

# **XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP**

## **DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS III**

**YURI NATHAN DA COSTA LANNES**

**MARCELO ANTONIO THEODORO**

**ANA CLAUDIA SILVA SCALQUETTE**

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

**Diretoria - CONPEDI**

**Presidente** - Profa. Dra. Samyra Haydée Dal Farra Naspolini - FMU - São Paulo

**Diretor Executivo** - Prof. Dr. Orides Mezzaroba - UFSC - Santa Catarina

**Vice-presidente Norte** - Prof. Dr. Jean Carlos Dias - Cesupa - Pará

**Vice-presidente Centro-Oeste** - Prof. Dr. José Querino Tavares Neto - UFG - Goiás

**Vice-presidente Sul** - Prof. Dr. Leonel Severo Rocha - Unisinos - Rio Grande do Sul

**Vice-presidente Sudeste** - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRIO - Rio de Janeiro

**Vice-presidente Nordeste** - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

**Representante Discente**: Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

**Conselho Fiscal:**

Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão

Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais

Prof. Dr. Valter Moura do Carmo - UFERSA - Rio Grande do Norte

Prof. Dr. Fernando Passos - UNIARA - São Paulo

Prof. Dr. Ednilson Donisete Machado - UNIVEM/UENP - São Paulo

**Secretarias**

**Relações Institucionais:**

Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná

Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia

Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal

**Comunicação:**

Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina

Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul

Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe

**Relações Internacionais para o Continente Americano:**

Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do Sul

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão

Prof. Dr. Felipe Chiarello de Souza Pinto - UPM - São Paulo

**Relações Internacionais para os demais Continentes:**

Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará

Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul

Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI - Santa Catarina

**Educação Jurídica**

Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba - PR

Prof. Dr. Rubens Beçak - USP - SP

Profa. Dra. Livia Gaigher Bosio Campello - UFMS - MS

**Eventos:**

Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo

Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina

Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

**Comissão Especial**

Prof. Dr. João Marcelo de Lima Assafim - UFRJ - RJ

Profa. Dra. Maria Creusa De Araújo Borges - UFPB - PB

Prof. Dr. Antônio Carlos Diniz Murta - Fumec - MG

Prof. Dr. Rogério Borba - UNIFACVEST - SC

D597

Direito, governança e novas tecnologias III[Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Yuri Nathan da Costa Lannes, Marcelo Antonio Theodoro, Ana Claudia Silva Scalquette – Florianópolis: CONPEDI, 2025.

Inclui bibliografia

ISBN: 978-65-5274-306-0

Modo de acesso: [www.conpedi.org.br](http://www.conpedi.org.br) em publicações

Tema: Os Caminhos Da Internacionalização E O Futuro Do Direito

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias. XXXII

Congresso Nacional do CONPEDI São Paulo - SP (4: 2025: Florianópolis, Brasil).

CDU: 34

# **XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP**

## **DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS III**

---

### **Apresentação**

O XXXII Congresso Nacional do CONPEDI, realizado nos dias 26, 27 e 28 de novembro de 2025, teve como sede a cidade de São Paulo, sendo acolhido com excelência pela Universidade Presbiteriana Mackenzie. O evento reafirmou a centralidade da pesquisa jurídica no enfrentamento dos desafios contemporâneos impostos pela transformação digital, pelas inovações tecnológicas e pelas novas formas de governança e controle institucional.

O GT10 – Direito, Governança e Novas Tecnologias III, realizado no dia 26 de novembro, reuniu pesquisadoras e pesquisadores de diversas regiões do Brasil para discutir os múltiplos impactos das tecnologias emergentes sobre os direitos fundamentais, a administração pública, a proteção de dados, a sustentabilidade e a ordem democrática.

Os artigos apresentados passaram por dupla avaliação cega por pares, garantindo rigor acadêmico e excelência científica. A partir da análise dos trabalhos, foram identificados seis eixos temáticos principais, que organizam os anais de forma a evidenciar os distintos focos de abordagem e permitir ao leitor um percurso estruturado pelo conteúdo:

**Proteção de Dados Pessoais, Privacidade e Identidade Digital** - Este eixo reúne estudos que exploram a proteção de dados pessoais sob a ótica da privacidade, da publicidade institucional, da sustentabilidade e da construção de novas categorias jurídicas, como a identidade digital.

1 - Big Data e direitos fundamentais: uma análise interdisciplinar dos impactos na privacidade e proteção de dados pessoais no ordenamento jurídico brasileiro

2 - Dados pessoais e desenvolvimento sustentável: fundamentos e desafios do direito à privacidade no século XXI

3 - A proteção de dados pessoais dos servidores públicos do Tribunal de Justiça do Distrito Federal e dos Territórios: conflito entre publicidade e privacidade?

4 - A proteção de dados pessoais como direito difuso e a sustentabilidade no uso de dados pessoais

5 - A proteção constitucional da identidade digital: um novo paradigma dos direitos da personalidade na era da informação

6 - A norma ABNT NBR ISO/IEC 27701 como instrumento de suporte à Lei Geral de Proteção de Dados

7 - A Lei Geral de Proteção de Dados Pessoais: os serviços extrajudiciais – governança e boas práticas

Inteligência Artificial, Sistema de Justiça e Direitos Fundamentais - Debate as aplicações da inteligência artificial no Judiciário e os dilemas éticos, institucionais e regulatórios que envolvem a sua adoção em contextos democráticos e de proteção aos direitos.

8 - A inteligência artificial e o Poder Judiciário: reflexões sobre a prestação jurisdicional e a concretização da cidadania

9 - Entre algoritmos e direitos: a reconstrução do direito frente ao capitalismo de vigilância

10 - Entre o algoritmo e a consciência: impactos das decisões automatizadas no Judiciário e a urgência da educação em direitos humanos

11 - A governança da inteligência artificial e os arranjos institucionais: entre inovação tecnológica e a proteção de garantias fundamentais

12 - Regular ou não a inteligência artificial, essa é a questão principal?

13 - O uso do sistema MIDAS pelo Tribunal de Justiça do Estado do Ceará: inovação tecnológica para a concretização do princípio da duração razoável do processo

14 - Entre a liberdade de expressão e os direitos da personalidade: desafios da inteligência artificial na propaganda eleitoral à luz da condição de pessoas expostas politicamente

15 - Inteligência artificial e proteção das comunidades indígenas em contextos globais

Governança Digital e Sustentabilidade – Reúne trabalhos que tratam da relação entre governança institucional e sustentabilidade, especialmente em temas como compliance ambiental, cidades inteligentes e estratégias de desenvolvimento sustentável.

16 - Governança digital sustentável e proteção de dados em cidades inteligentes: desafios jurídicos no Antropoceno

17 - Governança corporativa e compliance ambiental: estratégias para uma gestão sustentável e eficaz

18 - A inteligência artificial como instrumento de fortalecimento do compliance ambiental

19 - A democratização da energia no Brasil: uma análise sobre o acesso e as possibilidades originadas pela energia solar

Inclusão, Acessibilidade e Justiça Digital - Trabalhos que discutem as lacunas e desigualdades digitais, especialmente em relação à acessibilidade e à implementação de tecnologias digitais no poder público.

20 - Acessibilidade negligenciada: capacitar digital nas redes sociais do governo federal

21 - Jurimetria e o Direito brasileiro – estatística e conceitos preliminares – aplicabilidade

Infância, Direitos Digitais e Exposição Prematura - Este eixo foca nos desafios da regulação da exposição digital de crianças e adolescentes e nos caminhos jurídicos para proteção da infância no ambiente virtual.

22 - Adultização infantil no meio ambiente digital: entre lacunas regulatórias e a construção de caminhos de proteção jurídica

Plataformas Digitais, Regulação e Impactos Psicossociais - Reflete sobre os impactos sociais e econômicos das plataformas digitais, abordando questões regulatórias, manipulação de resultados e proteção do consumidor.

23 - A ascensão das plataformas de apostas digitais no Brasil: uma análise dos impactos psicossociais, da manipulação de resultados e dos desafios regulatórios

Os trabalhos reunidos neste volume demonstram o vigor da produção acadêmica brasileira em torno dos desafios impostos pelas tecnologias emergentes e reafirmam o papel do Direito como campo estratégico para a mediação entre inovação e proteção de garantias fundamentais. A todos os(as) pesquisadores(as), coordenadores(as) e avaliadores(as), registramos nossos agradecimentos por suas valiosas contribuições.

Desejamos uma leitura instigante e transformadora!

Ana Claudia Silva Scalquette - Universidade Presbiteriana Mackenzie

Marcelo Antonio Theodoro- Universidade Federal de Mato Grosso

Yuri Nathan da Costa Lannes – Faculdade de Direito de Franca

# **ENTRE ALGORITMOS E DIREITOS: A RECONSTRUÇÃO DO DIREITO FRENTE AO CAPITALISMO DE VIGILÂNCIA**

## **BETWEEN ALGORITHMS AND RIGHTS: THE RECONSTRUCTION OF LAW IN THE FACE OF SURVEILLANCE CAPITALISM**

**Rodrigo Palomares Maiolino De Mendonça**

### **Resumo**

O artigo analisa criticamente os impactos do capitalismo de vigilância sobre os direitos fundamentais na era digital, com base na obra de Shoshana Zuboff e no diálogo com autores como Doneda, Hoffmann-Riem e Fachin. O problema central consiste na inadequação das categorias jurídicas tradicionais para enfrentar os riscos sistêmicos impostos pela lógica extractiva, opaca e comportamental das grandes plataformas tecnológicas. O objetivo principal é propor caminhos normativos, éticos e institucionais que permitam reconfigurar o Direito como um sistema adaptativo, transparente e preventivo. Parte-se da hipótese de que a proteção efetiva da dignidade digital exige uma abordagem jurídica proativa, que atue desde o design dos sistemas tecnológicos e promova a governança algorítmica responsável. A metodologia é qualitativa, de natureza teórico-dogmática, com base em revisão bibliográfica interdisciplinar nos campos do Direito Constitucional, Filosofia Política e Teoria da Informação. O estudo incorpora estudos de caso, como o escândalo da Cambridge Analytica e decisões do STF, e analisa a tensão entre inovação e regulação à luz de iniciativas estatais como a Estratégia de Governo Digital e o Marco Legal da IA. Conclui-se que é necessária uma reconstrução normativa centrada na dignidade informacional, na transparência, na accountability e na participação democrática, sob risco de erosão das liberdades públicas e da própria estrutura do Estado Democrático de Direito. O Direito, nesse cenário, deve recuperar sua função mediadora entre a inovação tecnológica e os direitos fundamentais, garantindo soberania informacional e cidadania digital crítica.

**Palavras-chave:** Capitalismo de vigilância, Privacidade, Direitos fundamentais, Governança algorítmica, Direito digital

### **Abstract/Resumen/Résumé**

This article critically analyzes the impacts of surveillance capitalism on fundamental rights in the digital age, based on Shoshana Zuboff's work and in dialogue with scholars such as Doneda, Hoffmann-Riem, and Fachin. The central problem lies in the inadequacy of traditional legal categories to address the systemic risks posed by the extractive, opaque, and behavioral logic of major technology platforms. The main objective is to propose normative, ethical, and institutional pathways to reconfigure Law as an adaptive, transparent, and preventive system. The hypothesis is that the effective protection of digital dignity requires a proactive legal approach, acting from the design stage of technological systems and fostering

responsible algorithmic governance. The methodology is qualitative and theoretical-dogmatic, based on interdisciplinary literature review in the fields of Constitutional Law, Political Philosophy, and Information Theory. The study incorporates case studies such as the Cambridge Analytica scandal and rulings from the Brazilian Supreme Court, and analyzes the tension between innovation and regulation in light of state initiatives such as the Digital Government Strategy and the Artificial Intelligence Legal Framework. It concludes that a normative reconstruction centered on informational dignity, transparency, accountability, and democratic participation is necessary, under penalty of eroding public freedoms and the foundations of the Democratic Rule of Law. Law, in this scenario, must recover its mediating role between technological innovation and fundamental rights, ensuring informational sovereignty and critical digital citizenship.

**Keywords/Palabras-claves/Mots-clés:** Surveillance capitalism, Privacy, Fundamental rights, Algorithmic governance, digital law

## 1. Introdução

A ascensão das tecnologias digitais e sua integração sistêmica à vida social, política e econômica inauguraram uma nova lógica de organização da sociedade. No centro dessa transformação está a consolidação de um modelo informacional que opera a partir da coleta massiva, preditiva e exploratória de dados pessoais. Este artigo propõe uma análise crítica da obra de Zuboff (2021), que cunha o termo "capitalismo de vigilância" para descrever esse novo regime de acumulação, estruturado sobre a experiência humana como matéria-prima para mercados comportamentais. Ao mobilizar esse referencial teórico, propõe-se um diálogo com a evolução histórica dos direitos fundamentais, explorando como as três gerações desses direitos (liberdade, igualdade e solidariedade) são tensionadas, reconfiguradas e, em alguns casos, erodidas pela lógica algorítmica contemporânea.

O artigo também examina a chamada "guerra de dados", expressão que sintetiza a disputa global pelo domínio dos fluxos informacionais entre plataformas privadas, corporações transnacionais e Estados, com implicações profundas para a soberania individual e coletiva. Argumenta-se que o atual modelo de capitalismo informacional exige uma resposta normativa e institucional à altura dos riscos que impõe à liberdade, à dignidade e à cidadania. Assim, o texto se estrutura para oferecer uma contribuição crítica ao debate sobre a necessária reconstrução do Direito diante do avanço do poder computacional e da colonização dos comportamentos.

Adicionalmente, a abordagem adotada neste estudo é eminentemente interdisciplinar, abarcando contribuições do Direito Constitucional, da Filosofia Política e da Ciência da Computação. A metodologia baseia-se em pesquisa bibliográfica crítica, com ênfase em autores como Zuboff, Hoffmann-Riem, Doneda e Fachin, além do diálogo com pensadores contemporâneos como Han, Eubanks e Pariser. O objetivo final é refletir sobre alternativas normativas e institucionais que possam enfrentar os desafios impostos pela vigilância digital e resgatar os fundamentos democráticos em meio à crise de governança informacional global.

A era digital não apenas transformou as dinâmicas econômicas e sociais do século XXI, como também colocou em xeque os fundamentos teóricos e normativos do Direito. A ubiquidade das tecnologias digitais, a expansão acelerada da coleta e processamento de

dados pessoais e o surgimento de novas formas de poder algorítmico compõem o pano de fundo de uma profunda reconfiguração da experiência humana. O presente artigo insere-se nesse contexto de inflexão histórica e busca realizar uma leitura crítica sobre os desafios que o capitalismo de vigilância impõe aos direitos fundamentais, especialmente à autodeterminação informativa, à privacidade e à dignidade da pessoa humana.

O ponto de partida da análise é a obra de Shoshana Zuboff (2021), que introduz o conceito de "capitalismo de vigilância" para descrever um novo regime de acumulação econômica baseado na extração, tratamento e comercialização de excedentes comportamentais. Diferentemente do capitalismo industrial, que se fundamentava na exploração do trabalho físico, o capitalismo informacional apropria-se da subjetividade dos indivíduos: suas emoções, hábitos, preferências e padrões de comportamento. Essa apropriação, realizada de forma opaca, preditiva e não consentida, resulta em uma nova arquitetura de poder, na qual a liberdade é substituída por controle imperceptível e a autonomia individual cede lugar à modulação algorítmica.

O problema central investigado neste trabalho é a insuficiência das categorias jurídicas tradicionais (centradas na proteção formal da privacidade e na ideia de consentimento) diante da lógica extrativa e estrutural que rege as plataformas digitais. Os marcos regulatórios atuais, como a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) no Brasil e o Regulamento Geral sobre a Proteção de Dados (GDPR) na União Europeia, embora representem avanços normativos relevantes, mostram-se incapazes de enfrentar os mecanismos sistêmicos de vigilância comportamental que caracterizam a nova ordem informacional. A resposta jurídica, ao se limitar à proteção de dados pessoais em termos contratuais ou burocráticos, ignora a dimensão estrutural e política do fenômeno.

Nesse sentido, o objetivo principal do artigo é propor um diálogo crítico e interdisciplinar entre os fundamentos teóricos desenvolvidos por Zuboff e as contribuições doutrinárias de autores como Wolfgang Hoffmann-Riem, Danilo Doneda e Zulmar Fachin, com vistas à construção de um novo paradigma jurídico capaz de enfrentar os desafios impostos pela era da vigilância digital. Trata-se de identificar convergências normativas e epistemológicas que permitam vislumbrar caminhos para a reconstrução do Direito como instrumento de regulação efetiva, prevenção de danos informacionais e proteção da cidadania digital.

A hipótese que orienta esta investigação é a de que a superação das vulnerabilidades atuais depende da reconfiguração do Direito como um sistema adaptativo, ético e prospectivo, dotado de mecanismos capazes de regular a tecnologia desde sua concepção (*privacy by design*), com base na transparência algorítmica, na auditabilidade dos sistemas e na responsabilização de agentes econômicos e políticos que se beneficiam da assimetria informacional. Não se trata apenas de proteger os dados pessoais enquanto bens jurídicos isolados, mas de garantir a integridade da pessoa humana em sua dimensão informacional, reconhecendo que a apropriação indevida de dados constitui uma forma contemporânea de dominação e despossessão.

Para a construção dessa reflexão, adota-se uma metodologia de natureza qualitativa, com enfoque teórico-dogmático e abordagem interdisciplinar. O estudo parte de uma análise crítica da bibliografia especializada, combinando referências do Direito Constitucional, da Filosofia Política e da Teoria da Informação. São mobilizadas, em especial, as contribuições de Zuboff (2021), que oferece o marco teórico central; de Hoffmann-Riem (2021), com sua proposta de uma Teoria Geral do Direito Digital; de Doneda (2021), defensor da proteção de dados como extensão da personalidade; e de Fachin e Silva (2021), que realizam uma avaliação crítica do Marco Civil da Internet e suas insuficiências diante da complexidade do ecossistema digital. A análise é complementada pela consideração dos marcos normativos nacionais e internacionais, além de exemplos empíricos que ilustram os mecanismos de modulação algorítmica presentes nas grandes plataformas digitais.

As primeiras seções do artigo tratam da evolução histórica dos direitos fundamentais e de sua reorganização na era digital, destacando como a tradicional classificação em três gerações: 1<sup>a</sup>. Direitos civis e políticos (liberdade), 2<sup>a</sup>. Direitos sociais (igualdade) e 3<sup>a</sup>. Direitos difusos e coletivos (solidariedade). Elas se mostram inadequadas frente às novas formas de dominação informacional. Defende-se que a proteção de direitos no ambiente digital exige uma abordagem sistêmica, transversal e proativa, que reconheça a interdependência entre liberdade de expressão, privacidade, proteção de dados, segurança cibernética e acesso democrático à informação.

Em seguida, o artigo aprofunda a análise sobre o capitalismo de vigilância e a guerra de dados, examinando como a coleta e tratamento de dados pessoais se tornaram

recursos geopolíticos estratégicos, disputados por empresas transnacionais e Estados soberanos. Discute-se a erosão da autonomia individual, a normalização da vigilância, os riscos de discriminação algorítmica e a desestruturação da esfera pública provocada pela personalização extrema dos fluxos informacionais. Nesse contexto, autores como Eubanks (2018), Han (2017) e Pariser (2011) são mobilizados para evidenciar os efeitos psíquicos, sociais e políticos da vigilância digital sobre os indivíduos e as coletividades.

As seções finais propõem caminhos para a reconstrução do Direito diante da era digital. A partir das ideias de Hoffmann-Riem, argumenta-se que o Direito precisa ser reestruturado com base em princípios como a proteção por padrão (privacy by default), a explicabilidade dos algoritmos (explainability), a auditabilidade dos sistemas automatizados (auditability) e a participação democrática na formulação das normas digitais. Tais princípios devem ser incorporados aos marcos legais nacionais, como a LGPD e o Marco Civil da Internet, que carecem, ainda, de efetiva integração normativa, aparato fiscalizatório robusto e cultura jurídica voltada à dignidade informacional.

Por fim, nas considerações finais, sustenta-se que a proteção dos direitos fundamentais na era da inteligência artificial requer uma ação jurídica que vá além da reatividade. É necessário um esforço coletivo para desmantelar as arquiteturas extrativas de dados e reconstituir os fundamentos normativos da democracia em chave informacional. A dignidade digital deve ser erigida como princípio transversal do ordenamento jurídico, orientando a criação de políticas públicas inclusivas, a formação de uma cidadania crítica e vigilante e a promoção de uma governança tecnológica participativa e transparente. A crise atual não é apenas jurídica, mas civilizatória: exige repensar os modos de produção, circulação e apropriação do conhecimento na sociedade conectada.

Nesse sentido, este artigo não pretende oferecer respostas definitivas, mas contribuir com o debate urgente sobre os rumos do Direito na era digital, lançando luz sobre as possibilidades de resistência, emancipação e transformação diante de um modelo informacional que ameaça os pilares do constitucionalismo e os valores democráticos universais.

## **2. As gerações dos direitos fundamentais e seus desafios na era digital**

A doutrina constitucional costuma organizar os direitos fundamentais em três gerações. A primeira geração refere-se aos direitos civis e políticos, como a liberdade, a vida, a propriedade e a privacidade, nascidos no bojo das revoluções liberais (Bobbio, 1992). A segunda geração inclui os direitos sociais, culturais e econômicos, como educação, saúde e trabalho. A terceira contempla direitos difusos e coletivos, tais como o meio ambiente, o desenvolvimento sustentável, e, mais recentemente, a proteção de dados e o acesso à informação.

Na era digital, no entanto, essa tipologia enfrenta desafios, pois os direitos fundamentais se tornam interdependentes e vulneráveis diante de novas formas de dominação. O que se entendia como liberdade individual, por exemplo, se dilui em uma realidade marcada por vigilância constante, algoritmos opacos e ambientes controlados por inteligência artificial. A igualdade é abalada por vieses algorítmicos; e os direitos de solidariedade são enfraquecidos pelo esfacelamento do espaço público digital (Han, 2017).

Dessa forma, a tradicional divisão entre gerações de direitos precisa ser revista à luz das novas tecnologias. A proteção da privacidade (primeira geração) está ligada ao combate à discriminação algorítmica (segunda geração), e ambas dependem de uma infraestrutura digital transparente e regulada coletivamente (terceira geração). A realidade atual exige, portanto, uma abordagem sistêmica, que considere a transversalidade dos direitos na sociedade da informação.

Essa reinterpretação revela que os direitos não podem mais ser entendidos de maneira isolada. A digitalização da vida cotidiana exige que os operadores do Direito e os formuladores de políticas públicas considerem as interações entre liberdade de expressão, proteção de dados, segurança cibernética e transparência institucional como elementos indissociáveis de um mesmo conjunto normativo, voltado à proteção da dignidade humana no ambiente digital.

### **3. O capitalismo de vigilância e a transformação da experiência humana**

Zuboff (2021, p. 15) define o capitalismo de vigilância como uma nova ordem econômica que transforma unilateralmente a experiência humana em matéria-prima gratuita para processos comerciais de extração, previsão e venda. Inicialmente

desenvolvido pelo Google, esse modelo expandiu-se para outras big techs, transformando os chamados "excedentes comportamentais" (resíduos digitais não intencionais) em commodities preditivas.

Ao contrário do capitalismo industrial, que explorava o trabalho físico, o capitalismo de vigilância se estrutura sobre a captura da subjetividade: hábitos, emoções, escolhas. Essa dinâmica rompe com os princípios básicos da autonomia individual, pois atua com base na vigilância invisível e na manipulação preditiva de comportamentos, à revelia do consentimento (Zuboff, 2021, p. 63).

Trata-se de um regime assimétrico, que concentra poder informacional em poucas corporações e opera de maneira opaca, dificultando o controle social. A liberdade, nesse contexto, é transformada em simulacro. A personalização algorítmica e a gamificação moldam as decisões dos sujeitos, minando sua capacidade de autodeterminação. Como afirma Zuboff (2021, p. 78), a transformação do comportamento humano em objeto de manipulação sistemática compromete os pilares da democracia.

Além disso, a noção de privacidade sofre uma profunda reconfiguração. Tradicionalmente associada ao controle sobre a própria informação, a privacidade no capitalismo de vigilância é desconstruída, sendo substituída por um regime de opacidade intencional, onde o usuário é mantido na ignorância sobre a extensão da coleta e o uso de seus dados. Essa assimetria cognitiva compromete não apenas a liberdade individual, mas também a possibilidade de controle social e regulação efetiva.

Como destaca Doneda (2021, p. 101), a proteção de dados precisa ser entendida como uma extensão da personalidade, o que significa reconhecer que a apropriação indevida da informação pessoal constitui uma forma de despossessão identitária. O sujeito não apenas perde sua privacidade: ele é alienado de sua própria narrativa existencial, que passa a ser reconstruída por algoritmos de terceiros.

#### **4. A guerra de dados e a erosão da autonomia**

A disputa global por dados, muitas vezes travada de maneira invisível ao olhar do cidadão comum, representa um novo estágio na luta pelo poder no século XXI. Conforme observa Zuboff (2021, p. 103), essa guerra é caracterizada por uma assimetria radical entre aqueles que detêm os meios tecnológicos de coleta, análise e comercialização de

dados e aqueles que são objeto dessa extração contínua. Trata-se de uma guerra silenciosa e constante, em que Estados, plataformas digitais e corporações transnacionais competem pelo controle da informação e, por consequência, das subjetividades.

Doneda (2021, p. 112) destaca que os dados pessoais não devem ser vistos como meros ativos comerciais, mas como projeções da personalidade. Nesse sentido, a autodeterminação informativa é essencial para garantir a dignidade e a liberdade dos cidadãos. Contudo, a lógica mercantil vigente tem desfigurado essa compreensão, subordinando os direitos informacionais à lógica da rentabilidade.

O fenômeno da guerra de dados revela a existência de um novo território de conflito geopolítico e econômico. A extração de dados tornou-se central na política internacional, afetando diretamente a soberania informacional dos Estados. A exemplo disso, a coleta massiva de dados por empresas transnacionais com sede nos Estados Unidos, como Google, Amazon, Meta e Microsoft, confere aos Estados Unidos uma vantagem estratégica sobre outras nações (Zuboff, 2021, p. 116).

Essa concentração de poder informacional também tem implicações para a soberania dos indivíduos. Quando as decisões que afetam a vida cotidiana (como concessão de crédito, acesso a serviços públicos, oportunidades de emprego e exposição a conteúdos informativos) passam a ser mediadas por algoritmos opacos, o indivíduo perde o controle sobre seu destino. Como alerta Eubanks (2018), essa lógica de gestão algorítmica tende a reproduzir desigualdades históricas e a reforçar preconceitos sistêmicos.

A guerra de dados, portanto, não se restringe à coleta em si, mas envolve a modelagem de comportamentos, a manipulação de preferências e a construção de realidades personalizadas. Pariser (2011) já advertia para os riscos da "bolha de filtros", onde os indivíduos passam a viver em realidades informacionais isoladas, moldadas por algoritmos que priorizam relevância comercial sobre pluralidade democrática.

## **5. Direitos fundamentais sob ataque: o risco da normalização da vigilância**

A naturalização da vigilância digital representa uma ameaça direta à efetividade dos direitos fundamentais. Zuboff (2021, p. 91) enfatiza que o capitalismo de vigilância cria uma nova arquitetura de controle comportamental, baseada na vigilância contínua, na

predição e, por fim, na modulação de condutas. Esse sistema corrói os alicerces do Estado democrático de direito ao transformar o cidadão em objeto de monitoramento constante.

A liberdade individual, princípio estruturante da primeira geração de direitos, é minada quando as escolhas são guiadas por estímulos calculados, enviados em tempo real com base em padrões comportamentais previamente extraídos. A igualdade, valor central da segunda geração, é afetada pela reprodução de vieses algorítmicos, conforme demonstrado por Eubanks (2018), que evidencia como sistemas automatizados discriminam populações vulneráveis. Já os direitos de solidariedade, inerentes à terceira geração, são fragilizados pela ausência de espaços digitais comuns, uma vez que a personalização extrema desagrega o tecido da esfera pública.

Han (2017) adverte que o sujeito contemporâneo não percebe o controle que o cerca, pois a vigilância assume forma de liberdade. O uso ostensivo de redes sociais, plataformas de e-commerce e assistentes virtuais é percebido como conveniente, mas resulta em autovigilância e autocoerção. Trata-se de uma psicopolítica digital, na qual os sujeitos se tornam cúmplices involuntários do sistema que os vigia.

A questão da accountability também se impõe como desafio. Como responsabilizar algoritmos por decisões discriminatórias? Como garantir transparência nos sistemas de inteligência artificial? Hoffmann-Riem (2021, p. 142) propõe a criação de obrigações específicas para sistemas digitais, com base na proteção por design, na auditabilidade e na explicabilidade dos algoritmos. Sem tais medidas, os direitos fundamentais permanecem vulneráveis a violações sistemáticas, mascaradas sob o verniz da inovação tecnológica.

## **6. Perspectivas para o Direito na era digital**

A resposta jurídica aos desafios da era digital exige mais do que ajustes pontuais: requer uma reformulação estrutural dos paradigmas normativos. Hoffmann-Riem (2021, p. 135-168) defende a necessidade de uma nova teoria geral do Direito Digital, que vá além da simples adaptação das normas existentes. O autor propõe uma abordagem orientada por princípios como proteção por padrão, responsabilidade algorítmica e participação democrática na formulação de normas digitais.

A experiência da União Europeia com o Regulamento Geral de Proteção de Dados (GDPR) representa um avanço, ao estabelecer regras claras sobre consentimento, finalidade da coleta e portabilidade de dados. No entanto, como observa Zuboff (2021, p. 117), é insuficiente proteger os dados pessoais sem enfrentar o modelo econômico que se nutre da coleta massiva desses dados. Ou seja, a regulação precisa ir além da proteção formal da privacidade e atuar sobre as estruturas que sustentam o capitalismo de vigilância.

No Brasil, a Lei Geral de Proteção de Dados (LGPD) também constitui um passo importante, embora sua eficácia dependa do fortalecimento institucional da Autoridade Nacional de Proteção de Dados (ANPD), da capacidade de fiscalização e da educação digital dos cidadãos. Doneda (2021, p. 135) ressalta que a LGPD precisa ser interpretada à luz dos direitos fundamentais, sob pena de se transformar em mera formalidade burocrática.

Além disso, o Direito precisa atuar preventivamente, exigindo transparência algorítmica, auditabilidade e explicações compreensíveis sobre as decisões automatizadas. Isso envolve a reformulação de princípios clássicos, como a legalidade, a ampla defesa e o devido processo legal, que devem ser adaptados ao contexto das decisões mediadas por inteligência artificial. Trata-se de um esforço de reconstrução normativa, orientado por uma ética pública da informação.

## **7. O Marco Civil da Internet e a insuficiência normativa brasileira**

Fachin e Silva (2021, p. 230-254) realizam uma análise crítica do Marco Civil da Internet, apontando que, embora essa legislação represente um avanço normativo ao consagrar princípios como neutralidade da rede, privacidade e liberdade de expressão, ela se mostra limitada diante da complexidade do ecossistema digital contemporâneo.

A coleta contínua e invisível de dados, operada por algoritmos sofisticados, escapa ao controle previsto pelo Marco Civil (Fachin; Silva, 2021, p. 235). Falta à legislação brasileira um enfoque mais claro sobre transparência algorítmica, accountability e limitação da extração comportamental. A vulnerabilidade jurídica do cidadão conectado é acentuada pela lacuna entre a letra da lei e a realidade digital.

Ademais, a ausência de sanções efetivas, a dificuldade de fiscalização das plataformas globais e a escassa articulação entre os diferentes órgãos reguladores brasileiros comprometem a eficácia da proteção dos direitos fundamentais. A LGPD e o Marco Civil precisam dialogar de forma harmônica, consolidando um sistema robusto de governança digital. Fachin e Silva (2021, p. 248) enfatizam que a dignidade da pessoa humana deve nortear toda e qualquer revisão normativa, reafirmando o papel do Estado como garantidor dos direitos fundamentais digitais.

Nesse sentido, é fundamental que o ordenamento jurídico brasileiro avance na construção de uma doutrina dos direitos digitais, incorporando os princípios desenvolvidos no âmbito internacional e promovendo um ambiente digital mais transparente, equitativo e democrático.

## **8. Casos emblemáticos e decisões judiciais**

A discussão teórica sobre os riscos do capitalismo de vigilância torna-se ainda mais contundente quando examinada à luz de eventos concretos que evidenciam as falhas sistêmicas na proteção dos dados e na garantia da autodeterminação informativa. O escândalo envolvendo a Cambridge Analytica e o Facebook, revelado em 2018, é um marco nesse sentido. A empresa britânica acessou indevidamente os dados de mais de 87 milhões de usuários da rede social, utilizando-os para manipulação psicopolítica em campanhas eleitorais, como o referendo do Brexit e a eleição presidencial dos Estados Unidos em 2016 (Cadwalladr; Graham-Harrison, 2018, p. 2). O episódio ilustra de forma cristalina o uso de tecnologias para fins de vigilância e manipulação, à revelia do consentimento e da transparência, resultando em impactos diretos na soberania popular e no processo democrático.

A resposta institucional, embora significativa, mostrou-se tardia e fragmentada. No Reino Unido e nos Estados Unidos, a Cambridge Analytica enfrentou investigações parlamentares e sanções administrativas. Já o Facebook foi condenado a pagar uma multa recorde de 5 bilhões de dólares pela Federal Trade Commission (FTC), em razão da violação de privacidade dos usuários (FTC, 2019, p. 1). Tais medidas, contudo, não impediram a perpetuação da lógica extrativista das plataformas digitais, reforçando a percepção de que a responsabilização ainda é episódica e insuficiente.

No Brasil, o Supremo Tribunal Federal (STF) também tem enfrentado os desafios da proteção de dados no ambiente digital. Um marco relevante foi a ADI 6.387, em que o STF reconheceu a proteção de dados pessoais como um direito fundamental autônomo, ligado diretamente à dignidade da pessoa humana e à autodeterminação informativa. O ministro Alexandre de Moraes, relator da ação, destacou que "a proteção de dados deve ser compreendida como parte essencial da esfera de autonomia individual em uma sociedade hiperconectada" (STF, 2020, p. 12).

Essa decisão é de extrema relevância, pois eleva a proteção de dados ao patamar de cláusula pétreia, exigindo dos poderes públicos e das instituições privadas o máximo respeito à integridade informacional dos cidadãos. Além disso, a decisão fortalece o papel da Autoridade Nacional de Proteção de Dados (ANPD) e abre caminho para um controle mais rigoroso sobre o tratamento de dados no Brasil, inclusive por plataformas globais.

Esses exemplos concretos revelam que os riscos discutidos ao longo deste artigo (como a opacidade algorítmica, a captura da subjetividade e a erosão da autonomia) não são meras abstrações acadêmicas, mas problemas reais, com efeitos tangíveis sobre as instituições democráticas e os direitos das pessoas. A emergência de respostas institucionais, embora positiva, precisa ser acompanhada por transformações mais profundas no modelo regulatório e na arquitetura informacional das tecnologias digitais, sob pena de perpetuar a assimetria entre usuários e controladores de dados (Zuboff, 2021, p. 117).

## **9. Iniciativas estatais e o desafio do equilíbrio entre inovação e regulação**

A discussão sobre capitalismo de vigilância e os riscos à autodeterminação informativa não pode ignorar os esforços institucionais que vêm sendo empreendidos no âmbito estatal para lidar com os desafios da era digital. Nos últimos anos, o Brasil tem buscado consolidar um ambiente normativo e institucional que concilie o desenvolvimento tecnológico com a proteção de direitos fundamentais, ainda que esse equilíbrio permaneça frágil e incompleto.

Uma das iniciativas mais emblemáticas nesse contexto é a Estratégia de Governo Digital 2020–2022, instituída pelo Decreto nº 10.332/2020, que visa digitalizar serviços públicos, ampliar a interoperabilidade entre sistemas governamentais e consolidar o uso

de dados como instrumento de formulação de políticas públicas. A proposta avança em termos de eficiência administrativa, mas levanta preocupações quanto à transparência algorítmica e ao risco de adoção de soluções tecnológicas sem o devido debate público (Brasil, 2020).

Complementarmente, o Plano Nacional de Internet das Coisas (IoT) e o Marco Legal da Inteligência Artificial (PL 2.338/2023) também integram esse ecossistema normativo emergente. Embora tenham o mérito de fomentar a inovação e o desenvolvimento de tecnologias nacionais, tais instrumentos têm sido criticados pela ausência de mecanismos robustos de accountability, avaliação de impacto algorítmico e participação social (Martins, 2023, p. 214). A crítica central reside na dificuldade do Estado em combinar políticas indutoras de inovação com estruturas de controle preventivo e democrático.

Essa tensão entre inovação tecnológica e regulação excessiva é uma constante em ambientes jurídicos contemporâneos. De um lado, há o receio de que regulações rigorosas inibam o empreendedorismo digital, retardem o desenvolvimento de soluções de inteligência artificial e comprometam a competitividade internacional. De outro, observa-se que a ausência de balizas normativas claras e de instituições fiscalizadoras sólidas favorece a consolidação de ecossistemas opacos, centrados na extração de dados e na violação de direitos (Doneda, 2021, p. 109).

No plano internacional, esse dilema tem sido enfrentado por meio de instrumentos como o AI Act da União Europeia, que busca regular a inteligência artificial com base em critérios de risco, preservando a inovação em setores de baixo impacto e impondo restrições severas a sistemas considerados de alto risco. Essa abordagem baseada em "regulação proporcional ao risco" pode servir como inspiração para o ordenamento brasileiro, especialmente diante da fragmentação normativa que ainda caracteriza a atuação do Estado no campo digital (Calo, 2019, p. 42).

O Brasil, apesar de avanços importantes como a LGPD e a criação da Autoridade Nacional de Proteção de Dados (ANPD), ainda carece de um modelo coordenado de governança digital, que articule políticas de inovação com políticas de proteção da cidadania informacional. A ANPD, por exemplo, ainda possui limitações orçamentárias e operacionais que comprometem sua efetividade (Carvalho; Santiago, 2022, p. 87).

Nesse cenário, é essencial que a transformação digital do Estado brasileiro se fundamente não apenas em critérios de economicidade e eficiência, mas sobretudo na centralidade dos direitos fundamentais e na soberania informacional. Como adverte Zuboff (2021, p. 117), a legitimação do uso de tecnologias digitais exige uma infraestrutura normativa robusta, que previna abusos e preserve a autonomia dos cidadãos diante do avanço das arquiteturas de vigilância.

Portanto, o caminho a ser trilhado envolve integração normativa, fortalecimento institucional, criação de instâncias de participação social e incorporação sistemática de avaliações de impacto regulatório e ético em toda inovação tecnológica de cunho estatal. Apenas assim será possível equilibrar o binômio inovação-regulação em favor da democracia informacional.

## 10. Lições aprendidas

A disputa global por dados, muitas vezes travada de maneira invisível ao olhar do cidadão comum, representa um novo estágio na luta pelo poder no século XXI. Conforme observa Zuboff (2021, p. 103), essa guerra é caracterizada por uma assimetria radical entre aqueles que detêm os meios tecnológicos de coleta, análise e comercialização de dados e aqueles que são objeto dessa extração contínua. Trata-se de uma guerra silenciosa e constante, em que Estados, plataformas digitais e corporações transnacionais competem pelo controle da informação e, por consequência, das subjetividades.

Doneda (2021, p. 112) destaca que os dados pessoais não devem ser vistos como meros ativos comerciais, mas como projeções da personalidade. Nesse sentido, a autodeterminação informativa é essencial para garantir a dignidade e a liberdade dos cidadãos. Contudo, a lógica mercantil vigente tem desfigurado essa compreensão, subordinando os direitos informacionais à lógica da rentabilidade.

O fenômeno da guerra de dados revela a existência de um novo território de conflito geopolítico e econômico. A extração de dados tornou-se central na política internacional, afetando diretamente a soberania informacional dos Estados. A exemplo disso, a coleta massiva de dados por empresas transnacionais com sede nos Estados Unidos, como Google, Amazon, Meta e Microsoft, confere aos Estados Unidos uma vantagem estratégica sobre outras nações (Zuboff, 2021, p. 116).

Essa concentração de poder informacional também tem implicações para a soberania dos indivíduos. Quando as decisões que afetam a vida cotidiana (como concessão de crédito, acesso a serviços públicos, oportunidades de emprego e exposição a conteúdos informativos) passam a ser mediadas por algoritmos opacos, o indivíduo perde o controle sobre seu destino. Como alerta Eubanks (2018), essa lógica de gestão algorítmica tende a reproduzir desigualdades históricas e a reforçar preconceitos sistêmicos.

A guerra de dados, portanto, não se restringe à coleta em si, mas envolve a modelagem de comportamentos, a manipulação de preferências e a construção de realidades personalizadas. Pariser (2011) já advertia para os riscos da "bolha de filtros", onde os indivíduos passam a viver em realidades informacionais isoladas, moldadas por algoritmos que priorizam relevância comercial sobre pluralidade democrática.(Deseja que eu atualize também a lista de referências ao final do documento com base nos autores citados?)

A consolidação do capitalismo de vigilância, conforme descrito por Zuboff (2021, p. 13-118), representa uma inflexão histórica na relação entre poder, tecnologia e direitos fundamentais. A transformação da experiência humana em matéria-prima para algoritmos comerciais não apenas altera a dinâmica econômica global, mas desafia os próprios fundamentos do constitucionalismo contemporâneo. Os princípios estruturantes das três gerações de direitos fundamentais – liberdade, igualdade e solidariedade – encontram-se sob ataque num ambiente digital hostil à transparência, à autodeterminação e à justiça distributiva.

A guerra de dados, como fenômeno global, revela que a disputa por soberania informacional é hoje um dos eixos centrais do poder. O controle sobre fluxos de informação permite moldar preferências, influenciar decisões políticas e comerciais, e definir os contornos da realidade social percebida. Nesse cenário, a privacidade se torna um bem estratégico, e a proteção de dados passa a integrar o núcleo duro da dignidade da pessoa humana.

No caso brasileiro, a LGPD e o Marco Civil da Internet representam esforços iniciais relevantes, mas ainda insuficientes. Como argumentam Fachin e Silva (2021, p. 248), a ausência de um marco normativo mais robusto e de um aparato fiscalizatório

efetivo agrava a vulnerabilidade dos cidadãos frente às grandes plataformas digitais. A falta de articulação entre órgãos reguladores e a carência de cultura jurídica voltada à proteção da personalidade digital também comprometem a eficácia das normas em vigor.

Diante desse quadro, propõe-se uma reconstrução do sistema jurídico orientada por três eixos fundamentais: (1) a afirmação da centralidade da dignidade digital como princípio jurídico transversal; (2) a criação de mecanismos institucionais de governança tecnológica com participação social efetiva; e (3) o desenvolvimento de políticas públicas voltadas à educação digital crítica e à promoção da cidadania informacional.

É preciso, ademais, superar a dicotomia entre inovação tecnológica e proteção de direitos. A regulação não deve ser vista como obstáculo ao progresso, mas como instrumento de justiça social e de equilíbrio democrático. Um modelo de inovação comprometido com a ética pública pode – e deve – promover tecnologias que respeitem a privacidade, que sejam inclusivas, auditáveis e voltadas ao bem comum.

Como advertiu Zuboff (2021, p. 117), não basta proteger dados: é necessário desmantelar as arquiteturas de extração comportamental que se nutrem da assimetria informacional. Essa tarefa não é apenas jurídica, mas também política, cultural e epistemológica. Trata-se de recuperar a capacidade coletiva de governar o futuro digital, reapropriando-se da tecnologia como instrumento emancipatório e não como ferramenta de dominação.

Portanto, a resposta à crise instaurada pelo capitalismo de vigilância depende do compromisso ético com os direitos fundamentais, da mobilização institucional por marcos regulatórios eficazes e, sobretudo, da formação de uma cidadania ativa, crítica e vigilante. Somente assim será possível restaurar as condições de possibilidade de uma democracia informacional baseada em liberdade real, igualdade substancial e solidariedade digital.

## 11. Considerações finais

O presente artigo procurou investigar, sob uma perspectiva crítica e interdisciplinar, os impactos estruturais do capitalismo de vigilância sobre os direitos fundamentais na era digital, tomando como eixo central a obra de Shoshana Zuboff e dialogando com autores como Wolfgang Hoffmann-Riem, Danilo Doneda e Zulmar

Fachin. A análise revelou que o fenômeno da coleta massiva e opaca de dados pessoais (operada por grandes corporações digitais) configura uma nova arquitetura de dominação informacional, cujas consequências extrapolam o campo econômico e comprometem os fundamentos da dignidade humana, da autonomia individual e do Estado Democrático de Direito.

O resumo da pesquisa aponta que estamos diante de uma transformação profunda na relação entre tecnologia, poder e Direito. O avanço da inteligência artificial e dos sistemas algorítmicos não representa apenas um desafio técnico ou regulatório, mas impõe uma reconfiguração do próprio sujeito de direitos, que passa a ser monitorado, categorizado e modulado em tempo real. Nessa nova configuração, os dados pessoais deixam de ser meros ativos digitais e se tornam projeções da personalidade, elementos centrais da identidade e da liberdade dos indivíduos.

O problema central identificado no decorrer do estudo reside na inadequação das categorias jurídicas tradicionais para lidar com os efeitos complexos e sistêmicos do capitalismo de vigilância. A lógica informacional contemporânea opera à margem dos mecanismos clássicos de responsabilização e controle democrático, desafiando os pressupostos constitucionais que estruturam os direitos civis, políticos e sociais. A separação entre as gerações de direitos fundamentais se mostra obsoleta, uma vez que as novas tecnologias de extração e predição algorítmica impõem riscos simultâneos à liberdade, à igualdade e à solidariedade: os três pilares que sustentam o projeto normativo do constitucionalismo moderno.

Diante desse contexto, o objetivo geral do artigo foi promover uma reflexão crítica sobre a insuficiência das respostas jurídicas atuais e propor caminhos normativos, éticos e institucionais para a reconstrução do Direito na era digital. Para isso, o texto articulou os fundamentos teóricos da crítica ao capitalismo de vigilância com propostas doutrinárias voltadas à renovação da teoria do Direito Digital, destacando a centralidade da dignidade da pessoa humana como princípio orientador de todo o ordenamento jurídico.

A hipótese que sustentou a investigação é a de que o enfrentamento eficaz dos riscos impostos pelo capitalismo de vigilância exige um reposicionamento do Direito enquanto sistema adaptativo, preventivo e democrático. Esse novo modelo jurídico deve

ser capaz de agir não apenas sobre as consequências da vigilância, mas sobre suas causas estruturais, atuando desde o desenho técnico das tecnologias (por meio de princípios como *privacy by design*), exigindo transparência algorítmica, auditabilidade e responsabilização dos agentes que operam as infraestruturas digitais. Em suma, o Direito precisa recuperar sua função de mediação ética entre inovação tecnológica e justiça social, enfrentando a lógica de opacidade e exploração que define a era digital.

A metodologia adotada foi de natureza qualitativa, com abordagem teórico-dogmática e interdisciplinar, fundamentada na análise crítica da bibliografia especializada e dos marcos normativos nacionais e internacionais. Foram mobilizados conceitos oriundos do Direito Constitucional, da Filosofia Política, da Ciência da Computação e da Sociologia da Informação, o que permitiu uma leitura ampla e profunda do fenômeno em estudo. A partir dessa abordagem, foi possível evidenciar que a regulação jurídica da era digital não pode se restringir à atualização formal de dispositivos legais, mas requer uma transformação paradigmática, capaz de reposicionar o Direito como elemento central na defesa da autonomia informacional e da cidadania digital.

Com base nos dados analisados e nos argumentos desenvolvidos, pode-se afirmar que o capitalismo de vigilância constitui uma ameaça estrutural à democracia. O processo de coleta, tratamento e comercialização de dados pessoais realizado por plataformas digitais escapa ao controle dos próprios titulares dos dados, submetendo os indivíduos a dinâmicas de monitoramento constante, personalização de experiências e modulação de comportamento. Essa forma de poder, que atua de modo invisível e preditivo, compromete a liberdade de escolha,mina a esfera pública e naturaliza a vigilância como prática cotidiana.

Além disso, a concentração do poder informacional nas mãos de poucas corporações globais cria um cenário de assimetria cognitiva e econômica, em que os cidadãos tornam-se cada vez mais vulneráveis e os Estados, frequentemente, perdem sua capacidade de regular de forma efetiva as novas infraestruturas tecnológicas. A chamada "guerra de dados", conforme discutido ao longo do texto, expressa essa disputa geopolítica por soberania informacional, na qual os dados se convertem em instrumentos de dominação e vantagem estratégica.

Nesse cenário, as respostas jurídicas tradicionais (baseadas em modelos normativos fragmentados, em consentimentos formais e na reatividade institucional) mostram-se claramente insuficientes. A experiência brasileira, com o Marco Civil da Internet e a Lei Geral de Proteção de Dados, revela avanços importantes, mas ainda carece de integração normativa, capacidade fiscalizatória e mecanismos eficazes de enforcement. Conforme salientado por Fachin e Silva (2021), é imprescindível que essas normas sejam interpretadas sob a perspectiva dos direitos fundamentais, com ênfase na proteção da personalidade digital e na afirmação da dignidade humana como valor central do sistema jurídico.

Diante disso, as considerações finais deste artigo apontam para a urgência de uma reconstrução do Direito Digital que esteja à altura dos desafios contemporâneos. Essa reconstrução deve se orientar por três eixos fundamentais:

(i) Afirmação da dignidade digital como princípio transversal: a proteção dos dados pessoais deve ser compreendida como garantia da integridade da pessoa humana, e não apenas como mecanismo de compliance corporativo. A dignidade digital deve orientar todas as políticas públicas e decisões jurídicas relacionadas à tecnologia, informação e comunicação.

(ii) Criação de mecanismos institucionais de governança tecnológica com participação social efetiva: é necessário estabelecer estruturas regulatórias robustas, com competência técnica e legitimidade democrática, capazes de fiscalizar e auditar os sistemas algorítmicos utilizados por plataformas privadas e instituições públicas. A transparência, a explicabilidade e a auditabilidade devem ser princípios obrigatórios para toda tecnologia que interfira em direitos fundamentais.

(iii) Promoção de uma educação digital crítica e cidadã: a formação de uma cultura jurídica e política voltada à cidadania informacional é condição indispensável para que os indivíduos compreendam os riscos da vigilância digital e possam exercer seus direitos de maneira consciente e ativa. Sem uma população informada, a proteção de dados e a liberdade digital permanecem como abstrações formais, sem concretude prática.

Em síntese, a transição para uma sociedade verdadeiramente digital e democrática depende não apenas de inovações tecnológicas, mas, sobretudo, de escolhas políticas e

jurídicas comprometidas com os valores da justiça, da liberdade e da igualdade. O Direito, longe de ser um obstáculo ao progresso, deve ser compreendido como o instrumento privilegiado para garantir que o desenvolvimento tecnológico se alinhe ao bem comum e à proteção dos mais vulneráveis.

Assim, conclui-se que a superação do modelo atual de capitalismo de vigilância requer um esforço coletivo, transnacional e interdisciplinar, no qual juristas, legisladores, tecnólogos e cidadãos atuem conjuntamente para refundar os parâmetros de convivência digital. É necessário recuperar a capacidade coletiva de governar o futuro tecnológico, reapropriando-se da informação como bem público, da privacidade como valor inegociável e da cidadania como prática ativa e transformadora.

A era digital não pode ser sinônimo de regressão democrática. Ao contrário, deve ser a oportunidade para construir um novo pacto normativo, centrado na dignidade da pessoa humana, na soberania informacional e na justiça social: fundamentos inegociáveis de qualquer projeto de civilização verdadeiramente democrático.

## Referências

BRASIL. Decreto nº 10.332, de 28 de abril de 2020. **Institui a Estratégia de Governo Digital para o período de 2020 a 2022**. Diário Oficial da União, Brasília, 29 abr. 2020.

CADWALLADR, Carole; GRAHAM-HARRISON, Emma. **Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach**. The Guardian, Londres, 17 mar. 2018, p. 2.

CALO, Ryan. **Artificial Intelligence Policy: A Primer and Roadmap**. U.C. Davis Law Review, v. 51, p. 399-435, 2019.

CARVALHO, Vinícius; SANTIAGO, Ana. **A autoridade nacional de proteção de dados e os desafios da regulação efetiva no Brasil**. Revista de Direito, Estado e Telecomunicações, Brasília, v. 14, n. 2, p. 75-98, 2022.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 3. ed. São Paulo: Revista dos Tribunais, 2021, p. 29-71; 101-135.

EUBANKS, Virginia. **Automating Inequality: How High-Tech Tools Profile, Police,**

**and Punish the Poor.** New York: St. Martin's Press, 2018.

FACHIN, Zulmar; SILVA, Deise Marcelino da. **Avanços tecnológicos e a pessoa humana no século XXI: a (des)proteção do direito à privacidade no Marco Civil da Internet.** Revista Jurídica – UNICURITIBA, Curitiba, v. 5, n. 67, p. 230-254, 2021.

FEDERAL TRADE COMMISSION (FTC). **FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook.** 24 jul. 2019.

HAN, Byung-Chul. **Psicopolítica: neoliberalismo e as novas técnicas de poder.** Trad. Eliana Aguiar. Belo Horizonte: Autêntica, 2017.

HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital: transformação digital: desafios para o direito.** Trad. Ítalo Fuhrmann. Rio de Janeiro: Forense, 2021, p. 135-168.

MARTINS, Carla Veríssimo. **Governança algorítmica e proteção de dados pessoais no Brasil: desafios regulatórios da IA e da transformação digital do Estado.** Revista Direito Público, Brasília, v. 56, n. 2, p. 201-223, 2023.

PARISER, Eli. **The Filter Bubble: What the Internet Is Hiding from You.** New York: Penguin Press, 2011.

STF – Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade (ADI) 6.387. Relator: Min. Alexandre de Moraes.** Brasília, DF: STF, jul. 2020.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder.** Trad. George Schlesinger. São Paulo: Intrínseca, 2021, p. 13-118.