sociedade, uma nova maneira de difusão dos pensamentos e da comunicação coletiva.

O Ciberespaço se configura como um meio de socialização do homem que, por meio de relações dialéticas, apropria-se, age sobre este espaço, sendo os instrumentos aplicados a essa rede, os novos meios de o homem conhecer e interagir com diversos contextos globais. Assim, "o computador torna-se uma extensão do corpo humano", conforme explica Nicolaci da Costa (1998, p. 66), bem como o homem pode ter seu corpo fundido ou estendido por tecnologias, hibridizando-se em um organismo protético (Assis, 2010).

Em 1984, na era da Pós-Modernidade, o termo "Ciberespaço" teve seu prenúncio, quando inventado e usado, através do escritor William Gibson (1988), em seu livro "Neuromancer", que aborda um enredo em que a tecnologia, apesar de não ser um espaço físico e, sim, virtual, cria uma nova realidade

trazendo, consigo, novos conceitos, estilos, valores éticos e morais e novos princípios, já que a tecnologia, além de ser um espaço de interconexão mundial, fixou suas raízes numa sociedade Pós-Moderna (Assis, 2010).

No decorrer do desenvolvimento da internet, do Ciberespaço e de suas tecnologias que viabilizam a complementação desse espaço, a sociedade da época passou a identificar-se como sociedade da "era da informação". Com a ampliação do acesso à internet, buscou-se simular, ao máximo, a sociedade no estilo já conhecido, com o objetivo de atrair um maior público. Essa realidade agregou uma nova forma de socialização e trouxe, como aspecto central, modificações nas formas de relacionamento, encontros, com aspectos afetivos e cognitivos atrelados, ressaltando que, até há pouco tempo, as relações sociais se restringiam ao campo 'corpo presente' e, hoje, esse corpo se desloca, transcende à corporeidade para fundar um plano virtual de encontros (Honorato, 2006).

O Ciberespaço não é nada mais nada menos que uma comunidade virtual onde se permite que pessoas, independente de sua localização geográfica e espaço, criem vínculos sociais. Sua organização gira em torno de um conjunto de pessoas que criam laços e conexões sociais, contribuindo e agregando para produção de informações subjetivas, devido ao modo de interatividade que diverge dos grupos de equipes tradicionais.

A interação promovida pelo homem, com esse novo território (Ciberespaço), o impulsionou a imaginar e criar os elementos, a exemplo da linguagem a ser utilizada nesse espaço (Ferreira, 2007). Acerca dessa breve interpretação, pode-se analisar que o homem ultrapassou a materialidade, redimensionando o espaço concreto por meio da conectividade, transcendendo a localização, a presença e a forma como se relaciona com o novo mundo, um mundo conectado. Apesar de grande, esse novo mundo é tocável em qualquer ponto, devido a essa nova interatividade do ser humano que pode ser quem desejar e estar onde lhe aprouver.

É evidente que a revolução cibernética tem uma interferência significativa nos mais diversos aspectos da vida rotineira, influenciando tanto negativamente, quanto positivamente, transformando e intensificando a maneira de vivermos, de trabalharmos e de nos relacionarmos nos mais diversos campos. A integração de inúmeros contextos virtuais presentes, no dia a dia, através de diversas maneiras, a exemplo de grupos de web amigos e de web relacionamentos em comunidades virtuais, nos mais diversos segmentos como: educação, medicina, entretenimento, cultura, entre outros. São pontos capazes de criar um espaço de sociabilidade virtual, impactando e criando inúmeros conceitos éticos e morais nas relações humanas.

Como visto, no decorrer da história da existência humana, desde seus primórdios, pode-se enxergar que o homem, no seu processo de busca pelo conhecimento de interiorizar e de exteriorizar o mundo, foi capaz de ir além da materialidade e do espaço geográfico, transmutando o corpo físico, transcendendo espaços-temporais e construindo um corpo abstrato, excedendo o tempo e organização dele (passado, presente e futuro), criando maneiras tecnológicas capazes de “substituir” a natureza corpórea do homem, a transcendência da materialidade, através da concretização do Ciberespaço. Essa reconfiguração das relações humanas em rede recoloca, no plano jurídico, a discussão sobre os vínculos de solidariedade que sustentam a convivência social (Charlot; Machado, 2022).

Quanto ao conceito de privacidade, segundo Fernandez Junior (2014), ela vem se transformando através da evolução do Estado Social: a intimidade, e por seu turno, a privacidade, sempre estiveram ligadas ao sentido de propriedade, fundamentada na ideia de inviolabilidade do patrimônio: leia-se, do indivíduo, em sua casa. A doutrina aponta que a intimidade é derivada do pensamento liberal do século XIX, em que se pretendia, como óbice à tirania do governante, que um mínimo de privacidade fosse concedido à população, obstando, com isso, o abuso de poder pelos governantes. Com o advento do constitucionalismo social, há uma mudança no vetor

de proteção, de uma ideia individualista, passa-se ao plano coletivo e, em decorrência disso, uma preocupação por parte do Estado pode ser sentida para a necessária proteção de direitos fundamentais a todo e qualquer indivíduo contra a ação do poder econômico, estivesse ele onde estivesse, ou seja, de particulares ou do próprio Estado (Fernandez Júnior, 2014).

A privacidade, como já dito anteriormente, é o direito que toda pessoa tem de resguardar-se e manter indevassados os seus dados e as suas informações que lhe digam respeito, protegendo da ingerência alheia na sua vida privada e resguardando a dignidade da pessoa humana, nos permitindo decidir o que pode ser exposto de acordo com a vontade e o livre arbítrio de cada um, concedendo a forma sempre de maneira única e individual. Ela permite que seja possível controlar o acesso a certas pessoas e o seu compartilhamento. Diferente do sigilo, que é um direito constitucional que tem, como função, proteger dados importantes e específicos, não só para pessoas físicas como jurídicas também, com o intuito de garantir uma maior segurança a eles em todos os aspectos (Brasil, 2018).

O papel da privacidade é de extrema importância na sociedade moderna, já que é fundamental para o pleno exercício da liberdade individual, colocando em prática as características da nossa sociedade democrática e fazendo valer os direitos humanos de cada um. Ocorre que o próprio surgimento da Era Digital entregou, como uma de suas consequências, a perda da privacidade, que tem se mostrado uma realidade cada vez mais presente, causando impactos sérios aos cidadãos, devido à coleta e uso de dados de forma exacerbada em uma velocidade desapoderada trazendo, consigo, inúmeros problemas relacionados. Apesar de suas transformações positivas e benefícios, trouxe riscos devido ao seu uso de má-fé por usuários que enxergam a internet como “uma terra sem lei”.

A falta de privacidade faz com que os dados pessoais dos usuários sejam facilmente expostos e utilizados por terceiros sem autorização, para fins ardilosos e de maneiras ilegais. Percebe-se um grande aumento na ocorrência dos ataques cibernéticos, fomentando o surgimento desde o

crime organizado, até à desestabilização política, impondo a necessidade de leis robustas que consigam combater tais ameaças sem comprometer a liberdade fundamental (Trindade, 2024).

Portanto, a partir do momento em que se difundiu o uso de tecnologias de comunicação, em geral, com a possibilidade de divulgação de informações privadas do indivíduo, surgiu, então, essa preocupação de proteger os dados. Conforme Bruno Bioni (2020), é de extrema importância e necessidade que o titular esteja ciente do que acontece com seus dados.

O direito à privacidade teve sua base inicial em meados dos anos 1970, com o surgimento das primeiras leis que abordavam sobre a privacidade e proteção de informações pessoais, predispostas, a exemplo, no Código Civil, no Código do Consumidor e na Constituição Federal.

3 Lei Geral de Proteção de Dados (LGPD)

A Lei Geral de Proteção de Dados – LGPD – Lei n. 13.709 de 14 de agosto de 2018 – foi editada em um cenário de massificação dos dados na rede mundial de computadores, transformando-se a capacidade de uma tendência tecnológica, que organiza os aspectos da nossa vida e os comportamentos em, posteriormente, informações, monitorando, em tempo real, os usuários e levando serviços específicos, baseados nos dados de busca usados pelo usuário. A LGPD regula, assim, os dados comuns que serão tratados no Brasil, assim como a relação da cooperação do Brasil com outros países.

A LGPD conferiu especial importância à necessidade do consentimento do titular, destacada como um dos fundamentos desta legislação (artigo 2º, inciso II). A LGPD emerge com o objetivo de proteger os direitos fundamentais à liberdade, entre eles a privacidade, assim como o respeito à anuência dos cidadãos para disponibilização e tratamento dos seus dados.

Apesar de ser um tema já disposto e assegurado pela Constituição Federal, através do inciso XII, Art. 5º e, em alguns códigos, os legisladores brasileiros

criaram a Lei Geral de Proteção de Dados que dispõe, de maneira detalhada, sobre a proteção de dados pessoais dos cidadãos brasileiros, com o intuito de favorecer o acesso normativo a todos e protegê-los, segundo consta do Art. 17 da Lei Nº 13.709 de 14 de agosto de 2018 (Brasil, 2018) “Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade.”

A LGPD traz consigo princípios fundamentais para o bom funcionamento do sistema jurídico brasileiro em relação à execução da Proteção de Dados, espelhando a essência do direito, da ética, da justiça e da moral. A Lei possui 10 princípios básicos para garantir que os direitos fundamentais sejam garantidos aos cidadãos brasileiros, como podemos observar no Artigo 6º da LGPD, que ao versar sobre as atividades de tratamento de dados pessoais, recomenda-se observar a boa-fé em seus princípios e faz recomendações bem objetivas, ao que se referem quanto à finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas (Brasil, 2018).

O objetivo principal da LGPD é proteger e resguardar os direitos fundamentais de privacidade e liberdade de cada indivíduo e, ao mesmo tempo, garantir o livre desenvolvimento. Aplica-se aos dados das pessoas brasileiras, não só que estejam no Brasil mas, também, que estejam em território estrangeiro, os seus direitos estão resguardados, como podemos ver no art. 3º – “Aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados.” (Brasil, 2018).

A LGPD foi um marco regulatório fundamental no Brasil, estabelecendo diretrizes claras e requisitos específicos e estritos que abarcou, desde os dados mais básicos e simples, até os mais complexos, sensíveis e individuais. Além de garantir e assegurar aos titulares que seus dados, os seus direitos fundamentais de liberdade e de privacidade fossem cumpridos, como dito anteriormente, a Lei também

traz consigo procedimentos claros e especificações necessárias já que seu conteúdo é pessoal, estabelecendo que os dados pertencem ao indivíduo titular e não à empresa que o controla. Já o controlador, deverá sempre solicitar o consentimento específico do titular para o manejo de seus dados (Brasil, 2018).

Vale salientar que a LGPD, teve uma forte influência na sua criação, já que foi inspirada diretamente na “General Data Protection Regulation”, uma legislação europeia de proteção de dados, também conhecida através da sigla “GDPR” que revolucionou a maneira de como os dados pessoais eram tratados na Era digital. A sua origem se deu em meados de 2012, mas sua lei só foi publicada e posta em vigor no ano de 2018. Pode-se dizer que a GDPR é a pioneira em relação à proteção de dados pessoais que reverberou além de sua fronteira e, devido a sua amplitude e conteúdo fundamental para garantia dos direitos básicos, serviu de exemplo para a legislação brasileira, apesar de possuir normas acerca do tema em alguns Códigos.

Até então não havia no Brasil uma legislação específica e voltada à proteção da privacidade e criação de instrumentos que fossem efetivos para o controle de dados e, devido à necessidade e a corrente de eventos envolvendo o mau uso dos dados pessoais, foi se tornando, cada vez mais requisitada, a pressa e urgência na criação e na aprovação da LGPD.

Embora não fosse a única lei que abordasse questões relacionadas ao uso e tratamento de dados, ela foi a primeira legislação com uma estrutura direcionada para regular, de maneira concentrada, as atividades envolvendo o uso de dados pessoais. E, como dito no decorrer, já existiam leis na legislação brasileira quanto à proteção de dados que, apesar de não serem específicas e singulares, já eram um tema muito abordado e essencial para o bom funcionamento da sociedade e segurança dos cidadãos. Em 2012, por exemplo, foi criada a Lei Carolina Dieckmann (12.737/2012), que tipifica e pune os crimes cibernéticos e aborda sobre o uso indevido de dados e imagens pessoais.

Com o início da Era digital e sua disseminação, ficou cada vez mais indispensável diretrizes que abordassem a proteção de dados, uma vez que, nesse contexto da inserção de tecnologias no dia-a-dia, as informações mais pessoais dos indivíduos, como seu gênero, sua idade, ideologias, orientação sexual e, até mesmo, a sua localização, foram correndo o risco de serem expostas, gerando pressão para que houvesse a criação e implementação dessas regulamentações que fossem capazes de garantir a segurança dos indivíduos e protegê-los de eventuais exposições. A LGPD foi uma virada de chave devido aos crescentes e inúmeros tormentos e preocupações com a privacidade dos dados em um novo mundo digital.

Apesar de ter sido baseada e possuir bastante similaridade com a GDPR, a LGPD tem dispositivos que possuem diferenças de suma importância: algumas diferenças sutis e, outras, mais concretas. Apesar de ambas poderem ser adotadas por qualquer pessoa natural ou jurídica, obviamente dentro de suas respectivas áreas de competência e juízo, devido a sua aplicação geográfica, já que uma exerce em território brasileiro e, outra, em território europeu, os seus princípios regentes divergem: enquanto a LGPD tem, como princípios fundamentais, os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização, a GDPR prioriza os princípios da licitude, transparência, limitação das finalidades, minimização dos dados, exatidão, responsabilidade, conservação, integridade e confiabilidade (Modesto, 2021).

Outro ponto de diferença é acerca da relação titular e controlador de dados. A LGPD pleiteia que o controlador execute o trabalho com os dados conforme a orientação e permissão do titular, enquanto a GDPR exige que seja realizado um contrato entre as partes que deixe, de maneira explícita, a respeito do tratamento de dados, sempre possuindo, como requisito, ajustes claros para tal contrato. (Modesto, 2021). Porém, ambas regulamentações enfatizam sobre a importância do consentimento, justamente para garantir que os titulares tenham poder sobre a utilização de seus

dados. Outro exemplo seria referente à avaliação dos riscos ao impacto que pode ser causado. Ambas as leis exigem o relatório que observe, detalhe e exponha os riscos que determinada atividade pode causar à segurança dos dados.

No que se refere às sanções e penalidades previstas nas duas leis, LGPD, art. 52 e GDPR arts. 58 e 83, ambas possuem a mesma cláusula, que estipula multas e processos civis às partes, a depender do evento e da sua gravidade, divergindo apenas no valor de suas multas: uma podendo chegar até 20 milhões de euros e, no Brasil, limitadas a 50 milhões de reais ou 2% do valor final de faturamento da empresa (Modesto, 2021).

Apesar de possuírem mais características e divergências, essas foram apenas algumas diferenças que foram expostas para transmitir e ressaltar que, apesar de suas semelhanças, possuem condutas, princípios e maneiras de execução e interpretação que divergem entre si. Contudo, essas peculiaridades destacam que são regulamentações genéricas de amparo e essenciais que possuem e compartilham do mesmo propósito e alvo, visando e priorizando a proteção e garantia dos direitos fundamentais e de privacidade dos cidadãos. Também que sejam assegurados, transformando a experiência online e garantindo uma maior segurança e controle que seja concordante para a defesa da conformidade, demonstrando compromisso com os usuários e a importância da privacidade nesse novo mundo interconectado.

Segundo Rodrigo Otávio (2020), acerca da implementação da LGPD:

A implementação da LGPD é um reflexo do compromisso do Brasil com a proteção da privacidade e a promoção de práticas responsáveis no tratamento de dados pessoais. À medida que vivemos em um mundo digital em constante evolução, entender a LGPD é essencial para qualquer pessoa ou empresa que lide com dados pessoais. Cumprir essa regulamentação não apenas garante a conformidade legal mas, também, constrói a confiança dos clientes e a reputação empresarial. Portanto, mergulhar nas nuances da LGPD é crucial para todos que desejam navegar, com sucesso, no cenário da privacidade de dados no Brasil.

Em consonância com a citação acima, é de

extrema importância que todos, sejam indivíduos ou empresas, tenham entendimento acerca da LGPD para que ela seja aplicada de maneira ética, adequada e transparente no cenário atual, no qual, a privacidade e segurança da informação são cada vez mais visualizadas e valorizadas, garantindo uma maior proteção.

Diante das mudanças da Era Digital, um mundo completamente globalizado e conectado, não há dúvidas de que a proteção de dados é um dos temas mais imediatos e presentes no âmbito empresarial que necessitam ser enxergados com uma maior urgência. O fluxo intenso de dados e a troca de informação contínua, transforma o ambiente virtual fazendo ser necessária seguir a regulamentação estabelecida. A LGPD trouxe, consigo, um novo panorama onde expõe a importância inegável das organizações e empresas se moldarem a sua norma e princípios trazidos na sua legislação. Mas não é apenas um tópico sobre cumprir regulamentos, também é um tópico sobre o compromisso e a responsabilidade que a empresa pode ter com seu cliente e a proteção de seus dados e sua notoriedade, estruturando uma base sólida e protegida. Vale ressaltar que as organizações que não se encaixarem com os requisitos da LGPD poderão sofrer consequências, não só no âmbito de multas e sanções, como também limitações de suas atividades empresariais. (Brasil, 2018). Sendo assim, se torna um requisito que se não cumprido, afetará diretamente o mercado, já que é um reflexo do mesmo.

A implementação e adaptação da LGPD pode ser um grande obstáculo para as empresas e instituições, pois necessita de planejamento, projetos de implementação, fiscalização e monitoramento das medidas de segurança, além do treinamento devido à equipe e a necessidade básica de conhecimento e informações acerca do tema. Como a LGPD entrou em vigor, de fato, apenas em 2020, ainda é muito comum se deparar com inúmeras empresas brasileiras que não estão devidamente moldadas e ajustadas de acordo com as normas regentes, não cumprindo com as exigências legais cobradas. Essa realidade existente é alarmante e séria, uma vez que essas empresas podem ser punidas e sofrer com as penalidades legais, além de

gerar insegurança para seus clientes e deixá-los expostos. A implementação da

A adequação à LGPD é uma questão não só necessária, mas pertinente e significativa para as empresas.

Um dos principais desafios enfrentados nesse movimento para garantir que a Lei de Proteção de Dados seja seguida é a falta de acesso à informação e conscientização das empresas acerca da importância da Lei. Muitas empresas e seus colaboradores desconhecem não só o material da Lei, como também as consequências do não cumprimento dela e a situação arriscada em que estão se expondo, o que é inadmissível, pois é fundamental que as empresas assimilem que seguir a lei é uma obrigação legal, moral e ética, e suas violações implicam na cominação de punições e de sanções legais, não só danos legais como também de danos ligados à própria imagem e reputação da empresa.

A falta de treinamento dos funcionários e da equipe no panorama da LGPD, é outro grande problema. Se não houver uma capacitação apropriada desses colaboradores, a percepção da importância da proteção de dados e a necessidade de seguirem as imposições da lei, será inviável. Mesmo sendo uma lei relativamente nova, que está em constante processo de mudança e ajuste, é fundamental que a empresa e a equipe permaneçam sempre buscando, se atualizando e se mantendo informados para acompanhar a evolução e o aprimoramento de novas legislações e temas que sejam relevantes para o bom funcionamento da empresa, não só no quesito de buscar aconselhamento legal, mas no aprimoramento interno, se adequando às mudanças tecnológicas, evitando, assim, uma possível exposição. Quanto mais conhecimento tiverem, mais fácil será para se prevenir de futuros e possíveis desastres. Uma empresa que não detiver consigo investimentos na cibersegurança, estará vulnerável a qualquer momento a transgressões e ataques, podendo suceder esses problemas a seus clientes que confiaram seus dados pessoais, gerando danos irreparáveis para ambas as partes.

Por ser algo relativamente novo, o custo para implementação da LGPD pode ser um empecilho grande e caro para as organizações. A implementação da LGPD exige não só conhecimento do tema, mas também aplicações em tecnologia e uma equipe preparada e com o treinamento devido para que estejam aptos a exercerem os papéis que lhe foram conferidos. A depender do tamanho da empresa e da abundância de dados coletados de clientes, esse desafio se duplicará, tendo um aumento significativo nos custos. Essa atitude é necessária, e não deve ser considerada um gasto e, sim, um investimento que irá proporcionar mais segurança aos clientes, a seus dados pessoais e uma maneira de eludir problemas que possam vir a ocorrer no futuro. Sendo uma boa jogada de negócio, é um diferencial positivo, porque quanto mais segurança e comprometimento for demonstrado, mais garantida e positiva será a reputação da empresa, melhorando as estatísticas no mercado de trabalho e captando mais clientes, devido a sua qualidade e especialização.

Além disso, a LGPD requer a designação de um Encarregado de Proteção de Dados, também conhecido como “EPD”, que nada mais é do que uma função que garante que as organizações acatem e respeitem a lei, honrando com a privacidade dos proprietários dos dados. Intimando e notificando violações, o que acaba pressionando as empresas a assegurar a segurança dos dados. Mas, para que exista uma proteção adequada, se fazem necessárias que medidas de segurança sobre as informações pessoais sejam tomadas e mantidas de maneira rígida, para garantir o bom funcionamento das instituições, tornando a implementação de modelos de segurança apropriados que é outro grande desafio para implementação, porque exige um planejamento dos processos internos, estratégias e a capacitação e treinamento da equipe. A proteção apropriada é capaz de auxiliar na edificação de uma sociedade mais ética, justa, honesta e respeitosa com os direitos fundamentais e de privacidade dos cidadãos. Por isso é tão importante que as organizações se empenhem para afrontar esses empecilhos de forma séria e responsável, pois são indispensáveis para obter uma proteção efetiva.

Estar em conformidade com a LGPD significa estar de acordo com suas normas e com seus requisitos e fundamentos que são determinados na regulamentação da lei. Não existe uma maneira que seja exata para assegurar a conformidade com a LGPD, pois cada empresa trabalha de um jeito diferente, manejando seus próprios processos, estruturas e ferramentas da maneira que achar mais efetiva para a gestão de sua organização. A Lei Geral de Proteção de Dados impõe requisitos, dispostos em seus artigos, para regular as coletas, a segurança, a proteção, o tratamento, a divulgação, a movimentação, a exclusão e a movimentação dos dados pessoais. O primeiro passo seria entender o escopo material da lei, avaliar os clientes, as atividades de coletas e ver se a empresa se encaixa nos requisitos da lei e se a própria empresa faz parte da aplicabilidade da LGPD.

A fiscalização no que diz respeito a LGPD será preliminarmente efetivada pela Autoridade Nacional de Proteção de Dados (ANPD) que é um órgão do Governo Federal que tem como propósito, fiscalizar para que o cumprimento da Lei seja garantido, assegurando e zelando a proteção de dados. A Lei Geral de Proteção de Dados especifica a competência da ANPD, além de elaborar diretrizes e fiscalizar casos de irregularidades, como podemos observar no Art. 52 da Lei Geral de Proteção de Dados. (Brasil, 2018).

A coleta e o processamento de dados pessoais abarca dilemas éticos e jurídicos. A ética de dados é uma área que se faz presente, quando o assunto é o uso da LGPD. As empresas têm um grande tesouro em suas mãos, o acesso à coleta e divulgação dos dados pessoais. Apesar de a regulamentação da LGPD gerar uma maior transparência e estabilidade, se seguida de acordo com a sua conformidade, conciliando o uso dos dados pessoais com a garantia do direito fundamental de proteção de dados, os seus valores éticos e morais são tão importantes quanto garantir o uso devido das informações.

No que diz respeito à ética, segundo Cortella (2009, p. 102) afirma que:

É o que marca a fronteira da nossa convivência. É aquela perspectiva para olharmos os nossos princípios e os nossos valores para existirmos juntos; é o conjunto de seus princípios e valores que orientam a minha conduta.

Nesse sentido, segundo o autor Ênio Duarte Fernandez Júnior (2014), afirma:

Se por um lado o acesso a dados é tida como um benefício social, não menos verdade é que seu mau uso, seja por entidades públicas ou entes privados, faz tornar-se imprescindível um aperfeiçoamento das normas de proteção aos dados.

Quadro 1 – Comparativo entre a LGPD e o GDPR

ASPECTO	LGPD (LEI N. 13.709/2018)	GDPR (REGULAMENTO UE 2016/679)
TÉCNICA LEGISLATIVA	65 artigos, com disposições majoritariamente genéricas. O texto final não traz exposição de motivos nem orientações interpretativas do legislador; a justificativa consta apenas do PL 4.060/2012.	99 artigos, com disposições prescritivas e detalhadas, precedidas de 173 considerandos que oferecem conceitos, exemplos e explicações para a interpretação e aplicação do Regulamento.
ÂMBITO DE APLICAÇÃO	Art. 3º: alcança o tratamento realizado no território nacional, o que vise à oferta de bens ou serviços a pessoas localizadas no país e os dados aqui coletados. O art. 4º exclui fins particulares não econômicos, jornalísticos, artísticos, de segurança pública e de investigação penal; para fins acadêmicos incidem apenas os arts. 7º e 11. Há controvérsia quanto a entes despersonalizados, como condomínios.	Arts. 2º e 3º: alcança o tratamento no contexto de estabelecimento na União, a oferta de bens ou serviços a titulares na União e o controle de seu comportamento. Exclui atividades exclusivamente pessoais ou domésticas e a repressão penal. Aplica-se a fins jornalísticos, acadêmicos e artísticos, admitindo derrogações estatais (art. 85). Não suscita dúvida quanto a entes despersonalizados.
PRINCÍPIOS	Art. 6º: boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.	Art. 5º: licitude, lealdade e transparência; limitação das finalidades; minimização dos dados (equivalente à necessidade na LGPD); exatidão; limitação da conservação; integridade e confidencialidade; responsabilidade.

BASES LEGAIS	Art. 7º: dez hipóteses, entre elas consentimento, obrigação legal, políticas públicas, pesquisa, execução de contrato, exercício de direitos, proteção da vida, tutela da saúde, legítimo interesse e proteção do crédito. Dispensa o consentimento para dados tornados manifestamente públicos pelo titular.	Art. 6º: seis hipóteses — consentimento, execução de contrato, obrigação jurídica, interesses vitais, interesse público e legítimo interesse. Não prevê a proteção do crédito como base autônoma nem dispensa expressa para dados manifestamente públicos.
DIREITOS DO TITULAR	Arts. 17 a 22: informação, confirmação, acesso, cópia integral, correção, anonimização, bloqueio ou eliminação, portabilidade, revogação do consentimento, petição à autoridade, oposição, explicação e revisão de decisões automatizadas. Não assegura revisão humana. O direito ao esquecimento não é nomeado, mas o apagamento decorre do art. 18, IV e VI. Exercício gratuito e facilitado (art. 18, §§ 3º e 5º); defesa individual ou coletiva.	Arts. 12 a 22: informação, confirmação, acesso, cópia, retificação, limitação do tratamento, apagamento (direito a ser esquecido, nomeado), portabilidade, reclamação, oposição, explicação e não sujeição a decisão automatizada, além do direito à intervenção humana. Não prevê pedido de anonimização. Gratuito, salvo pedidos infundados ou excessivos (art. 12, 5). Admite mandato a entidade sem fins lucrativos (art. 80).
SANÇÕES ADMINISTRATIVAS	Art. 52: advertência, publicização da infração, bloqueio ou eliminação dos dados, suspensão parcial do banco por até seis meses, suspensão ou proibição do tratamento e multa de até 2% do faturamento, limitada a R\$ 50 milhões por infração. Aplicáveis isolada ou cumulativamente. Órgãos públicos sujeitam-se a todas, exceto multa. Admite acordo em incidentes individuais.	Arts. 58 e 83: advertências e repreensões, limitação temporária ou definitiva, proibição do tratamento e multa de até € 20 milhões ou 4% do volume de negócios anual (infrações graves), ou € 10 milhões ou 2% (demais). Estados-membros podem prever sanções adicionais (art. 84). O total não excede o teto de 4%.
AUTORIDADE DE CONTROLE	A ANPD é órgão da administração pública federal integrante da Presidência da República (art. 55-A), com autonomia técnica e decisória (art. 55-B), mas natureza jurídica transitória, conversível em entidade da administração indireta. Conselho Diretor com mandato de quatro anos (arts. 55-D e 55-E). Funções fiscalizatória, sancionatória, regulatória, educativa e de apreciação de reclamações (art. 55-J).	Cada Estado-membro institui uma ou mais autoridades (art. 51), que atuam com total independência e sem sujeição a influências externas (art. 52). Membros com conhecimento técnico exigido (art. 53) e mandato não inferior a quatro anos (art. 54). Poderes de investigação, correção, consultivos e de autorização (art. 58).
ÓRGÃO CONSULTIVO	Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, órgão consultivo da ANPD.	Não possui órgão equivalente.

Fonte: Adaptado de Modesto (2021).

4 Segurança da informação e privacidade

Atualmente, a segurança da informação e a privacidade se tornaram temas centrais no debate sobre a proteção de dados pessoais e a integridade das informações. Com o avanço das tecnologias e a crescente digitalização das relações sociais, torna-se imprescindível compreender a importância desses conceitos e os desafios que eles apresentam (Modesto, 2021).

A segurança da informação refere-se a um conjunto de práticas e medidas que visam proteger os dados contra acesso não autorizado, divulgação, alteração e destruição. Em um mundo onde

informações sensíveis, como dados financeiros e pessoais estão frequentemente armazenadas em plataformas digitais, a vulnerabilidade a ataques cibernéticos se intensifica. Empresas, governos e indivíduos precisam adotar medidas rigorosas para salvaguardar suas informações, utilizando criptografia, autenticação multifatorial e sistemas de detecção de intrusões (Boesing, 2021).

Por outro lado, a privacidade diz respeito ao direito do indivíduo de controlar suas informações pessoais e decidir como elas são coletadas, armazenadas e utilizadas. A crescente interconexão das redes sociais e aplicativos de mensagens, por exemplo, levanta questões éticas sobre a quantidade de dados que empresas coletam e como esses dados são utilizados. A legislação, como o Regulamento Geral sobre a Proteção de Dados (RGPD) na União Europeia e a Lei Geral de Proteção de Dados (LGPD)

no Brasil, busca estabelecer diretrizes claras sobre a proteção de dados pessoais, mas a implementação e a fiscalização ainda apresentam lacunas significativas (Modesto, 2021).

Segundo Modesto (2021), em nível internacional, a União Europeia é uma das líderes com o RGPD que estabelece normas rigorosas para a coleta, armazenamento e processamento de dados pessoais. O RGPD garante que os consumidores tenham controle sobre suas informações e impõe multas substanciais para violações. Nos Estados Unidos, a abordagem é mais fragmentada, com várias leis federais e estaduais abordando diferentes aspectos da proteção ao consumidor digital. A Lei de Privacidade do Consumidor da Califórnia (CCPA), por exemplo, dá aos residentes da Califórnia o direito de saber quais dados estão sendo coletados sobre eles e a capacidade de solicitar a exclusão dessas informações (Modesto, 2021).

Os desafios enfrentados na segurança da informação e na privacidade são diversos. Um dos principais é a educação e conscientização dos usuários. Muitas vezes, as pessoas subestimam os riscos envolvidos na exposição de suas informações pessoais, resultando em comportamentos que podem comprometer sua segurança. Além disso, o desenvolvimento contínuo de tecnologias, como a inteligência artificial traz, à tona, questões sobre como esses avanços podem ser utilizados para invadir a privacidade e manipular dados (Modesto, 2021; Oas, 2021).

Outra preocupação é a questão da responsabilidade das empresas em proteger os dados que coletam. Incidentes de vazamento de dados e fraudes têm mostrado que, muitas vezes, as organizações não estão suficientemente preparadas para proteger as informações de seus usuários. Isso não apenas compromete a confiança do consumidor, mas também pode resultar em sanções legais e financeiras (Malheiros, 2017).

A segurança da informação e a privacidade são fundamentais para garantir um ambiente digital seguro e confiável. A proteção dos dados pessoais

deve ser uma prioridade não apenas para as empresas e instituições, mas também para os indivíduos. À medida que a sociedade avança para um futuro cada vez mais digital, é essencial que todos os envolvidos – usuários, organizações e governos – trabalhem juntos para criar um ecossistema onde a segurança e a privacidade sejam respeitadas e valorizadas. Somente assim poderemos desfrutar dos benefícios da tecnologia sem abrir mão de nossos direitos fundamentais (Oas, 2021).

As tecnologias de segurança, como a criptografia, os sistemas de monitoramento e as soluções de autenticação multifatorial visam proteger informações sensíveis contra acessos não autorizados. Por exemplo, a segurança garante que dados pessoais, como senhas e informações financeiras permaneçam inacessíveis a invasores. No entanto, a implementação dessas tecnologias, muitas vezes, implica a recolha e o armazenamento de grandes volumes de dados, levantando preocupações sobre quem tem acesso às informações (Figueira, 2016).

Um dos principais desafios relacionados à privacidade é a vigilância em massa. Muitas tecnologias de segurança permitem que governos e empresas monitorem atividades em tempo real, o que, embora possa ser justificado em nome da segurança pública, pode resultar em abusos e na violação da lei. Além disso, a aplicação de tecnologias de segurança em ambientes digitais envolve frequentemente algoritmos e inteligência artificial, que podem perpetuar preconceitos e discriminações. Por exemplo, sistemas de reconhecimento facial têm sido criticados por sua baixa precisão na identificação de pessoas de grupos minoritários, resultando em erros que podem ter consequências graves para os indivíduos afetados (Alves et al., 2015).

Por outro lado, a luta pela privacidade não deve desconsiderar a importância da segurança. A proteção de dados é essencial para evitar fraudes, roubos de identidade e outras ameaças que podem comprometer a vida das pessoas. Assim, é necessário buscar um equilíbrio entre a segurança

proporcionada pelas tecnologias e a proteção da privacidade dos indivíduos. Políticas públicas e regulamentações rigorosas podem ser uma forma eficaz de garantir que o uso de tecnologias de segurança respeite os direitos fundamentais dos cidadãos (Malheiros, 2017).

A segurança da informação é fundamental não apenas para a proteção de dados pessoais, mas também para a manutenção da confiança dos consumidores e a integridade das operações de negócios. A violação de dados pode resultar em perdas financeiras significativas, danos à empresa e, até mesmo, consequências legais.

Um dos casos mais emblemáticos é o vazamento da Equifax, uma das maiores agências de crédito dos Estados Unidos. Em 2017, uma falha em um aplicativo web não atualizado, permitiu que hackers acessassem informações pessoais de cerca de 147 milhões de consumidores. Este incidente expôs a falta de medidas de cibersegurança e destacou a necessidade de atualização constante de sistemas e treinamentos para os funcionários (Portal G1, 2017).

Outro exemplo significativo é o caso do Facebook, que virou centro de controvérsia em 2019, quando dados de milhões de usuários foram expostos devido a uma configuração privada de privacidade. O incidente ressalta a importância da transparência na coleta e uso de dados, bem como a necessidade de as empresas desenvolverem estratégias de segurança. Este escândalo fez o Facebook perder US\$35 bilhões em horas (BBC News Brasil, 2018).

Estes casos revelam várias lições cruciais: em primeiro lugar, a atualização regular de softwares e sistemas é fundamental para proteger dados sensíveis; em segundo lugar, a educação dos funcionários sobre práticas de segurança cibernética pode reduzir o risco de erros humanos que levam a vazamentos. Além disso, as empresas devem adotar políticas claras de transparência e de responsabilidade em relação ao uso de dados dos consumidores. Neste contexto, é crucial que as empresas adotem práticas que garantam a

conformidade com a LGPD.

O primeiro passo para a conformidade com a LGPD é o mapeamento dos dados pessoais que a organização coleta, armazenamento e processo. Esse mapeamento deve incluir informações sobre a origem dos dados, especificamente do seu uso, dos setores que têm acesso a eles e o tempo de retenção (Paraná, 2021).

A educação dos colaboradores é essencial. A implementação de programas de treinamento regulares sobre a LGPD e a importância da proteção de dados ajuda a criar uma cultura organizacional que valorize a privacidade. A formação e capacitação dos colaboradores são essenciais, uma vez que muitos dados evidentes ocorrem por falhas humanas (Paraná, 2021).

Desenvolver políticas claras de privacidade e segurança da informação é fundamental. Essas políticas devem ser detalhadas como a empresa coleta, utiliza, armazena e compartilha dados pessoais. Além disso, é crucial que a organização implemente medidas de segurança, como criptografia e controles de acesso, para proteger os dados contra os indivíduos (Almeida; Santos, 2020).

A colaboração entre setores públicos e privados é crucial para fortalecer a segurança dos dados na internet. A criação de fóruns de discussão e compartilhamento de informações sobre ameaças cibernéticas pode contribuir para um ambiente mais seguro. Além disso, as iniciativas de educação e conscientização da população em geral sobre a proteção de dados pessoais devem ser ampliadas.

5 Considerações finais

A proteção de dados pessoais no ciberespaço é um dos temas mais urgentes e desafiadores da era digital. Em um ambiente caracterizado pela interconectividade global e pela velocidade de avanços tecnológicos, a Lei Geral de Proteção de Dados (LGPD) emergiu como um marco regulatório fundamental para assegurar a privacidade e proteger os direitos fundamentais no Brasil. No entanto,

apesar de seu progresso significativo, a aplicação prática da LGPD ainda enfrenta barreiras estruturais, educacionais e tecnológicas que demandam atenção contínua e estratégias inovadoras.

Esta pesquisa teve como objetivo geral avaliar a eficácia da LGPD na proteção de dados pessoais no Brasil, analisando suas limitações e propondo estratégias para aprimorar sua aplicação. A partir da análise realizada, destacaram-se como pontos fracos que a falta de conhecimento por parte dos cidadãos sobre seus direitos de privacidade e segurança digital é um dos principais obstáculos à implementação eficaz da LGPD. Muitos indivíduos ainda desconhecem práticas básicas de proteção, como a criação de senhas fortes ou a importância da autenticação em duas etapas. A pesquisa ressaltou que campanhas educativas são essenciais para fortalecer a segurança no ambiente digital e empoderar os cidadãos em relação à gestão de seus próprios dados.

A pesquisa evidenciou ainda a necessidade urgente de investimento em infraestrutura tecnológica por parte de organizações públicas e privadas. Ferramentas como criptografia avançada, firewalls e sistemas de monitoramento contínuo são indispensáveis para prevenir vazamentos de dados e ataques cibernéticos. Além disso, a adoção de modelos de governança integrada, inspirados em legislações internacionais como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, pode fortalecer a atuação da Autoridade Nacional de Proteção de Dados (ANPD) e promover maior segurança jurídica.

É de se ressaltar que o ciberespaço, apesar de seus benefícios, expõe indivíduos e organizações a sérios riscos, como fraudes financeiras, roubo de identidade e ataques cibernéticos que comprometem sistemas inteiros. A pesquisa revelou que o armazenamento de dados em servidores na nuvem e a coleta indiscriminada de informações pessoais por empresas e redes sociais agravam essas vulnerabilidades. Essa situação exige regulamentações mais detalhadas e medidas técnicas robustas para proteger dados sensíveis.

O estudo também destacou que violações de dados frequentemente cruzam fronteiras, tornando indispensável a cooperação internacional para harmonizar normas de segurança e proteção de dados. No âmbito local, é crucial que governos, empresas e a sociedade civil trabalhem juntos para implementar soluções que garantam a eficácia da LGPD e fomentem a confiança no ambiente digital.

Esta pesquisa trouxe à tona a relevância da LGPD como um instrumento transformador na governança da privacidade no Brasil, mas também expôs suas limitações. Entre as contribuições mais relevantes, evidenciam-se: a necessidade de criar um ciclo contínuo de revisão e atualização da LGPD para acompanhar os avanços tecnológicos e as novas formas de ameaça à privacidade; a importância de fortalecer a atuação da ANPD, garantindo maior fiscalização e suporte técnico às organizações públicas e privadas; a proposta de integração entre educação digital e inovação tecnológica como elementos-chave para proteger os dados pessoais e promover uma cultura de privacidade.

A questão dos dados pessoais no ciberespaço transcende a esfera técnica, envolvendo também aspectos éticos, sociais e políticos. Embora a LGPD represente um marco significativo, sua eficácia só será plenamente alcançada quando acompanhada por uma governança dinâmica e colaborativa. Em um mundo digital em constante evolução, proteger os dados não é apenas uma questão de conformidade legal, mas um compromisso com a dignidade, a segurança e a confiança dos cidadãos.

Dessa forma, esta pesquisa reforça a importância de consolidar a LGPD como uma ferramenta essencial para o desenvolvimento de um ciberespaço mais seguro e ético. Ao investir em educação, tecnologia e governança, o Brasil poderá avançar em direção a uma sociedade digital que respeite os direitos fundamentais e promova uma convivência digital mais justa e sustentável.

Referências

ALVES, G. M. S.; SOUZA, M. V. R.; SILVA, P. M. O. A importância da segurança da informação no ambiente digital para a saúde. *Revista Gestão.Org*, v. 13, Edição Especial,

ASSIS, E. C. P. de. Ciberespaço e pós-modernidade em *Neuromancer* de William Gibson. In: *Anais do VI ENECULT - Encontro de Estudos Multidisciplinares em Cultura*, Salvador, maio 2010. Salvador: UFBA, FACOM.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Relatório sobre a aplicação da LGPD e seus impactos. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/publicacoes>. Acesso em: 04 nov. 2024.

BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: A função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020.

BOESING, Gustavo. *Tratamento de dados pessoais nas redes sociais: a autonomia da vontade e a autodeterminação informativa*. 2021.

BRASIL - Lei nº 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm.

CHARLOT, Yan Capua; MACHADO, Carlos Augusto Alcântara. Contributos do princípio da fraternidade para uma renovação da formação jurídica e o alcance da justiça social. In: *Direitos Humanos, Fraternidade e Justiça Social na Sociedade em Rede*. [S.l.]: Editora, 2022. <https://doi.org/10.23899/9786589284284.3>.

CORTELLA, Mário Sérgio. Qual é a tua obra? Inquietações, propositivas sobre gestão, liderança e ética. *Petrópolis: Vozes*, 2009. p. 102.

FERNANDEZ JUNIOR, Enio Duarte. Brevíssimo aporte sobre o direito fundamental à privacidade e à intimidade na perspectiva do direito brasileiro sobre a proteção de dados pessoais. In: *Portal Âmbito Jurídico*. 2014

FERREIRA, M. L. (2007). Ser para si e ser para o outro: intersubjetividade e virtualidade, um olhar sobre as comunidades virtuais. *Ciência & Conhecimento*.

FIGUEIRA, Vitor Pinheiro. *Internet das Coisas: Um Estudo sobre Questões de Segurança, Privacidade e Infraestrutura*.

GIBSON, Willian. *Neuromancer*. São Paulo: Aleph, 2023.

HONORATO, E. J. S. (2006). Comunidade Virtual Orkut: uma análise psicossocial. In O. Z. Prado, F. Fortim & L. Cosentino. *Psicologia e Informática: produções do III*

Psicoinfo II. *Jornada do NPPI*. (pp. 31-47). São Paulo: Conselho Regional de Psicologia de São Paulo.

JUS BRASIL. O direito à privacidade na era digital: desafios e implicações jurídicas. Disponível em: <https://www.jusbrasil.com.br/artigos/o-direito-a-privacidade-na-era-digital-desafios-e-implicacoes-juridicas/1971830331>. Acesso em: 04 nov. 2024.

MALHEIROS, Á. F. C. A responsabilidade civil solidária das redes sociais no comércio eletrônico sob a ótica da teoria sistêmica dos contratos.

MODESTO, J. A. O Direito à Privacidade na Sociedade da Informação à Luz da Lei Geral de Proteção de Dados Pessoais: uma Análise da (In)Efetividade da Lei Nº 13.709/2018 no Brasil a Partir do Estudo Comparativo com o Regulamento Geral de Proteção de Dados da União Europeia. *Dissertação (Direito) - Universidade Federal de Alagoas. Faculdade de Direito de Alagoas. Programa de Pós-Graduação em Direito*, Maceió, 2021. 366 p.

NICOLACI-DA-COSTA, Ana Maria. *Na malha da rede: os impactos íntimos da internet*. Rio de Janeiro: Campus, 1998.

OAS (Organização dos Estados Americanos). *Princípios Atualizados sobre a Privacidade e a Proteção de Dados Pessoais*. Departamento de Direito Internacional; Secretaria de Assuntos Jurídicos, 2021. 50 p. Disponível em: https://www.oas.org/en/sla/iajc/docs/Publicacion_Principios_Atualizados_sobre_a_Privacidade_e_a_Protecao_de_Dados_Pessoais_2021.pdf. Acesso em: 30 out. 2024.

OTÁVIO, Rodrigo - OCTO LEGAL. *LGPD e GDPR: Entenda as principais semelhanças e diferenças*. Octo. Legal, 2020. Disponível em: <https://octo.legal/blog/lgpd-e-gdpr/>. Acesso em: 18 nov. 2024.

PARANÁ - CONTROLADORIA GERAL DO ESTADO DO PARANÁ. (2021). *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 31 out. 2024.

SIGILO. *Inclusão digital na era da proteção de dados pessoais*. Disponível em: <https://sigilo.org.br/inclusao-digital-na-era-da-protecao-de-dados-pessoais/>. Acesso em: 04 nov. 2024.

TRINDADE, Bruno Silva; JUNIOR, José Elias Seibert Santana. *Terrorismo cibernético e direitos civis: Explorando os limites do direito cibernético*. *Revista Foco*, v. 17, n. 5, p. e4901-e4901, 2024.

UNIÃO EUROPEIA. Regulamento Geral sobre a Proteção de Dados (GDPR). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679>.

OPEN ACCESS

REVISTA DE PROPRIEDADE INTELECTUAL, DIREITO CONTEMPORÂNEO E CONSTITUIÇÃO (PIDCC)

PREFIXO DOI 10.16928 · ISSN 2316-8080

<https://pidcc.com.br/>

EDITORA-CHEFE

Profa. Dra. Carla Eugenia Caldas Barros 

COMO CITAR · APA

Santos, J. M. (2025). A proteção da privacidade no ciberespaço: desafios e impactos da Lei Geral de Proteção de Dados no Brasil. *Revista de Propriedade Intelectual, Direito Contemporâneo e Constituição (PIDCC)*, 14(1), e20251401005. <https://doi.org/10.16928/e20251401005>

COMO CITAR · ABNT

SANTOS, Júlia Marques. A proteção da privacidade no ciberespaço: desafios e impactos da Lei Geral de Proteção de Dados no Brasil. *Revista de Propriedade Intelectual, Direito Contemporâneo e Constituição (PIDCC)*, v. 14, n. 1, e20251401005, 2025. DOI: 10.16928/e20251401005.

COPYRIGHT © 2025. Autores. Este é um artigo de acesso aberto distribuído sob os termos da licença [Creative Commons Attribution \(CC BY\)](#). O uso, distribuição ou reprodução em outros fóruns é permitido, desde que o(s) autor(es) original(is) e o(s) proprietário(s) dos direitos autorais sejam creditados e que a publicação original nesta revista seja citada, de acordo com a prática acadêmica aceita. Não é permitido nenhum uso, distribuição ou reprodução que não esteja em conformidade com esses termos.