FACULDADE SANTA LUZIA - FSL

CURSO DE BACHARELADO EM DIREITO

A RELAÇÃO ENTRE VIGILÂNCIA DIGITAL E O DIREITO À PRIVACIDADE:

DESAFIOS E PERSPECTIVAS JURÍDICAS NO BRASIL

ORIENTANDO(A): RAUL VICTOR MORENO DOS SANTOS

ORIENTADOR(A): PROF. ESP. LUÍS CLAUDIO DOS SANTOS RIBEIRO

SANTA INÊS - MA

2025

RAUL VICTOR MORENO DOS SANTOS

A RELAÇÃO ENTRE VIGILÂNCIA DIGITAL E O DIREITO À PRIVACIDADE:

DESAFIOS E PERSPECTIVAS JURÍDICAS NO BRASIL

Trabalho de conclusão de curso de graduação da Faculdade Santa Luzia-FLS como pré-requisito para obtenção do grau em Bacharelado em Direito.

Orientador: Prof. Esp. Luís Claudio dos Santos Ribeiro.

.

SANTA INÊS - MA

2025

(19374) FACULDADE SANTA LUZIA – FSL

RAUL VICTOR MORENO DOS SANTOS

A RELAÇÃO ENTRE VIGILÂNCIA DIGITAL E O DIREITO À PRIVACIDADE: DESAFIOS E PERSPECTIVAS JURÍDICAS NO BRASIL

Data da Defesa: 02 **de** Dezembro **de** 2025

BANCA EXAMINADORA

Luís Claudio dos Santos Ribeiro
Coordenador Adjunto
Curso Bacharel em Direito
Faculdade Santa Luzia - FSL

Orientador

Nome Completo

Filipe da Silva Coelho

Examinador 1

Nome Completo

Ester Moreira Silva

Examinador 2

Nome Completo

Nota: 1010 (Dez)

RESUMO

O avanço acelerado das tecnologias digitais transformou profundamente as dinâmicas sociais e expôs indivíduos e instituições a novos riscos informacionais. Nesse cenário, a tutela jurídica da privacidade tornou-se um dos maiores desafios do Direito contemporâneo. A pesquisa analisou a Lei Geral de Proteção de Dados (LGPD) como marco regulatório essencial para garantir a liberdade, a autodeterminação informativa e a proteção contra práticas abusivas de coleta, armazenamento e compartilhamento de dados. Verificou-se que, embora a LGPD represente significativo avanço civilizatório, sua efetividade depende da atuação contínua da Agência Nacional de Proteção de Dados (ANPD) e da adoção de políticas de governança informacional por organizações públicas e privadas. O estudo também examinou o monitoramento e a vigilância digital, evidenciando que o ambiente conectado intensifica práticas de controle informacional e aumenta a vulnerabilidade do usuário diante de ameaças cibernéticas e da superexposição de dados. Nas perspectivas futuras, constatou-se que a governança digital deve conciliar inovação tecnológica, ética e garantias fundamentais, especialmente diante da expansão da inteligência artificial, do *big data* e de mecanismos automatizados de vigilância. Conclui-se que a construção de uma sociedade digital justa exige o fortalecimento institucional, a cooperação entre Estado e sociedade e o desenvolvimento de uma cultura de segurança e responsabilidade no uso da informação, assegurando que o progresso tecnológico não comprometa a dignidade humana.

Palavras-chave: Vigilância digital. Privacidade. LGPD. Direitos Fundamentais.

ABSTRACT

The accelerated advancement of digital technologies has significantly transformed social dynamics and exposed individuals and institutions to new informational risks. In this context, the legal protection of privacy has become one of the greatest challenges for contemporary Law. This study examined the General Data Protection Law (LGPD) as an essential regulatory framework for ensuring freedom, informational self-determination, and protection against abusive practices of collecting, storing, and sharing personal data. The analysis demonstrated that, although the LGPD represents an important civilizational achievement, its effectiveness depends on the continuous action of the National Data Protection Authority (ANPD) and the adoption of robust information governance policies by public and private organizations. The research also addressed digital monitoring and surveillance, showing that the connected environment intensifies mechanisms of informational control and increases user vulnerability in the face of cyber threats and excessive data exposure. In assessing future perspectives, the study found that digital governance must reconcile technological innovation, ethics, and fundamental rights, especially considering the rapid expansion of artificial intelligence, big data, and automated surveillance tools. It concludes that building a fair digital society requires institutional strengthening, cooperation between the State and civil society, and the development of a culture of security and responsibility in the use of information, ensuring that technological progress does not compromise human dignity.

Keywords: Digital surveillance. Privacy. LGPD. Fundamental Rights.

A RELAÇÃO ENTRE VIGILÂNCIA DIGITAL E O DIREITO À PRIVACIDADE: DESAFIOS E PERSPECTIVAS JURÍDICAS NO BRASIL

[1] Raul Victor Moreno dos Santos
[2] Luís Claudio dos Santos Ribeiro

INTRODUÇÃO

Atualmente, o avanço das tecnologias utilizadas pelo homem está em um ritmo tão acelerado que o direito por diversas vezes não consegue acompanhá-lo. Porém, essas novas tecnologias implantadas necessitam da regulação de seu uso, por meio da análise dos seus riscos e proveitos em favor da sociedade. Damião (2018) aduz que o progresso dos meios digitais no ciberespaço é uma constante e que a Tecnologia da Informação (TI) vem evoluindo conforme novos protocolos e equipamentos surgem, exigindo um contínuo e infindável aprimoramento dos procedimentos de segurança.

A tecnologia tem grande influência sobre o cotidiano das pessoas, porque interfere, de certo modo, na escolha de vestimentas, na forma de comunicação e utilização de novas expressões idiomáticas, no trabalho, no lazer, inclusive na criminalidade. Lima (2020) afirma que as tecnologias de informação e comunicação interferem em todos os contextos sociais, sendo usadas tanto de forma positiva, conectando pessoas em todo mundo e possibilitando a transmissão de informação, como de forma negativa, servindo de meio para o cometimento de delitos.

Essa realidade, contudo, potencializou paradoxos e inúmeros desafios para ciência jurídica em geral e para os direitos humanos, em particular, definidos como um conjunto mínimo de direitos necessários para assegurar a vida do ser humano baseada na liberdade, igualdade e dignidade (Ávila; Woloszyn, 2017).

Nessa perspectiva, a vulnerabilidade dos usuários cresceu na mesma proporção da inovação tecnológica, especialmente em relação à vida privada e à intimidade, possibilitando a violação ou a quebra de sigilo de qualquer tipo de comunicações ou dados, sejam eletrônicos ou digitais, retirando seu pretenso caráter privativo. Para Damião (2018), o risco de ataques e ameaças no ciberespaço sempre existirá, diante da impossibilidade de ter 100% de segurança.

---

[1] Concludente do Curso de Direito da Faculdade Santa Luzia – Turma: 2021-1.
[2] Docente da Faculdade Santa Luzia. Mestrando em Contabilidade e Administração pela Fucape. Especialista em Direito Tributário. Especialista em Administração Pública. Especialista em Direito Administrativo e Gestão Pública. Especialista em Contabilidade Pública.

A criação de medidas paliativas e protetivas de dados pessoais, com objetivo de proteger a privacidade e intimidade do indivíduo é de suma importância, pois ao mesmo tempo que as informações chegam rapidamente, elas se propagam também de forma rápida, no que poderá ocorrer o vazamento dos dados pessoais do titular, situação que se mostra preocupante.

Nesse contexto, Ávila e Woloszyn (2017) asseveram que tanto o STF quanto o Legislativo têm sido confrontados com questões nas quais a privacidade entra em rota de colisão com outros direitos tutelados na Constituição, notadamente os direitos à liberdade de expressão e de informação e, mais recentemente, o "interesse público". Completam afirmando que, em casos mais exacerbados, a própria segurança nacional exige a flexibilização do sigilo que a Constituição garante sobre os dados e comunicações do indivíduo e merece ser considerada. Abrem-se, assim, oportunidades para a ponderação e relativização da garantia do sigilo.

A problemática que se apresenta diante do avanço tecnológico é a seguinte: como assegurar a proteção da privacidade e dos dados pessoais em uma sociedade marcada pela aceleração informacional e pela utilização em massa de recursos digitais, diante da insuficiência das normas jurídicas tradicionais para lidar com tais situações?

Nesse contexto, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) surge como resposta mais adequada e consolidada à problemática apresentada, estabelecendo diretrizes claras sobre a coleta, uso, armazenamento e compartilhamento de informações pessoais, além de prever sanções administrativas em caso de descumprimento.

Assim, o objetivo geral deste artigo voltasse aos impactos do avanço tecnológico sobre a proteção da privacidade e dos dados pessoais no ordenamento jurídico brasileiro, investigando a evolução normativa desde a Constituição Federal de 1988 até a promulgação da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), com o intuito de compreender em que medida a legislação vigente consegue assegurar os direitos fundamentais do indivíduo frente às vulnerabilidades e desafios do ambiente digital.

Justifica-se, portanto, o presente trabalho pelo desafio de encontrar o equilíbrio entre a inovação tecnológica (e o uso de dados para fins legítimos, como segurança e saúde) e a proteção integral dos direitos fundamentais à privacidade e à autodeterminação informativa, bem como discutir a efetividade das normas jurídicas

destinadas à proteção de dados, especialmente diante da promulgação da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).

A presente pesquisa caracteriza-se como sendo de natureza qualitativa e bibliográfica, uma vez que busca analisar, a partir de referenciais teóricos e doutrinários, as implicações da privacidade de dados, da vigilância digital e da segurança cibernética na sociedade da informação. A abordagem qualitativa é adequada porque permite compreender fenômenos sociais complexos relacionados ao uso das tecnologias digitais, considerando não apenas os aspectos técnicos, mas também os jurídicos e sociais que envolvem a proteção de direitos fundamentais.

Ademais, o presente trabalho fundamenta-se em obras clássicas e contemporâneas sobre privacidade, cibercultura e gestão da informação, bem como em artigos científicos, dissertações, trabalhos de conclusão de curso e legislações pertinentes. Autores como Lévy (2008), ao discutir a cibercultura, e Assmann (2000), ao tratar das transformações do aprender na sociedade da informação, oferecem bases teóricas para compreender o impacto das tecnologias digitais no comportamento social e informacional. Já Paesani (2014) e Ávila e Woloszyn (2017) discutem os aspectos jurídicos da privacidade, enquanto Canongia e Mandarino Júnior (2009), Damião (2018) e Moreira *et al.* (2023) contribuem para a compreensão da segurança cibernética e da gestão da informação.

O texto está organizado nas seguintes partes: a introdução, que apresenta o tema, os objetivos e a justificativa; o referencial teórico, que: 1) abordará as diretrizes da Lei Geral de Proteção de Dados quanto à inviolabilidade da intimidade, honra e imagem das pessoas físicas e jurídicas; 2) analisará o contexto da segurança jurídica relativa ao monitoramento e vigilância no ambiente digital, considerando a privacidade dos usuários e o destino dado às informações; 3) verificará a perspectiva governamental quanto a digitalização da vida social e institucional e o desafio de criar mecanismos eficazes para combater as violações de dados e os crimes cibernéticos; e as considerações finais, que sintetizam as fragilidades, os desafios e as perpectivas na implementação das políticas de segurança cibernética e na conscientização social sobre o uso ético da informação.

Dessa forma, o estudo pretende contribuir para o debate sobre a efetividade das garantias constitucionais frente às novas tecnologias, reforçando o papel do Direito como instrumento de equilíbrio entre o progresso tecnológico e a dignidade da pessoa humana.

1. A LEI GERAL DE PROTEÇÃO DE DADOS

A Lei nº 13.709/2018, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados (LGPD), foi promulgada com o objetivo de ser a principal lei que trata sobre os dados pessoais das pessoas físicas e jurídicas, conforme disposto no artigo 1º:

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

Essa abrangência demonstra a preocupação do legislador em assegurar que o tratamento de dados, independentemente do suporte utilizado, seja pautado por princípios éticos e jurídicos que assegurem a transparência, a segurança e o respeito à pessoa natural. Assim, a lei não se limita às atividades empresariais, mas também alcança órgãos públicos e entidades do terceiro setor. Esses princípios constituem o eixo norteador da interpretação e aplicação da norma.

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Outro aspecto relevante é a definição das bases legais que autorizam o tratamento de dados pessoais, elencadas no artigo 7º da LGPD. O consentimento do titular é uma das bases mais conhecidas, mas não a única. O tratamento pode ocorrer também para o cumprimento de obrigação legal ou regulatória, execução de políticas públicas, realização de estudos por órgãos de pesquisa, execução de contratos, exercício regular de direitos ou legítimo interesse do controlador, entre outros. Essa diversidade de bases confere flexibilidade à norma, permitindo sua aplicação a diferentes contextos.

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

A figura do titular dos dados pessoais ocupa papel central na LGPD, pois é em torno dele que gravitam os direitos assegurados pela lei. Entre os direitos do titular, previstos no artigo 18, estão: I) o direito de confirmação da existência do tratamento; II) o acesso aos dados; III) a correção de dados incompletos, inexatos ou desatualizados; IV) a anonimização ou eliminação dos dados desnecessários; V) a portabilidade dos dados para outro fornecedor de serviço; VI) a eliminação dos dados pessoais tratados com o consentimento do titular; VII) a informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII) a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e IX) a revogação do consentimento. Esses

direitos fortalecem a autonomia informacional do indivíduo e promovem maior equilíbrio nas relações digitais.

Além de ditar as normas para a proteção de dados das pessoas naturais e jurídicas, a Lei Geral de Proteção de Dados pensou na possibilidade de uma fiscalização especial, de modo que instituiu um órgão responsável pela sua aplicação e fiscalização, qual seja, a Agência Nacional de Proteção de dados (ANPD), autarquia de natureza especial vinculada ao Ministério da Justiça e Segurança Pública, dotada de autonomia funcional, técnica, decisória, administrativa e financeira, com patrimônio próprio e com sede e foro no Distrito Federal.

A referida autarquia exerce papel estratégico ao regulamentar aspectos técnicos, orientar empresas e instituições, além de zelar pela uniformidade na aplicação das normas. Sua atuação busca equilibrar a proteção do titular e a viabilidade das atividades econômicas, promovendo uma cultura de conformidade e responsabilidade.

As sanções administrativas, previstas no artigo 52, constituem instrumentos importantes para assegurar a observância da LGPD. Elas variam desde advertências até multas que podem atingir até 2% do faturamento da empresa, limitadas a cinquenta milhões de reais por infração. Também é possível aplicar sanções como publicização da infração, bloqueio ou eliminação dos dados pessoais relacionados à irregularidade. Esse aparato sancionatório reforça a necessidade de políticas internas de compliance e governança de dados nas organizações.

A responsabilidade civil decorrente do tratamento indevido de dados é outro ponto relevante. A LGPD estabelece que tanto o controlador quanto o operador dos dados podem ser responsabilizados por danos patrimoniais, morais, individuais ou coletivos. Isso significa que a proteção de dados transcende o âmbito administrativo e alcança o judicial, permitindo ao titular buscar reparação sempre que houver violação a seus direitos. Essa previsão fortalece o caráter coercitivo da lei e incentiva a adoção de medidas preventivas.

Como se vê, conforme Monteiro (2018, apud Moreira et al., 2023), a Lei Geral de Proteção de Dados (LGPD) procurou fornecer ao cidadão maior controle dos seus dados, bem como regular o uso de informações em negócios que utilizam dados pessoais em decisões automatizadas.

Ademais, no contexto econômico, a LGPD também desempenha função estratégica, pois contribui para o fortalecimento da confiança nas relações digitais e

para a competitividade das empresas brasileiras no mercado internacional. Em um cenário global em que a circulação de dados é essencial para os negócios, a conformidade com padrões internacionais de proteção de dados torna-se um diferencial. Assim, a LGPD atua não apenas como um instrumento jurídico de proteção, mas também como um fator de desenvolvimento econômico e tecnológico sustentável.

Atualmente, o medo do indivíduo em ter os dados vazados perante o Estado, é menor que para a sociedade, tendo em vista que a internet pertence a todos mundialmente e os usuários devem utilizar a internet de forma responsável, para que não ocorra danos irreparáveis. Neste sentido, Liliana Minardi Paesani defende que:

> A utilização dos computadores determinou uma transformação qualitativa nos efeitos decorrentes da coleta de informações. A tecnologia, com a inserção de mecanismos cada vez mais sofisticados de difusão de informações, tem contribuído para um estreitamento crescente do circuito privado, na medida em que possibilita, até a longa distância, a penetração na intimidade da pessoa. Hoje não é o governo que ameaça a privacidade, é o comércio pela Internet. A web transformou-se num mercado e, nesse processo fez a privacidade passar de um direito a um commodity. O poder informático indica não só a possibilidade de acumular informações em quantidade ilimitada sobre a vida de cada indivíduo, isto é, suas condições físicas, mentais, econômicas ou suas opiniões religiosas e políticas, mais também de confrontar, agregar, rejeitar e comunicar as informações assim obtidas (Paesani, 2014).

Embora possa parecer desastroso, uma vez que a finalidade da web não é atingir a privacidade de seus usuários, temos que tais incidentes são o resultado da intrínseca característica da internet. A rede foi criada para interligar usuários sem mediadores, ou seja, sem a participação de qualquer ente, público ou privado, nessa relação (Barreto Júnior, 2018).

Todavia, o legislador brasileiro buscou regulamentar as interações existentes no ciberespaço, estabelecendo, entre os seus inúmeros dispositivos legais, como é o caso da LGPD, princípios, garantias, direitos e deveres para o uso da Internet no Brasil, disciplinando a proteção de dados pessoais.

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o **respeito à privacidade**;
> II - a autodeterminação informativa;
> III - **a liberdade de expressão, de informação, de comunicação e de opinião**;
> IV - a **inviolabilidade da intimidade, da honra e da imagem**;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, **a dignidade e o exercício da cidadania** pelas pessoas naturais. (grifo nosso)

Parece, então, razoável considerar que a questão do sigilo de dados e das comunicações, face às novas tecnologias digitais como a internet, envolvendo mensagens de dados, textos e voz via aplicativos, não está devidamente tutelada na Constituição e, como consequência, o desenvolvimento do direito à privacidade e à intimidade das pessoas pelo legislador e pela jurisprudência termina por avançar os limites do texto constitucional (Ávila; Woloszyn, 2017).

Conforme Damião (2018), o Brasil é um dos países mais vulneráveis do mundo quando tratamos de segurança da informação. E essa vulnerabilidade, na visão de Lima (2020), se dá devido o número elevado de usuários com liberdade para acessar, transferir, enviar e difundir informações, cujo controle é dificultado em virtude da estrutura descentralizada e não hierarquizada da Internet. No cenário global, Canongia e Mandarino Júnior (2009) lembram que as vulnerabilidades e ameaças são crescentes na Sociedade da Informação, o que torna a proteção jurídica de dados questão estratégica para o Estado e para as organizações.

Cabe salientar que a LGPD encontrou desafios ao ser implementada, sendo necessária tanto a adequação das organizações, na forma de investimentos em sistemas e no treinamento dos colaboradores quanto a efetiva realização de atividades de fiscalização por parte dos entes responsáveis (Cunha, 2021, *apud* Moreira et al., 2023).

Nessa esteira, Damião (2018) aduz que o desafio para harmonizar o avanço da tecnologia com a segurança dos dados sensíveis é gigantesco. Reforça que o progresso dos meios digitais no ciberespaço é uma constante, e que esse avanço gera a necessidade de aprimoramento dos procedimentos de segurança.

Por isso, pode-se afirmar que a Lei Geral de Proteção de Dados (LGPD) representa um avanço civilizatório no direito brasileiro, ao consolidar a proteção de dados como um direito fundamental e estabelecer um marco regulatório compatível com os desafios da era digital. Sua efetividade, contudo, depende da conscientização de todos os agentes envolvidos – Estado, empresas e cidadãos – sobre a importância da ética no uso da informação. A implementação da cultura de proteção de dados é, portanto, o caminho para o equilíbrio entre inovação tecnológica e respeito à dignidade humana.

2. MONITORAMENTO E VIGILÂNCIA NO AMBIENTE DIGITAL

O desenvolvimento social e tecnológico tornou mais evidente o papel da informação como uma habilitadora da ação humana. Nessa era conhecida como sociedade da informação, diferentes recursos tecnológicos são usados para armazenamento e transmissão de dados e informação (Moreira *et al.*, 2023).

De fato, conforme destaca Vieira (2017), nos últimos tempos, os avanços tecnológicos da informação vêm revolucionando a vida do indivíduo em sociedade numa rapidez que preocupa até mesmo os estudiosos do assunto, isso porque o ingresso desses avanços tecnológicos não trouxe somente fatores positivos, mas também fatores negativos que chegam a prejudicar a convivência em sociedade, o que evidencia a tensão entre inovação e privacidade no mundo conectado.

No contexto das redes sociais, Barreto Júnior *et al.* (2018) ressaltam que a sociedade da Informação, ao inovar a lógica comunicacional no mundo, requer do Direito o olhar atento à proteção da privacidade, dignidade e, por reflexo, dos efeitos da superexposição de dados pessoais que resultam da utilização da internet. Do nosso ponto de vista, isso reflete a dualidade entre liberdade comunicacional e controle digital.

Por isso, o ambiente digital, caracterizado pela constante coleta de dados, coloca o indivíduo sob uma vigilância contínua. Nessa mesma esteira, Razzolini Filho (2020, apud Moreira *et al.*, 2023) aduz que, com os novos recursos tecnológicos e as variadas formas de interação propiciadas por eles, existe um excesso de informação circulando em diferentes ambientes. Isso demanda monitoramente e controle informacional, além de vigilância responsável.

Nesse sentido, o controle informacional passou a ser parte das dinâmicas sociais e econômicas, transformando a forma como indivíduos e organizações interagem e são observados. Entretanto, esse controle é intensificado por um cenário de constante ameaça cibernética. Damião (2018) adverte que os ataques cibernéticos cresceram em importância e em larga escala e que a preocupação com a segurança cibernética reside na proteção da imensa quantidade de dados sensíveis, pessoais e institucionais, que possuem nossos bancos de dados.

Conforme Moreira *et al.* (2023), o monitoramento de fluxos informacionais em ambientes digitais têm sido motivo de preocupação devido às questões relacionadas com a privacidade dos usuários e com o destino dado às informações, que são

coletadas à medida que atividades são realizadas.

Cabe ressaltar que o controle informacional também está profundamente relacionado à segurança cibernética, uma vez que o avanço das tecnologias amplia tanto o poder de coleta quanto o de violação de dados. Esse movimento evidencia o paradoxo da era digital: quanto maior a inovação, maior também o potencial de vulnerabilidade.

Como observa Canongia e Mandarino Júnior (2009), a segurança cibernética vem se caracterizando cada vez mais como uma função estratégica de governo, e essencial à manutenção e preservação das infraestruturas críticas de um país, tais como saúde, energia, defesa, transporte, telecomunicações, da própria informação, entre outras.

Moreira *et al.* (2023) enfatizam que as interações neste ambiente revelam um estado de permanente vigilância, seja por necessidades relacionadas a interesses de empresas ou organizações, seja para coibir práticas ilícitas as mais diversas, suscitando preocupações relacionadas com o tratamento dos dados coletados e processados, com importantes implicações éticas e legais, e que podem não estar devidamente cobertas pelos instrumentos legais.

Todavia, a vigilância não se restringe às ações governamentais e corporativas. Ela permeia a vida cotidiana dos cidadãos, tornando-se onipresente e rotineira. Ball e Webster (2003, *apud* Moreira *et al.*, 2023), reforça essa visão ao enfatizar que as pessoas são vigiadas ao fazerem ligações telefônicas, ao acessarem a Internet, ao interagirem com aplicativos, ao realizarem compras, ao percorrerem ruas ou estradas monitoradas por câmeras de segurança capazes de reconhecimento por imagem para identificar pessoas e/ou veículos, e ao pagarem pedágios.

Nesse diapasão, a vigilância digital tem ultrapassado os limites das relações interpessoais e assume papel central nas políticas de Estado e estratégias empresariais. Canongia e Mandarino Júnior (2009) afirmam que o grande desafio consiste em harmonizar duas dimensões: a primeira dimensão diz respeito à cultura do compartilhamento, da socialização, da transparência, da criação de conhecimento; a segunda refere-se às questões de proteção, segurança, confidencialidade e privacidade. Essa dualidade demonstra que o controle informacional busca conciliar liberdade e segurança, embora nem sempre consiga equilibrá-las.

Quando se aborda o monitoramento da informação é preciso considerar a questão ética, pois esse procedimento envolve, potencialmente, os dados de milhões de pessoas (Moreira *et al*., 2023). Por isso, o aspecto ético da vigilância digital tem sido um dos maiores desafios contemporâneos, haja vista que, na visão de Ball e Webster (2003, *apud* Moreira *et al.*, 2023), a coleta e categorização de dados não são operações eticamente neutras. Essa realidade demonstra que a vigilância digital extrapola a mera coleta de informações e passa a representar um campo de disputa ética e política.

No contexto organizacional, o monitoramento da informação se tornou indispensável para a tomada de decisões e a mitigação de riscos, ajudando as organizações a cumprirem seus objetivos. A respeito, Moreira *et al.* (2023) é categórico ao pontuar que a informação precisa ser monitorada em perspectivas distintas, envolvendo: a) elemento político; b) elemento econômico; c) elemento tecnológico; d) elemento ambiental; e) elemento legal; f) elemento informacional. Esse controle de fluxos informacionais é tanto uma ferramenta de gestão quanto um instrumento de poder.

Ademais, a vigilância digital e o controle informacional compõem a espinha dorsal da sociedade contemporânea, que depende de dados para funcionar, mas precisa de limites para preservar a dignidade humana. Moreira *et al.* (2023) sintetizam esse dilema ao afirmar que o simples fato de carregarem consigo celulares habilita processos de vigilância. A vigilância, antes pensada como a monitoração ou interceptação da ação de inimigos, é hoje rotineira e onipresente.

Por fim, Vieira (2017) enfatiza a importância de demonstrar o direito à privacidade para a vida de cada indivíduo nesse ambiente cibernético:

> Considerando a dinamicidade do direito, este procura se ajustar à contemporaneidade e passa a tratar do direito à privacidade dos que se movimentam no espaço cibernético e se veem diante de dilemas decorrentes do confronto tecnológico em face da interferência do direito à privacidade do indivíduo.
> Desse modo, a proteção do direito à privacidade do indivíduo deve ser vista como um direito fundamental a ser resguardado contra as intromissões dos avanços do mundo moderno tecnológico, visto que somente o indivíduo tem o direito de escolher o que terceiro possa saber de sua vida privada (Vieira, 2017).

Diante disso, o monitoramento digital deve ser repensado sob uma perspectiva ética e jurídica que garanta o equilíbrio entre segurança, transparência e liberdade individual. Portanto, o desafio futuro consiste em regular o uso dessas

tecnologias sem comprometer os direitos fundamentais à liberdade, à dignidade e à privacidade.

3. PERSPECTIVAS FUTURAS DA PROTEÇÃO DE DADOS E DA VIGILÂNCIA DIGITAL

O Brasil, conforme Canongia e Mandarino Júnior (2009), tem governança estabelecida e legislação vigente no campo da segurança da informação e comunicações, e vem construindo seu arcabouço normativo no âmbito do governo federal que, apesar de recente, se comparado ao arcabouço de leis, normas e padrões dos países desenvolvidos, tem destaque de atuação e reconhecimento nacional e internacional de sua competência em temas diretamente correlacionados à segurança cibernética.

Nesse contexto, as perspectivas futuras da proteção de dados e da vigilância digital apontam para um cenário regulatório em constante evolução, marcado pela tentativa de conciliar a inovação tecnológica acelerada com a salvaguarda dos direitos fundamentais dos titulares, em face de ameaças cibernéticas cada vez mais sofisticadas.

Essas perspectivas indicam um cenário de crescente complexidade e interdependência entre tecnologia, direito e ética, haja vista que o avanço das tecnologias de informação e comunicação tende a ampliar o alcance da vigilância e o poder de coleta de dados, exigindo respostas jurídicas e institucionais mais robustas.

Entretanto, a vigilância digital se apresenta como um desafio paradoxal. Se, por um lado, ela é um instrumento de prevenção e segurança, por outro, pode representar um risco de violação dos direitos humanos. Frank La Rue, relator especial da ONU, adverte que:

> A vigilância de comunicações deve ser considerada como um ato altamente intrusivo que, potencialmente, interfere com os direitos à liberdade de expressão e privacidade e ameaça as bases de uma sociedade democrática. A legislação deve estipular que a vigilância de comunicações só deve ocorrer nas circunstâncias mais excepcionais e ex clusivamente sob a supervisão de uma autoridade judicial independente (Rodriguez, 2013, *apud* Ávila; Woloszyn, 2017)

A respeito, Vieira (2017) adverte que a Constituição Federal de 1988 destaca no seu art. 5º, inciso X, a proteção ao direito da privacidade e à intimidade do indivíduo, demonstrando que qualquer forma de vigilância deve estar subordinada à Constituição e aos direitos da personalidade, sob pena de degenerar em controle abusivo.

Essa advertência conduz à reflexão sobre os limites éticos e jurídicos da vigilância em sociedades democráticas, ao passo que o aprimoramento legislativo possa priorizar a harmonização entre o desenvolvimento tecnológico e a garantia dos direitos fundamentais, como é o caso da privacidade no contexto da hiperconectividade.

As legislações recentes, como o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), representam marcos importantes, mas ainda demandam consolidação prática e institucional. Por isso, as futuras políticas de proteção de dados devem se basear em uma governança digital democrática e inclusiva.

Embora o sigilo de dados, correspondência e comunicações reste assegurado nas diversas esferas do sistema global de proteção e defesa dos direitos humanos – quer convencionais ou extraconvencionais – e tenha sido incorporado nos textos constitucionais dos países onde vige o constitucionalismo democrático, o maior desafio dos tempos atuais é saber exatamente como garanti-los em um sistema global digital caracterizado pela inexistência de fronteiras materiais (Ávila; Woloszyn, 2017).

Nesse sentido, a construção de um ambiente digital seguro requer parcerias entre governos, empresas e sociedade civil, com o objetivo de fortalecer a confiança nas plataformas e garantir a transparência no uso das informações. A cooperação institucional é, portanto, o caminho para uma governança digital mais justa e participativa.

As projeções indicam que a vigilância digital se tornará cada vez mais sofisticada e imperceptível, impulsionada por tecnologias como a inteligência artificial e a análise de *big data*. Aliás, uma das tendências mais aguardadas é a Regulamentação da Inteligência Artificial (IA), com iniciativas como o PL nº 2338/2023 no Brasil, em tramitação no Congresso nacional, propondo diretrizes para o uso ético e responsável da tecnologia, assegurando às pessoas afetadas por sistemas de inteligência artifical os seguintes direitos:

> Art. 5º Pessoas afetadas por sistemas de inteligência artificial têm os seguintes direitos, a serem exercidos na forma e nas condições descritas neste Capítulo:
> I - direito à informação prévia quanto às suas interações com sistemas de inteligência artificial;
> II - direito à explicação sobre a decisão, recomendação ou previsão tomada por sistemas de inteligência artificial;
> III - direito de contestar decisões ou previsões de sistemas de inteligência artificial que produzam efeitos jurídicos ou que impactem de maneira significativa os interesses do afetado;
> IV - direito à determinação e à participação humana em decisões de sistemas de inteligência artificial, levando-se em conta o contexto e o estado da arte do desenvolvimento tecnológico;
> V - direito à não-discriminação e à correção de vieses discriminatórios diretos, indiretos, ilegais ou abusivos; e
> VI - direito à privacidade e à proteção de dados pessoais, nos termos da legislação pertinente.

A perspectiva de uma sociedade hiperconectada, na qual a internet das coisas e a inteligência artificial coletam e processam dados pessoais de forma autônoma, requer a redefinição das normas de proteção. O relatório do Centro Criptológico Nacional da Espanha (2015, *apud* Ávila; Woloszyn, 2017) prevê que o volume de dados pessoais que se recopilará abarcará todo tipo de informação pessoal e terá um enorme valor econômico. Essa previsão indica que a proteção de dados deve se adaptar a um novo cenário de economia informacional e vigilância onipresente, universal e geral.

Como se vê, o futuro da proteção de dados e da vigilância digital deverá se apoiar em um novo paradigma ético e jurídico, capaz de conciliar segurança, liberdade e dignidade humana. Nesse ínterim, Vieira (2017) reforça que é necessário proteger as informações privadas contra as invasões de terceiros mal-intencionados e demonstrar a importância desse direito para a vida de cada indivíduo. Assim, as perspectivas futuras apontam para a consolidação de uma cidadania digital consciente, onde a tecnologia sirva à pessoa humana e não o contrário.

Ademais, a perspectiva governamental de combate à violação de dados deve ir além das respostas punitivas. É imprescindível a construção de uma cultura de segurança informacional, baseada em educação tecnológica, transparência institucional e cooperação internacional. A respeito, Damião (2018) lembra que a falta de crença nas reais ameaças virtuais aumenta as vulnerabilidades e, por consequência, o risco de uma possível invasão ou coleta de dados sigilosos. Assim, a formação de cidadãos digitalmente conscientes é, portanto, um requisito essencial para a sustentabilidade da segurança informacional

Por fim, o Estado deve se consolidar como garantidor de um ambiente digital

seguro e democrático, no qual a proteção de dados e a liberdade de expressão coexistam em harmonia, corroborando para a preservação da dignidade humana e da confiança social na era digital. Assim, o desafio do futuro será equilibrar a segurança e a liberdade, construindo uma sociedade informacional mais justa, transparente e consciente.

CONSIDERAÇÕES FINAIS

O estudo realizado ao longo deste trabalho permitiu refletir sobre a complexa relação entre o avanço tecnológico e a tutela jurídica da privacidade e dos dados pessoais. Observou-se que o desenvolvimento acelerado das tecnologias digitais trouxe consigo inúmeras possibilidades de comunicação, interação social e facilidades no cotidiano, mas também provocou desafios sem precedentes para o ordenamento jurídico, especialmente no que tange à preservação da intimidade e à proteção contra abusos na utilização das informações pessoais.

A análise demonstrou que a vulnerabilidade do indivíduo cresceu na mesma proporção da inovação tecnológica. As informações circulam em grande escala e velocidade, tornando a vida privada cada vez mais exposta, o que possibilita violações de direitos fundamentais, seja por meio da coleta excessiva de dados, do monitoramento constante de hábitos de consumo, ou ainda da prática de crimes digitais. Essa fragilidade não se limita à esfera individual, pois envolve também questões coletivas, de segurança pública e de governança digital. Assim, a privacidade deixou de ser apenas um direito individual abstrato, para tornar-se um dos pilares da cidadania contemporânea.

O ordenamento jurídico brasileiro, apesar de seus avanços, mostrou-se inicialmente insuficiente para lidar com a complexidade do ambiente digital. As primeiras previsões constitucionais e civis garantiam a inviolabilidade da vida privada de maneira genérica, sem abarcar os riscos específicos decorrentes das novas tecnologias.

A promulgação da Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018) representou um marco civilizatório, consolidando a proteção de dados como um direito fundamental. Os resultados obtidos pela pesquisa evidenciam que a LGPD trouxe avanços consideráveis, mas seu pleno êxito depende não apenas da previsão legal, mas também da efetiva implementação e fiscalização de suas

disposições. Todavia, o êxito da LGPD depende da conscientização social e da efetiva atuação fiscalizatória da Agência Nacional de Proteção de Dados (ANPD).

Outro ponto relevante identificado é o papel do Estado diante do monitoramento e da vigilância no espaço digital. Embora tais práticas possam ser justificadas em nome da segurança pública e da prevenção de crimes, elas trazem riscos significativos à liberdade e à dignidade humana. Surge, assim, a necessidade de ponderar entre o interesse público e a proteção da esfera privada do indivíduo. O desafio consiste em evitar que a justificativa da segurança nacional ou do interesse coletivo sirva de pretexto para abusos e violações sistemáticas da privacidade.

Além disso, a pesquisa mostrou que a construção de uma sociedade digital justa depende de uma governança global cooperativa. Nesse contexto, o maior desafio dos tempos atuais é saber exatamente como garantir o sigilo e a privacidade em um sistema global digital caracterizado pela inexistência de fronteiras materiais. Desse modo, a efetividade das normas internas está vinculada à harmonização com padrões internacionais e à cooperação entre Estados e instituições.

O futuro da proteção da privacidade dependerá não apenas da eficácia das normas jurídicas, mas da capacidade de todos os atores sociais – Estado, empresas e cidadãos – de atuarem de forma ética e responsável no uso da informação. A consolidação de uma cultura de proteção de dados, associada ao fortalecimento institucional da Agência Nacional de Proteção de Dados – ANPD e ao compromisso internacional com a segurança cibernética, será fundamental para que o Brasil consiga enfrentar os riscos impostos pelo ambiente digital e, ao mesmo tempo, aproveitar suas potencialidades em favor do desenvolvimento humano e social.

Ademais, conclui-se que o avanço tecnológico é irreversível e deve ser entendido como parte integrante da sociedade contemporânea, e que o futuro da vigilância digital dependerá da criação de mecanismos jurídicos e éticos capazes de garantir a transparência, a responsabilidade e a limitação do poder informacional, assegurando que o desenvolvimento tecnológico ocorra sem comprometer a dignidade humana e os direitos fundamentais. Nesse compasso, o Direito, embora apresente certa morosidade em relação às inovações, deve buscar mecanismos ágeis de atualização e adaptação, de modo a equilibrar os benefícios da tecnologia com a preservação dos direitos fundamentais. Por fim, a privacidade, a intimidade e a proteção dos dados pessoais são valores que não podem ser relativizados em nome exclusivo do progresso tecnológico ou de interesses econômicos.

REFERÊNCIAS

ASSMANN, Hugo. A metamorfose do aprender na sociedade da informação. Ciência da informação, Brasília, v. 29, p. 07-15, 2000. Disponível em: <https://www.scielo.br/j/ci/a/ShzKdLbqJDPfssvSw9xWPrw>. Acesso em: 04 out. 2025.

ÁVILA, Ana Paula Oliveira; WOLOSZYN, André Luis. A tutela jurídica da privacidade e do sigilo na era digital: doutrina, legislação e jurisprudência. Revista de Investigações Constitucionais, Curitiba, v. 4, n. 3, p. 167-200, set./dez. 2017. Disponível em: <https://www.scielo.br/j/rinc/a/kdqYTvJ7GWsS75twG6f37Bc/?lang=pt>. Acesso em: 16 out. 2025.

BARRETO JÚNIOR, Irineu Francisco et. al. Marco civil da internet e o direito à privacidade na sociedade da informação. Revista Direito, Estado e Sociedade, n. 52, p. 114-133, jan/jul, 2018. Disponível em: <https://doi.org/10.17808/des.52.835>. Acesso em: 16 out. 2025.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm> Acesso em: 20 set. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 22 set. 2025.

BRASIL. Senado Federal. Projeto de Lei nº 2.338/2023. Dispõe sobre o uso da Inteligência Artificial. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233> . Acesso em: 16 out. 2025. Texto Original.

CANONGIA, C; MANDARINO JUNIOR, R. Segurança cibernética: o desafio da nova Sociedade da Informação. Parcerias Estratégicas, Brasília, v. 14, n. 29, p. 21-46, 2010. Disponível em: <http://seer.cgee.org.br/index.php/parcerias_estrategicas/article/viewFile/349/342>. Acesso em: 06 out. 2025.

CANCELIER, Mikhail Vieira de Lorenzi. O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro. Florianópolis, n. 76, p. 213-240, ago. 2017. Disponível em: <https://www.scielo.br/j/seq/a/ZNmgSYVR8kfvZGYWW7g6nJD/?format=pdf&lang=pt>. Acesso: 17 set. 2025.

DAMIÃO, André Kohler. Guerra cibernética: proteção cibernética monitoramento de redes e sistemas e levantamentos de vulnerabilidades. 2018. Trabalho de Conclusão de Curso (Especialização em Ciências Militares com ênfase em Gestão Operacional). Escola de Aperfeiçoamento de Oficiais, Rio de Janeiro, 2018. Disponível em: <https://bdex.eb.mil.br/jspui/bitstream/123456789/3574/1/Cap%20Andre.pdf>. Acesso em: 14 set. 2025.

LÉVY, Pierre. As tecnologias da inteligência: o futuro do pensamento na era da informática. 1. ed., 15. reimpr. São Paulo: Editora 34, 2008. Disponível em: <https://mundonativodigital.wordpress.com/wp-content/uploads/2016/03/cibercultura-pierre-levy.pdf>. Acesso em: 20 set. 2025.

LIMA, Juliana Dantas. Discurso de ódio em ambiente virtual: contribuições da gestão da informação para aumento da eficiência na investigação policial. 2020. Dissertação (Programa de Mestrado em Ciência da Informação). Universidade Federal de Santa Catarina, Santa Catarina, 2020. Disponível em: <https://repositorio.ufsc.br/bitstream/handle/123456789/216647/PCIN0231-D.pdf>. Acesso em: 17 set. 2025.

MOREIRA, Arnaldo Luis Darg et al. Vigilância e privacidade no ambiente digital. RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação. 2023. Disponível em: <https://www.scielo.br/j/rdbci/a/BQwBvhQN4PFMY7hv65xQhys/?lang=pt>. Acesso em: 19 set. 2025.

PAESANI, Liliana Minardi. Direito e Internet: Liberdade de Informação, Privacidade e Responsabilidade Civil. 7. ed., São Paulo: Atlas, 2014.

RAZZOLINI FILHO, Edelvino. Introdução à gestão da informação: a informação para organizações no século XXI. Curitiba: Juruá, 2020.

VIEIRA, Waleska Duque Estrada. A privacidade no ambiente cibernético: Direito fundamental do usuário. Revista da ESMESC - Publicação contínua, v. 24, n. 30, 197-217, 2017. Disponível em: <https://doi.org/10.14295/revistadaesmesc.v24i30.p197>. Acesso em: 08 out. 2025.