# DO CAPITALISMO DE VIGILÂNCIA À REGULAÇÃO DEMOCRÁTICA: DESAFIOS JURÍDICOS E ÉTICOS NA ERA DOS DADOS[1]

# FROM SURVEILLANCE CAPITALISM TO DEMOCRATIC REGULATION: LEGAL AND ETHICAL CHALLENGES IN THE AGE OF DATA

DOI: 10.19135/revista.consinter.00021.12
Recebido/Received 26/05/2025 – Aprovado/Approved 07/08/2025

*Anderson Filipini Ribeiro*[2] – *https://orcid.org/0009-0008-5145-2476*
*Filipe de Mello Sampaio Cunha*[3] – *https://orcid.org/0009-0005-7142-8885*
*Natalia Maria Ventura da Silva Alfaya*[4] – *https://orcid.org/0000-0002-0312-3677*

**Resumo**

A era digital intensificou o uso de tecnologias de monitoramento e a coleta massiva de dados pessoais, configurando a chamada sociedade da vigilância. Esse fenômeno, protagonizado por Estados e corporações, desafia a proteção de direitos fundamentais, especialmente a privacidade, a liberdade e a autodeterminação informativa. A vigilância digital, inicialmente justificada pela segurança, tornou-se estruturante nas relações sociais, econômicas e políticas, impondo reflexão sobre seus limites éticos e jurídicos. O problema central deste estudo é compatibilizar o uso de tecnologias de vigilância com a preservação dos direitos fundamentais. Formulam-se duas hipóteses: (i) a ausência de regulamentações robustas e mecanismos de controle social favorece práticas abusivas e desproporcionais; (ii) é possível harmonizar inovação tecnológica e prote-

---

1 A revisão linguística deste manuscrito foi realizada por Paola Filipini Ribeiro.

2 Doutorando em Direito; Mestre em Direito; Bacharel em Direito e em Teologia; Especialização em Direito, Internet e Sociedade, Direito Civil e Processual Civil, Direito do Trabalho, Direito Penal, e Direito Militar. Habilitações linguísticas, nível B1, nos idiomas: Espanhol (DELE), francês (DELF) e italiano (CILS). Lattes: http://lattes.cnpq.br/0703783803020290. direito.andersonfilipini@gmail.com, https://orcid.org/0009-0008-5145-2476.

3 Mestrando em Direito pelas Faculdades Londrina, possui graduação em Ciência Política pela Universidade de Brasília, e Direito pelo Centro Universitário Processus, especialização em Gestão Pública, Gestão de Processos BPM-CBOK, bem como Gestão das Águas e Sustentabilidade dos Recursos Hídricos no Brasil. Ex-Diretor da Agência Nacional de Águas e Saneamento Básico (ANA). Presidente do Instituto de Regulação, Inovação e Sustentabilidade (IRIS). Lattes: http://lattes.cnpq.br/4680398321828617. E-mail: filipemgm@gmail.com., https://orcid.org/0009-0005-7142-8885

4 Doutora em Ciências Jurídicas e Sociais. Mestra em Direito Negocial. Graduada em Direito. Advogada. Docente. Pesquisadora do grupo Democracia, Cidadania e Estado de Direito – DeCIED e junto ao Instituto Gilvan Hansen – IGH. Pesquisando, especialmente, nas áreas de Democracia e participação democrática, constitucionalismo latino-americano, modernidade periférica, tendo como bases teóricas principais Jürgen Habermas e Jessé Souza. E-mail: naty.alfaya@gmail.com. Lattes: http://lattes.cnpq.br/9731930696524695, https://orcid.org/0000-0002-0312-3677

Os autores declaram que este artigo pode ter contado, de forma assistiva, com ferramentas de inteligência artificial generativa, sendo, contudo, todo o conteúdo, argumentos, análises e conclusões integralmente concebidos, validados e aprovados pelos autores, que assumem responsabilidade acadêmica plena pelo trabalho.

ção de direitos fundamentais por meio de arcabouço normativo democrático, transparente e eticamente orientado. O objetivo geral é analisar os impactos da vigilância digital sobre direitos fundamentais, enfatizando deveres regulatórios de Estado e empresas. Os objetivos específicos incluem discutir riscos da coleta indiscriminada de dados, avaliar a efetividade das legislações e propor caminhos para uma governança digital ética e democrática. A metodologia consiste em revisão bibliográfica qualitativa com base em doutrina, legislação e relatórios técnicos. Conclui-se que a vigilância em massa impõe desafios inéditos à democracia, exigindo fortalecimento da cidadania digital, aprimoramento regulatório e políticas públicas que conciliem inovação, proteção de direitos e justiça informacional.

**Palavras-chave:** Vigilância digital; Privacidade; Proteção de dados; Direitos fundamentais; Governança digital.

**Abstract**

The digital age has intensified the use of monitoring technologies and the massive collection of personal data, shaping the so-called surveillance society. This phenomenon, led by states and corporations, challenges the protection of fundamental rights, especially privacy, freedom, and informational self-determination. Initially justified by security needs, digital surveillance has become a structural element of social, economic, and political relations, requiring reflection on its ethical and legal boundaries. The central problem of this study is reconciling the use of surveillance technologies with the preservation of fundamental rights. Two hypotheses are proposed: (i) the absence of robust regulations and effective social control mechanisms favors abusive and disproportionate practices; (ii) it is possible to harmonize technological innovation and the protection of fundamental rights through a democratic, transparent, and ethically oriented regulatory framework. The general objective is to analyze the impacts of digital surveillance on fundamental rights, emphasizing the regulatory duties of the state and companies. The specific objectives include discussing the risks of indiscriminate data collection, assessing the effectiveness of existing legislation, and proposing pathways for an ethical and democratic digital governance. The methodology consists of a qualitative bibliographic review based on legal doctrine, legislation, and technical reports. The study concludes that mass surveillance imposes unprecedented challenges to democracy, requiring the strengthening of digital citizenship, regulatory improvement, and public policies that reconcile innovation, rights protection, and informational justice.

**Keywords:** Digital surveillance; Privacy; Data protection; Fundamental rights; Digital governance.



## 1 INTRODUÇÃO

A sociedade contemporânea atravessa uma profunda transformação decorrente do avanço exponencial das tecnologias digitais e da ampla conectividade proporcionada pela internet, pelas redes móveis e pelas infraestruturas de dados em nuvem. Tais inovações vêm remodelando as formas de produção, comunicação, consumo e governança, ao mesmo tempo em que permitem um grau de monitoramento e controle social sem precedentes na história da humanidade. Essa reconfiguração estrutural, muitas vezes invisível aos olhos dos cidadãos comuns, é um dos traços mais marcantes daquilo que estudiosos como Shoshana Zuboff denominam de "capitalismo de vigilância" – um modelo econômico baseado na captura, processamento e

comercialização dos dados pessoais dos indivíduos como matéria-prima para a predição e a modulação de comportamentos.

Não se trata apenas de um fenômeno técnico, mas de uma reconfiguração política, jurídica e ética dos fundamentos da vida em sociedade. A digitalização dos processos sociais e administrativos, combinada com o poder de análise massiva de dados, tem permitido que governos e empresas coletem informações sensíveis em tempo real, muitas vezes sem o devido consentimento ou controle por parte dos titulares. Esse cenário desafia os modelos tradicionais de proteção da privacidade, exigindo uma reinterpretação dos direitos fundamentais à luz dos novos paradigmas tecnológicos. A vigilância, antes associada a mecanismos punitivos ou de segurança nacional, hoje se estende às atividades cotidianas dos indivíduos: hábitos de consumo, preferências ideológicas, deslocamentos urbanos, interações sociais e até mesmo dados biométricos e genéticos.

A literatura contemporânea sobre o tema tem apontado para uma crescente erosão dos espaços de anonimato, intimidade e autodeterminação informacional. Como adverte Stefano Rodotá, a privacidade na era digital deixou de ser um luxo ou uma esfera reservada e passou a ser uma condição de possibilidade da liberdade e da dignidade humanas. Em outras palavras, a vigilância ubíqua – operada por sensores, câmeras, algoritmos e inteligência artificial – redefine as fronteiras entre o público e o privado, tornando imperativo um debate profundo sobre os limites éticos e jurídicos da atuação estatal e empresarial no ciberespaço.

Nesse contexto, a relevância do presente estudo se evidencia tanto do ponto de vista científico quanto social. Do ponto de vista jurídico, a sociedade da vigilância desafia os pilares do constitucionalismo contemporâneo, em especial no que tange à proteção da esfera privada, à igualdade de tratamento e ao devido processo legal. A coleta massiva de dados pode levar à discriminação algorítmica, ao controle de massas e à supressão de liberdades civis, corroendo os fundamentos do Estado Democrático de Direito. Do ponto de vista social, há um claro desequilíbrio de poder entre os cidadãos e os entes que detêm capacidade técnica e econômica para processar grandes volumes de informações pessoais, ampliando assim a vulnerabilidade das populações já marginalizadas e dificultando a efetivação da justiça social.

O problema central que orienta esta investigação reside, portanto, na tensão entre os direitos individuais e os deveres institucionais em uma sociedade hiperconectada, em que a vigilância deixou de ser uma exceção para tornar-se uma lógica estrutural. Como assegurar, nesse novo paradigma, que os avanços tecnológicos não sejam utilizados para fins autoritários, discriminatórios ou mercantis que violem a autonomia dos indivíduos? Como equilibrar a necessidade de segurança pública com o respeito às garantias fundamentais? Quais os limites éticos, jurídicos e democráticos da vigilância em larga escala?

Partindo do problema central identificado, formulam-se duas hipóteses principais que orientam esta investigação. A primeira hipótese sustenta que, na ausência de regulamentações robustas e mecanismos eficazes de controle social, o avanço das tecnologias de vigilância tende a produzir um desequilíbrio estrutural entre a proteção da privacidade e as exigências de segurança, favorecendo práticas de coleta massiva de dados que violam direitos fundamentais. Essa hipótese pressupõe que a insuficiência de salvaguardas jurídicas e institucionais não apenas fragiliza a autode-

terminação informacional, mas também amplia riscos de discriminação algorítmica e vigilância abusiva por parte de agentes estatais e privados.

A segunda hipótese parte da premissa de que é possível compatibilizar inovação tecnológica e proteção dos direitos fundamentais mediante a adoção de um arcabouço normativo democrático, transparente e baseado em princípios éticos claros. Nessa perspectiva, legislações como a LGPD brasileira e o GDPR europeu oferecem pistas relevantes, mas ainda carecem de efetividade prática diante da opacidade algorítmica e da transnacionalidade dos fluxos de dados. Essa hipótese considera que a aplicação consistente desses marcos, combinada a mecanismos de auditoria, participação social e accountability, poderia mitigar os riscos inerentes à sociedade de vigilância e promover um ambiente digital mais equilibrado, justo e respeitoso à dignidade humana.

Assim, a investigação parte da compreensão de que o teste empírico e teórico dessas hipóteses permitirá identificar se o atual arranjo normativo e institucional é capaz de responder adequadamente aos desafios impostos pela vigilância digital. Ao articular o diagnóstico sobre as fragilidades regulatórias com a análise comparada de experiências internacionais, busca-se não apenas confirmar ou refutar as hipóteses, mas também oferecer subsídios concretos para o aprimoramento das políticas públicas e das práticas empresariais no tratamento de dados pessoais. Dessa forma, a pesquisa pretende contribuir para o delineamento de um modelo de governança digital que assegure a efetividade dos direitos fundamentais, harmonizando inovação, segurança e justiça informacional.

A justificativa do estudo repousa na urgência de se compreender e regulamentar os mecanismos de vigilância que moldam a vida social e institucional na era digital. Ainda que haja avanços normativos relevantes, como a promulgação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) no Brasil e o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), permanece uma lacuna significativa entre a legislação formal e as práticas efetivas de monitoramento exercidas tanto por órgãos públicos quanto por plataformas digitais privadas. A crescente sofisticação dos sistemas de inteligência artificial e a opacidade dos algoritmos agravam esse desafio, pois muitas decisões automatizadas que afetam diretamente a vida dos cidadãos – como concessão de crédito, ofertas de emprego, triagem de segurança e acesso a políticas públicas – ocorrem sem transparência, accountability ou possibilidade de contestação.

Assim, o presente artigo tem como objetivo geral analisar os impactos da vigilância digital sobre os direitos fundamentais, à luz da atuação do Estado e das empresas no tratamento e controle de dados pessoais. De forma mais específica, busca-se: (i) compreender os riscos e desafios jurídicos relacionados à coleta e tratamento massivo de dados; (ii) examinar as implicações da vigilância para a privacidade, liberdade, igualdade e dignidade dos indivíduos; (iii) avaliar o papel do Estado na regulação e fiscalização dessas práticas; e (iv) propor caminhos para o fortalecimento de uma governança digital ética, democrática e voltada à proteção dos direitos humanos.

A metodologia adotada é a revisão bibliográfica de caráter qualitativo, com enfoque interdisciplinar, incorporando referenciais das áreas do Direito, da Ciência Política, da Sociologia e da Filosofia. São examinadas obras clássicas e contemporâ-

neas de autores como Ferdinand Lassale, Stefano Rodotá, Shoshana Zuboff, Holmes e Sunstein, entre outros, além de documentos normativos nacionais e internacionais, pareceres técnicos e relatórios de pesquisa sobre proteção de dados, vigilância digital e direitos fundamentais. O método permite uma análise crítica das práticas de vigilância, observando seus efeitos concretos sobre a cidadania e o ordenamento jurídico, com vistas à formulação de propostas regulatórias adequadas ao contexto atual.

A estrutura do artigo está dividida em seis partes, além da introdução e das considerações finais. O segundo capítulo apresenta as perspectivas teóricas e doutrinárias sobre o fenômeno da vigilância digital, contextualizando suas origens, fundamentos e implicações. O terceiro capítulo discute o papel do Estado, suas responsabilidades constitucionais e as tensões entre segurança e liberdade. No quarto capítulo, analisa-se a atuação das empresas privadas e o desafio de compatibilizar os modelos de negócios baseados em dados com a proteção dos direitos fundamentais. O quinto capítulo aborda os impactos concretos da vigilância sobre os direitos da personalidade, com destaque para a privacidade, o direito ao esquecimento e a discriminação algorítmica. O sexto capítulo examina os desafios e as perspectivas para o futuro, propondo alternativas normativas, éticas e institucionais para uma governança digital que respeite os princípios democráticos.

Em síntese, este estudo propõe-se a contribuir para o debate acadêmico e institucional sobre os limites e possibilidades da vigilância digital em uma sociedade plural, democrática e comprometida com a promoção dos direitos humanos. A reflexão crítica sobre os dispositivos normativos existentes, os riscos de um controle tecnológico desregulado e as estratégias para a construção de uma cidadania digital ativa constituem os principais aportes da pesquisa. Em um mundo cada vez mais orientado por dados, algoritmos e plataformas digitais, garantir a liberdade, a transparência e a justiça informacional é uma tarefa coletiva e urgente – uma tarefa que exige não apenas leis, mas também consciência crítica, responsabilidade institucional e participação social.

## 2 PERSPECTIVAS CONTEMPORÂNEAS SOBRE VIGILÂNCIA E DIREITO

A sociedade contemporânea é marcada por um intenso debate sobre a vigilância digital e seus impactos nos direitos fundamentais. Para compreender esse fenômeno acerca da interseção entre constituição, privacidade, liberdade e regulação estatal, Lassale argumenta que a Constituição não é um mero conjunto de normas jurídicas, mas sim a expressão das forças sociais dominantes em determinada época. Assim, no contexto da vigilância digital, a Constituição deve refletir os desafios impostos pela tecnologia ao equilíbrio entre segurança e privacidade (Lassale, 1998).

Discutindo sobre a vigilância digital, Rodotá reforça a ideia de que a privacidade é um direito essencial na era da informação. Para ele, a vigilância em massa realizada por Estados e empresas representa um risco significativo à autonomia dos indivíduos. Nesse sentido, a privacidade não pode ser vista apenas como um direito individual, mas como um pilar fundamental para a manutenção da democracia e da dignidade humana (Rodotá, 2008).

A relação entre liberdade, segurança e regulação estatal segundo Holmes e Sunstein não existe sem uma estrutura que a sustente, sendo necessária uma regulação eficaz para equilibrar os interesses do Estado e dos cidadãos. Nesse contexto, a vigilância digital pode ser justificada sob o pretexto da segurança pública, mas, sem mecanismos de controle adequados, pode levar à supressão de direitos fundamentais (Holmes; Sunstein, 2019).

Zuboff, por sua vez, introduz o conceito de capitalismo de vigilância, destacando o papel das grandes corporações no monitoramento de dados. Segundo a autora, empresas de tecnologia capturam informações pessoais para prever e influenciar o comportamento dos indivíduos, criando uma economia baseada na extração e comercialização de dados. Esse modelo, além de comprometer a privacidade, também redefine as relações de poder na sociedade contemporânea (Zuboff, 2021).

De acordo com Corrêa e Fagundes Filho, a neutralidade da rede e a proteção de dados pessoais são temas centrais na sociedade de vigilância. A ausência de uma regulação eficiente pode resultar na exploração desenfreada das informações dos usuários por empresas que operam em mercados digitais desregulados (Corrêa; Fagundes Filho, 2022).

Silva destaca que a positivação da proteção de dados como direito fundamental é uma necessidade urgente na era do capitalismo de vigilância. O autor argumenta que a manipulação de informações pessoais sem consentimento explícito compromete a autodeterminação informacional dos indivíduos, exigindo uma abordagem jurídica que assegure maior controle sobre os próprios dados (Silva, 2021).

O avanço tecnológico fortalece o empoderamento do Estado em práticas de vigilância. Figueiredo et al., argumenta que a coleta e o tratamento de dados pessoais tornam-se instrumentos de controle social, desafiando os princípios constitucionais de privacidade e proteção de dados. A expansão dessas práticas sem regulamentação adequada pode gerar cenários de abuso e discriminação (Figueiredo et al., 2021).

A perspectiva histórica também auxilia na compreensão desse fenômeno, tendo em vista que segundo Monteagudo (2021), a democracia contemporânea enfrenta desafios inéditos diante da vigilância ubíqua, que compromete a transparência e a confiança nas instituições. O autor ressalta a necessidade de políticas públicas que limitem a invasão da privacidade em nome da segurança nacional (Monteagudo, 2021).

Martin (2024) discute o abandono digital e a necessidade de um dever de vigilância parental na internet. A ausência de supervisão pode expor crianças e adolescentes a riscos, tornando imprescindível o desenvolvimento de mecanismos de proteção adequados para esse público vulnerável.

No que tange à regulamentação de algoritmos, Verbicaro (2022) aponta os desafios inerentes à governança digital, alertando que a tomada de decisões automatizadas baseada em dados pessoais pode levar à discriminação algorítmica, reforçando desigualdades e ameaçando princípios democráticos. A segurança pública é frequentemente utilizada como justificativa para a intensificação da vigilância, quando desprovida de critérios claros, pode se transformar em uma ferramenta de repressão estatal, impactando diretamente os direitos humanos (Alberti, 2022).

A proteção da privacidade na sociedade da informação exige novos parâmetros jurídicos. A esse respeito, Canavez, Santos e Mendes (2022) defendem o reconhecimento de novos direitos fundamentais para garantir que os cidadãos tenham maior autonomia sobre seus dados, resguardando-se contra abusos tanto do setor público quanto do privado. Siqueira et al. (2023) analisam a (in)aplicabilidade desse direito no ordenamento jurídico brasileiro, destacando os desafios em equilibrar liberdade de expressão e proteção da reputação individual.

O consentimento dos usuários na coleta de dados é outro ponto crítico. Acerca dessa questão, Souza e Lima (2021) discutem o alcance desse consentimento, ressaltando que, muitas vezes, os termos de uso das plataformas digitais são excessivamente complexos, dificultando uma decisão informada por parte dos cidadãos.

Portanto, a era digital exige novas abordagens regulatórias para garantir que a vigilância não se torne uma ameaça irreversível às liberdades individuais, havendo a necessidade de um equilíbrio entre inovação tecnológica e respeito aos direitos fundamentais, evitando que a democracia seja corroída por práticas abusivas de monitoramento (Monteagudo, 2021).

## 3 O PAPEL DO ESTADO NA SOCIEDADE DE VIGILÂNCIA

A proteção da privacidade e dos dados pessoais tornou-se uma responsabilidade fundamental do Estado na era da sociedade de vigilância. Alberti (2022, p. 116), destaca que a:

> *Vigilância em massa tem sido justificada como um mecanismo de segurança pública, mas frequentemente entra em conflito com garantias fundamentais, como a privacidade e a proteção de dados. Nesse contexto, cabe ao Estado equilibrar esses interesses, assegurando que a coleta e o uso de informações pessoais não ultrapassem os limites impostos pelos direitos humanos.*

No cenário normativo, diversas regulamentações foram implementadas para garantir a proteção de dados e a privacidade. A Lei Geral de Proteção de Dados – LGPD no Brasil, inspirada no Regulamento Geral de Proteção de Dados – GDPR europeu, visa estabelecer limites claros para o tratamento de informações pessoais (Canavez; Santos; Mendes, 2022). Essas regulamentações buscam conferir maior autonomia aos cidadãos sobre seus dados, impondo sanções a empresas e órgãos que não cumpram as diretrizes estabelecidas.

A neutralidade da rede também se apresenta como um aspecto essencial na proteção dos dados pessoais, evitando práticas discriminatórias e garantindo a equidade no acesso à informação. Corrêa e Fagundes Filho (2022) discutem como a manutenção desse princípio se torna desafiadora diante do avanço das tecnologias de monitoramento e do crescimento das grandes corporações digitais, que frequentemente capturam dados sem o devido consentimento.

No contexto da vigilância estatal, um dos principais desafios é o embate entre segurança pública e direitos individuais. Conforme analisa Silva (2021), a positivação da proteção de dados como direito fundamental se faz necessária para evitar que medidas governamentais voltadas à segurança acabem por ferir garantias fundamentais. Esse debate se intensifica com o avanço das tecnologias de reconhecimento facial e monitoramento em espaços públicos.

Figueiredo et al. (2021) ressaltam que a coleta massiva de dados pode transformar-se em um instrumento de repressão, colocando em risco a autonomia individual e o direito à privacidade. Assim, torna-se imprescindível que a legislação imponha limites rígidos ao uso dessas tecnologias pelo poder público.

A teoria constitucional de Lassale (1998) também contribui para esse debate ao demonstrar que a Constituição reflete as forças sociais predominantes. Nesse sentido, a inclusão da proteção de dados como direito fundamental representa uma resposta da sociedade às novas ameaças impostas pela era digital, exigindo que o Estado desempenhe um papel ativo na regulação e fiscalização das práticas de vigilância.

No contexto da infância e adolescência, Martin (2024) alerta para a necessidade de vigilância parental no ambiente digital, destacando o abandono digital como uma nova problemática. Corroborando com esse abandono digital, a ausência de regulamentações específicas para proteger menores de idade no espaço virtual reforça a importância da atuação estatal na criação de mecanismos eficazes de proteção e controle.

A democracia também sofre impactos com a crescente vigilância, pois segundo Monteagudo (2021) a vigilância ubíqua e os riscos que ela representa para as liberdades civis, aumentam quando utilizada como ferramenta de repressão política. O Estado, portanto, deve garantir que seus mecanismos de controle não se tornem instrumentos de cerceamento da participação democrática.

Rodotá (2008) argumenta que a privacidade se tornou um direito essencial, especialmente em um cenário em que governos e corporações acumulam volumes gigantescos de informações pessoais. Nesse aspecto, a atuação estatal deve, portanto, priorizar a garantia desse direito, promovendo um equilíbrio entre inovação tecnológica e proteção da dignidade humana.

No que diz respeito à relação entre liberdade, segurança e regulação estatal, conforme Holmes e Sunstein (2019), a liberdade depende diretamente da capacidade do Estado de fornecer mecanismos de proteção e segurança. Assim, a regulamentação da vigilância deve ser acompanhada de medidas que garantam transparência e controle social sobre o uso das informações coletadas.

O capitalismo de vigilância, conceito amplamente discutido por Zuboff (2021), reforça o papel do Estado na regulação das grandes corporações tecnológicas que ao capturarem e comercializarem dados pessoais, desafiam o poder regulatório estatal e impõem novos desafios à proteção da privacidade e à autodeterminação informacional dos cidadãos.

A aplicabilidade das tecnologias disruptivas, como o reconhecimento facial, em sistemas de vigilância pública no Brasil levanta questionamentos sobre sua compatibilidade com o direito constitucional à privacidade. Silva (2022) analisa como a ausência de regulamentação específica pode resultar em abusos e violações de direitos fundamentais.

A questão do direito ao esquecimento também se insere nesse debate. Nesse sentido, Siqueira et al. (2023) examinam a (in) aplicabilidade desse direito no ordenamento jurídico brasileiro, evidenciando a necessidade de proteção contra a perpetuidade de informações prejudiciais na internet, cabendo ao Estado estabelecer

diretrizes claras para equilibrar o direito à informação e a proteção da reputação individual.

Souza e Lima (2021) discutem como, na sociedade da informação, o consentimento se tornou um instrumento muitas vezes ilusório, sendo necessário que o Estado adote medidas que garantam um controle mais efetivo sobre a coleta e o uso das informações pessoais.

A regulação dos algoritmos, como destaca Verbicaro (2022), representa um dos maiores desafios na proteção da privacidade. O uso crescente de inteligência artificial na tomada de decisões governamentais exige um arcabouço normativo que impeça práticas discriminatórias e assegure a transparência na utilização desses sistemas.

Dessa forma, a atuação estatal na sociedade da vigilância deve priorizar a proteção dos direitos fundamentais, garantindo que a busca por segurança não se transforme em um instrumento de controle excessivo. A adoção de políticas públicas que promovam a transparência, o consentimento informado e a fiscalização rigorosa sobre o uso de tecnologias de vigilância é essencial para a preservação das liberdades individuais na era digital.

## 4 O PAPEL DAS EMPRESAS E A VIGILÂNCIA PRIVADA

A coleta massiva de dados por empresas de tecnologia tem se tornado uma das principais características da sociedade da informação. Essas corporações atuam como intermediárias no fluxo de dados, coletando informações pessoais a partir de diferentes fontes, como redes sociais, aplicativos e dispositivos conectados. Segundo Zuboff (2021), essa dinâmica configura o chamado "capitalismo de vigilância", no qual os dados dos usuários são transformados em mercadoria para fins comerciais e de previsibilidade comportamental.

O consentimento do usuário, embora seja um princípio fundamental na proteção de dados, muitas vezes se apresenta de forma questionável. Conforme destacam Canavez, Santos e Mendes (2022), as políticas de privacidade frequentemente utilizam linguagem complexa e pouco acessível, levando os usuários a conceder permissões sem compreender completamente as implicações de seus atos. Esse cenário levanta o debate sobre a real validade do consentimento no contexto da vigilância privada.

Segundo Verbicaro (2021), a regulamentação do uso de algoritmos é um dos principais desafios do Marco Civil da Internet, pois afeta diretamente os direitos fundamentais dos cidadãos. Assim, a falta de clareza nos processos algorítmicos compromete a autonomia dos indivíduos e aumenta os riscos de discriminação e manipulação digital.

A responsabilidade corporativa na era digital se tornou uma questão central nos debates sobre proteção de dados e direitos fundamentais. Como apontam Souza e Lima (2021), as empresas precisam adotar medidas efetivas de governança de dados, assegurando que as informações coletadas sejam utilizadas de maneira ética e em conformidade com a legislação vigente. Isso inclui a implementação de mecanismos de auditoria e compliance para evitar abusos.

A Lei Geral de Proteção de Dados – LGPD no Brasil e o Regulamento Geral de Proteção de Dados – GDPR na União Europeia são marcos regulatórios que esta-

belecem diretrizes para a coleta e o tratamento de dados pessoais. Nesse contexto, de acordo com Corrêa e Fagundes Filho (2022), a neutralidade da rede e a segurança da informação são aspectos essenciais para garantir a privacidade dos usuários diante do avanço da vigilância digital.

A massiva coleta de dados por empresas privadas também tem impactos significativos na segurança pública e na proteção dos direitos individuais. Monteagudo (2021) destaca que a utilização de tecnologias de vigilância por corporações pode resultar na restrição de liberdades e no monitoramento excessivo, criando um ambiente propício para violações de direitos fundamentais.

As tecnologias disruptivas, como o reconhecimento facial, também são tema de preocupação no debate sobre privacidade e segurança digital, pois conforme Silva (2022), esses sistemas têm sido amplamente utilizados por empresas e pelo Estado, muitas vezes sem transparência ou controle adequado, levantando questionamentos sobre a efetividade dos direitos constitucionais à privacidade.

A aplicação de sanções e penalizações é uma medida necessária para garantir que as empresas cumpram suas obrigações em relação à proteção de dados. Segundo Siqueira et al. (2023), a discussão sobre o direito ao esquecimento exemplifica a necessidade de criar mecanismos para que os indivíduos possam controlar suas informações pessoais e exigir a remoção de conteúdos prejudiciais.

Se alerta que a legislação também precisa acompanhar as inovações tecnológicas para evitar lacunas que permitam abusos, pois conforme Lassale (1998), a Constituição deve refletir a realidade social e econômica do seu tempo, garantindo proteção eficaz contra violações dos direitos fundamentais.

Rodotá (2008) enfatiza que a privacidade deve ser resguardada como um direito essencial na sociedade da vigilância. A interação entre Estado e corporações na gestão de informações pessoais deve seguir princípios democráticos, evitando que os cidadãos sejam reduzidos a meros objetos de controle.

Outro aspecto relevante é o abandono digital, no qual a exposição excessiva de crianças e adolescentes na internet evidencia a necessidade de maior vigilância parental e regulação. Martin (2024) argumenta que o princípio da proteção integral exige que tanto o Estado quanto as empresas garantam a segurança digital de menores.

A economia de dados e os modelos de negócios baseados na exploração de informações pessoais também devem ser analisados criticamente. A esse respeito, Holmes e Sustein (2019) apontam que a liberdade individual depende diretamente de regulações eficazes, pois sem elas, o poder econômico das empresas pode comprometer a autodeterminação dos indivíduos.

Portanto, a sociedade contemporânea enfrenta desafios constantes para equilibrar inovação tecnológica e direitos fundamentais. Como ressaltam dos Reis Silva (2021), a positivacão da proteção de dados como um direito fundamental é essencial para garantir que os avanços digitais ocorram de maneira justa e ética, resguardando a dignidade dos cidadãos.

## 5 IMPACTOS DA VIGILÂNCIA SOBRE DIREITOS FUNDAMENTAIS

A vigilância massiva promovida por empresas e governos tem levantado questões complexas sobre a proteção dos direitos da personalidade e da privacidade

na era digital. A coleta indiscriminada de dados pessoais por meio de dispositivos eletrônicos e plataformas digitais compromete a autonomia individual e cria um ambiente de monitoramento constante. Como destaca Alberti (2022), a segurança frequentemente é utilizada como justificativa para a ampliação da vigilância, mas essa prática pode resultar na restrição de direitos fundamentais.

A privacidade, tradicionalmente considerada um direito inalienável, tem sido relativizada diante dos avanços tecnológicos e das demandas do mercado digital. Discutindo a esse respeito, Canavez, Santos e Mendes (2022) apontam que o crescimento da sociedade da informação exige o reconhecimento de novos direitos fundamentais, incluindo o direito à proteção de dados pessoais. A regulamentação desses direitos é essencial para evitar abusos e garantir que os indivíduos mantenham o controle sobre suas informações.

A questão do direito ao esquecimento emerge como um desafio na contemporaneidade, especialmente no contexto da internet. Corrêa e Fagundes Filho (2022) discutem como a neutralidade da rede mundial de computadores impacta a proteção de dados pessoais, destacando que a perpetuação de informações pode ser prejudicial à dignidade dos indivíduos. Dessa forma, a possibilidade de exclusão de registros desatualizados ou prejudiciais torna-se um aspecto fundamental da proteção da personalidade.

O capitalismo de vigilância, conceito abordado por Silva (2021), transforma dados pessoais em mercadoria, explorando informações privadas para fins econômicos. Esse modelo compromete a soberania dos indivíduos sobre suas próprias informações e reforça desigualdades sociais, uma vez que o controle sobre os dados é amplamente detido por grandes corporações tecnológicas.

O uso de tecnologias disruptivas tem aprofundado os desafios relacionados à vigilância, particularmente no que tange ao reconhecimento facial em espaços públicos. Figueiredo et al. (2021) destacam que a coleta e o tratamento massivo de dados biométricos representam um instrumento de controle estatal e empresarial, podendo comprometer liberdades individuais e gerar discriminação automatizada.

A essência constitucional da proteção da privacidade é debatida por Lassale (1998), que argumenta que uma constituição eficaz deve refletir as necessidades sociais de sua época. Nesse sentido, a inclusão da proteção de dados como direito fundamental reflete a evolução da sociedade e a necessidade de salvaguardar os cidadãos contra abusos tecnológicos.

A vigilância digital também impacta grupos vulneráveis, como as crianças e adolescentes. Martin (2024) ressalta que o abandono digital e a falta de um dever de vigilância parental adequado podem expor menores a riscos significativos, exigindo políticas públicas mais eficazes para garantir a proteção infantil no ambiente digital.

A democracia também é afetada por esse cenário, conforme argumenta Monteagudo (2021), que discute os riscos da vigilância ubíqua para as instituições democráticas. O monitoramento excessivo da população pode minar a liberdade de expressão e inibir a participação política, enfraquecendo os princípios democráticos.

Rodotá (2008) explora como a vida na sociedade da vigilância impacta os direitos individuais, alertando para a necessidade de um equilíbrio entre segurança e liberdade. Para o autor, é fundamental que os Estados implementem mecanismos de regulação e controle sobre a coleta e o uso de dados pessoais.

A implementação de tecnologias de reconhecimento facial é uma preocupação crescente. Silva (2022) discute as implicações da utilização dessas ferramentas em sistemas de vigilância pública, destacando o risco de violação da privacidade e a possibilidade de erros na identificação de indivíduos, que podem resultar em injustiças.

O direito ao esquecimento é um tema polêmico na jurisprudência brasileira, Siqueira et al. (2023) analisam a (in)aplicabilidade desse direito no ordenamento jurídico, demonstrando que a falta de uma regulamentação clara pode gerar conflitos entre liberdade de expressão e proteção da privacidade.

Holmes e Sunstein (2019) argumentam que a garantia de direitos fundamentais depende da existência de uma estrutura regulatória eficiente, voltada à proteção de dados, que requer legislação robusta e fiscalização para evitar abusos por parte do setor privado e do Estado.

Verbicaro (2021) destaca que o Marco Civil da Internet ainda apresenta lacunas na regulamentação da inteligência artificial e dos mecanismos de tomada de decisão automatizados, necessitando de aprimoramentos para garantir a transparência e a responsabilidade dos agentes envolvidos.

A resistência a essa dinâmica exige uma atuação conjunta entre sociedade civil, governos e instituições reguladoras, promovendo maior transparência e responsabilidade na utilização das informações pessoais.

## 6 DESAFIOS E PERSPECTIVAS PARA O FUTURO

A crescente digitalização da sociedade tem impulsionado a necessidade de regulamentações mais eficazes para lidar com os desafios impostos pela vigilância em massa. A ausência de marcos normativos robustos compromete a proteção dos direitos fundamentais, como a privacidade e a autodeterminação informativa. Conforme Alberti (2022), a segurança pública muitas vezes é utilizada como justificativa para a ampliação da vigilância estatal e corporativa, sem que haja um devido equilíbrio entre proteção e liberdade individual. Dessa forma, torna-se imprescindível a criação de políticas que limitem a coleta e o uso indiscriminado de dados pessoais.

A evolução dos direitos digitais reflete a urgência do reconhecimento de novas garantias fundamentais na sociedade da informação. Canavez, Santos e Mendes (2022) argumentam que a privacidade e a proteção de dados passaram a ser considerados direitos essenciais para o exercício da cidadania digital. No entanto, a efetivação desses direitos ainda encontra barreiras estruturais e legislativas, sendo necessário um esforço coletivo entre Estado, empresas e sociedade civil para garantir que as normas acompanhem o avanço tecnológico sem comprometer liberdades individuais.

No contexto da sociedade de vigilância, a neutralidade da rede e a proteção de dados pessoais são temas de grande relevância. Corrêa e Fagundes Filho (s.d.) destacam que a implementação de regulações que assegurem um ambiente digital mais democrático e seguro é fundamental para mitigar os impactos da hiperconectividade. A falta de transparência na coleta e uso de informações pessoais pelos provedores de serviços de internet compromete o direito à privacidade, exigindo maior fiscalização e regulamentação.

A positivação da proteção de dados como direito fundamental emerge como um mecanismo essencial para garantir maior segurança jurídica aos cidadãos. Se-

gundo Silva (2021), a consolidação desse direito na esfera constitucional é uma resposta à crescente exploração econômica dos dados pessoais, especialmente no contexto do capitalismo de vigilância. Sem uma base jurídica sólida, os indivíduos permanecem vulneráveis à mercantilização de suas informações e ao uso indevido de seus dados.

A regulamentação da vigilância estatal deve levar em consideração a necessidade de equilíbrio entre segurança e liberdade. Figueiredo et al. (2021) ressaltam que o empoderamento tecnológico do Estado de vigilância tem implicações diretas sobre o direito constitucional à privacidade. Assim, a implementação de mecanismos de controle e fiscalização se torna indispensável para evitar abusos e assegurar que a coleta de dados atenda a critérios estritos de necessidade e proporcionalidade.

O debate sobre ética e transparência na vigilância digital é crucial para garantir uma governança mais responsável das tecnologias emergentes. Lassale (1998) destaca que a Constituição reflete a realidade social e deve evoluir conforme as transformações tecnológicas e culturais. Dessa forma, a atualização dos marcos normativos é necessária para garantir que os princípios democráticos sejam preservados em um cenário de crescente monitoramento digital.

A regulamentação das tecnologias disruptivas, como o reconhecimento facial, também demanda uma abordagem mais criteriosa. Silva (2022) alerta que o uso indiscriminado desse tipo de tecnologia em espaços públicos pode comprometer a efetividade do direito à privacidade, reforçando práticas discriminatórias e ampliando a vigilância estatal sem o devido controle social. Assim, políticas que estabeleçam limites claros para o uso dessas ferramentas são fundamentais para garantir sua aplicação de forma ética e responsável.

Stephen e Sunstein (2019) enfatizam que a liberdade individual está intrinsecamente ligada à existência de regulamentações que garantam direitos e deveres no ambiente digital. Dessa forma, o desenvolvimento de normas mais rígidas sobre a coleta, armazenamento e compartilhamento de dados é essencial para assegurar a dignidade e a autonomia dos cidadãos.

Portanto, a criação de um arcabouço regulatório sólido e atualizado deve ser acompanhada de um amplo debate público sobre os impactos da vigilância digital. Souza e Lima (2021) defendem que a participação da sociedade civil na formulação de políticas de proteção de dados é um fator determinante para a construção de um modelo mais transparente e democrático. Somente por meio do diálogo e da cooperação entre diferentes setores será possível enfrentar os desafios da vigilância digital e garantir a efetivação dos direitos fundamentais na era da informação.

## 7 CONSIDERAÇÕES FINAIS

A presente análise permitiu compreender os complexos desafios impostos pela sociedade da vigilância na era digital, destacando os impactos profundos da coleta e tratamento massivo de dados sobre os direitos fundamentais. Ao longo do estudo, foram explorados os limites da privacidade, o avanço das tecnologias de monitoramento e a urgência da criação de regulamentações eficazes que protejam os cidadãos em um cenário marcado pela hiperconectividade e pelo uso intensivo de dados pessoais.

A crescente interconectividade, impulsionada por algoritmos sofisticados e sistemas de inteligência artificial, tem intensificado as práticas de vigilância por parte de governos e corporações. Isso torna indispensável um debate ético, jurídico e político sobre os rumos da governança digital, exigindo maior transparência na formulação e aplicação de políticas de controle de dados. Os mecanismos de vigilância, embora frequentemente justificados com base na segurança pública, não podem se converter em instrumentos de repressão, manipulação ou exclusão social.

Um dos grandes dilemas contemporâneos reside no esforço para encontrar um equilíbrio legítimo entre segurança e privacidade. A justificativa do monitoramento como ferramenta de prevenção a crimes e ameaças à ordem pública não pode ser utilizada como subterfúgio para a supressão de garantias individuais. Ao mesmo tempo, a ausência de mecanismos eficazes de fiscalização e de accountability por parte das autoridades públicas e empresas privadas expõe os indivíduos a riscos de exposição, discriminação e desinformação. Torna-se, portanto, essencial estabelecer normas claras que assegurem os princípios da finalidade, da proporcionalidade e da minimização de dados, resguardando a dignidade e a autonomia dos usuários no ambiente digital.

A proteção de dados precisa ser encarada como um direito fundamental em sentido pleno, com status constitucional e operacionalização efetiva. Para isso, é imperativo o fortalecimento das políticas públicas que assegurem sua implementação, bem como a capacitação de órgãos de controle, como autoridades de proteção de dados e defensorias públicas digitais. O sistema jurídico deve evoluir de modo a oferecer não apenas sanções aos abusos, mas também garantias de reparação e mecanismos preventivos.

Além da perspectiva normativa, destaca-se a importância da cidadania digital como elemento central na resistência à vigilância excessiva. O empoderamento informacional dos cidadãos, por meio da educação crítica e da conscientização sobre os seus direitos no espaço digital, é condição indispensável para a construção de uma cultura de privacidade. Nesse sentido, o ensino sobre proteção de dados e privacidade nas escolas, universidades e espaços públicos deve ser incorporado como conteúdo transversal, fomentando uma postura ativa de proteção e exigência de direitos por parte da sociedade.

Outro aspecto que merece destaque é a comparação internacional dos marcos normativos. Experiências como o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, a Lei de Privacidade da Califórnia (CCPA) e a Lei de Proteção de Dados Pessoais da África do Sul (POPIA) demonstram caminhos distintos de regulamentação, com diferentes graus de sucesso e eficácia. A partir dessas experiências, é possível identificar boas práticas e princípios fundamentais, como o privacy by design, a obrigação de prestação de contas (accountability) e o direito à portabilidade dos dados. A análise comparada também revela a necessidade de adaptação das normas nacionais às especificidades culturais, econômicas e tecnológicas de cada país, garantindo que os direitos fundamentais não sejam subordinados a interesses econômicos ou políticos.

A vigilância digital, além de um problema jurídico, é também uma questão ética e civilizatória. O avanço das tecnologias de reconhecimento facial, rastreamento em tempo real, escuta automatizada e monitoramento de redes sociais desafia os

limites daquilo que se entende por liberdade, intimidade e anonimato. Em sociedades democráticas, a proteção dos espaços de autonomia pessoal é indispensável à construção de identidades, ao dissenso político e à pluralidade cultural. A vigilância excessiva, por sua vez, tende a homogeneizar comportamentos e instaurar uma lógica de controle e punição incompatível com os valores republicanos.

Do ponto de vista institucional, é necessário garantir que as autoridades de proteção de dados tenham independência funcional, recursos técnicos e orçamentários adequados e canais efetivos de interação com os cidadãos. O enforcement dos direitos digitais exige um aparato institucional robusto, capaz de fiscalizar, aplicar sanções, conduzir investigações e promover a cultura da proteção de dados. Nesse aspecto, o papel do Ministério Público, do Judiciário e das organizações da sociedade civil é central para assegurar o cumprimento da legislação e coibir práticas abusivas.

A atuação das empresas também precisa ser repensada. A responsabilidade corporativa no uso ético dos dados deve ir além do cumprimento formal das leis. É preciso adotar políticas de compliance que incluam auditorias externas, mecanismos de revisão algorítmica, comitês de ética em tecnologia e programas contínuos de treinamento. Empresas que coletam, armazenam e utilizam dados de forma massiva devem assumir compromissos transparentes com a sociedade, inclusive quanto à explicabilidade e aos critérios usados na personalização de conteúdo, preços dinâmicos, classificação de perfis e exclusões automatizadas.

No contexto educacional, a promoção da literacia digital é essencial para que os indivíduos compreendam como seus dados são coletados, processados e utilizados, e que possam exercer seus direitos de forma informada e consciente. Isso inclui desde o entendimento sobre o funcionamento de cookies e algoritmos até o conhecimento sobre os direitos de acesso, retificação, oposição e exclusão de dados. O desenvolvimento de competências digitais não é apenas uma ferramenta de inclusão, mas uma estratégia de resistência ao controle social e de fortalecimento da cidadania.

No que tange ao futuro, é possível prever que as práticas de vigilância se tornarão cada vez mais sofisticadas, integradas e onipresentes. Tecnologias emergentes como o 6G, a computação quântica, a internet das coisas e a neurotecnologia ampliam a capacidade de captura e inferência de dados, incluindo aqueles relacionados a padrões cerebrais, comportamentos inconscientes e emoções. Isso exige uma revisão contínua dos marcos regulatórios e uma reflexão profunda sobre os limites do que é aceitável em termos de intervenção tecnológica na vida privada.

As tecnologias de reconhecimento facial, por exemplo, vêm sendo utilizadas para fins diversos, como policiamento preditivo, controle de fronteiras, seleção de candidatos a empregos e concessão de crédito. Sem critérios claros de proporcionalidade, transparência e auditoria, esses sistemas podem reforçar vieses discriminatórios, criminalizar populações vulneráveis e perpetuar desigualdades estruturais. É urgente que se estabeleçam limites éticos e jurídicos rígidos à implementação dessas ferramentas, assegurando que seu uso esteja sempre subordinado ao interesse público legítimo e aos direitos fundamentais.

Adicionalmente, o uso de inteligência artificial na tomada de decisões públicas – como concessão de benefícios, triagem de pacientes ou alocação de recursos – deve ser pautado por princípios de justiça algorítmica, imparcialidade, auditabilidade e explicabilidade. O risco de discriminação automatizada é real e deve ser enfrenta-

do com políticas públicas rigorosas, incluindo a obrigatoriedade de relatórios de impacto algorítmico, consulta pública prévia e mecanismos de contestação.

A vigilância digital também levanta questões importantes sobre os limites da soberania nacional. Muitas vezes, os dados dos cidadãos de um país são processados em servidores localizados no exterior, sob jurisdição de outras legislações. Isso exige acordos internacionais que garantam o respeito aos direitos fundamentais transnacionais e a interoperabilidade entre sistemas de proteção de dados. A cooperação internacional é crucial para enfrentar práticas transfronteiriças de violação de privacidade, como espionagem cibernética, comércio ilegal de dados e propaganda política direcionada.

Por fim, é fundamental que o debate sobre vigilância digital não se restrinja a especialistas e instituições. A participação cidadã na formulação de leis, políticas e padrões técnicos é essencial para garantir que as tecnologias respeitem a diversidade, os valores democráticos e os direitos humanos. A transparência algorítmica e a justiça digital só serão efetivas se forem acompanhadas por espaços públicos de deliberação, controle social e corresponsabilidade.

Portanto, a sociedade da vigilância impõe desafios que exigem respostas rápidas, assertivas e sustentáveis. A busca pelo equilíbrio entre inovação tecnológica, segurança e proteção dos direitos fundamentais deve ser um compromisso contínuo, ancorado na ética, na legalidade e na justiça social. O fortalecimento da governança digital, aliado à participação ativa da sociedade civil, à capacitação institucional e à criação de um ecossistema normativo eficiente, será determinante para garantir que a era digital se desenvolva de maneira justa, plural e democrática, preservando a liberdade, a diversidade e a dignidade dos indivíduos.

## 4 REFERÊNCIAS

ALBERTI, Marcia de Oliveira Souza. *Vigilância em massa e segurança. Segurança Pública, Cidadania e Direitos Humanos: pesquisas, relatos e reflexões 2*, p. 116, 2022.

CANAVEZ, Luciana Lopes; SANTOS, Isadora Beatriz Magalhães; MENDES, Daniella Salvador Trigueiro. *Vigilância, proteção de dados e privacidade: o reconhecimento de novos direitos fundamentais na sociedade da informação.* Revista de Direito, Governança e Novas Tecnologias, v. 8, p. 68-86, 2022.

CORRÊA, Paulo Sérgio Gaspar; FAGUNDES FILHO, Antonio. *Neutralidade da rede mundial de computadores e os impactos da proteção de dados pessoais na sociedade de vigilância.*

FIGUEIREDO, Letícia Fraga de et al. *O empoderamento tecnológico do estado de vigilância frente ao direito constitucional à privacidade e à proteção de dados: a coleta e o tratamento de dados pessoais como instrumento de controle*. 2021.

LASSALE, Ferdinand. *A Essência da Constituição*. Trad.: Walter Stonner. 4. Ed. Rio de Janeiro: Lumen Juris, 1998.

MARTIN, Júlia Saes. *Abandono digital e dever de vigilância parental sob a ótica do princípio da proteção integral à criança*. 2024.

MONTEAGUDO, Ricardo. *Democracia em tempos de vigilância ubíqua.* Quaestio Iuris (QI), v. 14, n. 4, 2021.

RODOTÁ, Stefano. *A Vida na Sociedade da Vigilância: a privacidade hoje*. Trad.: Danilo Doneda a Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SILVA, Guilherme Brito Araújo da. *Aplicabilidade das tecnologias disruptivas de reconhecimento facial em sistemas de vigilância pública no Brasil: implicações da efetividade do direito constitucional à privacidade.* 2022.

SILVA, Lucas dos Reis. *A proteção de dados e sua necessidade de positivação como direito fundamental na era do capitalismo de vigilância*. Repositório de Trabalhos de Conclusão de Curso, 2021.

SIQUEIRA, Dirceu Pereira et al. *Direitos da personalidade e o julgamento ainda curi: análise sobre a (in) aplicabilidade do direito ao esquecimento no ordenamento jurídico brasileiro.* Revista de Constitucionalização do Direito Brasileiro, v. 6, n. 1, p. 1-25, 2023.

SOUZA, Diego Chagas de; LIMA, João Vitor Sangiacomo Meira. *O alcance do consentimento na proteção de dados pessoais: perspectivas sobre a sociedade de vigilância na era da informação.* Revista Eletrônica da PGE-RJ, v. 4, n. 3, 2021.

STEPHEN, Holmes. SUSTEIN, Cass R. *O Custo dos Direitos: por que a liberdade depende dos impostos*. Trad.: Marcelo Brandão Cipolla. São Paulo: Martins Fontes, 2019.

VERBICARO, Dennis. *Desafios na regulamentação de algoritmos sob o marco civil da internet.*

ZUBOFF, Shoshana. *A Era do Capitalismo de Vigilância*. Trad.: George Schlesinger. São Paulo: Intrínseca, 2021.

ALBERTI, Márcia de Oliveira Souza. Vigilância em massa e segurança. In: _____. Segurança pública, cidadania e direitos humanos: pesquisas, relatos e reflexões. v. 2. [S.l.]: [s.n.], 2022. p. 116.

CANAVEZ, Luciana Lopes; SANTOS, Isadora Beatriz Magalhães; MENDES, Daniella Salvador Trigueiro. Vigilância, proteção de dados e privacidade: o reconhecimento de novos direitos fundamentais na sociedade da informação. Revista de Direito, Governança e Novas Tecnologias, v. 8, p. 68–86, 2022.

CORRÊA, Paulo Sérgio Gaspar; FAGUNDES FILHO, Antonio. Neutralidade da rede mundial de computadores e os impactos da proteção de dados pessoais na sociedade de vigilância. [S.l.], [s.d.]. (Trabalho acadêmico em fase de publicação). (Se for artigo já publicado, inserir dados completos.)

FIGUEIREDO, Letícia Fraga de et al. O empoderamento tecnológico do Estado de vigilância frente ao direito constitucional à privacidade e à proteção de dados: a coleta e o tratamento de dados pessoais como instrumento de controle. Revista Brasileira de Políticas Públicas e Internacionais, v. 6, n. 1, 2021. (Verificar título da revista e completar caso necessário.)

LASSALE, Ferdinand. A essência da constituição. Tradução de Walter Stonner. 4. ed. Rio de Janeiro: Lumen Juris, 1998.

MARTIN, Júlia Saes. Abandono digital e dever de vigilância parental sob a ótica do princípio da proteção integral à criança. [S.l.], 2024. Trabalho acadêmico. (Se for TCC, dissertação ou artigo, especificar.)

MONTEAGUDO, Ricardo. Democracia em tempos de vigilância ubíqua. Quaestio Iuris, v. 14, n. 4, 2021. Disponível em: https://www.e-publicacoes.uerj.br/index.php/quaestioiuris/article/view/59308. Acesso em: 26 maio 2025.

RODOTÁ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SILVA, Guilherme Brito Araújo da. Aplicabilidade das tecnologias disruptivas de reconhecimento facial em sistemas de vigilância pública no Brasil: implicações da efetividade do direito constitucional à privacidade. [S.l.], 2022. Trabalho de conclusão de curso. (Especificar se for monografia, dissertação, etc.)

SILVA, Lucas dos Reis. A proteção de dados e sua necessidade de positivação como direito fundamental na era do capitalismo de vigilância. Repositório de Trabalhos de Conclusão de Curso – Faculdade de Direito da Universidade Federal de Minas Gerais, 2021. Disponível em: [inserir link se houver].

SIQUEIRA, Dirceu Pereira et al. Direitos da personalidade e o julgamento “Ainda Curi”: análise sobre a (in)aplicabilidade do direito ao esquecimento no ordenamento jurídico brasileiro. Revista de Constitucionalização do Direito Brasileiro, v. 6, n. 1, p. 1–25, 2023.

SOUZA, Diego Chagas de; LIMA, João Vitor Sangiacomo Meira. O alcance do consentimento na proteção de dados pessoais: perspectivas sobre a sociedade de vigilância na era da informação. Revista Eletrônica da PGE-RJ, v. 4, n. 3, 2021. Disponível em: https://revistapge.rj.gov.br. Acesso em: 26 maio 2025.

STEPHEN, Holmes; SUNSTEIN, Cass R. O custo dos direitos: por que a liberdade depende dos impostos. Tradução de Marcelo Brandão Cipolla. São Paulo: Martins Fontes, 2019.

VERBICARO, Dennis. Desafios na regulamentação de algoritmos sob o marco civil da internet. Revista de Direito, Inovação e Novas Tecnologias, [S.l.], 2022. (Completar com volume, número, páginas ou link.)

ZUBOFF, Shoshana. A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder. Tradução de George Schlesinger. São Paulo: Intrínseca, 2021.