FACULDADE FASIPE CUIABÁ
CURSO DE DIREITO

SAYLLA KATYELE VAZ E SILVA

PROTEÇÃO DA PRIVACIDADE ONLINE E DESAFIOS EMERGENTES: UMA ANÁLISE DO DIREITO DIGITAL NA ERA DA TECNOLOGIA

Cuiabá/MT

2024

CURSO DE DIREITO

SAYLLA KATYELE VAZ E SILVA

PROTEÇÃO DA PRIVACIDADE ONLINE E DESAFIOS EMERGENTES: UMA ANÁLISE DO DIREITO DIGITAL NA ERA DA TECNOLOGIA

Trabalho de Conclusão de Curso apresentado à Banca Avaliadora do Departamento de Direito, da Faculdade Fasipe Cuiabá, como requisito parcial para a obtenção do título de Bacharel em Direito.

Orientador: Prof. Me. Wellington Cavalcanti da Silva.

Cuiabá/MT

2024

SAYLLA KATYELE VAZ E SILVA

PROTEÇÃO DA PRIVACIDADE ONLINE E DESAFIOS EMERGENTES: UMA ANÁLISE DO DIREITO DIGITAL NA ERA DA TECNOLOGIA

Trabalho de conclusão de Curso apresentado à Banca Avaliadora do Curso de Direito – Faculdade Fasipe Cuiabá como requisito parcial para a obtenção do título de Bacharel em Direito.

Aprovado em: ____/____/_____

Me. Wellington Cavalcanti da Silva
Professor Orientador:
Departamento de Direito – FASIPE

Professor(a) Avaliador(a):
Departamento de Direito - FASIPE

Professor(a) Avaliador(a):
Departamento de Direito - FASIPE

Departamento de Direito - FASIPE
Coordenador do Curso de Direito

Cuiabá/MT

2024

DEDICATÓRIA

A todas as pessoas que em minha caminhada demonstraram paciência e carinho.
Em especial, àquelas que me incentivaram a seguir sempre em frente.

AGRADECIMENTOS

- A meus pais;

- Ao professor orientador;

- Aos demais professores do curso de Direito da Fasipe Cuiabá;

- A todos que direta e indiretamente contribuíram para a realização deste trabalho e permitiram o enriquecimento de minha aprendizagem, em especial

EPÍGRAFE

“Eu sei que nada sei” (Sócrates)

SILVA, Saylla Katyele Vaz e. **Proteção da privacidade online e desafios emergentes**: uma análise do direito digital na era da tecnologia. 2023. 48 folhas. Trabalho de Conclusão de Curso – FASIPE Cuiabá.

RESUMO

O objeto do trabalho corresponde ao direito digital e a proteção por privacidade online. A proteção da privacidade online é um tema de grande relevância na era digital, em que a tecnologia está inserida em quase todos os aspectos da vida cotidiana. Com o aumento do uso da internet e de dispositivos conectados, surgem também desafios que exigem uma análise do direito digital. Uma das questões-chave é o equilíbrio entre a coleta de dados e a proteção da privacidade dos usuários. Assim, o problema de pesquisa foi: do presente trabalho foi: Como o direito digital pode proteger a privacidade online em face dos desafios da era tecnológica? Diante desses aspectos, o objetivo da presente pesquisa foi analisar a contribuição do direito digital para cumprimento da proteção à privacidade online, do consumidor. O trabalho se utiliza de abordagem qualitativa, com desenvolvimento de revisão de literatura desenvolvida com fontes que abordam a temática. Este trabalho se justifica pela importância de proteger a privacidade como um aspecto fundamental da liberdade individual e da confiança na tecnologia. A rápida evolução tecnológica gerou lacunas legais que precisam ser abordadas para proteger o interesse público. Estudar essa temática pode contribuir para o debate, conscientização e educação, oferecendo insights e soluções inovadoras para proteger a privacidade online na era atual. Neste sentido, foi de grande valia, a análise de diversas fontes sobre proteção da privacidade online no âmbito do direito digital. Os resultados revelaram os desafios e soluções para proteger os consumidores na era digital, em destaque para a regulamentação da coleta e uso de dados pessoais, enfatizando a necessidade de regulamentos e transparência das empresas. Apesar dos desafios, o direito digital oferece ferramentas adequadas para proteger a privacidade online.

PALAVRAS-CHAVE: Dados pessoais. Internet. Segurança.

SILVA, Saylla Katyele Vaz e. **Online privacy protection and emerging challenges**: an analysis of digital law in the age of technology. 2023. 48 pages. Course Completion Work – FASIPE Cuiabá.

ABSTRACT

The object of the work corresponds to digital law and online privacy protection. Protecting online privacy is a topic of great relevance in the digital age, where technology is embedded in almost every aspect of everyday life. With the increase in the use of the internet and connected devices, challenges also arise that require an analysis of digital law. One of the key issues is the balance between data collection and protecting users' privacy. Thus, the research problem was: of the present work: How can digital law protect online privacy in the face of the challenges of the technological era? Given these aspects, the objective of this research was to analyze the contribution of digital law to complying with online privacy protection for consumers. The work uses a qualitative approach, with the development of a literature review developed with sources that address the topic. This work is justified by the importance of protecting privacy as a fundamental aspect of individual freedom and trust in technology. Rapid technological evolution has generated legal gaps that need to be addressed to protect the public interest. Studying this topic can contribute to debate, awareness and education, offering insights and innovative solutions to protect online privacy in this era. In this sense, the analysis of various sources on the protection of online privacy within the scope of digital law was of great value. The results revealed the challenges and solutions to protect consumers in the digital age, highlighting the regulation of the collection and use of personal data, emphasizing the need for regulations and transparency for companies. Despite the challenges, digital law offers adequate tools to protect online privacy.

KEYWORDS: Personal data. Internet. Security.

SUMÁRIO

INTRODUÇÃO

Nos últimos tempos, a internet se tornou uma ferramenta amplamente utilizada por uma grande parcela da população, trazendo consigo uma série de vantagens, como a facilitação da comunicação entre indivíduos e o acesso rápido e fácil a uma variedade de informações. Como em qualquer aspecto da vida, o uso da internet também acarreta suas próprias consequências, e é essencial tomar precauções adequadas ao compartilhar dados pessoais online.

Dessa forma, é perceptível que, com a popularização da internet e de aplicativos, as pessoas tendem a se distanciar cada vez mais das interações humanas diretas, optando por se conectar predominantemente no mundo digital. Esse fenômeno pode, por sua vez, resultar em uma maior exposição à vulnerabilidade da privacidade e da intimidade dos indivíduos.

Na era da digitalização, é imprescindível que a legislação evolua para proteger os direitos fundamentais, especialmente os direitos digitais, que estão relacionados à liberdade de expressão e à privacidade. Esses direitos digitais envolvem a capacidade das pessoas de acessar, utilizar, criar e publicar conteúdo digital, bem como de interagir com computadores, dispositivos eletrônicos e redes de comunicação (ZANINI, 2023).

Portanto, o advento da tecnologia digital transformou a forma como as pessoas interagem, compartilham e conduzem as vidas. A crescente ubiquidade da internet e o constante avanço das tecnologias digitais geraram inúmeros benefícios, proporcionando facilidades, conveniências e oportunidades inimagináveis anteriormente. Mas, essa revolução tecnológica trouxe consigo desafios, especialmente no que diz respeito à proteção da privacidade online (ZANINI, 2023).

As tecnologias digitais estão redefinindo como os direitos essenciais, a liberdade de expressão e acesso à informação, são exercidos, protegidos e ameaçados. Estão surgindo novos direitos à medida que a sociedade se adapta a essa transformação tecnológica. Consequentemente, a legislação está se ajustando a essa nova realidade, desenvolvendo

marcos regulatórios que promovam os direitos digitais e a cidadania digital, ao mesmo tempo que regulamentam o acesso seguro e transparente à informação online (VIEIRA; BRITO; TOLARDO, 2019).

À medida que a sociedade moderna se torna cada vez mais interconectada, os direitos digitais e a privacidade tornaram-se pontos centrais de discussão. A era da tecnologia trouxe consigo a necessidade de adaptar o arcabouço jurídico existente para garantir que os cidadãos estejam protegidos em um mundo digital em constante evolução (FARIAS, 2020).

A necessidade de salvaguardar os dados pessoais e combater os crimes cibernéticos motivou a promulgação da Lei Geral de Proteção de Dados (LGPD), resultado de uma demanda crescente tanto da sociedade quanto das autoridades brasileiras. Desde o início da década, empresas e indivíduos têm buscado soluções para os desafios da segurança virtual, especialmente diante do aumento do cibercrime (BRASIL, 2018).

A LGPD introduz uma série de conceitos jurídicos inovadores, como dados pessoais e sensíveis, estabelecendo direitos significativos para os titulares dos dados e impondo obrigações específicas para o controle e compartilhamento de informações. Compreende todas as informações relacionadas a pessoas identificadas ou identificáveis, bem como dados sensíveis, como origem racial ou étnica, convicções religiosas, filosóficas ou políticas, informações sobre saúde ou vida sexual, e dados genéticos ou biométricos (MELO, 2022).

Em um mundo cada vez mais digital e interconectado, a proteção dos dados pessoais e a privacidade online tornam-se questões cruciais para garantir os direitos dos cidadãos e promover o desenvolvimento da sociedade. Embora a LGPD e o Marco Civil da Internet representem avanços importantes na regulamentação e proteção dos dados pessoais e da privacidade online no Brasil, ainda é necessário promover uma conscientização e cultura mais amplas sobre a importância da proteção dos dados pessoais e da privacidade online (SOARES, 2020).

A análise da mitigação e fragilidade da privacidade na era digital evidencia o crescente nível de exposição dos cidadãos diante da revolução tecnológica e da velocidade com que as informações são compartilhadas. Ao longo das últimas décadas, a internet tem sido adotada por um vasto número de pessoas, trazendo consigo uma série de benefícios, como a facilitação da interação entre usuários e o acesso rápido e amplo à informação. Sendo assim, é inegável que todas essas vantagens vêm acompanhadas de consequências, sendo essencial tomar precauções adequadas ao utilizar a internet, especialmente ao compartilhar qualquer tipo de dado com outras pessoas (DINIZ, 2016).

Com a popularização da internet e dos aplicativos, observa-se uma crescente desconexão das relações humanas, enquanto as pessoas se tornam mais conectadas ao mundo digital. Essa transição pode resultar em uma maior vulnerabilidade da privacidade e intimidade dos indivíduos. Portanto, é importante destacar que o direito à privacidade é protegido constitucionalmente, sendo um dos direitos e garantias fundamentais assegurados no Brasil.

A proteção da privacidade online é uma questão premente na sociedade contemporânea, em que a tecnologia digital permeia quase todos os aspectos da vida cotidiana. Com o crescente uso da internet, redes sociais, dispositivos móveis e outras plataformas digitais, surge uma preocupação cada vez maior com a segurança e o uso adequado dos dados pessoais dos usuários. O Direito Digital é fundamental na garantia da privacidade online, estabelecendo normas e regulamentações para proteger os direitos individuais e coletivos dos cidadãos em um ambiente virtual em constante evolução. (TEIXEIRA; CHELIGA, 2019).

Portanto, o presente trabalho justifica-se pelo fato de que a proteção da privacidade é essencial para preservar a liberdade individual e garantir a confiança na tecnologia. As lacunas legais resultantes da rápida evolução tecnológica precisam ser abordadas para proteger o interesse público. Sendo assim, estudar sobre a temática pode contribuir para o debate, conscientização e educação, fornecendo informações e soluções inovadoras para proteger a privacidade online na era digital.

Ao fornecer uma compreensão mais aprofundada das complexidades envolvidas na proteção da privacidade online, esta pesquisa pode contribuir para o desenvolvimento de estratégias e mecanismos mais robustos de proteção de dados. A análise dos desafios emergentes e das melhores práticas no campo do direito digital ajudará a orientar formuladores de políticas, profissionais do direito, empresas e usuários finais na promoção de uma cultura de privacidade online responsável e ética. Em última análise, espera-se que este estudo contribua para o avanço do conhecimento e aprimoramento das políticas de proteção da privacidade na era da tecnologia digital.

O problema da pesquisa é: Como o direito digital pode proteger a privacidade online em face dos desafios da era tecnológica?

O objetivo geral foi analisar a contribuição do direito digital para cumprimento da proteção à privacidade online do consumidor. Os objetivos específicos são: descrever a concepção da sociedade da internet e direito digital; discorrer sobre a natureza jurídica dos

dados pessoais; verificar a Lei Geral de Proteção de Dados Pessoais e a interface com a proteção de privacidade.

A pesquisa em questão se caracteriza, quanto à natureza, como uma pesquisa básica, conforme definido por Gil (2019). Esse tipo de pesquisa tem como finalidade principal a busca por novos conhecimentos fundamentais para o progresso da ciência, sem uma aplicação prática imediata como objetivo.

Quanto ao método empregado para a coleta de dados, a pesquisa é categorizada como bibliográfica, pois buscou-se, de maneira interpretativa, fontes primárias e secundárias, como doutrinas, jurisprudência, artigos, manuais e recursos eletrônicos, visando compreender os aspectos essenciais do tema. Trata-se de uma revisão de literatura, que sintetiza conhecimentos e incorpora a aplicação de resultados de estudos relevantes na prática, oferecendo um panorama atualizado sobre a temática específica ao identificar, analisar e sintetizar resultados de estudos independentes sobre o mesmo assunto.

Dessa forma, o estudo adota uma abordagem qualitativa e descritiva, embasada na pesquisa bibliográfica, conduzida por meio da consulta a livros e publicações em periódicos científicos e afins. Foram examinadas e analisadas publicações relacionadas ao tema, com o objetivo de investigar os mecanismos jurídicos destinados a combater os crimes cibernéticos no Brasil. A seleção da literatura foi limitada a trabalhos produzidos no país entre os anos de 2014 e 2024, sendo incluídos apenas os materiais que se alinham com a temática proposta, enquanto os que não se relacionavam foram excluídos do escopo da pesquisa.

1. A EVOLUÇÃO DA TECNOLOGIA DIGITAL

Este capítulo tem como objetivo introduzir e analisar as concepções e características do tema central deste estudo, que é o direito digital e sua relação com a proteção da privacidade online. Foram abordados as definições essenciais, os principais conceitos envolvidos e os aspectos que permeiam esse campo r do direito, especialmente na era digital. Ao compreender as várias fundamentações teóricas e ação do direito digital e da proteção da privacidade online, há um preparo para entendimento dos desafios e as oportunidades que surgem nesse cenário em constante evolução tecnológica.

1.1 A Sociedade na Era da Informação

A rede mundial de computadores passou a exercer influência e relevância significativas nos padrões diários de uma considerável parte da população. É possível afirmar que isso se aplica até mesmo a toda sociedade, uma vez que alterou os métodos de interação, disseminação de dados e participação individual em diferentes níveis, localmente, nacionalmente e globalmente. Dessa forma, a troca de informações e ideias progrediu e se deu de maneira mais fluida e rápida. O diálogo instantâneo, que já era viável por meio do telefone, adquiriu novas dimensões e visualizações graças às redes de internet (MACIEL, 2019).

Conforme Maciel (2019), desde os tempos em que as informações eram registradas em papel até a era dos meios de comunicação como rádio e televisão, a chegada da internet trouxe consigo um aumento significativo no número de indivíduos que não apenas consomem essas notícias, mas também as compartilham e expressam suas opiniões, resultando em uma ampliação do volume de informações e conteúdo disponíveis para serem transmitidos e debatidos. A participação ativa nas redes sociais e em outras formas de mídia proporcionou um novo espaço para a formação de opiniões e ideias, além de influenciar o cotidiano das pessoas.

As tecnologias de informação e comunicação tiveram um impacto profundo no mercado de trabalho, resultando na formação de uma nova estrutura social e na facilitação da troca de conhecimento e execução de tarefas. Levando ao surgimento de novas oportunidades de emprego e à superação das limitações tradicionais dos modelos de organização de redes, já que agora é possível comandar e transmitir virtualmente. Indicando uma nova forma de integração, capitalismo e economia (SARLET, 2018).

Segundo Sarlet (2018), a comunicação social foi impulsionada pela proliferação de espaços de interação instantânea, influenciando a elaboração, disseminação e transmissão de informações políticas. As mídias sociais, por sua vez, tornaram-se ferramentas significativas para atividades ideológicas, ampliando as reações e ações dos indivíduos no debate político.

O surgimento da internet tornou possível que as pessoas expressem suas opiniões de forma dinâmica e direta, e que o fluxo livre de informações seja mais acessível do que nunca. Sendo assim, é importante que toda essa liberdade esteja sujeita a diretrizes legais, garantindo que a liberdade de um não prejudique a do outro. Transforma a dinâmica entre aqueles que criam ideias e aqueles que consomem informações, permitindo que as pessoas compartilhem perspectivas e opiniões, facilitando a formação de novos conhecimentos e o acesso a informações atualizadas de forma contínua (SARLET, 2018).

Os princípios mencionados encontram respaldo na Convenção Americana sobre Direitos Humanos, particularmente em seu artigo 13, que aborda a "Liberdade de pensamento e expressão". Neste dispositivo, é estabelecido que toda pessoa tem o direito fundamental à liberdade de pensamento e expressão. Esse direito compreende a capacidade de buscar, receber e divulgar informações e ideias de qualquer natureza, sem restrições territoriais, seja verbalmente, por escrito, em formato impresso ou artístico, ou por meio de qualquer outro método escolhido pelo indivíduo (OLIVEIRA, 2020).

Sendo assim, o que caracteriza e define a sociedade contemporânea é a utilização da informação, que se destaca pela rápida e eficiente capacidade de processamento e armazenamento de conhecimento. A internet é uma ferramenta fundamental ao integrar indivíduos, ressaltando a importância da inclusão digital, acesso à informação e conhecimento. Como uma plataforma aberta, a rede oferece uma ampla gama de recursos aos usuários, refletindo diretamente na sociedade em conjunto, incluindo o Estado e a economia de maneira geral.

A internet, surgida nos Estados Unidos por volta do início da década de 1970, foi concebida como uma rede de computadores destinada a conectar grupos acadêmicos,

cientistas e o governo federal, incluindo os militares. Seu advento permitiu a ampla circulação de mercadorias e informações, facilitou a comunicação entre pessoas distantes e proporcionou oportunidades para a exposição de pequenas empresas, contribuindo para um aumento no consumo e na dependência de produtos que antes não estavam facilmente acessíveis no cenário globalizado (MOURA; FREIRE, 2019).

De acordo com Oliveira (2020), o progresso da internet propiciou significativo avanço na circulação de mercadorias e informações, além de aproximar indivíduos distantes geograficamente. Abrindo portas para pequenos negócios e impulsionou o consumo, gerando uma maior dependência de produtos anteriormente menos acessíveis. A realização de transferências e pagamentos bancários por meio da internet tornou-se uma prática comum entre empresas e indivíduos inseridos na cadeia globalizada.

O surgimento do crime cibernético coincide com o avanço da tecnologia da informação e a disseminação da internet, que possibilitou a interconexão de computadores e dispositivos móveis em escala global. Com o aumento do uso da internet e a dependência crescente da sociedade em relação à tecnologia, os crimes cibernéticos se tornaram uma ameaça cada vez mais comum e sofisticada, demandando medidas de segurança e uma constante atualização das leis e regulamentos que regem o ambiente digital (MOURA; FREITE, 2019).

Segundo Oliveira (2020), os primeiros indícios de cibercrime remontam ao surgimento da internet e dos primeiros computadores na década de 1970 nos Estados Unidos. Os primeiros delitos virtuais remontam ao período da Guerra Fria, quando sistemas governamentais foram alvo de invasões e espionagem eletrônica.

Na era da tecnologia, internet e ambiente digital, tornou-se imperativo que a legislação se adaptasse para proteger e preservar os direitos dos cidadãos. Sendo criado o Marco Civil da Internet, que trata de maneira significativa o tema em questão. Esta legislação, oficialmente conhecida como Lei n° 12.965, de 23 de abril de 2014, foi criada com o objetivo de estabelecer diretrizes para os usuários da rede. Desde o seu artigo inicial, a norma define princípios, garantias, direitos e deveres para o uso da internet no Brasil, além de fornecer orientações para a União, Estados, Distrito Federal e Municípios (BRASIL, 2014).

O artigo 6° do Marco Civil da Internet, que diz: “na interpretação desta Lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da internet, seus usos e costumes particulares e **sua importância para a promoção do**

desenvolvimento humano, econômico, social e cultural" (BRASIL, 2014, grifo nosso), sendo assim, pode-se dizer que a internet é um direito humano e fundamental.

No artigo 7º da mencionada lei, é estabelecido que a internet é um recurso essencial para o exercício da cidadania, concedendo determinados direitos aos usuários da rede global de computadores em seus diferentes itens. O acesso à conexão deve ser acessível a todos, como assegurado no inciso IV, que proíbe a suspensão da conexão à internet, exceto em caso de inadimplência decorrente do uso da mesma. Esse dispositivo reforça a importância do acesso à internet e adiciona um critério adicional para que esse direito seja considerado fundamental.

Gonçalves (2017) critica o artigo 7º, argumentando que o texto não reforça valores fundamentais e não vai além na declaração dos direitos, deixando de vincular esses direitos diretamente aos fundamentos essenciais. Apesar dessa crítica, ao analisarmos a lei e o contexto deste trabalho, percebe-se que, mesmo que o artigo tenha suas limitações, ele é importante como um dos marcos legais que garantem o acesso à internet como um direito, especialmente ao enfatizar a cidadania e o direito ao acesso à internet.

Dessa forma, Oliveira (2020) destaca que, o acesso à informação é um princípio fundamental estabelecido na Constituição da República Federativa do Brasil de 1988, conforme definido nos artigos 5º, inciso XXXIII, 37, inciso II, parágrafo 3, e no artigo 216, parágrafo 2. A Emenda Constitucional 115/2022 incluiu o inciso LXXIX na Constituição Federal, estabelecendo a proteção de dados pessoais, inclusive nos meios digitais, como um direito fundamental, a ser garantido conforme a legislação vigente. Destaca-se também a Lei nº 12.527, conhecida como Lei de Acesso à Informação, que estabelece diretrizes sobre o acesso à informação e se aplica a todas as esferas governamentais: União, Estados, Distrito Federal e Municípios, encorpando assim o Direito Digital, que foi apresentado na seção a seguir.

1.2 Processo Histórico do Direito Digital

O surgimento do Direito Digital foi motivado pela urgência em regular questões decorrentes do avanço da tecnologia e da ampliação da internet, fatores que causaram transformações significativas nos comportamentos e na sociedade. Esse ramo do direito também foi criado para enfrentar os novos desafios apresentados pela chamada "Sociedade da Informação" (PIMENTEL, 2018, p.3). Ainda segundo Araújo (2017, p. 24), o Direito Digital é

um direito com um “modus operandi diferente, sendo, na verdade, a extensão de diversos ramos da ciência jurídica, que cria novos instrumentos para atender a anseios e ao aperfeiçoamento dos institutos jurídicos em vigor”.

Portanto, o Direito Digital é resultado das interações sociais e da circunscrição dentro e fora do seu ramo de atuação. As rápidas mudanças em um curto espaço de tempo demandam a necessidade de desenvolver uma característica específica: a agilidade na criação de leis para lidar com sociedades altamente informatizadas, devido ao impacto provocado por essa busca por regulamentações normativas.

Com a evolução tecnológica contínua, o Direito acompanha essas transformações para assegurar que os direitos fundamentais, individuais, sociais, trabalhistas, entre outros, sejam plenamente respeitados. Os profissionais jurídicos especializados em Direito Digital são os encarregados de proteger os direitos relacionados à imagem, propriedade intelectual e industrial, segurança da informação e direitos autorais.

Ao longo dos anos, a tecnologia se integrou na sociedade, permitindo que todos tenham acesso instantâneo a uma vasta gama de recursos por meio de dispositivos como celulares, computadores e tablets. Essa integração resultou em uma interconexão global, onde empresas adaptaram seus negócios para alcançar maior visibilidade na internet. Esse crescimento também trouxe consigo desafios como *hacking,* plágio e vazamento de dados pessoais, aumentando as infrações ao Código de Defesa do Consumidor e desrespeito a marcas e patentes. Portanto, quando surgem violações em larga escala, é necessário que o Direito aborde e estude essas condutas para garantir a segurança jurídica (PINHEIRO, 2021).

Segundo Pinheiro (2021), o Direito Digital oferece a oportunidade de aplicar uma série de princípios e soluções já utilizados no ordenamento jurídico brasileiro e internacional, preenchendo lacunas e alcançando resultados satisfatórios. Assim, estabelece uma conexão entre o Direito Codificado e o Direito Costumeiro, utilizando elementos como generalidade, uniformidade, continuidade, durabilidade e publicidade para fundamentar sua atuação.

A jurisprudência, segundo Pinheiro (2021), é incumbida de equilibrar a interação entre conduta e autoridade, um processo que requer uma interpretação precisa do contexto social, estabelecendo regulamentos que assegurem a estabilidade das expectativas por meio de sua efetividade e aceitação, os quais devem integrar e adaptar-se às mudanças por meio de um arcabouço flexível capaz de perdurar ao longo do tempo. Essa evolução nos conduz ao campo do Direito Digital.

1.3 A aplicação do direito digital

O Direito Digital, também conhecido como Direito Virtual, representa uma evolução de todas as áreas jurídicas que se relacionam com a sociedade digital ou o ambiente online. Ele incorpora os princípios e conceitos do direito tradicional, ao mesmo tempo em que introduz inovações em diversas áreas de atuação, como o direito internacional, da propriedade intelectual, constitucional, dos direitos humanos, da bioética, das pesquisas científicas e genéticas, civil, penal, administrativo, tributário, financeiro, ambiental, processual, previdenciário, trabalhista, eleitoral, médico, entre outros (CAMARGO, 2021).

Conforme Araújo (2017), a disciplina jurídica conhecida como Direito Digital é considerada uma área relativamente nova dentro do campo do direito. É comum apontar a Portaria Interministerial 147, de 31 de maio de 1995, emitida pelos ministros da Comunicação e da Ciência e Tecnologia, como o primeiro marco legal nesse domínio, pois regulamentou o uso dos meios da rede pública de telecomunicações para o acesso e a prestação de serviços de conexão à Internet.

Entende-se que o Direito Digital parte do pressuposto de que toda interação envolvendo textos e mídias, seja por ação humana ou por meio de máquinas, resulta em direitos, deveres, obrigações e responsabilidades. Para regular essas relações entre seres humanos e máquinas, o Direito Digital utiliza diversos mecanismos, como analogia, costumes e princípios gerais do direito, a fim de resolver os conflitos que possam surgir. Sendo assim, é importante ressaltar que a internet não é o foco principal do estudo do Direito Digital, mas sim um componente que requer atenção jurídica, assim como todas as outras inovações tecnológicas (PINHEIRO, 2021).

Pinheiro (2021) ressalta as principais características do DD, que incluem celeridade, dinamismo, auto-regulação, escassez de leis formais, embasamento legal na prática habitual, uso de analogia e resolução por arbitragem. Esses elementos o assemelham à *Lex Mercatoria*, que consiste em um conjunto de normas, princípios e práticas derivados do comércio, sem estar estritamente definido em um único sistema jurídico, possuindo alcance global e adaptando-se às leis internas de cada país de acordo com os princípios gerais que regem as relações comerciais e os valores universais do Direito, como a boa-fé, o princípio de dar a cada um o que é seu (*suum cuique tribuere*), o princípio de não prejudicar ninguém (*neminem laedere*) e o princípio de viver honestamente (*honeste vivere*).

O DD utiliza os costumes como base, assim como o Direito Costumeiro, também conhecido como *Common Law*, que se apoia no histórico de decisões de casos concretos para embasar ações judiciais, criando um banco de dados de precedentes com base nos costumes da

sociedade. A prática costumeira deve ser considerada, especialmente no Direito Digital, onde é necessário agilidade para resolver conflitos devido à rápida evolução tecnológica, que pode tornar as tecnologias obsoletas em um curto período de tempo. É fundamental reconhecer que o Direito é um conjunto de comportamentos e linguagens, uma realidade que se torna cada vez mais evidente nos dias de hoje (CAMARGO, 2021).

No que diz respeito ao primeiro elemento caracterizador do Direito Digital, a relação jurídica, seus fundamentos teóricos remontam aos princípios estabelecidos desde a Escola Alemã da Pandectística, no século XIX. Esses princípios implicam na presença de dois sujeitos, um suporte fático e um vínculo de atributividade que os une (LIMA, 2021). As relações jurídicas no âmbito do Direito Digital envolvem tanto aquelas previstas pelo legislador, como um contrato de fornecimento de internet conforme estipulado pelo Marco Civil da Internet (MCI), quanto uma ampla gama de novas relações contratuais e de consumo, anteriormente desconhecidas, que serão identificadas e regulamentadas na prática jurídica. O objeto dessas relações jurídicas são os dados tratados, que podem envolver interesses não apenas econômicos, mas também individuais e difusos (VIDAL, QUINELATO, 2019).

No aspecto dos dados pessoais, conforme definido pela Lei Geral de Proteção de Dados (LGPD), referem-se às informações de titularidade de uma pessoa natural. Segundo Galiano et al (2020), o Direito Digital também compreende dados que não possuem uma titularidade imediata definida, mas que estão inseridos em alguma relação jurídica, como os dados públicos de interesse coletivo, tratados pelo Estado, como os registros de vacinação. Esses dados de interesse difuso também merecem proteção jurídica, especialmente no que diz respeito à transparência e ao acesso público garantido, além da garantia de sua qualidade e integridade, que é responsabilidade da Administração Pública.

O Direito Digital resulta da interação entre as áreas do Direito e da Computação. Assim que o ambiente virtual foi estabelecido, tornou-se necessário desenvolver também o Direito Digital. Embora essa seja a teoria, a prática mostrou-se bastante divergente. Sendo assim, de modo geral, o Quadro 1 traz a apresentação de um breve histórico desse direito no Brasil:

Quadro 1 – Processo Histórico do Direito Digital no Brasil

Período	**Descrição**
Década de 1970	Surgimento das primeiras discussões sobre a proteção de dados pessoais, com influência internacional.
Anos 1980	Promulgação da Constituição Federal de 1988, que reconhece a intimidade, vida privada e imagem das pessoas.

Período	Descrição
Década de 1990	Crescimento da internet e necessidade de regulamentação específica para lidar com questões digitais.
2010	Aumento da preocupação com a privacidade online e discussões sobre a necessidade de uma lei de proteção de dados.
2012	Promulgação da Lei Carolina Dieckmann (Lei nº 12.737/2012)
2018	Sanção da Lei Geral de Proteção de Dados (LGPD), estabelecendo regras para o tratamento de dados pessoais.
2019	Criação da Autoridade Nacional de Proteção de Dados (ANPD) para fiscalizar e aplicar a LGPD.
2020	Entrada em vigor da LGPD, obrigando empresas e órgãos públicos a se adequarem às novas normas de proteção de dados.

Fonte: Autoria própria, com base nas mencionadas legislações, 2024.

O quadro apresenta um resumo cronológico do desenvolvimento do direito digital no Brasil ao longo das décadas, assim evidenciando a trajetória histórica da legislação brasileira no âmbito do DD, demonstrando a evolução das políticas de proteção de dados ao longo do tempo.

A primeira fase da integração do DD na esfera jurídica, em âmbito global, apresenta uma diversidade de abordagens nos diferentes países. Para explorar essa questão, Cantu (2016) propõe uma categorização da terminologia, que varia conforme o estágio de desenvolvimento de cada nação. O Estágio inicial ou básico: observa-se um progresso limitado e uma incipiente evolução da informática jurídica e do DD, devido à pouca relevância atribuída à matéria por parte dos professores de Direito nas universidades, bem como pelos funcionários governamentais. A inclusão da informática jurídica nos currículos das faculdades de Direito ainda está em fase de planejamento, com o intuito de iniciar o desenvolvimento da doutrina nacional.

O Estágio ascendente ou progressivo, caracteriza-se pela distinção clara entre a informática jurídica e o DD, sendo considerados ramos relacionados, porém independentes um do outro. O DD é reconhecido como um ramo autônomo do Direito e é incluído nos currículos das principais faculdades de Direito do país, separado da matéria de informática jurídica. Na Europa, recomenda-se agrupar ambas as áreas sob a concepção de "Informática e Direito", considerando esta definição mais ampla (CANTU, 2016).

O Estágio avançado ou próspero, enfatiza-se a necessidade e importância de um trabalho legislativo no âmbito do DD, com normas específicas que regulamentem sua aplicação, visto que alcançou relevância e reconhecimento na doutrina e jurisprudência. Há

desenvolvimento e consolidação da legislação, doutrina e jurisprudência nacional sobre o DD, com controvérsias de casos práticos tanto em âmbito nacional quanto internacional, chegando à Corte Suprema do país (CANTU, 2016).

Cantu (2016) pontua que o Estágio culminante ou inovador, destaca-se o progresso significativo no desenvolvimento da informática jurídica meta-documental ou decisória, com centros de pesquisa explorando sistemas de inteligência artificial aplicados ao Direito e desenvolvendo teses de doutorado nessa área. Projetos práticos e específicos de utilização da inteligência artificial no Direito estão em desenvolvimento.

Assim, a complexidade multidisciplinar dessa área se dispersa em diferentes interpretações para cada ramo jurídico, resultando na perda de sua autonomia, na falta de consenso doutrinário e na escassez de estudos específicos na formação de profissionais do Direito. Mesmo com essa realidade, é possível vislumbrar avanços, ainda que lentos e ineficientes. A demanda social impulsiona o desenvolvimento por meio de legislações, doutrinas e autonomia para o Direito Digital (CANTU, 2016).

Por ser uma área multidisciplinar, o Direito da Informática passou décadas sem contar com normas específicas no Brasil. Na jurisprudência, sempre que surgia algum problema jurídico virtual, a solução era buscar analogia com o ramo do direito que melhor se adequasse à questão. Se envolvesse crime cibernético, recorria-se ao Direito Penal; se fosse um contrato, acionava-se o Direito Empresarial ou Comercial, e assim por diante. Essa falta de autonomia apenas contribuiu para retardar o avanço brasileiro nessa área (SILVA; SANTOS, 2021).

Nos últimos anos, novas leis e tipificações vêm sendo criadas e aprovadas, tornando o campo do DD um dos mais promissores no mercado. Afinal, a tecnologia continua evoluindo, trazendo consigo não apenas inovações, mas também uma série de novos problemas. Um marco significativo nesse contexto ocorreu em maio de 2011, quando um hacker invadiu o computador pessoal da atriz Carolina Dieckmann, obtendo acesso a diversas fotos íntimas dela. O criminoso então a chantageou, exigindo pagamento para não divulgar as fotos na internet. Diante da recusa da atriz, todas as imagens foram publicadas online, desencadeando uma grande repercussão virtual (SILVA; SANTOS, 2021).

Esse incidente gerou debates acalorados sobre crimes cibernéticos, revelando a falta de normas adequadas para lidar com esses problemas cada vez mais comuns no âmbito jurídico. O clamor popular, amplificado pela mídia, pressionou o sistema judiciário brasileiro a criminalizar condutas praticadas no ambiente virtual. Como resultado desse movimento, o

projeto de lei conhecido como Lei Carolina Dieckmann foi aprovado em tempo recorde, pouco mais de um ano após o ocorrido. A Lei nº 12.737/2012 representa uma alteração no Código Penal Brasileiro, direcionada a crimes virtuais e delitos informáticos, especialmente invasões de computadores e dispositivos eletrônicos sem autorização, marcando assim um avanço significativo para o Direito Digital (BRASIL, 2012; BRASIL, 1941).

Essa legislação impacta o Direito Penal ao introduzir os artigos 154-A e 154-B no Código Penal Brasileiro, além de modificar a redação dos artigos 266 e 298. Ela reflete uma tendência legal em garantir segurança no ambiente virtual, abordando crimes resultantes do uso indevido de informações e materiais pessoais que afetam a privacidade online, como fotos e vídeos (BRASIL, 1941).

Embora haja um consenso público sobre a importância de proteger a privacidade online, a Lei Carolina Dieckmann tem suscitado debates, especialmente devido à sua redação vaga e à falta de aspectos técnicos claros. Por exemplo, não fica claro se a invasão do próprio dispositivo configura crime, o que pode gerar interpretações divergentes entre os profissionais do Direito e, consequentemente, incertezas em casos específicos.

Outro problema é a ausência de especificação sobre o tipo de dispositivo em que o crime pode ser cometido, deixando espaço para interpretações por parte das autoridades judiciais e do Ministério Público. Embora a Lei Carolina Dieckmann represente um marco inicial na proteção dos dados pessoais dos cidadãos contra criminosos virtuais, é evidente que ainda há espaço para aprimoramento da legislação, a fim de eliminar ambiguidades em sua interpretação.

Outro marco importante para o Direito Digital foi a Lei Geral de Proteção de Dados (LGPD) foi elaborada com o propósito de estabelecer diretrizes para o uso de informações pessoais. Ela busca conceder ao titular dos dados o poder de decisão sobre suas próprias informações, tendo um impacto semelhante ao que o Código de Defesa do Consumidor teve quando foi introduzido e passou a vigorar. Hoje em dia, é comum referir-se ao Código de Defesa do Consumidor em diversas situações empresariais, pois praticamente todas as empresas o observam.

A LGPD (2018) segue um trajeto semelhante; porém com uma adoção ainda mais rápida do que a observada com o Código de Defesa do Consumidor (BRASIL, 1990; BRASIL, 2018). Ela se tornou importante para todas as empresas, independentemente de estarem no ambiente online ou offline, sendo desde microempreendedores individuais até multinacionais.

De acordo com a LGPD, é exigido que os Controladores de Dados designem um Encarregado de Dados. Além disso, a legislação estipula que o Encarregado de Proteção de Dados (DPO) seja encarregado de servir como ponto de contato entre a empresa ou órgão público (potenciais controladores), os titulares dos dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD) (BRASIL, 2018).

O DPO tem a responsabilidade de garantir que a empresa esteja em conformidade com a LGPD, é essencial. Esse participa ativamente de todas as operações da empresa, fornecendo opiniões sobre produtos, serviços e processos estabelecidos. Entre suas diversas funções, o DPO avalia se os processos, produtos ou serviços estão em conformidade com a LGPD.

A LGPD, sancionada em 2018, previu um período de adaptação de dois anos para o país se ajustar à nova legislação. Inicialmente, o requisito para o DPO incluía a necessidade de possuir "conhecimento jurídico regulatório", sugerindo que o DPO deveria ser um profissional da área jurídica. Quando uma Medida Provisória foi emitida para criar a ANPD e fazer alterações na redação da LGPD, a parte que exigia "conhecimento jurídico regulatório" foi removida do texto. Essa mudança foi feita para evitar a restrição da atuação do DPO apenas a profissionais jurídicos, ampliando assim as oportunidades para outros profissionais.

A LGPD representa um marco significativo em nosso sistema jurídico no que diz respeito à proteção de dados. À medida que nos aprofundamos no mundo digital, torna-se cada vez mais importante regulamentar o âmbito do Direito Digital. A implementação da LGPD é um passo essencial nesse sentido, refletindo o compromisso em proteger a privacidade e os direitos dos cidadãos em um ambiente virtual em constante evolução (BRASIL, 2018).

2.A PROTEÇÃO DE DADOS NA LEGISLAÇÃO

2.1 A proteção de dados como Direito Fundamental

Os dados pessoais são informações que identificam ou tornam identificável uma pessoa física, direta ou indiretamente. Esta definição envolve uma ampla gama de informações, desde detalhes básicos, como nome e endereço, até dados mais sensíveis, como histórico médico e opiniões políticas (CALSING, 2019).

Os avanços tecnológicos impulsionaram numerosos países a iniciar esforços para regulamentar as novas situações que emergiam, as quais poderiam ameaçar a segurança de seus cidadãos. O movimento em direção à proteção dos dados pessoais teve seu início em 1970, quando a Alemanha promulgou a primeira Lei de proteção de dados. Um ano depois, influenciado por esse marco, foi iniciada a primeira Lei Federal de Proteção de Dados Pessoais, que entrou em vigor no Estado de Hesse em 1979. Desde então, mais de 100 legislações específicas foram implementadas em todo o mundo (AZEVEDO, 2014).

Por muitos anos, o debate girou em torno da possibilidade de regulamentar um espaço virtual que transcende as fronteiras nacionais. A ideia de que seria inviável regulamentar um espaço global prevaleceu por um longo período.

> No Brasil, a discussão envolvia ‘se’ e ‘como’ o espaço virtual devia ser regulado e, nesse sentido, como a utilização da rede surgiu antes de qualquer previsão legal e rapidamente se expandiu e ocupou lugar de destaque no mundo, a primeira providencia para suprir a lacuna jurídica foi lançar mão da analogia, com o uso de velhas regras criadas tendo em vista outras situações, quando possível (AZEVEDO, 2014, p. 91).

Assim, mesmo sem uma legislação específica, o Brasil consagrou em sua Constituição Federal de 1988 - como direitos fundamentais invioláveis - a proteção da intimidade, da vida privada e da imagem das pessoas, além da garantia da inviolabilidade do sigilo de

correspondência. De acordo com Mendes (2014), o artigo 5º, inciso X da Constituição, estabelece esse conjunto de direitos:

> possível extrair uma tutela ampla da personalidade e da vida privada do cidadão, nas mais diversas situações em que ele se encontra. Não faria sentindo excluir exatamente as situações em que a sua vida privada está sujeita a uma maior violação, como é o caso do processamento de dados pessoais. Afinal, muitas vezes, o tratamento de dados configura, hoje, uma ameaça muito mais grave à intimidade e à vida privada do homem médio do que os perigos "tradicionais", [...]. Assim, não há dúvidas de que a Constituição Federal protege o homem médio desses riscos, que raramente ocorrem na vida real, não haveria sentido em negar-lhe a proteção constitucional perante os bancos de dados, que constituem um risco constante e diário para todos os cidadãos (MENDES, 2014, p. 71).

No âmbito jurídico, a natureza jurídica dos dados pessoais envolve diversas questões importantes. Conforme Calsing (2019), os dados pessoais são considerados um elemento relevante para a proteção da privacidade e da dignidade das pessoas. Nesse sentido, eles estão sujeitos a uma série de legislações e regulamentos que visam garantir sua adequada proteção e uso responsável.

Desse modo, é relevante ressaltar que os dados pessoais é um elemento significativo na economia e na sociedade contemporânea. Empresas e governos utilizam essas informações para uma variedade de propósitos, incluindo personalização de serviços, análise de mercado e tomada de decisões políticas. Portanto, a proteção eficaz dos dados pessoais é essencial para promover a confiança dos cidadãos e o funcionamento ético das instituições (SOARES, 2020).

Conforme Soares (2020), a natureza jurídica dos dados pessoais requer uma análise aprofundada dos princípios e conceitos do direito, bem como das legislações específicas aplicáveis. Essa deve considerar não apenas as questões teóricas, mas também os desafios práticos associados à proteção de dados em um mundo digitalizado e interconectado.

A relevância da proteção jurídica dos dados pessoais reside no fato de que esses dados, juntamente com as informações derivadas deles, podem representar virtualmente uma pessoa perante a sociedade. Tanto entidades sociais públicas quanto privadas identificam indivíduos por meio de códigos e números computadorizados, com base nos quais são tomadas decisões que impactam suas vidas e identidades. Portanto, os dados pessoais tornam-se parte integrante da própria identidade do indivíduo, dada sua importância para a representação das pessoas na sociedade moderna (MENDES, 2018).

Segundo Mendes (2014, p.123), a questão de "a quem pertencem os dados pessoais" é considerada uma questão inadequada. A natureza do bem protegido, a personalidade a que os

dados pessoais se referem, requer que a proteção de dados pessoais seja entendida não como um direito de propriedade, mas como um aspecto dos direitos da personalidade. Afinal, o direito à proteção de dados não trata de uma relação de propriedade, ou seja, a relação entre proprietários e seus bens. Trata-se, na verdade, da regulação de uma ordem comunicativa e informacional, que é inerentemente multidimensional, visando equilibrar os direitos de proteção, defesa e participação do indivíduo nos processos comunicativos.

Nesse processo, entende-se que o direito à proteção de dados deve ser concebido não como uma garantia de propriedade, mas como a proteção da personalidade do indivíduo contra os riscos associados à coleta, processamento e circulação de dados pessoais. Na relação entre sujeito de direito e objeto de direito, os dados pessoais funcionam como um reflexo, onde o próprio sujeito se vê refletido, fazendo com que sujeito e objeto se tornem quase uma única entidade (CAMARGO, 2021).

Conforme Mendes (2014), é difícil a manutenção das categorias tradicionais, especialmente aquelas que descrevem os elementos da relação jurídica, especialmente quando lidamos com uma grande quantidade de dados pessoais relacionados a uma única pessoa. Não se trata de transformar os dados pessoais em propriedade funcionalizada ou de reificar a personalidade humana. Portanto, acredita-se que a melhor forma de proteção está na preservação dos próprios direitos da personalidade, priorizando a dignidade humana.

Ainda para Mendes (2014), no que diz respeito à dignidade da pessoa humana, um valor central no ordenamento jurídico brasileiro e um conjunto de direitos, incluindo os dados pessoais, pode ser considerado um dos mais importantes valores constitucionais. A filosofia de Immanuel Kant serve como base para a fundamentação e conceituação da dignidade da pessoa humana no pensamento ocidental, como destacado pela doutrina jurídica mais influente.

Percebe-se que a Constituição Federal de 1988, embora seja considerada como um documento de estabilidade e garantia, também deve ser flexível o suficiente para se adaptar às mudanças, permitindo diversas interpretações. Mendes (2018), argumenta que a Constituição deve ser passível de interpretação, abrindo espaço para o desenvolvimento da história e das necessidades dos cidadãos. Com essas características, é possível encontrar disposições que possam regular a proteção de dados, mesmo em uma constituição elaborada antes das grandes mudanças tecnológicas.

Dessa forma, a Constituição de 1988 estabelece os fundamentos para as futuras leis de proteção de dados no Brasil. Fortes (2016), argumenta que a legislação brasileira inicialmente

abordava a questão da informação através das garantias à liberdade de expressão e do direito à informação, que devem ser equilibradas com a proteção da personalidade e, especialmente, com o direito à privacidade. Diante da ausência de uma legislação específica sobre o tema, é necessário realizar uma interpretação complexa dos dispositivos presentes não apenas na Constituição Federal, mas também em legislações ordinárias e em diversos códigos, como o Civil, Penal e do Consumidor, visando sempre preservar a privacidade e a personalidade do indivíduo.

A Constituição de 1988, influenciada pelo recente fim da Ditadura Militar no país e em resposta aos diversos abusos cometidos pelo Estado durante esse período, introduziu o habeas data como um recurso eficaz utilizado pelos cidadãos contra o Estado. Regulamentado pela Lei 9.507/97, o *habeas data*[1] visa garantir o acesso a informações pessoais que estejam sob posse exclusiva de órgãos governamentais, permitindo até mesmo a correção desses dados pelos cidadãos. Além da Constituição, as legislações dos Códigos Penal, Civil e do Consumidor também abordaram a proteção de dados pessoais, demonstrando a preocupação crescente com os riscos trazidos pelo ciberespaço.

No que se refere ao assunto do habeas data, é relevante mencionar a jurisprudência do Tribunal Regional Federal da 5ª Região:

> TRIBUTÁRIO E CONSTITUCIONAL. HABEAS DATA. DIREITO AO ACESSO DE INFORMAÇÕES. ART. 5º, INCISO LXXII DA CONSTITUIÇÃO FEDERAL. PRECEDENTE DO C. STF 673.707. MANTIDA A CONCESSÃO DA ORDEM.APELAÇÃO IMPROVIDA. 1- Trata-se de habeas data objetivando à certidão informativa, demonstrando a existência ou inexistência de créditos não alocados atinentes aos CNPJ's das impetrantes disponíveis nos sistemas informatizados da Receita Federal. 2- A Lei n.º 12.527/2011, em seu art. 11, estabelece que o contribuinte ter direito ao acesso às informações contidas em órgão ou entidade pública, a qual tem o dever de autorizar ou conceder o acesso imediato às informações ao contribuinte: Art. 11- O órgão ou entidade pública deverá autorizar ou conceder o acesso imediato à informação disponível. 3- A possibilidade do acesso e obtenção de informações do contribuinte constantes em banco de dados da Secretaria da Receita Federal por meio de habeas data é direito consolidado no C.STF, através do julgamento do RE n.º 673.707/MG, ao qual foi atribuída a repercussão geral da matéria. 4- Na hipótese dos autos, o Sistema de Conta Corrente da Secretaria da Receita Federal do Brasil - SINCOR e todos os outros sistemas de dados de informação cadastral do contribuinte registram apontamentos de apoio à arrecadação federal e outras informações ao armazenar os débitos e créditos existentes acerca dos contribuintes. Enquadrando-se, assim, de acordo com o entendimento firmado em sede de repercussão geral, no conceito mais amplo de arquivos, bancos ou registros de dados, entendidos em sentido genérico para abranger tudo que dissesse respeito ao interessado, direta ou indiretamente. Portanto,

[1] como instrumento para a requisição das informações pessoais em posse do poder público, em particular dos órgãos responsáveis pela repressão durante o regime militar e, portanto, não apresentava influência direta da experiência europeia ou norte-americana relativa à proteção de dados pessoais, já em pleno desenvolvimento à época (DONEDA, 2020, p. 24).

> deve assegurar ao contribuinte o acesso a tudo que envolva seu registro como apontamentos, anotações e assentamentos nos órgãos governamentais ou de caráter público, não dificultando este conhecimento. 5- Sentença mantida. Apelação improvida (STF. RECURSO EXTRAORDINÁRIO 673.707 MINAS GERAIS).

Observa-se que, a proteção de dados pessoais também foi abordada de maneira indireta em legislações como a Lei nº 5.534/1968, o Código de Defesa do Consumidor e a Lei 12.527/2011 (lei de acesso à informação), entre outros dispositivos legais. Em síntese, a Lei nº 13.709/2018 representa um marco significativo na proteção de dados no Brasil, trazendo avanços substanciais na garantia desse direito, que é de extrema importância para a sociedade contemporânea.

2.2 O Marco Civil da Internet e a LGPD

O Marco Civil da Internet representa o principal instrumento jurídico que estabelece os princípios, garantias, direitos e responsabilidades para o uso da Internet no Brasil. Em seu Artigo 1º, fica explícito que essa legislação se aplica em todo o território nacional, orientando a atuação das esferas federal, estadual, distrital e municipal. Baseado nos Direitos Humanos e nos princípios consagrados na Constituição Federal de 1988, o Marco Civil da Internet tem como pilar o respeito à liberdade de expressão no uso da internet no país, reconhecendo sua dimensão global (BRASIL, 2014).

No Artigo 2º, é reconhecida a importância do respeito aos Direitos Humanos, ao desenvolvimento da personalidade e ao exercício da cidadania nos ambientes digitais, destacando a pluralidade, diversidade e finalidade social da rede. A normativa também enfatiza, neste estágio inicial, a essencialidade da liberdade de expressão no ambiente virtual brasileiro. Embora possa parecer contraditório ou ambíguo equiparar liberdade de expressão e proteção da privacidade online, é relevante considerar o princípio da proporcionalidade para resolver conflitos entre princípios e regras (QUEIROZ, 2016).

O Artigo 3º apresenta os princípios norteadores do Marco Civil da Internet, incluindo a garantia da liberdade de expressão, comunicação e manifestação de pensamento, a proteção da privacidade e dos dados pessoais, a neutralidade de rede, a segurança da rede, a responsabilização dos agentes conforme suas atividades, entre outros. O documento ressalta, no Artigo 7º, o acesso à internet como um componente essencial para o exercício da cidadania, estabelecendo direitos assegurados aos usuários, como a inviolabilidade da intimidade e da vida privada. O Marco Civil da Internet regula de forma clara e ampla as

relações entre liberdade de expressão e proteção à privacidade no ambiente virtual (BRASIL, 2014).

O Marco Civil da Internet estipula a manutenção da neutralidade da rede, a preservação da estabilidade, segurança e funcionalidade da rede por meio de medidas técnicas alinhadas aos padrões internacionais e o incentivo ao emprego de boas práticas. Também prevê a responsabilização dos agentes conforme suas atividades, conforme estabelecido pela legislação, e a preservação da natureza participativa da rede, assim como a liberdade dos modelos de negócios promovidos na internet, desde que não entrem em conflito com os demais princípios estabelecidos na Lei (BRASIL, 2014).

No Artigo 7º, o documento destaca a importância do acesso à internet como um elemento fundamental para a prática da cidadania, delineando os direitos garantidos aos usuários, como a inviolabilidade da intimidade e da vida privada, com proteção e reparação por danos materiais ou morais resultantes de violações. A legislação ainda estabelece definições sobre a proteção e disponibilização de dados pessoais e do conteúdo de comunicações privadas, com foco na preservação da intimidade, vida privada, honra e imagem das partes envolvidas, evidenciando a abordagem clara e abrangente do Marco Civil da Internet na regulamentação das interações entre liberdade de expressão e proteção da privacidade no ambiente online (BRASIL, 2014).

A outra legislação abordada neste estudo é a Lei nº 13.709, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), sancionada em 14 de agosto de 2018. Em contraste com o Marco Civil da Internet, a LGPD é uma legislação mais abrangente, composta por 65 artigos divididos em 10 capítulos. Para os propósitos deste trabalho, serão destacadas apenas as disposições relacionadas à liberdade de expressão e à proteção dos direitos de personalidade, que são os focos tanto do projeto principal quanto deste texto. Aprovada em 2018, a LGPD entrou em vigor em 18 de setembro de 2020, modificando alguns aspectos do Marco Civil da Internet e introduzindo sanções administrativas que passaram a ser aplicadas a partir de agosto de 2021, conforme estabelecido pela Lei 14.010/20.

A LGPD representa um marco legal que regulamenta a coleta, proteção e transferência de dados pessoais no Brasil. Seu principal objetivo é garantir um maior controle aos cidadãos sobre suas informações pessoais, exigindo consentimento explícito para a coleta e uso desses dados, além de obrigar a oferta de opções para que os usuários possam visualizar, corrigir e excluir suas informações.

Nota-se que, a LGPD introduziu alterações nos incisos dos artigos 7º e 16 do Marco Civil da Internet, os quais tratam da proteção de dados. Seus fundamentos estão estabelecidos no Artigo 2º, que envolve o respeito à privacidade, autodeterminação informativa, liberdade de expressão, informação, comunicação e opinião, inviolabilidade da intimidade, honra e imagem, desenvolvimento econômico e tecnológico, livre iniciativa, livre concorrência, defesa do consumidor, direitos humanos, livre desenvolvimento da personalidade, dignidade e exercício da cidadania pelas pessoas naturais. O Artigo 3º da LGPD estipula que suas regras se aplicam a qualquer operação de tratamento de dados realizada por pessoa física ou jurídica, de direito público ou privado, independentemente do meio ou localização, desde que determinadas condições sejam atendidas.

Portanto, mesmo que uma empresa esteja sediada em um país estrangeiro, a Lei Geral de Proteção de Dados Pessoais do Brasil pode ser aplicada a ela, contanto que realize o tratamento de dados em território nacional. É importante observar a distinção que a LGPD faz em relação aos dados aos quais esta lei não se aplica, conforme disposto no Artigo 4º. Esses dados incluem:

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

A LGPD dedica um artigo completo, o Artigo 5º, para definir uma série de termos técnicos relevantes utilizados na proteção de dados e em questões relacionadas. Esse artigo estabelece a distinção entre dados pessoais e dados pessoais sensíveis, entre outras classificações. Segundo esse dispositivo, um dado pessoal é definido como uma informação que está relacionada a uma pessoa natural identificada ou identificável. Já um dado pessoal sensível é aquele que aborda informações como origem racial ou étnica, convicção religiosa, opinião política, entre outros, quando vinculado a uma pessoa natural. São introduzidos conceitos como dados anonimizados, que se referem a informações de titulares que não podem ser identificados utilizando meios técnicos razoáveis disponíveis no momento do tratamento, entre outros conceitos apresentados na legislação (BRASIL, 2018).

Os princípios estabelecidos pela LGPD estão elencados no Artigo 6º, e incluem o princípio da boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade de dados,

transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas. No Capítulo II, a LGPD aborda especificamente o tratamento de dados, fornecendo informações sobre as situações em que os dados podem ser tratados, as regras para o uso de dados com o consentimento do titular e os procedimentos que devem ser seguidos quando o titular solicitar informações sobre o tratamento de seus dados. Essas disposições estão presentes nos Artigos 7º, 8º e 9º da lei (BRASIL, 2018).

O Artigo 8º, embora breve, aprofunda-se em um aspecto crucial para o tratamento de dados, que é o consentimento. De acordo com a legislação brasileira, o consentimento deve ser obtido por escrito ou por outro meio que demonstre claramente a manifestação de vontade do titular. São estabelecidas diretrizes para garantir que o consentimento seja obtido de forma adequada e para permitir que o titular revogue seu consentimento a qualquer momento, entre outras disposições relacionadas (BRASIL, 2018).

A LGPD também dedica atenção especial ao tratamento de dados pessoais de crianças e adolescentes, estabelecendo regras específicas nesse sentido no Artigo 14. O tratamento de dados pessoais dessa categoria só é permitido com a autorização de pelo menos um dos pais ou responsáveis legais, exceto em situações específicas previstas na lei, como contato único sem armazenamento ou para proteção das crianças e adolescentes. Essas regras visam proteger os direitos desses grupos vulneráveis (BRASIL, 2018).

Assim como o Marco Civil da Internet, a LGPD demonstra preocupação em regulamentar as relações jurídicas entre a proteção de dados e a liberdade de expressão. A apresentação dessas leis brasileiras evidencia a busca do legislativo por respostas jurídicas para lidar com os desafios apresentados pela evolução tecnológica e seu impacto nos direitos fundamentais, como a liberdade de expressão e a proteção à privacidade.

3. OS DESAFIOS EMERGENTES

3.1 O Direito Digital e a Privacidade dos Dados

O debate em torno da privacidade tem ressurgido com frequência, especialmente em relação aos dados pessoais e à informação, que desempenham papéis centrais em diversos contextos jurídicos na sociedade contemporânea. Contudo, afirmar a importância da informação como um dado moderno não é uma verdade absoluta, pois é possível questionar sua relevância em épocas anteriores (DONEDA, 2020).

Segundo Doneda (2020), ao considerar as expressões "informação" e "dado", é preciso reconhecer que ambas têm uma ação significativo em várias situações, o que resulta em certa banalização de seus usos. Ambas as expressões representam um fato ou uma realidade específica. Cada uma possui suas particularidades. Enquanto o termo "dado" sugere uma conotação mais fragmentada e inicial, como uma informação em potencial antes de ser interpretada ou processada, a "informação" transcende essa simbolização e alcança o nível da cognição.

Embora não se refira explicitamente ao seu significado, a informação implica uma purificação de seu conteúdo, proporcionando uma certa clareza e instrumentalidade para reduzir dúvidas. É importante notar que tanto a comunidade acadêmica quanto a legislação frequentemente tratam esses termos de forma intercambiável (SILVA, 2016).

Atualmente, a manipulação da informação é mais destacada do que em períodos históricos, especialmente devido ao avanço tecnológico, que facilita desde a coleta e o tratamento até a transmissão dos dados. Esse avanço tecnológico amplia a utilidade da informação, tornando-a essencial em uma variedade de contextos e aumentando sua capacidade de influenciar a vida cotidiana das pessoas. A principal mudança iniciada pelos computadores é a organização da informação, substituindo a dispersão anterior por uma estrutura mais organizada (SILVA, 2016).

A interligação entre a informação de natureza pessoal e a privacidade se estabelece a partir de uma lógica básica que associa um maior grau de privacidade à menor divulgação de

informações pessoais, e vice-versa. Embora essa lógica não resolva completamente a complexidade dessa relação, ela serve como ponto de partida para exemplificar como a proteção dos dados pessoais passou a ser respaldada no sistema jurídico brasileiro, como um desdobramento da proteção do direito à privacidade (DONEDA, 2020).

Com o aumento da importância da informação de maneira geral, é em torno dela que o debate sobre a privacidade se intensifica, especialmente no contexto dos dados pessoais. A proteção dos dados pessoais não apenas resguarda a privacidade, mas também abre caminho para uma ação mais ampla, na qual outros interesses devem ser considerados, levando em conta os diversos métodos de controle possibilitados pela manipulação desses dados pessoais (DONEDA, 2020).

A proteção de dados pessoais constitui uma disciplina que abarca, em grande medida, questões relacionadas ao direito à privacidade. Ela representa um instrumento fundamental na construção da própria esfera privada e, consequentemente, no fomento do livre desenvolvimento da personalidade. A transição da privacidade para a proteção dos dados pessoais é guiada por critérios metodológicos que visam promover a funcionalidade de alguns dos valores essenciais do ordenamento jurídico. Essa evolução ressaltou a necessidade do direito civil confrontar uma série de elementos com os quais não estava familiarizado, seja pela sua completa novidade ou pela extensão a domínios previamente alheios, devido a uma longa tradição patrimonialista (DONEDA, 2020).

Para uma compreensão da questão, é importante que o operador jurídico leve em consideração não apenas os interesses subjacentes, mas também o que eles representam de forma mais ampla, além de simplesmente a violação da privacidade. No cerne desse processo, permanece uma constante referência objetiva a uma regulamentação dos dados pessoais, que se mantém conectada à disciplina da privacidade, da qual é uma evolução, atualizando-a e introduzindo características distintas.

Essa conexão entre a abordagem dos dados pessoais e o controle foi especificamente destacada pelo Ministro Ruy Rosado de Aguiar em uma decisão emitida no ano de 1995.

> A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos e privados, na prevenção ou

> repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica. A importância do tema cresce de ponto quando se observa o número imenso de atos da vida humana praticados através da mídia eletrônica ou registrados nos disquetes de computador (SUPREMO TRIBUNAL DE JUSTIÇA, 1995).

Em síntese, a proteção dos dados pessoais aborda o tema da privacidade, mas modifica seus elementos, reforça suas diretrizes e aborda os pontos centrais dos interesses envolvidos. Portanto, o Estado brasileiro reivindica o direito de proteger as informações privadas, especialmente no ambiente digital, como parte essencial da governança em diversos setores, visando garantir a liberdade de expressão, o respeito aos direitos humanos e a privacidade das pessoas, além de uma governança multissetorial no ciberespaço (PINHEIRO, 2021).

A legislação brasileira de proteção de dados teve origem com o Projeto de Lei Complementar nº 53 de 2018, promulgado pelo então Presidente Michel Temer em agosto do mesmo ano (BRASIL, 2018). A Lei Geral de Proteção de Dados, ou LGPD, estabeleceu um marco legal para instituições públicas e privadas, garantindo a proteção dos dados pessoais em qualquer contexto de tratamento de informações que possam ser associadas a uma pessoa identificada ou identificável, independentemente do meio ou entidade responsável pelo tratamento (PINHEIRO, 2021).

Essa regulamentação técnica não se limita apenas a regras e orientações, mas também incorpora direitos, princípios e obrigações relacionadas ao uso de bases de dados pessoais, que são ativos importantes na sociedade atual. A lei tem como objetivo principal proteger os direitos fundamentais de privacidade, liberdade e desenvolvimento da personalidade, estabelecendo o princípio da boa-fé em todos os tipos de tratamento de dados pessoais (PINHEIRO, 2021).

O texto da LGPD inclui diversos itens e princípios de controle técnico para garantir a governança adequada da segurança da informação, visando assegurar o cumprimento dos direitos previstos, com foco no progresso dos direitos humanos. Inspirada no Regulamento Europeu de Proteção de Dados Pessoais, a lei brasileira é composta por 10 capítulos e 65 artigos, sendo menor que a legislação europeia, que possui 11 capítulos e 99 artigos (PINHEIRO, 2021).

Assim, a versão brasileira é mais concisa e, em certos aspectos, adota uma interpretação mais ampla, o que pode resultar em alguma ambiguidade legal, uma vez que permite espaço para interpretações subjetivas em situações que demandariam maior

objetividade. Um exemplo disso é observado nos prazos estabelecidos: enquanto o Regulamento Europeu de Proteção de Dados Pessoais define prazos específicos, como 72 horas, a legislação brasileira menciona um "prazo razoável" (PINHEIRO, 2021).

Nota-se que a legislação mencionada anteriormente passou por alterações posteriormente, por meio da Medida Provisória nº 869 de 2018, que foi convertida na Lei nº 13.853/2019. Esta legislação resultou na criação da ANPD, que exerce uma função relevante no processo de implementação, padronização e aplicação das normas (BRASIL, 2018). Em relação a esse assunto, Doneda enfatiza:

> Assim, em 27 de dezembro de 2018, o Poder Executivo publicou a Medida Provisória n. 869/2018 166, criando a Autoridade Nacional de Proteção de Dados (ANPD) e modificando uma série de outros pontos da lei. A estrutura proposta então era a da ANPD como um órgão público, formalmente localizado dentro da estrutura da Presidência da República (DONEDA, 2020, p. 312).

Trata-se de um órgão pertencente à Administração Pública encarregado de supervisionar e implementar a Lei Geral de Proteção de Dados em todo o território brasileiro. Seu principal propósito é garantir os direitos fundamentais de privacidade e liberdade, bem como orientar, fiscalizar e promover a aplicação da LGPD, incluindo a imposição de sanções em casos de violações no tratamento de dados (PINHEIRO, 2019). A estruturação da ANPD foi estabelecida por meio do Decreto nº 10.474 de 26 de agosto de 2016. De acordo com o disposto, o órgão está subordinado à Casa Civil da Presidência da República, sendo as nomeações de responsabilidade do presidente (BRASIL, 2020).

É relevante ressaltar que a criação da ANPD visa auxiliar na proteção do mercado e na implementação da proteção de dados, buscando garantir a aplicação e o benefício da lei, seja por meio de pareceres técnicos e normas complementares, seja por meio de procedimentos de inspeção. Idealmente, a ANPD deveria funcionar como uma autoridade nacional independente, capacitada para alcançar sustentabilidade e eficiência, conforme previsto no Regulamento Europeu de Proteção de Dados Pessoais (PINHEIRO, 2021).

Conforme Pinheiro (2021), a legislação em questão foi elaborada com o objetivo de conferir maior independência e fortalecer a proteção da privacidade dos titulares dos dados. Os aspectos prioritários foram a garantia de transparência, segurança e respeito ao usuário, orientando as normas de regulamentação. Confiar funções de fiscalização e monitoramento a profissionais que não considerem a perspectiva do indivíduo pode resultar em decisões distantes e conflitantes com os objetivos da referida lei. Houve uma modificação introduzida pela Lei nº 14.010 de 2020, que prorrogou a aplicação das multas estipuladas pelo artigo 52. Isso destaca

que, embora seja uma legislação recente, a Lei Geral de Proteção de Dados já passou por importantes alterações.

Com a entrada em vigor no ano de 2020, tanto organizações privadas quanto públicas foram obrigadas a revisar seus processos e procedimentos para se alinharem com o tratamento e a coleta de dados pessoais. A Lei Geral de Proteção de Dados estabelece direitos aos titulares de dados (como apropriar/modificar dados, acessar informações, revogar consentimento, apagar dados), define as responsabilidades dos agentes de tratamento (realizar o tratamento conforme o propósito e a necessidade, cientes de que a não conformidade resulta em penalidades que incluem advertências, multas simples limitadas a 50 milhões de reais por violação, multas diárias, eliminação de dados, bloqueio de dados, proibição total das atividades relacionadas ao tratamento de dados pessoais) e estabelece condições essenciais para a realização legítima do tratamento de dados (consentimento informado do titular dos dados, finalidade específica e indicada, minimização dos dados, acesso à informação, transparência das ações e garantias de privacidade e segurança dos dados) (PINHEIRO, 2021).

Para implementar o que é previsto na legislação e garantir uma governança de privacidade e proteção de dados sustentável, é fundamental atuar em três áreas: i) tecnológica (utilização de soluções); ii) governança (revisão de políticas e contratos); e iii) educacional (treinamento e conscientização das equipes) (PINHEIRO, 2021). Nesse processo de adaptação, de acordo com as perspectivas de Doneda, é importante considerar que:

> A LGPD, apesar de, como verificado, procurar sistematizar a problemática relacionada ao tratamento de dados pessoais e proporcionar um eixo em torno do qual a disciplina passa a se estruturar, não cumpre essa tarefa meramente com a absorção de elementos já presentes na nossa ordem jurídica. Na verdade, a lei apresenta diversos elementos novos que, por si sós, causaram certo impacto, o fato de consolidarem em uma normativa toda a matéria foi somente o primeiro deles: com a LGPD, passa a integrar o ordenamento toda uma nova série de institutos próprios da disciplina da proteção de dados, de direitos do titular, um enfoque novo de tutela dos titulares é proporcionado pelas regras de demonstração e prestação de contas (accountability), são considerados elementos que levam em conta o risco em atividades de tratamento de dados pessoais e muitas outras (DONEDA, 2020, p. 254-255).

Assim, a referida legislação é considerada complexa e de grande impacto, pois estabelece diversos procedimentos especiais e reitera princípios já presentes em outras leis, como o Marco Civil da Internet e a Constituição Federal em vigor (BRASIL, 1988).

Há a necessidade de realizar uma extensa harmonização com as legislações em vigor, como a Lei de Acesso à Informação, demandando um cuidadoso trabalho de adaptação, especialmente no âmbito público. Especificamente no contexto da Administração Pública, é crucial prestar atenção ao capítulo IV, especialmente a partir do artigo 23, que estipula que o

tratamento de dados pessoais deve ser pautado pelo princípio da transparência, e o uso legal das informações pelas entidades públicas deve estar em conformidade com o interesse público, restrito aos objetivos públicos e alinhado com as competências da entidade (PINHEIRO, 2021).

Para melhorias na abordagem do direito à privacidade dos dados online no Brasil, foi instaurada a ADI - Ação Direta de Inconstitucionalidade, pelo Conselho Federal da Ordem dos Advogados do Brasil (CFOAB) em 20 de abril de 2020, em contestação à Medida Provisória n. 954, datada de 17 de abril de 2020, que versa sobre:

> o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. (BRASIL, 2020, p. 5).

O artigo 2º da medida provisória estabelece que as empresas de telecomunicação que prestam Serviço Telefônico Fixo Comutado (STFC) e Serviço Móvel Pessoal (SMP) são obrigadas a fornecer ao Instituto Brasileiro de Geografia e Estatística (IBGE), por meio eletrônico, uma lista contendo os nomes, números de telefone e endereços de seus clientes, sejam eles pessoas físicas ou jurídicas.

Segundo a Conselho Federal da Ordem dos Advogados do Brasil, o compartilhamento de dados exigido pela Medida Provisória, que inclui a lista de nomes, números de telefone e endereços de consumidores, tanto pessoas físicas quanto jurídicas, viola o princípio fundamental da dignidade da pessoa humana, assim como as cláusulas essenciais que garantem a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, além do sigilo de dados e da autodeterminação informativa, conforme estabelecido nos artigos 1º, III, e 5º, X e XII, da Constituição Federal.

O Conselho da OAB requereu com urgência a concessão de uma liminar. A Ministra Rosa Weber, a quem a ação foi distribuída, deferiu a liminar em 24 de abril de 2020, determinando que o IBGE não solicitasse a disponibilização dos dados mencionados na medida provisória e, caso já o tivesse feito, que suspendesse tal pedido, comunicando imediatamente à(s) operadora(s) de telefonia. A decisão da Corte, referendada pelo plenário do STF em 07/05/2020, ressaltou que o respeito à privacidade e à autodeterminação informativa são fundamentos específicos da proteção de dados pessoais, conforme estabelecido pela LGPD. Houve reconhecimento de inconstitucionalidade devido à ausência de mecanismos de proteção de dados na medida provisória, à desproporcionalidade da medida (compartilhamento de dados pessoais de milhões de brasileiros) em relação aos objetivos

pretendidos (produção de estatística amostral oficial) e à falta de um relatório de impacto à proteção de dados pessoais anterior ao tratamento dos dados coletados, conforme previsto na Medida Provisória nº 954.

Em meio às diversas ponderações apresentadas nos votos, destacou-se o reconhecimento de uma tutela constitucional mais ampla e abstrata dos dados pessoais em comparação com o direito à inviolabilidade da esfera íntima e da vida privada, como evidenciado em um trecho do voto da Ministra Cármen Lúcia.

> Somos uma sociedade de dados, [...] realmente não há dados insignificantes. O que pode ser significante ou insignificante é o uso que do dado é feito, que, com a conectividade possível, faz com que todos nós tenhamos de estar atentos a isto que hoje é uma sociedade que depende de dados para passar não apenas informações, mas dados que acabam levando a uma modificação enorme na convivência, quer por seu vazamento, uso indevido, pela malversação desses dados [...]. (BRASIL, 2020, p. 123).

Mendes e Fonseca (2020) ressaltam a importância do mencionado acórdão, equiparando seu significado histórico ao clássico julgamento do Tribunal Constitucional alemão em 1983, sobre a Lei do Recenseamento daquele país. No acórdão, o Supremo Tribunal Federal (STF) mencionou expressamente o conceito de autodeterminação informativa, já consagrado na Lei 13.709/18 (LGPD), enfatizando a importância exercida pelo cidadão no controle do uso de seus dados. Destacou-se a existência de finalidades legítimas para o processamento dos dados e a necessidade de implementação de medidas de segurança para protegê-los.

Nessa decisão, conforme Napolitano (2015), o STF não apenas ponderou a favor da proteção da privacidade diante de uma possível intromissão abusiva e desproporcional do Estado, mesmo sob a justificativa de garantir o direito à informação, como também reconheceu o direito fundamental à proteção de dados, exigindo uma justificativa constitucional para impor limitações à autodeterminação informativa.

3.3 Os desafios emergentes

De modo geral, o Quadro 2 traz a apresentação de alguns desafios e oportunidades para a privacidade e proteção de dados:

Quadro 2 - Desafios e oportunidades para a privacidade e proteção de dados

Desafios	**Oportunidades**
Aumento da coleta de dados pessoais	Melhorias na segurança cibernética

Desafios	**Oportunidades**
Crescente sofisticação de ataques	Desenvolvimento de tecnologias de proteção
Desafios legais e regulatórios	Maior conscientização pública sobre privacidade
Vulnerabilidades em dispositivos IoT (Internet das Coisas)	Avanços em técnicas de anonimização de dados
Proteção contra vazamentos de dados	Criação de empregos na área de proteção de dados
Complexidade na conformidade com leis	Inovações em ferramentas de gestão de consentimento
Desafios na gestão de consentimento	Aumento da transparência e responsabilidade corporativa

Fonte: adaptado de Grimaldi, 2023.

Os desafios e oportunidades futuras no âmbito da privacidade e proteção de dados constituem elementos de suma importância para a compreensão e abordagem adequada desse cenário em constante transformação. Um dos desafios prementes reside na questão da coleta excessiva de dados, fenômeno intrínseco à era digital em que estamos inseridos. As atividades online que engendramos diariamente geram um volume considerável de informações pessoais, frequentemente coletadas em quantidades desproporcionais por empresas e organizações. Tal prática suscita preocupações relevantes, uma vez que pode resultar em violações de privacidade e em uma maior vulnerabilidade a riscos de segurança cibernética.

Ademais, a ameaça constante representada pelos vazamentos e ataques cibernéticos constitui outro desafio substancial nesse contexto. O aumento do armazenamento de dados online tem acompanhado uma crescente apreensão quanto ao potencial roubo de informações sensíveis, como números de cartões de crédito e dados de identificação pessoal. Tais incidentes têm o potencial de ocasionar danos consideráveis aos indivíduos afetados, ressaltando a importância de estratégias eficazes de proteção e segurança de dados.

Um desafio de relevância é a falta de conscientização acerca dos riscos inerentes ao compartilhamento de informações pessoais na esfera online. Muitos indivíduos ainda não possuem plena ciência dos perigos associados a essa prática, bem como das medidas de segurança digital que deveriam ser adotadas. Tal falta de conscientização os torna suscetíveis a abusos e violações de dados, realçando a necessidade premente de iniciativas voltadas à educação e conscientização sobre práticas seguras de privacidade digital.

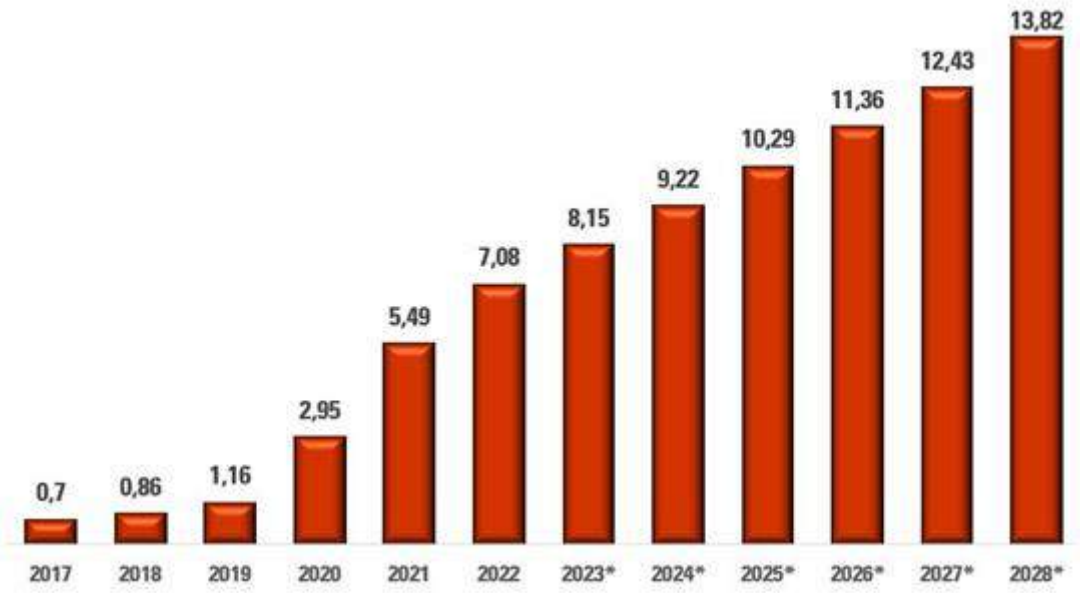
Dessa forma, surgem diversas oportunidades promissoras para aprimorar a proteção da privacidade e dos dados pessoais. A implementação de legislações e regulamentações mais rigorosas, a exemplo do Regulamento Geral de Proteção de Dados (GDPR) na União Europeia e da Lei Geral de Proteção de Dados (LGPD) no Brasil, fornece um arcabouço legal

sólido para a gestão adequada das informações pessoais e a salvaguarda dos direitos individuais.

Os avanços tecnológicos oferecem soluções promissoras para aumentar a segurança e a confidencialidade das informações na esfera digital. Ferramentas de privacidade e configurações de segurança cada vez mais sofisticadas também estão se tornando mais acessíveis, conferindo aos usuários um maior controle sobre suas informações pessoais.

Considerando os crimes cibernéticos, a pesquisa de Kodja (2023) relata esses fatos perpetrados no período compreendido entre os anos de 2017 e 2022, o custo agregado alcançou a cifra de US$18,24 trilhões, superando o Produto Interno Bruto (PIB) acumulado da Índia, a qual figura como a quinta maior economia global no mesmo intervalo temporal.

Figura 1 – Custo estimado dos crimes cibernéticos no mundo 2017 – 2028 trilhões de dólares



Fonte: BANCO MUNDIAL, 2023.

Conforme Kodja (2023), ao projetar as estimativas para o período de 2023 a 2028, prevê-se que os delitos cibernéticos acumularão o montante de US$65,27 trilhões, representando um incremento de 95% em relação ao período anterior. Dessa forma, o Índice Nacional de Segurança Cibernética constitui uma métrica que avalia a capacidade dos países em prevenir ameaças e gerenciar incidentes cibernéticos, além de mensurar a eficácia das medidas adotadas por pessoas, empresas e entidades governamentais na proteção contra crimes cibernéticos, por meio de mecanismos legais e tecnológicos.

Ainda segundo Kodja (2023), dentre as principais ameaças analisadas pelo referido índice incluem-se a acessibilidade aos serviços eletrônicos, a violação da integridade dos dados, caracterizada por modificações não autorizadas, bem como a violação da

confidencialidade dos dados, que se manifesta por meio da exposição de informações sigilosas.

Entre os 176 países objeto de análise, conforme o estudo de Kodja (2023), o Brasil se posiciona na 71ª colocação no que concerne à sua postura em segurança cibernética. A nação brasileira apresenta como principais vulnerabilidades a ausência de supervisão estruturada dos provedores de serviços digitais, a inexistência de um plano de gestão para incidentes cibernéticos de larga escala e a reduzida participação em acordos internacionais de segurança cibernética.

Os Estados Unidos ocupam a 45ª posição, ficando atrás de nações como Rússia, Ucrânia e Arábia Saudita. A colocação inferior dos Estados Unidos se deve, em grande parte, à fragilidade dos serviços de certificação eletrônica, os quais são fundamentais para assegurar a segurança das transações online, bem como à falta de uma entidade governamental dedicada à análise e contenção das ameaças digitais (KODJA, 2023).

No que concerne aos ataques cibernéticos mais perigosos, a proximidade dos indivíduos no cenário digital tornou-se uma vantagem para fraudadores e criminosos, facilitando a identificação de vulnerabilidades e vítimas. Apesar dos esforços conjuntos dos setores público e privado para conter algumas formas de ataques online, o cibercrime continua representando uma ameaça para os usuários da internet (KODJA, 2023).

A conscientização e a educação contribuem de forma significativa na promoção de práticas seguras de privacidade digital. À medida que os indivíduos se tornam mais cientes dos riscos associados ao compartilhamento de informações online e das melhores práticas de proteção de dados, estão mais bem preparados para salvaguardar sua privacidade e segurança.

Em síntese, apesar dos desafios significativos enfrentados, como a coleta excessiva de dados e os riscos de segurança cibernética, também se delineiam oportunidades promissoras, como a implementação de legislações mais rigorosas e o desenvolvimento de tecnologias inovadoras. Todavia, é imperativo que a conscientização e a educação continuem a ser pilares fundamentais na busca pela proteção efetiva de nossas informações pessoais em um ambiente digital em constante evolução.

4. CONSIDERAÇÕES FINAIS

No presente trabalho, realizou-se uma análise do direito digital na era da tecnologia, considerando sua influência na proteção da privacidade. Esta pesquisa se torna ainda mais relevante no atual cenário da sociedade, marcado pelo crescente uso de tecnologias digitais e pela preocupação crescente com a privacidade dos dados pessoais.

Ao longo do estudo, explorou-se não apenas os aspectos legais da LGPD, mas também suas implicações práticas para a sociedade. Considerando que a proteção dos dados, torna-se essencial n mundo globalizados, em que as informações são céleres, tendo assim que se adaptar às novas exigências legais e aos desafios que surgem na proteção dos dados pessoais.

Para isso, utilizou-se metodologias bibliográfica e legislativa, bem como análise jurisprudencial, a fim de obter uma visão ampla sobre o tema. Explorou-se as concepções e processo histórico legislativo relacionado à proteção de dados no Brasil e no mundo, destacando as principais mudanças trazidas pela LGPD e suas implicações para a sociedade.

Apesar das muitas questões ainda não resolvidas e relevantes relacionadas à proteção da liberdade de expressão, privacidade e proteção de dados pessoais no ambiente online, é evidente que o Estado brasileiro, especialmente o Legislativo Federal e o Supremo Tribunal Federal, tem se esforçado para fornecer respostas jurídicas que abordem e salvaguardem esses direitos. Observado através de iniciativas legislativas como o Marco Civil da Internet e a LGPD, além da jurisprudência desenvolvida, como no caso da ADI 6387. Assim, busca-se estabelecer critérios interpretativos que sejam adequados, necessários e proporcionais, de acordo com os princípios dos direitos fundamentais constitucionalmente garantidos, como a liberdade de expressão e a proteção à privacidade.

Sobre os direitos conferidos aos titulares de dados pela LGPD, bem como as responsabilidades das organizações no tratamento dessas informações. Em relação aos desafios enfrentados na implementação efetiva da LGPD, como a adequação de políticas e

processos internos das empresas e a necessidade de fiscalização por parte da Autoridade Nacional de Proteção de Dados (ANPD).

Nota-se que a LGPD representa um marco importante na proteção da privacidade e no controle do tratamento de dados pessoais no Brasil. Sendo assim, ressalta-se a importância de continuar monitorando e avaliando sua eficácia na prática, bem como de buscar soluções para os desafios encontrados ao longo do processo de implementação.

Em síntese, a análise do Direito Digital e da proteção dos dados revela um cenário complexo e em constante evolução, marcado pela necessidade de conciliar a liberdade de expressão e o acesso à informação com a preservação da privacidade e da segurança dos indivíduos. A promulgação de leis como o Marco Civil da Internet e a Lei Geral de Proteção de Dados representa avanços significativos na regulamentação e garantia dos direitos dos cidadãos no ambiente online.

Diante dos desafios emergentes, é fundamental que as legislações sejam constantemente revisadas e atualizadas para acompanhar o ritmo das transformações tecnológicas e garantir uma proteção eficaz dos dados pessoais. Observa-se que, é imprescindível fomentar a conscientização e a cultura de proteção dos dados entre os usuários, empresas e órgãos públicos, visando assegurar um ambiente digital mais seguro e respeitoso dos direitos individuais.

REFERÊNCIAS BIBLIOGRÁFICAS

ARAÚJO, M. B. de. **Comércio eletrônico**; Marco Civil da Internet; Direito Digital. Rio de Janeiro: Confederação Nacional do Comércio de Bens, Serviço e Turismo, 2017.

AZEVEDO, A.C. C. **Marco Civil da Internet no Brasil**. Rio de Janeiro: Alta Books, 2014, p. 90.

BRASIL. **Código de Processo Penal**. Decreto 3689/1941. Disponível em: https://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-3689-3-outubro-1941-322206-normaatualizada-pe.html. Acesso em: 20 ago. 2023.

BRASIL. **Lei nº 5.534/1968**, o Código de Defesa do Consumidor. Dispõe sobre a obrigatoriedade de prestação de informações estatísticas e dá outras providências.

BRASIL. **Constituição Federal**. Constituição da República Federativa do Brasil de 1988. Publicada no Diário Oficial da União, Brasília, 05 out. 1988.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências

BRASIL**. Lei nº 12.737/2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.

BRASIL. **Lei N° 12.965** de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Diário Oficial da União, 2014.

BRASIL. **Medida Provisória 869**, de 2018. Dispõe sobre a criação da Autoridade Nacional de Proteção de Dados. Diário Oficial da União, Poder Executivo

BRASIL. **Lei n° 13.709**, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).

BRASIL. **Lei nº 13.853/2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências.

BRASIL. **Lei 14.010/20**. Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19) .

BRASIL. **Emenda Constitucional nº 115**, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

CALSING, R. de A. **Proteção de dados pessoais e autoridade de controle**: perspectivas e desafios para o Brasil sob a ótica do direito comparado. Programa de pós-doutoramento em Direito 2019

CAMARGO, M. Introdução ao direito digital. In: **Cartilha de Direito Digital.** Comissão de Direito Digital. OAB, Niterói, 2021.

CANTU, R. **La Informática Jurídica en las Facultades de Derecho de América Latina,** 2016. Disponível em: http://libros-revistas-derecho.vlex.es/vid/informaticafacultades-america-latina-107318 . Acesso em 30 Jan. 2024.

DINIZ, M. H. **Curso de Direito Civil Brasileiro**: Teoria Geral do Direito Civil. 33ª ed. São Paulo: Saraiva, 2016.

DONEDA, D. C. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. -- 2. ed. -- São Paulo: Thomson Reuters Brasil, 2020.

FARIAS, P. L. Go. de. **A advocacia na era digital**: uma análise sobre possíveis impactos práticos e jurídicos das novas tecnologias na dinâmica da advocacia privada / Pedro Lima Gondim de Farias. 2020. 118f.: il.

FORTES, V. B. **Os direitos de Privacidade e a proteção de dados pessoais da internet**. Rio de Janeiro: Editora Lumen Juris, 2016. p, 12.

GALIANO, A. et al. I dati non personali: la natura e il valore. **Rivista Italiana di Informatica e Diritto,** Florença, ano 2, f. 1, p. 61-77, mar. 2020.

GIL, A. C. **Como elaborar projetos de pesquisa.** 7. ed. - São Paulo: Atlas, 2019.

GONÇALVES, V. H. P. **Marco civil da internet comentado**. 1ª ed. Imprenta: São Paulo, Atlas, 2017.

GRIMALDI, F. **Privacidade e proteção de dados:** os desafios e oportunidades em um mundo digital. Migalhas, 2023. Disponível em: https://www.migalhas.com.br/depeso/388492/privacidade-e-protecao-de-dados Acesso em: 20 Ago. 2023.

KODJA, C. **Crimes cibernéticos e as principais ameaças impostas pelas milícias digitais.** Pesquisa realizada em 2023. Disponível em: https://investnews.com.br/colunistas/claudia-kodja/crimes-ciberneticos-e-as-principais-ameacas-impostas-pelas-milicias-digitais/ Acesso em: 20 Ago. 2023.

LIMA, D. C. O valor dos dados: breves considerações sobre monetização, controle e proteção. **Revista de Direito e as Novas Tecnologias**, São Paulo, v. 11, abr./jun. 2021.

MACIEL, R. F. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18)** - 1ª Edição. Goiânia: RM Digital Education, 2019.

MELO, V. P. **O direito à privacidade digital e a proteção de dados**. Instituição de Ensino Superior São Judas Tadeu da rede Ânima Educação. 2022.

MENDES, L. S. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. (IDP: linha de pesquisa acadêmica). p. 123-124.

MENDES, L. S. Habeas data e autodeterminação informativa: os dois lados da mesma moeda. **Direitos Fundamentais & Justiça**. Belo Horizonte, ano 12, n. 39, p. 185-216, jul./dez. 2018.
MENDES, L. S.; FONSECA, G. STF reconhece direito fundamental à proteção de dados: comentários sobre o referendo da Medida Cautelar nas ADIs 6387, 6388, 6389, 6390 e 6393. **Revista de Direito do Consumidor** | vol. 130/2020 | p. 471 - 478 | Jul - Ago / 2020 DTR\2020\8441.

MOURA, N. M. M. de; FREIRE, C. C. (Orient.). **A efetivação do direito à privacidade digital e proteção de dados no Brasil.** 2019. 72 f. TCC (graduação em Direito) - Faculdade de Direito do Recife - CCJ - Universidade Federal de Pernambuco - UFPE - Recife, 2019.

NAPOLITANO, C. J. Liberdade de imprensa no Supremo Tribunal Federal: análise comparativa com a Suprema Corte dos Estados Unidos. **Intercom – RBCC**, São Paulo, v.38, n.1, p. 19-36, jan./jun. 2015.

OLIVEIRA, R. **O legítimo interesse e a LGPD**: Lei Geral de Proteção de Dados Pessoais. 1. ed. São Paulo: Thomas Reuters, 2020.

PIMENTEL, J.E.de S. Introdução ao direito digital. **Revista Jurídica ESMP-SP**, V.13, 2018: 16 - 39

PINHEIRO, P. P. **Direito digital**. 2. ed. São Paulo: Saraiva, 2021.

QUEIROZ, T. **Marco Civil da Internet**: um estudo da sua criação sob a influência dos direitos humanos e fundamentais, a neutralidade da rede e o interesse público versus privado. 2016.

SARLET, I. W. **A Eficácia dos Direitos Fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13º ed. Editora do Advogado: São Paulo, 2018.

SILVA, K. R. M.; SANTOS, N. dos. **A dificuldade de aplicabilidade do direito digital à privacidade:** memória coletiva, liberdade de expressão e esquecimento. Goiânia-GO 2021.

SILVA, J. A. da. Curso de direito constitucional positivo. - 39. ed., rev. e atual. até a Emenda Constitucional n. 90, de 15.9.2015. São Paulo: Malheiros, 2016.

SOARES, R. R. **Lei de Proteção de Dados – LGPD**: Direito à Privacidade no Mundo Globalizado, 2020 (Graduação em Direito) – Pontifícia Universidade Católica de Goiás

SUPREMO TRIBUNAL FEDERAL. **Recurso Extraordinário nº 673.707** Minas Gerais. Brasília, 08 de agosto de 2012. Ministro Luiz Fux. Relator. Documento assinado digitalmente

SUPERIOR TRIBUNAL DE JUSTIÇA. **Portaria Interministerial nº 147**, de 31 de maio de 1995.

SUPREMO TRIBUNAL FEDERAL, **ADI 6387/2020**. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629 Acesso em: 13 Marc. 2024.

TEIXEIRA, T.; CHELIGA, V. **Inteligência artificial e Aspectos Jurídicos**. Salvador: Editora Juspodvim, 2019. p.50.

UOL. **Brasil é o segundo país no mundo com maior número de crimes**. São Paulo, 2016. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2018/02/15/brasil-e-o-segundo-pais-no-mundo-com-maior-numero-de-crimes-ciberneticos.htm Acesso em: 05 Nov. 2023.

VIDAL, C. B. S.; QUINELATO, P. D. O valor patrimonial do dado pessoal em base de dados tutelada por direito autoral. **Ius Gentium**, [s. l.], v. 10, n. 1, p. 126-144, jan./abr. 2019.

VIEIRA, P., BRITO, I., TOLARDO, I. **Direito digital:** da regularização de um novo ambiente ao limite da liberdade de expressão, 2019.

ZANINI, A. J. **Blockchain e o direito na área digital**. Centro Universitário Curitiba (Unicuritiba), Curitiba, 2023. Disponível em:https://repositorio.animaeducacao.com.br/bitstream/anima/34585/1/tcc%20ana%20finalizado.docx.pdf Acesso em: 05 Nov. 2023.