Revista Multidisciplinar do Nordeste Mineiro, v.11, 2025
ISSN 2178-6925
DOI: 10.61164/rmnm.v11i1.4099

ANÁLISE DAS MEDIDAS LEGAIS NO AMBIENTE DIGITAL E SEUS IMPACTOS NOS DIREITOS DOS USUÁRIOS DA REDE MUNDIAL

ANALYSIS OF LEGAL MEASURES IN THE DIGITAL ENVIRONMENT AND THEIR IMPACTS ON THE RIGHTS OF WEB USERS

Luma Marques Matos
Graduanda em Direito, Faculdade de Ensino Superior de Linhares, Brasil
E-mail: luma.m.matos@gmail.com
Alexandre Jacob
Mestre, Faculdade de Ensino Superior de Linhares, Brasil
E-mail: alexandre.jacob10@gmail.com

Recebido: 01/06/2025 – Aceito: 14/06/2025

Resumo:

A salvaguarda da privacidade na internet tornou-se um assunto fundamental na era digital, onde informações pessoais são coletadas, processadas e distribuídas em uma escala sem precedentes. Este artigo examina as principais iniciativas legais implementadas globalmente para proteger a privacidade dos usuários online e suas repercussões nos direitos básicos dos indivíduos. A investigação inclui legislações como o Regulamento Geral sobre Proteção de Dados da União Europeia, a Lei Geral de Proteção de Dados no Brasil, entre outras normas internacionais. O estudo busca responder ao seguinte questionamento quais são os principais desafios e avanços legais na proteção da privacidade dos usuários no ambiente digital, e como essas medidas impactam os direitos fundamentais no Brasil e no mundo? Além disso, o estudo analisa como esses regulamentos influenciam o comportamento das empresas no ambiente digital e a balança entre privacidade e liberdade de expressão. Para analisar os textos, artigos, materiais doutrinários e também legislações, será realizado o método dedutivo-lógico, objetivando analisar como se dará a atuação da aplicação dos conceitos e dispositivos legais.

Palavras-chave: Direito digital. Proteção de dados. Ambiente digital. Normas internacionais. Liberdade de expressão.

Abstract:

Safeguarding privacy on the Internet has become a key issue in the digital age, where personal information is collected, processed, and distributed on an unprecedented scale. This article examines the main legal initiatives implemented globally to protect the privacy of online users and

their impact on the basic rights of individuals. The investigation includes legislation such as the General Data Protection Regulation of the European Union, the General Data Protection Law in Brazil, among other international standards. The study seeks to answer the following question: what are the main legal challenges and advances in protecting the privacy of users in the digital environment, and how do these measures impact fundamental rights in Brazil and worldwide? In addition, the study analyzes how these regulations influence the behavior of companies in the digital environment and the balance between privacy and freedom of expression. To analyze the texts, articles, doctrinal materials, and legislation, the deductive-logical method will be used, aiming to analyze how the application of legal concepts and provisions will take place.

***Keywords**: Digital Law. Data protection. Digital environment. International standards. Freedom of expression.*

1. Introdução

Com o rápido desenvolvimento das tecnologias da informação e comunicação, a internet consolidou-se como um elemento indispensável da vida contemporânea, impactando profundamente o mercado de trabalho, as interações sociais e o acesso à informação. Contudo, esse ambiente digital trouxe consigo novos riscos, sobretudo no que diz respeito à privacidade dos usuários e ao uso inadequado de seus dados pessoais. Nesse contexto, garantir uma proteção jurídica eficaz aos dados tornou-se uma questão urgente e de alcance global, especialmente frente à crescente exploração comercial e aos mecanismos de vigilância digital.

Diante dessa realidade, foram elaboradas diversas normas com o objetivo de regulamentar o uso da internet e assegurar a proteção da privacidade no meio virtual. No Brasil, destacam-se o Marco Civil da Internet (Lei nº. 12.965/2014) e a Lei Geral de Proteção de Dados Pessoais (Lei nº. 13.709/2018), que representam marcos relevantes no ordenamento jurídico digital. Essas legislações estabeleceram garantias, deveres e responsabilidades tanto para os usuários quanto para as empresas e o poder público, buscando harmonizar o direito à privacidade com a liberdade de expressão e os avanços tecnológicos, ao mesmo tempo em que impõem limites à coleta e ao tratamento de informações pessoais.

O desenvolvimento tecnológico e a intensificação da digitalização nas atividades humanas modificaram a forma como nos comunicamos, atuamos no mercado de trabalho e consumimos. Contudo, essa revolução digital apresenta

ISSN 2178-6925
DOI: 10.61164/rmnm.v11i1.4099

desafios consideráveis para a salvaguarda da privacidade pessoal, visto que os dados individuais estão, cada vez mais, expostos à coleta e utilização por empresas e autoridades governamentais. A privacidade, reconhecida como um direito essencial, encontra-se sob risco no mundo digital, o que demanda uma resposta legal forte e eficaz.

Em complemento à análise do cenário nacional, o estudo também aborda normas internacionais, como o Regulamento Geral sobre a Proteção de Dados (GDPR), da União Europeia, e o *California Consumer Privacy Act* (CCPA), dos Estados Unidos, evidenciando um movimento global em favor da proteção da privacidade. Apesar dos avanços normativos, ainda existem entraves consideráveis, como a dificuldade de responsabilização das plataformas digitais, os elevados custos de adaptação por parte das empresas e a constante ameaça representada pelas inovações tecnológicas. Diante disso, este artigo busca compreender de que forma o ordenamento jurídico atual tem enfrentado esses desafios e quais soluções podem ser adotadas para assegurar um ambiente digital mais seguro, ético e equilibrado.

2. Histórico da Internet e Regulação

A internet surgiu em meio ao contexto da Guerra Fria, por volta da década de 1950 e início dos anos 1960. Alguns pesquisadores afirmam que uma das motivações para sua criação foi o medo dos Estados Unidos de que sua infraestrutura de comunicações fosse destruída em um possível ataque nuclear da União Soviética. O ponto de partida para a criação da internet foi um projeto militar norte-americano chamado *Advanced Research Projects Agency Network*, (ARPANET) que traduzido seria “Rede de Agências para Projetos de Pesquisas Avançadas” (Pinheiro, 2024).

A financiadora do projeto foi a empresa ARPA, hoje *Defense Advanced Research Projects Agency* (DARPA), uma agência do Departamento de Defesa dos EUA na época. A ARPA nasceu em 1958, logo após o lançamento do satélite soviético Sputnik, ela foi como uma resposta dos EUA a fim de passar a ideia de superioridade tecnológica para o mundo que se desenvolvia em conhecimento

ISSN 2178-6925
DOI: 10.61164/rmnm.v11i1.4099

científico. O objetivo da ARPANET era criar uma rede de computadores resiliente e descentralizada capaz de sobreviver a possíveis interrupções, inclusive físicas, como a de proteger e garantir a comunicação entre cientistas e militares ao considerar possíveis bombardeios pela União Soviética. Assim, todo trabalho no contexto da Guerra Fria continuaria funcionando mesmo diante de possíveis danos (Pinheiro, 2024).

Foram realizadas pesquisas conjuntas por órgão governamentais, universidades e centros de pesquisa que resultaram na interconexão de computadores em rede, o que permitiu que os usuários envolvidos participassem do aperfeiçoamento de softwares para a internet. Através do software, foi produzida a chamada World Wide Web – Rede Mundial de Computadores, um sistema inicial de hipertexto que poderia ser acrescentado novas informações pelos usuários que tivessem acesso e conexão com a rede.

Em 1994, a Netscape Communications disponibilizou uma nova versão de software na Web, a chamada Netscape Navigator, e em seguida, a então empresa Microsoft lançou o Windows 95 com a Internet Explorer. A Internet moderna surge em 1990 de forma descentralizada, flexível e proporcionando liberdade aos desenvolvedores, solidariedade e cooperação entre os cientistas, engenheiros e estudantes da época que participaram ativamente na sua criação (Ruaro, 2015).

Manuel Castells (2003) analisou a chamada cultura hacker, afirmando que esta nasceu da tradição acadêmica na busca por prestígio e reconhecimento, o que foi algo importante no desenvolvimento da Internet. O autor entende que a cultura hacker diz respeito ao conjunto de valores e crenças que nasceu entre as redes de programadores de computador que interagiam entre si de forma on-line, o que conclui que tal cultura tem por base uma concepção técnica e meritocrática que surge na busca pela excelência e melhoria do desenvolvimento tecnológico, e isso diz sobre liberdade para criar, apropriar e redistribuí-lo na rede. O autor conclui que a liberdade é um valor fundamental para cultura hacker, mas que vem sendo disseminado em diversos setores da sociedade (Castells, 2003).

Há de se considerar que com o avanço da internet na atualidade, a imagem dos hackers foi pintada como vilão virtual a partir da normalização dos

Revista Multidisciplinar do Nordeste Mineiro, v.11, 2025
ISSN 2178-6925
DOI: 10.61164/rmnm.v11i1.4099

crimes cibernéticos. Segundo Guilherme Schmidt (2014), crimes cibernéticos são condutas típicas, antijurídicas e culpáveis praticadas contra ou com a utilização dos sistemas da informática. E, se tratando de tais condutas, nasceu na Web o conceito maligno de *hacker*, o chamado *Black Hat Hacker*, que traduzido são os Hackers de Chapéu Preto, que são criminosos que invadem redes de computadores com intenções maliciosas, como a propagação de malware, no intuito de destruir determinados arquivos, números de cartões ou senhas, e em alguns casos, são evitados em troca de dinheiro, às vezes milhões. Não que tais comportamentos justifiquem a demonização global dos hackers em geral. Ocorre que a figura do hacker tem sido importante no serviço de inteligência governamentais e nas atividades empresariais, principalmente no descobrimento de falhas de segurança a fim de proteger de grandes ameaças virtuais as Pessoas Jurídicas contratantes, e esses profissionais da informática são chamados *White Hat Hackers*, ou, Hacker de Chapéu Branco (Schmidt, 2014).

É necessário separar o joio do trigo para que todos os profissionais de um sistema não sejam condenados e/ou mal-vistos socialmente por conta de criminosos que atuam em benefício próprio. Já é sabido que nas raízes da internet, a figura hacker possui sua relevância no conhecimento científico e aprimoramento técnico da Web, considerado, assim, a base de sua liberdade profissional.

Nota-se que o impacto da internet no meio social atingiu altas proporções, pois as navegações compõem a estrutura organizacional da sociedade, incluindo o mercado, vida pessoal e a busca por informações em mundo que não para de mudar. O acesso à internet tornou-se tão importante que passa a ser um direito básico do cidadão, uma vez que, aqueles que não detém acesso à internet, estarão excluídos de acesso a informação, atualidade, direitos, capacitação e dentre outros.

Como mostra o artigo 7º da Lei nº. 12.965:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I – Inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> II – Inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;

ISSN 2178-6925
DOI: 10.61164/rmnm.v11i1.4099

> III – Inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
> IV – Não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;
> V – Manutenção da qualidade contratada da conexão à internet;
> VI – Informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
> VII – Não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
> VIII – Informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais [...] (Brasil, 2014).

Também, a pessoa do Estado enfrenta dificuldades que põe em xeque sua soberania social e levam a discussão dos danos que um hacker mal-intencionado pode lhe causar. Conclui-se que, se o Estado que é soberano e possui profissionais do bem a seu favor, se preocupa com os impactos negativos que podem ser causadas por hackers maliciosos (Ruaro, 2015), a que segurança virtual o cidadão poderá descansar quanto a sua privacidade?

A internet só chegou no Brasil em 1988 de forma experimental, onde houve uma tentativa de conexão entre o Laboratório Nacional de Computação Científica, situado no estado do Rio de Janeiro e a Universidade de Maryland, situado nos Estados Unidos. Por não haver recursos disponíveis para ser utilizado com a internet para uma conexão de maior qualidade, somente foi possível trocar e-mails e compartilhar arquivos. No final do ano de 1994, a internet foi lançada de maneira experimental para comercialização pela Empresa Brasileira de Telecomunicação (Embratel), que, até então, era uma empresa de economia mista a qual foi criada ainda na ditadura militar.

Entretanto, ainda havia um monopólio na distribuição da internet no Brasil que só foi quebrado em 1995, após um decreto do então Ministro das Comunicações, Sérgio Mota, que permitiu o acesso de empresas privadas na exploração e fornecimento do serviço de internet no Brasil.

Com a popularização do ambiente virtual e a notável relevância na vida da população em geral, o número de usuários foi crescendo gradativamente. O que de início não passou de cinco mil usuários testando o recurso virtual, hoje, o

ISSN 2178-6925
DOI: 10.61164/rmnm.v11i1.4099

Brasil possui mais de 80% da população que detém acesso à internet (Silva; Otávio, 2023).

3. Contexto Histórico e Legal da Proteção da Privacidade

Historicamente, o conceito de privacidade evoluiu ao longo dos séculos, ganhando maior relevância com a Declaração Universal dos Direitos Humanos de 1948, que reconheceu o direito à privacidade como um direito fundamental. No entanto, foi apenas com a revolução digital que as legislações começaram a focar na proteção dos dados pessoais, culminando na adoção de normas específicas para regulamentar o tratamento dessas informações no ambiente digital.

Para compreender a proteção legal da privacidade on-line, é essencial explorar o conceito de privacidade. Pesquisadores como Daniel Solove (2025) apontam que a privacidade deve ser analisada sob diferentes perspectivas, incluindo o controle sobre a distribuição de informações pessoais. Mas foi no ano de 2014 que a primeira Lei federal foi publicada no Brasil, a Lei nº. 12.965/2014, chamada de Marco Civil da Internet, considerada a Constituição da Internet no Brasil.

O acontecimento de repercussão nacional pode ter servido de contexto para o surgimento dessa lei: o vazamento de 30 fotos fotografias pessoais da atriz Carolina Dieckmann, incluindo imagens íntimas, no ano de 2011. Carolina foi alvo de chantagem por parte de um grupo que solicitava o pagamento de R$ 10.000,00 para evitar a publicação das fotos no mundo virtual. Em 2012 foi promulgada a Lei 12.737 que ficou conhecida como a Lei Carolina Dieckmann (MGIS, 2023).

O Marco Civil foi a primeira Lei Federal que regulamentou direitos, deveres e princípios no uso da Internet no Brasil, resguardando a liberdade, privacidade e neutralidade de rede nos ambientes virtuais. Há de se considerar que houve uma demora extensa para que o Brasil tivesse sua própria regulamentação quanto aos comportamentos dos indivíduos nos ambientes virtuais. Em 2016, uma nova lei que regulava sobre a proteção de dados dos usuários foi promulgada, a chamada Lei Gral de Proteção de Dados (LGPD). Essa nova lei não reforçava o Marco

ISSN 2178-6925
DOI: 10.61164/rmnm.v11i1.4099

Civil, mas complementava uma questão que gerava polêmicas na época, o tratamento de dados pessoais. E essa realidade incomodou o Governo e o forçou a tomar medidas quanto a relações dos controladores de dados para com os titulares.

A LGPD é uma norma cuja elaboração surge em um contexto de Governo digital, intitulado Governo eletrônico (e-Gov) até 2016. Este último, por sua vez, foi uma estratégia de modernização do Estado que teve como objetivo melhorar a qualidade de suas informações e fornecer serviços aos cidadãos por meios eletrônicos, reduzindo a burocracia e tornando seus canais de comunicação mais padronizados e acessíveis (MGIS, 2023). Isso se refere ao envolvimento da pessoa do Estado no tratamento de dados por meio do Governo Digital. Para D'Oliveira e Cunha (2024), a LGPD no contexto das políticas de informação é mais um instrumento normativo que traz escopo de aplicação, regras e sanções sobre o uso e armazenamento de informações.

Nela há redistribuição dos recursos de informações que altera e flexibiliza as posições de poder. Isto é um movimento inicial de gestão social da informação produzida acerca do cidadão. Assim, o reflexo político da LGPD é da implementação de um Governo Digital que está envolvido com o mercado de dados. A referida lei passa a atuar como instrumento normativo que apresenta formas de aplicação, regras e sanções sobre o uso e armazenamento da informação.

4. O Marco Civil da Internet, a Lei Geral de Proteção de Dados e a Proteção da Privacidade no Brasil

A análise do Marco Civil da Internet (Lei nº. 12.965/2014) é essencial para o estudo da privacidade online no Brasil. Esta lei regula os direitos e deveres dos utilizadores da Internet, com ênfase na neutralidade da rede, na proteção dos dados pessoais e na privacidade. Além disso, o Marco Civil da Internet estabeleceu regras para o uso da internet, que até então, para muitos cidadãos brasileiros era considerada como “terra sem lei”, já que pelo princípio da legalidade previsto no art. 5º, II da Constituição da República de 1988 e art. 1º do

ISSN 2178-6925
DOI: 10.61164/rmnm.v11i1.4099

Código Penal brasileiro não há crime sem lei anterior que o defina. Na prática, a violação de direitos em ambientes virtuais não constituiria crime típico no ordenamento jurídico brasileiro.

A referida lei é considerada a Constituição da Internet por apresentar artigos essenciais na regulação as relações virtuais que já se inicia no art. 3° apresentando os princípios gerais:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I – Garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II – Proteção da privacidade;
> III – Proteção dos dados pessoais, na forma da lei;
> IV – Preservação e garantia da neutralidade de rede;
> V – Preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI – Responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII – Preservação da natureza participativa da rede;
> VIII – Liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte (Brasil, 2014).

O artigo 7º do Marco Civil garante aos internautas o direito à inviolabilidade da vida privada e da vida privada, além da proteção dos dados pessoais, o que reforça o entendimento constitucional de proteção, mesmo que não esteja taxativo o ambiente virtual em seu texto. A doutrina também reconhece o Marco Civil como um avanço no reconhecimento dos direitos dos usuários da Internet. Autores como Patrícia Peck Pinheiro (2024) afirmam que esta legislação foi pioneira em garantir a proteção específica dos dados pessoais, impondo aos prestadores de serviço de internet a obrigação de armazenar e tratar esta informação de forma segura e transparente.

Para Jesus e Milagre (2016, p.194) “O Marco Civil é considerado uma vitória da sociedade brasileira. Uma reclamação da sociedade civil, em 2009, que repudiou as iniciativas no sentido de criminalizar condutas na Internet, exigindo, antes, que o Congresso desse uma carta de direitos dos internautas”. Nesse sentido, observa-se que os autores apresentam o Marco Civil como uma

Revista Multidisciplinar do Nordeste Mineiro, v.11, 2025
ISSN 2178-6925
DOI: 10.61164/rmnm.v11i1.4099

conquista para sociedade que observava a internet existindo sem regras e quem pudesse punir, na garantia dos seus direitos fundamentais.

O Marco Civil regulamentou as relações na internet de uma forma satisfatória para uma Lei que inaugurou a temática digital e jurídica em país sem referência no assunto. Todavia, a população levantava debates, e um deles era sobre a responsabilização ou não das plataformas digitais por conteúdo de terceiros, o que trouxe à tona debate sobre os artigos 18 e 19 da referida Lei.

> Art. 18 O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros.
> Art. 19 Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.
> §1º A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.
> §2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5º da Constituição Federal.
> §3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais.
> §4º O juiz, inclusive no procedimento previsto no §3º, poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação (Brasil, 2014).

Foi instaurada pela Lei nº. 13.709/2018, sendo o marco legal brasileiro de proteção de dados pessoais de maior importância, onde é aplicável a qualquer procedimento de dados realizado por todo o território nacional. Sendo este, um código inspirado em regulamentações internacionais como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia. A LGPD estabelece a respeito da garantia dos princípios e direitos para os titulares dos dados e deliberando obrigações para empresas e entidades que processam esses dados.

O preceito tem como referência o GDPR e, começou a valer em setembro de 2020, sendo seu desígnio regulamentar a administração de dados pessoais no Brasil. Essa legislação garante aos titulares direitos como acesso, correção,

Revista Multidisciplinar do Nordeste Mineiro, v.11, 2025
ISSN 2178-6925
DOI: 10.61164/rmnm.v11i1.4099

eliminação e portabilidade dos dados, definindo dados pessoais, dados sensíveis e estabelecendo regras claras de consentimento, segurança e transparência no uso dessas informações.

Segundo Silveira; Avelino e Souza (2016, p. 218), "A LGPD surgiu para atender a uma necessidade global de intercambiar dados pessoais de maneira mais segura, mitigando os riscos deste processo", tendo em vista que os serviços disponibilizados na Internet prestados pelas organizações públicas ou privadas transformou a informação em um dos ativos mais valiosos, especialmente dados pessoais.

É entendido que o dado pessoal é capaz de especificar uma pessoa natural, pois ela passa a ser uma pessoa identificável por quem detém tais informações, como nome, gênero, Registro Geral, Cadastro de Pessoa Física, Carteira Nacional de Habilitação, endereço, telefone e etc. Já o dado sensível é aquele capaz que pode fazer da pessoa um alvo de discriminação, pois envolve etnia, religião, vida sexual, dados genéticos e filiação política. O dado anonimizado é aquele que, por si só, não é capaz de identificar o titular da informação. Ao considerar a liberdade do titular ao ceder seus dados ao controlador, é necessário cumprir alguns requisitos para que seus direitos sejam cumpridos a qualquer tempo, de acordo com o art. 18 da Lei nº. 13.709/2018. São eles:

> Art. 18 [...]
> I – Confirmação da existência de tratamento;
> II – Acesso aos dados;
> III – Correção de dados incompletos, inexatos ou desatualizados;
> IV – Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> V – Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
> VI – Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
> VII – Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII – Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> IX – Revogação do consentimento, nos termos do § 5º do art. 8º desta Lei (Brasil, 2018).

Para a doutrina, a Lei em questão representa um importante progresso na proteção da privacidade digital no Brasil, garantindo maior controle dos cidadãos

ISSN 2178-6925
DOI: 10.61164/rmnm.v11i1.4099

sobre suas informações e assim, cria um ambiente jurídico mais seguro para o uso de informações digitais na tecnologia.

5. Considerações Finais

Se reafirma a indispensabilidade de medidas legais vigorosas para a proteção da privacidade no ambiente digital, evidenciando assim o papel central que essas regulamentações encenam na salvaguarda dos direitos fundamentais dos indivíduos no contexto da internet. A arguição executada ao longo do estudo evidenciou que legislações, tanto nacionais quanto internacionais não apenas estabelecem padrões normativos para o tratamento e a proteção de dados pessoais, como também promovem maior transparência e controle aos usuários sobre suas informações pessoais.

Essas medidas legais exercem um impacto direto e positivo na vida dos usuários de rede mundial, visto que ratificam a proteção de seus direitos medulares, limitando práticas abusivas, como a coleta indiscriminada de dados e a exploração comercial não autorizada. Salienta-se ainda, que a criação de um extremo regulamentário eficaz é essencial para o fortalecimento da confiança dos usuários no ambiente digital, coadjuvando assim para um espaço mais ético e responsável.

Todavia, é primordial anuir que a implementação dessas regulamentações também apresenta desafios significativos para as organizações. A carência de concessão impõe a necessidade em investimentos substanciais em tecnologia, reestruturação de processos internos e aperfeiçoamento de colaboradores. Conclui-se então, que, as empresas devem encontrar harmonia entre a garantia da privacidade dos dados e o sustento da capacidade de inovar, o que se demonstra desafiador no atual cenário em que vivemos, de rápidas mudanças tecnológicas.

Em suma, constata-se que as medidas legais focalizadas na proteção da privacidade não somente são fundamentais para a composição de um ambiente digital mais criterioso e respeitoso, bem como para um reflexo da crescente consciência social e jurídica a respeito da importância da privacidade na era da

ISSN 2178-6925
DOI: 10.61164/rmnm.v11i1.4099

informação. O incremento da proteção da privacidade deve ser visto como um compromisso comum, envolvendo governos, empresas e a sociedade civil, objetivando assegurar que o desenvolvimento tecnológico entre em concordância com princípios de responsabilidade, transparência e respeito aos direitos fundamentais dos indivíduos.

6. Referências

BRASIL. **Constituição da República Federativa do Brasil**. Brasília-DF: Senado, 1988. Disponível em: https://tinyurl.com/29ucwd3a. Acesso em: 11 abr. 2025.

BRASIL. **Lei nº. 12.965 de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília-DF: Senado, 2014. Disponível em: https://tinyurl.com/47cw98p9. Acesso em: 30 abr. 2025.

BRASIL. **Lei nº. 13.709 de 14 de agosto de 2018**. Lei geral de proteção de dados pessoais (LGPD). Brasília-DF: Senado, 2018. Disponível em: https://tinyurl.com/mtcea948. Acesso em: 30 abr. 2025.

CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003.

D'OLIVEIRA, Nadine Passos Conceição; CUNHA, Francisco José Aragão Pedroza. Lei geral de proteção de dados (LGPD): a relação entre as políticas e os regimes de informação. **Revista Digital de Biblioteconomia e Ciência da Informação**, v. 22, 2024.

JESUS, Damásio; MILAGRE, José Antônio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

MGIS. Ministério da Gestão e da Inovação em Serviços. **Estratégia de governança digital**: do eletrônico ao digital. Brasília-DF: MGIS, 2023.

PINHEIRO, Patrícia Peck. **Direito digital aplicado 6.0**. São Paulo: Revista dos Tribunais, 2024.

RUARO. R. L. Privacidade e autodeterminação informativa obstáculos ao estado de vigilância? **Arquivo Jurídico**, v. 2, n. 1, 2015.

SCHMIDT, Guilherme. Crimes cibernéticos. **Jus Brasil**, 05 nov. 2014. Disponível em: https://tinyurl.com/yeywmh9c. Acesso em: 30 abr. 2025.

ISSN 2178-6925
DOI: 10.61164/rmnm.v11i1.4099

SILVA, Victor Hugo; OTÁVIO, Murillo. Acesso à internet cresce no Brasil e chega a 84% da população em 2023, diz pesquisa. **G1 Tecnologia**, 16 nov. 2023. Disponível em: https://tinyurl.com/228nxvd5. Acesso em: 30 abr. 2025.

SILVEIRA, Sérgio Amadeu; AVELINO, Rodolfo; SOUZA, Joyce. A privacidade e o mercado de dados pessoais. **LIINC em Revista**, v. 12, n. 2, 2016.

SOLOVE, Daniel. Inteligência artificial e privacidade. **77 Florida Law Review**, v. 1, 2025.