

IX ENCONTRO VIRTUAL DO CONPEDI

**DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS
III**

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 Haydêe 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. Edinilson 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: Luiz Alberto Pereira Ribeiro; Regina Vera Villas Boas; Paulo Campanha Santana – Florianópolis: CONPEDI, 2026.

Inclui bibliografia

ISBN: 978-65-5274-590-3

Modo de acesso: www.conpedi.org.br em publicações

Tema: Constituição, Processo e Justiça Social: o papel da jurisdição constitucional na efetivação de direitos

2. Direito. 3. Governança e novas tecnologias. IX Encontro Virtual do CONPEDI (2: 2026: Florianópolis, Brasil).

CDU: 34



Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS III

Apresentação

Texto de apresentação do livro do GT 52 - DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS III

O “IX Encontro Virtual do CONPEDI – Sociedade Científica do Direito no Brasil” foi realizado de forma virtual entre os dias 22 e 26 de junho de 2026. Este evento exemplar foi um marco de excelência acadêmica e colaboração científica, reunindo pesquisadores e estudiosos de diversas áreas do Direito.

Destacamos especialmente o Grupo de Trabalho – GT 52, intitulado “Direito, Governança e Novas Tecnologias III”, que se destacou pela profundidade e relevância dos temas abordados. Sob a coordenação dos Professores- Drs. Luiz Alberto P. Ribeiro (UEL e PUC/PR), Paulo Campanha (Mackenzie/Brasília) e Regina Vera Villas Bôas (PUC/SP), o GT proporcionou um espaço privilegiado para a discussão de questões fundamentais no campo do direito, governança e das novas tecnologias.

Neste GT foram apresentados trabalhos de elevada qualidade e importância crítica, sob os seguintes títulos:

1 MODERAÇÃO DE CONTEÚDO, GOVERNANÇA DE PLATAFORMAS DIGITAIS E DIREITOS FUNDAMENTAIS: PARÂMETROS CONSTITUCIONAIS PARA O BRASIL.

2 MERCADOS DE CARBONO E O NOVO SISTEMA BRASILEIRO DE COMÉRCIO DE EMISSÕES (SBCE).

6 GOVERNANÇA E REGULAÇÃO DA INFRAESTRUTURA PARA VEÍCULOS ELÉTRICOS EM CONDOMÍNIOS NO BRASIL: RISCOS, RESPONSABILIDADE CIVIL E DESIGUALDADE DE ACESSO

7 ENTRE O VIÉS HUMANO E O ALGORÍTMICO: DESAFIOS DA RACIONALIDADE PROCESSUAL NA ERA DA INTELIGÊNCIA ARTIFICIAL.

8 ENTRE A CELERIDADE E A EFICÁCIA: OS DESAFIOS DA AUTOMAÇÃO NO INSTITUTO NACIONAL DO SEGURO SOCIAL.

9 EMPRESAS TRANSNACIONAIS, RELAÇÕES DE TRABALHO E GOVERNANÇA DIGITAL NAS CONTRATAÇÕES PÚBLICAS: ANÁLISE CRÍTICA À LUZ DA LEI Nº 14.133/2021.

10 ECONOMIA DOS DADOS E GOVERNANÇA ALGORÍTMICA: PERFILAMENTO E VULNERABILIDADE DIGITAL DO CONSUMIDOR NA SOCIEDADE INFORMACIONAL.

11 DEMÔNIO DE LAPLACE, PREVISIBILIDADE E CONTROLE: PROBLEMÁTICAS EPISTEMOLÓGICAS, ÉTICAS E DE JUSTIÇA NAS DECISÕES JURÍDICO ADMINISTRATIVAS BASEADAS EM BIG DATA, ALGORITMOS E INTELIGÊNCIA ARTIFICIAL.

12 DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS E A TUTELA ESPECIAL NO TRATAMENTO DOS DADOS SENSÍVEIS: DA ESFERA DA PRIVACIDADE À DIGNIDADE DA PESSOA HUMANA E AUTODETERMINAÇÃO INFORMATIVA.

13 DIREITO PROCESSUAL E HOMOTRANSFOBIA ALGORÍTMICA: POR UM DEVER DE CUIDADO JURISDICIONALIZADO.

16 AUTOMAÇÃO DAS DECISÕES JUDICIAIS E OS LIMITES CONSTITUCIONAIS DA INTELIGÊNCIA ARTIFICIAL NO ESTADO DEMOCRÁTICO DE DIREITO.

17 AUTORIA E ORIGINALIDADE NA ERA DA INTELIGÊNCIA ARTIFICIAL: DESAFIOS JURÍDICOS DA PROTEÇÃO AUTORAL DIANTE DAS CRIAÇÕES AUTOMATIZADAS E DA AUTOPUBLICAÇÃO DIGITAL.

18 CAPITALISMO DE VIGILÂNCIA E DIREITOS FUNDAMENTAIS SOCIAIS: OS LIMITES JURÍDICOS DA EXPLORAÇÃO ECONÔMICA DE DADOS PESSOAIS NO BRASIL.

19 CAPITALISMO DE VIGILÂNCIA E HIPERCONSUMO: REFLEXÕES SOBRE A CRISE DA AUTONOMIA NA SOCIEDADE DIGITAL.

20 ADVOCACIA PÚBLICA E GOVERNANÇA INFORMACIONAL NA ADMINISTRAÇÃO PÚBLICA: PROTEÇÃO DE DADOS, POLÍTICAS PÚBLICAS E CONTROLE DE JURIDICIDADE.

A qualidade dos trabalhos apresentados neste GT 52 foi notável, refletindo o compromisso dos participantes com a pesquisa de alto nível e a inovação acadêmica. As contribuições dos estudiosos trouxeram insights significativos e promoveram um debate enriquecedor sobre os desafios contemporâneos e as perspectivas futuras nessas áreas cruciais que envolvem o Direito.

O IX Encontro Virtual do CONPEDI não apenas consolidou seu papel como um canal de referência no cenário acadêmico nacional e internacional, como também reafirmou o compromisso com a qualidade científica e a excelência na produção do conhecimento jurídico.

Os coordenadores do GT 52 deixam aqui abraços fraternos e cumprimentos a todos os participantes do CONPEDI e aos leitores dos presentes textos.

Prof. Dr. Luiz Alberto P. Ribeiro (UEL e PUC/PR)

Prof. Dr. Paulo Campanha (Mackenzie/Brasília)

Profa. Dra. Regina Vera Villas Bôas (PUC/SP)

CAPITALISMO DE VIGILÂNCIA E DIREITOS FUNDAMENTAIS SOCIAIS: OS LIMITES JURÍDICOS DA EXPLORAÇÃO ECONÔMICA DE DADOS PESSOAIS NO BRASIL

SURVEILLANCE CAPITALISM AND FUNDAMENTAL SOCIAL RIGHTS: THE LEGAL LIMITS OF THE ECONOMIC EXPLOITATION OF PERSONAL DATA IN BRAZIL

Luiz Do Carmo Cleto Rocha Filho
José Carlos Francisco dos Santos ¹

Resumo

A expansão das plataformas digitais alterou a forma como a vida social é explorada economicamente, na medida em que buscas, compras, interações e hábitos de navegação agora alimentam cadeias de coleta e monetização de dados pessoais. A partir dessa dinâmica, o capitalismo de vigilância começou a envolver dimensões materiais da cidadania, já que perfis podem interferir no acesso ao crédito e em todos os direitos sociais. Nesse diapasão, o presente artigo tem o seguinte problema de pesquisa: quais limites jurídicos incidem sobre a exploração econômica de dados pessoais no Brasil quando práticas de perfilamento, predição e classificação automatizada afetam direitos sociais e podem ampliar desigualdades? O objetivo é compreender de que modo a Constituição Federal de 1988, o Marco Civil da Internet, a LGPD e a jurisprudência do Supremo Tribunal Federal delimitam a atuação de plataformas, empresas e agentes públicos no tratamento de informações pessoais. Para isso, a pesquisa adota abordagem qualitativa, natureza bibliográfica e documental, método dedutivo e procedimento jurídico-dogmático, com apoio em doutrina abalizada, legislação, julgados e relatórios institucionais. Com o desenvolvimento do artigo, os achados deixam claro que o consentimento, considerado de forma isolada, não oferece proteção suficiente em ambientes digitais caracterizados por dependência cotidiana, baixa transparência e contratos de adesão. Logo, conclui-se que a exploração econômica de dados pessoais somente se harmoniza com o ordenamento brasileiro quando observa finalidade, necessidade, transparência, segurança e possibilidade real de controle pelo titular.

and with social rights as a whole. Against this backdrop, this article is guided by the following research problem: what legal limits apply to the economic exploitation of personal data in Brazil when profiling, prediction, and automated classification practices affect social rights and may deepen inequalities? The objective is to understand how the 1988 Federal Constitution, the Brazilian Civil Rights Framework for the Internet, the LGPD, and the case law of the Brazilian Supreme Federal Court delimit the actions of platforms, companies, and public agents in the processing of personal information. To this end, the research adopts a qualitative approach, with bibliographic and documentary nature, a deductive method, and a legal-dogmatic procedure, supported by established legal scholarship, legislation, court decisions, and institutional reports. Throughout the development of the article, the findings make clear that consent, when considered in isolation, does not provide sufficient protection in digital environments marked by everyday dependence, low transparency, and adhesion contracts. Thus, it is concluded that the economic exploitation of personal data is compatible with the Brazilian legal order only when it observes purpose limitation, necessity, transparency, security, and a real possibility of control by the data subject.

Keywords/Palabras-claves/Mots-clés: Informational society, Digital platforms, Profiling, Fundamental rights, Collective privacy

1 INTRODUÇÃO

Em um primeiro momento, é preciso começar o texto afirmando que a expansão das plataformas digitais alterou a forma pela qual a vida social, o consumo, o trabalho, a circulação urbana, o acesso ao crédito, a publicidade e a fruição de serviços públicos passaram a ser mediados por sistemas automatizados de coleta e classificação de informações pessoais. A partir da formulação de Zuboff (2019), o capitalismo de vigilância pode ser entendido como um arranjo econômico no qual rastros comportamentais, preferências, buscas, localização, interações e padrões de navegação adquirem valor mercantil ao alimentar técnicas de predição, segmentação publicitária e modulação de condutas.

Essa dinâmica também dialoga com a tradição dos estudos de vigilância de Lyon (2018), para quem a classificação digital de populações produz efeitos sociais que vão além da esfera íntima do titular, alcançando oportunidades, acessos e vulnerabilidades distribuídas coletivamente.

No Brasil, essa discussão é notória diante da convivência entre uma economia digital fortemente dependente de plataformas e um sistema constitucional que protege a dignidade da pessoa humana, a igualdade material, a privacidade, a proteção de dados pessoais e os direitos sociais. A Constituição Federal de 1988, após a Emenda Constitucional nº 115 de 2022, incluiu expressamente a proteção de dados pessoais entre os direitos e garantias fundamentais (Brasil, 2022), enquanto a Lei Geral de Proteção de Dados Pessoais estabeleceu limites ao tratamento informacional mediante princípios como finalidade, adequação, necessidade, transparência, segurança, prevenção, responsabilização e vedação à discriminação (Brasil, 2018).

Em perspectiva jurisprudencial, a suspensão cautelar da Medida Provisória nº 954 de 2020 pelo Supremo Tribunal Federal, nas ADIs 6.387, 6.388, 6.389, 6.390 e 6.393, corroborou com a compreensão de que tratamentos massivos de informações pessoais exigem justificativa legítima, salvaguardas técnicas e controle jurídico proporcional ao risco produzido (Brasil, 2020).

A partir de tal contextualização, o problema de pesquisa pode ser formulado nos seguintes termos: quais são os limites jurídicos aplicáveis à exploração econômica de dados pessoais no Brasil quando a coleta, o cruzamento, a inferência e a monetização de informações afetam o exercício de direitos fundamentais sociais, como saúde, educação, trabalho, moradia, assistência, consumo, crédito e participação em políticas públicas?

Buscando responder essa pergunta, o objetivo deste artigo é compreender os limites jurídicos da exploração econômica de dados pessoais no ordenamento brasileiro, com atenção

aos efeitos sociais decorrentes do perfilamento, da publicidade comportamental e da classificação automatizada de indivíduos e grupos.

Para tanto, a metodologia adotada corresponde a uma pesquisa qualitativa, de natureza bibliográfica e documental, orientada pelo método dedutivo e pelo procedimento jurídico-dogmático. Nesse caminho, a pesquisa usa a doutrina abalizada sobre capitalismo de vigilância, economia informacional, proteção de dados, privacidade social, perfilamento algorítmico e direitos fundamentais sociais, com levantamento em bases como Portal de Periódicos da CAPES, SciELO, Google Scholar, Biblioteca Digital Brasileira de Teses e Dissertações, SSRN e repositórios institucionais.

As buscas foram realizadas por termos como “capitalismo de vigilância”, *surveillance capitalism*, “economia dos dados”, “proteção de dados pessoais”, “autodeterminação informativa”, “privacidade coletiva” e “direitos sociais e plataformas digitais”.

No campo documental, foram analisados a Constituição Federal de 1988, o Marco Civil da Internet, a Lei Geral de Proteção de Dados Pessoais, a Emenda Constitucional nº 115 de 2022 e normas vinculadas à governança digital, com consulta a fontes oficiais, como Planalto, Congresso Nacional, Autoridade Nacional de Proteção de Dados e Diário Oficial da União.

A pesquisa também abrangeu julgados do Supremo Tribunal Federal sobre proteção de dados e autodeterminação informativa, em especial as ADIs 6.387, 6.388, 6.389, 6.390 e 6.393, além de relatórios técnicos da ANPD, CGI.br, CETIC.br, IBGE, OCDE e União Europeia, quando pertinentes à compreensão da exploração econômica de informações pessoais.

2 FORMAÇÃO HISTÓRICA E CONCEITUAL DO CAPITALISMO DE VIGILÂNCIA

Na economia industrial, o valor era associado à capacidade de produzir bens em escala, organizar trabalho fabril, controlar estoques, reduzir tempo de produção e ampliar mercados consumidores, tendo a fábrica como ambiente privilegiado de extração de riqueza. Ainda que a informação sempre tenha integrado a administração empresarial, ela aparecia, em regra, como registro auxiliar da produção, da circulação e do consumo, e não como matéria econômica autônoma. Daniel Bell, ao publicar *The Coming of Post-Industrial Society* em 1973, já percebia que conhecimento, serviços especializados e previsão técnica ganhariam crescente relevância na organização social, embora sua formulação ainda estivesse ligada à sociedade pós-industrial e à expansão do setor de serviços, sem alcançar a forma atual de exploração algorítmica da experiência humana (Bell, 1973).

Com a difusão da informática, das redes telemáticas e, posteriormente, da internet comercial, essa função instrumental foi alterada de modo gradual, onde a informação agora alimenta operações de classificação, cálculo, recomendação e antecipação de condutas. Santos (2021, p. 36) ensina que “essa evolução tecnológica culminou em um ambiente globalizado conectado pela internet e disciplinado pela Web, que fornece uma possibilidade infinita quanto à disseminação de informação”.

João Carlos Rebello Caribé situa esse percurso no contexto em que:

É possível que o capitalismo de vigilância tenha sido construído a partir de uma sucessão de falhas, eventos e oportunidades, percebidos ou construídos em diversas “cestas” e perspectivas, em contextos distintos, mas de alguma forma coordenados. Aspectos técnicos, comportamentais, legais, econômicos, sociais e estruturais precisam ser observados nesta construção (Caribé, 2019, p. 6).

Nessa profundidade, Manuel Castells, ao tratar da sociedade em rede, observou que a economia informacional organiza produção, consumo e poder por fluxos quase instantâneos de informação, capital e comunicação, em uma dinâmica na qual redes técnicas condicionam os próprios mercados e suas formas de coordenação (Castells, 2010). Nessa ambiência, o registro digital já não fica restrito ao documento, ao cadastro ou ao arquivo empresarial, pois cada busca, clique, localização, compra, curtida, pausa de visualização, rota e interação passa a integrar uma infraestrutura de cálculo voltada à extração econômica.

A passagem do registro ao ativo econômico ocorreu quando a informação pessoal foi incorporada aos modelos de negócio como elemento de precificação, segmentação e previsão, algo presente na chamada “era dos dados”. Esse período é conhecido como um momento onde “[...] produção, coleta, armazenamento e análise de dados se tornaram parte fundamental da sociedade e da economia, a informação é vista como um ativo valioso, e a capacidade de processar grandes quantidades de dados em tempo real é vista como uma vantagem competitiva” (Santos, 2022, p. 2).

Hal Varian, economista-chefe do Google, registrou que transações mediadas por computador produzem grandes volumes de informações, abrindo espaço para novas técnicas econométricas e de aprendizado estatístico aplicadas à vida econômica (Varian, 2014). Nesse ínterim, tal visão tem valor histórico uma vez que mostra a naturalização da coleta massiva como subproduto útil da mediação digital, embora o problema jurídico surja quando esse subproduto orienta escolhas, ordena visibilidades e interfere na esfera de liberdade dos sujeitos.

O caso *Google* é um exemplo nato dessa transformação. Em 1998, Sergey Brin e Lawrence Page apresentaram o Google como protótipo de mecanismo de busca que utilizava a estrutura hipertextual da web para classificar páginas, com base em uma lógica diferente da

simples correspondência de palavras, já que os *links* eram tratados como sinais de relevância no algoritmo *PageRank* (Brin; Page, 1998).

A inovação inicial estava na ordenação mais qualificada da informação disponível na rede, com promessa de melhorar a busca em um ambiente digital em rápida expansão. De tal modo, a mudança econômica surgiu quando a capacidade de indexar, hierarquizar e registrar interações foi acoplada a um sistema publicitário capaz de transformar rastros comportamentais em receita recorrente.

A primeira engrenagem desse modelo foi o *AdWords*, lançado em 2000 com 350 anunciantes, conforme carta dos fundadores do Google divulgada em 2009, em referência aos primeiros experimentos publicitários da empresa. O mecanismo oferecia anúncios textuais vinculados às buscas, com aparência mais discreta do que os *banners* dominantes nos anos 1990, ao mesmo tempo em que aproximava intenção do usuário e oferta comercial. A mudança técnica foi acompanhada por uma mudança econômica, haja vista que a consulta digitada no campo de busca foi interpretada como sinal de interesse, desejo, urgência, medo, curiosidade ou predisposição de consumo (Google, 2009).

A segunda engrenagem apareceu com o *AdSense*, que expandiu a publicidade para páginas de terceiros e permitiu ao Google servir anúncios vinculados ao conteúdo de sites parceiros. No formulário S-1 apresentado à *Securities and Exchange Commission* em 2004, a empresa descreveu o *AdSense for content* como tecnologia automatizada que analisava o conteúdo das páginas e exibia anúncios em frações de segundo, demonstrando a união entre indexação, automação e monetização de atenção (Google, 2004).

É possível dizer que nesse momento a publicidade digital começou a agir por correspondências dinâmicas entre conteúdo, contexto, usuário e até mesmo por expectativa de conversão.

Esse arranjo explica a gênese do capitalismo de vigilância na formulação de Shoshana Zuboff. Em artigo publicado em 2015 intitulado “*Big other: surveillance capitalism and the prospects of an information civilization*”, a autora identificou uma lógica de acumulação própria da esfera conectada, tendo as práticas institucionais do *Google* como lente principal para compreender a extração, a mercantilização e o controle de condutas no ambiente informacional (Zuboff, 2015).

Nas palavras de Koerner (2021, p. 01):

O capitalismo de vigilância é uma mutação do capitalismo da informação, que nos coloca diante de um desafio civilizacional. As Big Techs – seguidas por outras firmas, laboratórios e governos – usam tecnologias da informação e comunicação (TIC) para

expropriar a experiência humana, que se torna matéria-prima processada e mercantilizada como dados comportamentais. O usuário cede gratuitamente as suas informações ao concordar com termos de uso, utilizar serviços gratuitos ou, simplesmente, circular em espaços onde as máquinas estão presentes.

A expressão “excedente comportamental” designa justamente a parcela de informações produzida para além da necessidade imediata de prestação do serviço, posteriormente convertida em produtos preditivos destinados a mercados publicitários e, de forma mais ampla, a mercados de antecipação e modificação de comportamento.

A relevância histórica desse excedente está em sua origem aparentemente banal. Ao pesquisar uma rota, consultar sintomas, assistir a um vídeo, comparar preços ou permanecer alguns segundos diante de determinada postagem, a pessoa oferece sinais que, isoladamente, parecem frágeis, dispersos e pouco expressivos.

Entretanto, agregados em escala e processados por sistemas estatísticos, esses sinais permitem inferir preferências, vulnerabilidades, ciclos de vida, inclinações políticas, padrões de consumo, riscos de inadimplência, localização provável e grau de suscetibilidade a estímulos. Por isso, posteriormente Zuboff (2019) descreve essa economia como uma ordem que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais de extração, previsão e venda, e essa definição ajuda a perceber que a vigilância, aqui, atua como método de acumulação.

A publicidade comportamental forneceu o primeiro mercado de grande escala para esse modelo. Diferentemente da publicidade contextual tradicional, vinculada ao tema de uma página ou ao perfil presumido de um veículo, a publicidade comportamental acompanha o usuário por múltiplos ambientes e cria inferências a partir de sua trajetória digital. Por exemplo:

Ao “observar” o comportamento dos clientes, com o objetivo de ofertar livros com maior chance de compra, a Amazon pavimentou o capitalismo de vigilância, em outras palavras, a Amazon extraía dados dos clientes, e os modelava na busca de padrões, e através de homofiliav, estabelecia relacionamentos, produzindo indicações para o cliente, visando “aprimorar” a sua experiência. Dez anos depois, em 2007, a Amazon lançou o Kindle, o leitor de e-book, e passou a extrair dados também dos hábitos de leitura de seus clientes, tais como interesse, horário de leitura, destaques e compartilhamento de texto (Caribé, 2019, p. 6).

Nesse prisma, relatórios financeiros de 2004 já mostravam a dependência do Google em relação à receita publicitária, com US\$ 3,189 bilhões de receita anual naquele exercício e crescimento de 118% em comparação a 2003, sinalizando o êxito econômico de um modelo fundado na transformação da atenção rastreada em receita mensurável (Google, 2005).

Porém, é preciso afirmar aqui que a arquitetura técnica dessa economia foi acompanhada por disputas de propriedade intelectual e por pedidos de patente voltados ao refinamento de

perfis. Em 2005, por exemplo, foi publicado pedido de patente relacionado à geração de informações de usuários para publicidade direcionada, no qual perfis poderiam ser inferidos por associação entre documentos, usuários e topologias de grafos (Google, 2005).

Ou seja, percebe-se que o perfil não nasce exclusivamente de uma informação declarada voluntariamente pelo titular, já que decorre, muitas vezes, de inferências produzidas a partir de correlações invisíveis para a pessoa afetada. Por exemplo, uma pessoa que pesquisa dores nas costas, acessa páginas sobre cadeiras ergonômicas e consulta vídeos de alongamento pode ser inserida em um perfil de interesse relacionado à saúde ou ao trabalho sedentário, mesmo sem ter declarado qualquer informação sobre sua condição física, sua rotina profissional ou suas preferências de consumo.

Daí a necessidade de diferenciar coleta, perfilamento, predição e modulação. Primeiramente, a coleta é a captura de informações fornecidas, observadas ou inferidas em determinada interação digital. Já o perfilamento é a organização desses elementos em categorias úteis para avaliação de características pessoais, econômicas, psicológicas ou comportamentais (Sampaio; Costa, 2025).

O Regulamento Geral de Proteção de Dados da União Europeia define *profiling* como tratamento automatizado destinado a avaliar aspectos pessoais, inclusive desempenho no trabalho, situação econômica, saúde, preferências, interesses, confiabilidade, comportamento, localização ou movimentos, definição que permite compreender a amplitude jurídica do fenômeno (União Europeia, 2016).

A predição, por sua vez, acontece quando o perfil deixa de retratar condutas passadas e começa a estimar comportamentos futuros. Ora, não se trata aqui de conhecer a pessoa em sentido humanístico, todavia, de produzir probabilidades de ação em contextos selecionados (Badr, 2026). A predição comercial estima quem comprará, desistirá, migrará de serviço, aceitará um preço, clicará em uma propaganda ou permanecerá mais tempo em determinada plataforma, enquanto a predição social pode afetar crédito, seguro, emprego, policiamento, educação e acesso a oportunidades.

Frank Pasquale denominou essa opacidade de *black box society*, chamando atenção para sistemas que classificam indivíduos sem oferecer transparência adequada sobre critérios, bases informacionais e consequências da decisão automatizada (Pasquale, 2015).

Para Machado (2018), a modulação de comportamento é a etapa mais delicada para o Direito. Nesse estágio, a informação extraída e a predição calculada orientam intervenções no ambiente de escolha do indivíduo, por meio de ranqueamento, recomendação, notificação, preço personalizado, desenho de interface, escassez artificial, estímulos emocionais e

arquitetura de atenção. “[...] A modulação opera como uma forma de controle, em um novo regime de dominação. Ou seja, cada molde social ao qual o indivíduo tem que se adaptar é uma forma de exercício de controle” (Meireles, 2021, p. 38).

Karen Yeung denominou esse mecanismo de *hypernudge*, ao tratar do *Big Data* como forma de regulação por desenho, na qual técnicas algorítmicas produzem orientações adaptativas, contínuas e personalizadas, capazes de conduzir decisões sem comando jurídico explícito e sem coerção formal (Yeung, 2017).

Essa questão aproxima o capitalismo de vigilância da teoria jurídica da liberdade de Honneth (2017), considerando que o problema não está tão-só na existência de anúncios personalizados, uma vez que práticas de recomendação acompanham a vida comercial há décadas. A singularidade do modelo contemporâneo está na escala, na opacidade, na velocidade e na capacidade de aprendizado contínuo, já que os sistemas digitais testam respostas em tempo real, ajustam estímulos e incorporam reações do usuário ao próprio ciclo de extração.

Para o direito, a autonomia fica comprimida quando escolhas formalmente livres são preparadas por ambientes informacionais desenhados para explorar vulnerabilidades cognitivas, afetivas e sociais.

A doutrina recente sobre colonialismo de informações acrescenta outro plano interpretativo. Na acepção de Couldry e Mejias (2019), as relações informacionais contemporâneas normalizam a apropriação da vida humana como recurso econômico, em continuidade com lógicas históricas de extração, embora agora voltadas à captura permanente de atividades, vínculos e experiências cotidianas.

A comparação tem alcance teórico posto que move o foco do ato individual de consentir para a infraestrutura social que torna a conexão quase obrigatória, isto é, trabalhar, estudar, consumir, circular, comunicar e acessar serviços públicos depende cada vez mais de ambientes nos quais a coleta foi incorporada à própria forma de participação social.

Nesse diapasão, a privacidade individual, embora basilar na nossa sociedade, mostra limites para compreender os efeitos do capitalismo de vigilância. A tradição liberal formulou a privacidade como proteção contra intromissões indevidas, tendo como referência clássica o “direito de ser deixado só”, expressão associada ao artigo de Warren e Brandeis de 1890. No ambiente informacional contemporâneo, a lesão nem sempre aparece como invasão visível da intimidade, já que muitas violações ocorrem por recombinação, inferência, segmentação e uso secundário de informações dispersas.

Doneda (2019) foi feliz ao mostrar que a proteção de informações pessoais supera a tutela negativa da vida privada, alcançando a autodeterminação informativa e a disciplina do tratamento como condição de liberdade em sociedades informatizadas.

A dimensão social dos dados pessoais decorre precisamente de sua natureza relacional, tendo em vista que informações sobre uma pessoa permitem inferir características de outras, principalmente quando indivíduos compartilham território, renda, escola, profissão, religião, etnia, hábitos de consumo, condições de saúde, preferências culturais ou redes de sociabilidade. Salomé Viljoen formula essa questão ao ensinar que relações informacionais produzem interesses supraindividuais, de modo que direitos centrados só no titular não conseguem responder aos efeitos populacionais de sistemas preditivos e classificatórios (Viljoen, 2021).

Assim sendo, o tratamento de informações pessoais afeta grupos, categorias e comunidades, mesmo quando o ponto de coleta parece individual. Justamente sobre essa questão, Chiara Antonia Spadaccini de Teffé explica que:

Entende-se que a criação de perfis pode perpetuar estereótipos e ampliar a segregação social. Ela também pode prender uma pessoa em uma categoria e restringi-la às preferências sugeridas, o que prejudicaria sua liberdade de escolher, por exemplo, certos produtos ou serviços, como livros, música ou feeds de notícias. Em alguns casos, a criação de perfil pode levar a previsões imprecisas. Em outros, pode levar à negação de serviços e bens e discriminação injustificada (Teffé, 2022, p. 28-29).

Por exemplo, podemos citar quando uma plataforma identifica que moradores de determinada região pesquisam com frequência sobre desemprego, transporte precário e crédito de curto prazo, essa informação pode alimentar classificações comerciais sobre todo o grupo residente naquele território, alcançando pessoas que nunca realizaram tais buscas, passando a serem tratadas como parte de uma categoria econômica presumida.

A privacidade de grupo alarga essa compreensão ao trazer que os efeitos do tratamento massivo de dados vão além da esfera individual. Nessa seara, grupos podem sofrer danos mesmo quando seus integrantes não são nominalmente identificados, já que a classificação algorítmica atua por padrões, correlações e probabilidades (Taylor; Floridi; Van der Sloot, 2017).

Esse diagnóstico importa aqui considerando que a exploração econômica de informações pessoais raramente se encerra no indivíduo isolado, envolvendo bairros, faixas de renda, padrões de saúde, segmentos raciais, comunidades religiosas, públicos vulneráveis e grupos politicamente mobilizáveis

Tendo em vista isso, a dogmática jurídica brasileira já apresenta elementos para essa interpretação ampliada. A Lei nº 13.709, de 14 de agosto de 2018, disciplina o tratamento de

dados pessoais em meios físicos e digitais, tendo como objetivos a proteção da liberdade, da privacidade e do livre desenvolvimento da personalidade da pessoa natural, enquanto o art. 20 prevê direito à revisão de decisões tomadas unicamente com base em tratamento automatizado que afetem interesses do titular (Brasil, 2018).

A Emenda Constitucional nº 115, promulgada em 10 de fevereiro de 2022, inseriu a proteção de dados pessoais entre os direitos e garantias previstos no art. 5º da Constituição, além de fixar competência privativa da União para legislar sobre a matéria (Brasil, 2022).

Esse movimento normativo foi antecedido por um marco jurisprudencial de elevada pertinência constitucional. No julgamento cautelar das ADIs 6.387, 6.388, 6.389, 6.390 e 6.393, em 2020, o Supremo Tribunal Federal analisou a validade da Medida Provisória nº 954/2020, editada durante a emergência sanitária da Covid-19, que autorizava empresas prestadoras do Serviço Telefônico Fixo Comutado e do Serviço Móvel Pessoal a compartilharem com o IBGE a relação de nomes, números de telefone e endereços de seus consumidores, com a finalidade declarada de viabilizar entrevistas estatísticas por meio remoto (Brasil, 2020).

A controvérsia não se limitava ao interesse público na produção de informações oficiais durante a pandemia, alcançando a suficiência das salvaguardas jurídicas para o tratamento de dados pessoais em larga escala, uma vez que a medida provisória não delimitava os critérios de necessidade, finalidade, segurança, transparência, eliminação posterior dos dados e controle contra usos desviados. Ao referendar a cautelar deferida pela ministra Rosa Weber, o Plenário do STF suspendeu a eficácia da medida, assentando que o compartilhamento massivo de informações pessoais, ainda que orientado por finalidade estatal legítima, exige base normativa compatível com a proteção da intimidade, da vida privada, do sigilo e da autodeterminação informativa (Brasil, 2020).

Nesse julgamento, a Corte reconheceu que a proteção de dados pessoais possui conteúdo constitucional próprio, extraído do art. 5º, X e XII, da Constituição Federal, em diálogo com a dignidade da pessoa humana e com a exigência de limitação do poder informacional exercido pelo Estado e por agentes privados.

Vale afirmar que o precedente em questão antecedeu a Emenda Constitucional nº 115/2022 e corroborou para materializar a leitura segundo a qual a circulação de dados pessoais, em sociedades digitalizadas, exige controle material sobre finalidade, proporcionalidade, segurança e prevenção de danos coletivos decorrentes de tratamentos informacionais em escala populacional.

O STF registrou que a MP 954/2020 alcançaria uma quantidade muito expressiva de usuários de telefonia fixa e móvel, o que ampliava o risco de afetação à intimidade e à vida

privada caso o fluxo informacional ocorresse sem desenho normativo seguro. Conforme divulgado pelo próprio Supremo, a maioria dos ministros entendeu que a previsão legal era insuficiente para autorizar o compartilhamento pretendido, justamente pela ausência de garantias adequadas quanto à finalidade, ao modo de tratamento e à proteção posterior das informações transferidas ao IBGE.

No plano conceitual, a passagem da privacidade individual à dimensão social das informações pessoais exige abandonar a ideia de que o consentimento resolve, sozinho, a legitimidade do tratamento. Sobre tal questão, Bruno Bioni explica que o consentimento apresenta limites funcionais em ambientes de alta opacidade técnica, nos quais o titular raramente compreende o ciclo completo de coleta, compartilhamento, inferência e monetização (Bioni, 2019).

A consequência jurídica é objetiva, já que a validade do tratamento precisa ser aferida também por finalidade, necessidade, transparência, prevenção, não discriminação, responsabilização e possibilidade real de controle, com atenção aos riscos coletivos gerados por sistemas preditivos.

A contribuição de Julie Cohen auxilia a fechar esse percurso histórico e conceitual. Para a autora, o capitalismo informacional não nasce fora do Direito, pois depende de escolhas jurídicas sobre propriedade intelectual, contratos, responsabilidade, concorrência, proteção de dados, arquitetura de plataformas e circulação de informação (Cohen, 2019).

Essa observação evita versar o capitalismo de vigilância como resultado espontâneo da inovação tecnológica, uma vez que sua expansão foi viabilizada por regimes de permissividade regulatória, contratos de adesão extensos, desenho opaco de interfaces, concentração de infraestrutura e naturalização da coleta permanente como preço invisível da vida conectada.

3 LIMITES JURÍDICOS À EXPLORAÇÃO ECONÔMICA DE DADOS PESSOAIS NO BRASIL NA PERSPECTIVA DOS DIREITOS FUNDAMENTAIS SOCIAIS

Nesse segundo momento do artigo, é pertinente começar afirmando que a exploração econômica de informações pessoais no Brasil exige um entendimento a partir de uma cadeia produtiva própria, diversa da circulação tradicional de mercadorias, na qual a experiência cotidiana é convertida em registro, o registro em perfil, o perfil em probabilidade e a probabilidade em ativo negociável.

Essa cadeia tem início na coleta aparentemente banal de cliques, pesquisas, curtidas, geolocalização, tempo de permanência em telas, histórico de compras, contatos, identificadores

de aparelho e metadados, alcançando etapas menos visíveis de armazenamento em nuvem, cruzamento entre bases, enriquecimento por *data brokers*, inferências comportamentais e monetização por publicidade dirigida, ranqueamento e precificação dinâmica. Com efeito, a conversão da vida social em registros quantificáveis reorganiza relações de poder e de mercado em torno da extração contínua de rastros pessoais (Van Dijck, 2014).

Essa cadeia econômica recebeu maior sofisticação com a publicidade comportamental, especialmente a partir dos anos 2000, quando mecanismos de busca, redes sociais, aplicativos móveis e ecossistemas de anúncios começaram a operar com identificadores e segmentações por propensão de consumo. O capitalismo de vigilância designa esse arranjo de apropriação de experiências humanas para produção de previsões comercializáveis, em um modelo cuja receita deriva da capacidade de antecipar e influenciar condutas futuras (Zuboff, 2019).

Em outra perspectiva teórica, o capitalismo informacional depende de arquiteturas jurídicas, contratuais e técnicas que naturalizam a captura de informações pessoais como condição de participação social (Cohen, 2019).

Nesse cerne, a etapa mais delicada está sobre o cruzamento e a inferência. Ora, um aplicativo de mobilidade pode registrar rotas frequentes, horários de circulação e endereços recorrentes, ao mesmo tempo em que uma plataforma de comércio eletrônico agrega buscas, abandonos de carrinho, tempo de visualização e meios de pagamento, permitindo inferências sobre renda, rotina, interesses, estado de saúde, religião, gravidez, orientação política ou vulnerabilidade financeira.

A categoria de informação pessoal sensível, prevista na LGPD, alcança origem racial ou étnica, convicção religiosa, opinião política, saúde, vida sexual, biometria e genética, embora a economia digital chegue a atributos semelhantes por vias indiretas, mediante *proxies* aparentemente neutros, como CEP, tipo de aparelho, horário de acesso e padrão de consumo (Brasil, 2018).

A partir daí, surge um problema jurídico ainda pouco tratado em abordagens sobre consentimento, que é o fato que a pessoa titular raramente negocia de modo real as condições de tratamento de suas informações, uma vez que a vida cotidiana foi integrada a plataformas de comunicação, estudo, trabalho, transporte, consumo, lazer, crédito e acesso a serviços públicos. Nesse ambiente, o consentimento está próximo de uma autorização aderida em massa, pressionada por dependência funcional e baixa inteligibilidade dos termos de uso.

McDonald e Cranor (2008) chegaram a esse resultado a partir de uma estimativa do tempo necessário para que usuários da internet lessem políticas de privacidade dos sites visitados ao longo de um ano. As autoras partiram da quantidade média de páginas acessadas

por usuários norte-americanos, estimaram o tempo de leitura de políticas de privacidade típicas e converteram esse tempo em custo econômico, considerando o valor da hora em atividades domésticas e laborais. No cálculo principal, cada usuário gastaria cerca de 244 horas por ano lendo integralmente essas políticas, o que equivaleria a aproximadamente 40 minutos por dia. Em escala nacional, tomando como referência cerca de 221 milhões de usuários de internet nos Estados Unidos, isso representaria cerca de 53,8 bilhões de horas anuais destinadas apenas à leitura desses documentos (McDonald; Cranor, 2008).

Outrossim, ao atribuírem valor monetário ao tempo consumido, os autores citados estimaram que a leitura integral das políticas de privacidade alcançaria aproximadamente US\$ 3.534 por usuário ao ano, com custo social total próximo de US\$ 781 bilhões anuais nos Estados Unidos. Mesmo em cenário mais moderado, voltado à leitura superficial ou ao simples exame das políticas, os custos permaneceriam elevados, demonstrando que o modelo centrado na disponibilização formal de documentos longos transfere ao indivíduo uma carga incompatível com a experiência cotidiana de navegação digital (McDonald; Cranor, 2008).

No Brasil, a função e os limites do consentimento foram trabalhados a partir da ideia de que a autodeterminação informacional exige mais que um clique em caixas padronizadas, de maneira especial quando a arquitetura da plataforma induz adesão, oculta alternativas ou condiciona serviços indispensáveis ao fornecimento excessivo de informações (Bioni, 2019).

A LGPD acolhe essa preocupação de modo expresso. O art. 5º, XII, define consentimento como manifestação “livre, informada e inequívoca”, enquanto o art. 8º, *caput*, exige que essa manifestação ocorra por escrito ou por outro meio capaz de demonstrar a vontade do titular. A mesma lógica aparece no art. 8º, § 4º, ao estabelecer que o consentimento deve se referir a finalidades determinadas, considerando nulas as autorizações genéricas para tratamento de dados pessoais. Com isso, a lei afasta a ideia de que a simples aceitação formal de termos extensos e padronizados possa legitimar qualquer forma de exploração econômica das informações pessoais (Brasil, 2018).

Ademais, o art. 6º da LGPD submete todo tratamento de dados à boa-fé e a princípios como finalidade, adequação, necessidade, livre acesso, transparência, segurança, prevenção, não discriminação e responsabilização. Nessa toada, isso significa que o consentimento, embora relevante, não funciona como autorização ilimitada para coleta, cruzamento, inferência e monetização de dados. Mesmo quando há anuência do titular, o controlador permanece juridicamente vinculado à compatibilidade entre o tratamento realizado e a finalidade informada, à limitação do uso ao mínimo necessário e à prestação de contas sobre a conformidade de sua atuação com a legislação de proteção de dados (Brasil, 2018).

A dependência cotidiana das plataformas altera o peso jurídico da liberdade contratual. Em redes sociais, aplicativos bancários, sistemas de entrega, ambientes virtuais de aprendizagem, *marketplaces*¹ e serviços de autenticação, a recusa ao tratamento pode resultar em exclusão prática de espaços de sociabilidade, estudo, renda e consumo.

A doutrina de *platform capitalism* mostra que plataformas digitais atuam por efeitos de rede, expansão de ecossistemas fechados, extração de informações de múltiplos lados do mercado e concentração de capacidade analítica, quadro esse que reduz a margem de escolha individual e fortalece modelos de adesão com desequilíbrio estrutural (Srnicek, 2017). Nessa ambiência, o consentimento isolado perde aptidão para legitimar práticas opacas de vigilância comercial.

Os direitos sociais ingressam nessa discussão haja vista que a exploração econômica de informações pessoais já influencia oportunidades de trabalho, acesso ao crédito, contratação de seguros, ofertas educacionais, preços de produtos, planos de saúde, moradia, assistência social e circulação urbana.

Sistemas de triagem curricular podem reproduzir padrões históricos de exclusão ao ranquear candidatos por trajetória escolar, endereço, lacunas laborais ou histórico de navegação, enquanto modelos de crédito podem penalizar moradores de determinadas regiões ou consumidores sem histórico bancário formal. No campo do *big data*, modelos preditivos podem gerar impacto discriminatório mesmo sem intenção de discriminar, porquanto aprendem com registros sociais abalizados por desigualdades anteriores (Barocas; Selbst, 2016).

Essa afetação possui materialidade social. Em políticas públicas, sistemas automatizados de elegibilidade, pontuação de risco e controle de fraudes podem atingir com maior severidade pessoas pobres, famílias dependentes de benefícios e grupos racializados, transferindo a decisão pública para modelos matemáticos pouco contestáveis (Eubanks, 2018).

Em mercados privados, a formação de uma “sociedade pontuada” permite que escores invisíveis influenciem crédito, reputação, emprego e seguros, reduzindo a capacidade da pessoa de compreender e contestar classificações que afetam sua vida material (Citron; Pasquale, 2014).

No plano constitucional brasileiro, a proteção de informações pessoais precisa dialogar com a dignidade da pessoa humana, a igualdade, a privacidade, a intimidade, a livre iniciativa e a função social da ordem econômica. A Constituição de 1988 assegura direitos sociais no art.

¹ “Os *marketplaces* são plataformas digitais que conectam vendedores de mercadorias e prestadores de serviços àqueles desejam comprar os produtos ou tomar tais serviços, por meio da intermediação dessas operações” (Cunha; Pecis, 2023, p. 2).

6º, entre eles educação, saúde, alimentação, trabalho, moradia, transporte, lazer, segurança, previdência social, proteção à maternidade e à infância e assistência aos desamparados, ao mesmo tempo em que, após a Emenda Constitucional nº 115 de 2022, inseriu expressamente a proteção de informações pessoais no art. 5º, LXXIX, inclusive em meios digitais (Brasil, 1988).

A ordem econômica constitucional também limita a monetização de informações pessoais. O art. 170 da Constituição submete a livre iniciativa à valorização do trabalho humano, à justiça social, à defesa do consumidor, à redução das desigualdades regionais e sociais e à repressão ao abuso do poder econômico (Brasil, 1988), de modo que a extração de informações pessoais para discriminação de preços, manipulação de vulnerabilidades ou exclusão de consumidores não encontra abrigo em uma compreensão patrimonialista do mercado digital. A proteção de dados, nessa linha, obra como limite à mercantilização da pessoa e como condição de acesso igualitário a bens e serviços sociais.

O Marco Civil da Internet, Lei nº 12.965 de 2014, antecipou alguns limites ao estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil, incluindo proteção da privacidade, proteção de dados pessoais, neutralidade de rede, preservação da estabilidade e responsabilização de agentes conforme suas atividades. O art. 7º assegura ao usuário inviolabilidade da intimidade e da vida privada, sigilo do fluxo de comunicações, informações claras sobre coleta, uso, armazenamento e tratamento, além de consentimento expresso para coleta, uso, armazenamento e tratamento de informações pessoais quando a hipótese legal exigir. O art. 3º, VIII, preserva a liberdade dos modelos de negócio na internet, desde que compatíveis com os demais princípios da lei, afastando qualquer pretensão de converter inovação econômica em autorização para vigilância irrestrita (Brasil, 2014).

A LGPD, Lei nº 13.709 de 2018, definiu o tratamento como toda operação realizada com dados pessoais, incluindo coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, eliminação, avaliação, controle, modificação, comunicação e transferência (Brasil, 2018).

A esse respeito, tal amplitude impede que empresas isolem cada etapa da cadeia econômica como atos indiferentes, já que a lei alcança o ciclo inteiro de circulação informacional. Antes da lei brasileira, a tutela contemporânea da privacidade já vinha sendo compreendida como controle sobre fluxos informacionais, em superação da visão restrita à proteção contra intromissões domésticas ou exposições indevidas (Bueno; Sampaio Neto, 2024).

Os princípios do art. 6º da LGPD formam o núcleo material da limitação jurídica. Sob esse prisma, a finalidade exige propósito legítimo, específico e informado, adequação impõe

compatibilidade entre tratamento e contexto, necessidade determina limitação ao mínimo informacional útil, livre acesso e transparência garantem conhecimento sobre a operação, segurança e prevenção exigem medidas contra incidentes, qualidade assegura exatidão e atualização, vedação à discriminação impede usos abusivos ou ilícitos, ao passo que responsabilização obriga o controlador a demonstrar conformidade (Brasil, 2018).

A monetização ostenta feição juridicamente abusiva quando o tratamento rompe a finalidade declarada, captura informações além do necessário, produz perfis opacos, impede contestação, utiliza inferências sensíveis, induz escolhas por *dark patterns* ou condiciona acesso a serviço relevante ao fornecimento desmedido de informações. Bem como, também existe abuso quando a plataforma usa rastreamento entre sites e aplicativos para compor perfil comportamental alheio à expectativa legítima do usuário, principalmente em serviços de saúde, educação, crédito, trabalho ou assistência.

A teoria da integridade contextual de Nissenbaum (2010) afirma que a violação de privacidade ocorre quando o fluxo informacional desrespeita normas sociais do contexto em que a informação surgiu, ainda que algum elemento tenha sido entregue voluntariamente.

A abusividade está presente em práticas de *real-time bidding*, nas quais informações de navegação e atributos do usuário alimentam leilões de publicidade em frações de segundo, com múltiplos agentes recebendo sinais sobre perfil, localização, dispositivo, interesses e comportamento provável. Embora o usuário veja exclusivamente um anúncio, a cadeia envolve anunciantes, plataformas de demanda, plataformas de oferta, corretores de audiência, redes de mensuração e intermediários técnicos, formando um ambiente de difusão informacional de difícil auditoria. Logo, a consequência disso é a criação de uma “sociedade de caixa-preta”, na qual pessoas são avaliadas sem acesso suficiente aos critérios que ordenam oportunidades e restrições (Pasquale, 2015).

O Código de Defesa do Consumidor também incide sobre essa economia, especialmente quando a coleta e a monetização de informações pessoais aparecem associadas a contratos de adesão, publicidade direcionada, ofertas personalizadas e práticas que exploram vulnerabilidade. Para tanto, o art. 6º reconhece direitos básicos à informação adequada, proteção contra publicidade enganosa e abusiva e prevenção de danos, enquanto o art. 39 veda exigir vantagem manifestamente excessiva e prevalecer-se da fraqueza ou ignorância do consumidor, consideradas idade, saúde, conhecimento ou condição social (Brasil, 1990).

A tutela consumerista, coadunada à LGPD, permite qualificar como abusivas práticas de *profiling* que manipulam vulnerabilidades econômicas, emocionais ou informacionais em lugar de aprimorar a experiência de uso (Faleiros Júnior; Basan, 2022).

Ainda, a discussão alcança o art. 20 da LGPD, que assegura ao titular o direito de solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas decisões destinadas a definir perfil pessoal, profissional, de consumo e de crédito ou aspectos da personalidade (Brasil, 2018).

Conforme já citado, os algoritmos podem influenciar concessão de crédito estudantil, aprovação de aluguel, contratação de trabalhador, seleção de entregadores, ofertas de planos de saúde e precificação de serviços essenciais. A partir disso, o limite jurídico exige explicabilidade suficiente, contestabilidade, governança, proporcionalidade, vedação à discriminação e auditoria compatível com o impacto produzido.

A exploração econômica de informações pessoais também será ilícita quando a anonimização funcionar como aparência de proteção. No art. 12, a LGPD exclui dados anonimizados de seu campo de aplicação quando o titular não puder ser identificado por meios técnicos razoáveis, mantendo cautela quando o processo puder ser revertido ou quando informações forem utilizadas para formação de perfis comportamentais (Brasil, 2018).

Em mercados de alta capacidade computacional, bases supostamente anônimas podem ser recombinações com localização, horários, preferências e padrões de mobilidade, permitindo reidentificação ou segmentação de grupos vulneráveis. A promessa de anonimização plena perde fundamento diante da expansão de bases auxiliares e técnicas de recombinação (Ohm, 2010).

Em uma última abordagem, a Resolução CD/ANPD nº 4 de 2023 organizou parâmetros de dosimetria e aplicação de sanções administrativas, permitindo advertência, multa, publicização da infração, bloqueio, eliminação de dados e outras medidas previstas na LGPD, conforme gravidade, boa-fé, vantagem auferida, reincidência, cooperação, políticas de governança e adoção de mecanismos de prevenção (ANPD, 2023).

A Resolução CD/ANPD nº 15 de 2024, relativa à comunicação de incidentes de segurança, corroborou com deveres de mitigação, transparência e comunicação à autoridade e aos titulares quando houver risco ou dano relevante (ANPD, 2024).

CONSIDERAÇÕES FINAIS

Após o desenvolvimento deste artigo, a exploração econômica de dados pessoais já não pode ser tratada como efeito colateral da vida digital. Ora, quando cada clique, busca, localização, compra, rota e interação passa a alimentar perfis, previsões e decisões

automatizadas, a pergunta que se impõe é a seguinte: até que ponto o mercado pode transformar a experiência humana em mercadoria?

O trabalho defendeu do começo ao fim que a promessa de conveniência não pode servir como disfarce para práticas que classificam pessoas, exploram vulnerabilidades e interferem no acesso a crédito, trabalho, consumo, educação, saúde e participação social.

No Brasil, a Constituição, o Marco Civil da Internet, a LGPD e a atuação do Supremo Tribunal Federal apontam para um mesmo limite, o fato que os dados pessoais não são matéria-prima livre para extração econômica ilimitada. A vida conectada exige proteção jurídica capaz de alcançar a coleta, o cruzamento, a inferência, a monetização e o uso discriminatório de informações, especialmente quando tais práticas atingem grupos inteiros e aumentam desigualdades já existentes.

Diante disso, a questão final é inevitável: que democracia se sustenta quando escolhas individuais são moldadas por sistemas invisíveis? Que liberdade existe quando o consentimento se resume a aceitar termos que ninguém consegue ler, negociar ou compreender? A resposta jurídica precisa ser firme. A inovação digital só encontra legitimidade quando respeita a pessoa, preserva direitos sociais e impede que a vigilância seja convertida em método permanente de lucro.

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Resolução CD/ANPD nº 15, de 24 de abril de 2024**. Aprova o Regulamento de Comunicação de Incidente de Segurança. Brasília, DF: ANPD, 2024. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024>. Acesso em: 02 maio 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023**. Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Brasília, DF: ANPD, 2023. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077>. Acesso em: 03 maio 2026.

BADR, EID. **Direito à Autodeterminação Comportamental Digital**: uma proposta de proteção fundamental da liberdade econômica contra a manipulação algorítmica por perfis preditivos. Editora Database, 2026.

BAROCAS, Solon; SELBST, Andrew D. Big Data's disparate impact. **California Law Review**, Berkeley, v. 104, n. 3, p. 671-732, 2016.

BELL, Daniel. **The coming of post-industrial society**. New York: Basic Books, 1973.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 05 maio 2026.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 08 maio 2026.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 06 maio 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709compilado.htm. Acesso em: 04 maio 2026.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/18078compilado.htm. Acesso em: 09 maio 2026.

BRASIL. Supremo Tribunal Federal. **Medida cautelar na Ação Direta de Inconstitucionalidade nº 6.387/DF**. Relatora: Ministra Rosa Weber. Brasília, DF: STF, 2020. Disponível em: <https://www.stf.jus.br/arquivo/cms/noticianticiastf/anexo/adi6387mc.pdf>. Acesso em: 01 maio 2026.

BRIN, Sergey; PAGE, Lawrence. The anatomy of a large-scale hypertextual Web search engine. **Computer Networks and ISDN Systems**, Amsterdam, v. 30, n. 1-7, p. 107-117, 1998.

BUENO, Maria Eduarda Briz; SAMPAIO NETO, Walter Francisco. Direito digital: A ética e a privacidade no contexto digital. **Revista Unifev: Ciência & Tecnologia**, v. 4, n. 2, p. 34-49, 2024.

CARIBÉ, João Carlos Rebello. Uma perspectiva histórica e sistêmica do capitalismo de vigilância. **Revista Inteligência Empresarial**, v. 41, p. 5-13, 2019.

CASTELLS, Manuel. **The rise of the network society**. 2. ed. Chichester: Wiley-Blackwell, 2010.

CITRON, Danielle Keats; PASQUALE, Frank. The scored society: due process for automated predictions. **Washington Law Review**, Seattle, v. 89, n. 1, p. 1-33, 2014.

COHEN, Julie E. **Between truth and power: the legal constructions of informational capitalism**. New York: Oxford University Press, 2019.

COULDRY, Nick; MEJIAS, Ulises A. Data colonialism: rethinking big data's relation to the contemporary subject. **Television & New Media**, Thousand Oaks, v. 20, n. 4, p. 336-349, 2019.

CUNHA, Carlos Renato; PECIS, Luiza França. Responsabilidade tributária das plataformas de marketplace no sistema tributário nacional. **Revista do Instituto de Direito Constitucional e Cidadania**, v. 8, n. 2, p. e090-e090, 2023.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

EUBANKS, Virginia. **Automating inequality**: how high-tech tools profile, police, and punish the poor. New York: St. Martin's Press, 2018.

FALEIROS JÚNIOR, José Luiz de Moura; BASAN, Arthur Pinheiro. Algoritmos, perfilização e contratos eletrônicos de consumo. **Revista Direitos Culturais**, v. 17, n. 43, p. 41-70, 2022.

GOOGLE INC. **Form 10-K for the fiscal year ended December 31, 2004**. Washington, DC: U.S. Securities and Exchange Commission, 2005. Disponível em: <https://www.sec.gov/Archives/edgar/data/1288776/000119312505065298/d10k.htm>. Acesso em: 11 maio 2026.

GOOGLE INC. **Form S-1 Registration Statement**. Washington, DC: U.S. Securities and Exchange Commission, 2004. Disponível em: <https://www.sec.gov/Archives/edgar/data/1288776/000119312504073639/ds1.htm>. Acesso em: 12 maio 2026.

GOOGLE INC. **Generating user information for use in targeted advertising**. Inventor: Krishna Bharat. US Patent Application Publication US20050131762A1. Washington, DC: United States Patent and Trademark Office, 2005. Disponível em: <https://patents.google.com/patent/US20050131762A1/en>. Acesso em: 10 maio 2026.

GOOGLE. **The 2008 Founders' Letter**. Mountain View: Google, 2009. Disponível em: <https://abc.xyz/investor/founders-letters/2008/default.aspx>. Acesso em: 09 maio 2026.

HONNETH, Axel. **O direito da liberdade**. Martins Editora, 2017.

KOERNER, Andrei. Capitalismo e vigilância digital na sociedade democrática. **Revista Brasileira de Ciências Sociais**, v. 46, n. 105, p. 1-6, 2021.

LYON, David. **The culture of surveillance**: watching as a way of life. Cambridge: Polity Press, 2018.

MACHADO, Débora. A modulação de comportamento nas plataformas de mídias sociais. **J. Souza., R. Avelino., & S. Amadeu da Silveira, A sociedade de controle: Manipulação e modulação nas redes digitais**, p. 47-69, 2018.

MCDONALD, Aleecia M.; CRANOR, Lorrie Faith. The cost of reading privacy policies. **I/S: A Journal of Law and Policy for the Information Society**, Columbus, v. 4, n. 3, p. 543-568, 2008.

MEIRELES, Adriana Veloso. Algoritmos e autonomia: relações de poder e resistência no capitalismo de vigilância. **Opinião Pública**, v. 27, n. 1, p. 28-50, 2021.

NISSENBAUM, Helen. **Privacy in context**: technology, policy, and the integrity of social life. Stanford: Stanford University Press, 2010.

OHM, Paul. Broken promises of privacy: responding to the surprising failure of anonymization. **UCLA Law Review**, Los Angeles, v. 57, p. 1701-1777, 2010.

PASQUALE, Frank. **The black box society**: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

SAMPAIO, José Adércio Leite; COSTA, Ana Carolina Marques Tavares. Capitalismo de vigilância e modulação do comportamento humano: o ambiente digital como espaço favorável à manipulação do eleitor?. **Opinião Jurídica**, v. 24, n. 52, 2025.

SANTOS, José Carlos Francisco dos. Organização da informação e do conhecimento jurídico com vieses digitais e eletrônicos. **Revista de Direito, Governança e Novas Tecnologias**, v. 7, n. 2, p. 35-51, 2021

SANTOS, José Carlos Francisco. Da sociedade da informação e do conhecimento à era dos dados: perspectivas interdisciplinares contemporâneas das áreas jurídicas e da ciência da informação. **Revista do Instituto de Direito Constitucional e Cidadania – IDCC**, Londrina, v. 7, n. 2, e062, jul./dez., 2022.

SRNICEK, Nick. **Platform capitalism**. Cambridge: Polity Press, 2017.

TEFFÉ, Chiara Antonia Spadaccini de. **Dados pessoais sensíveis**: uma análise funcional da categoria e das hipóteses de tratamento. 2022. 310 f. Tese (Doutorado em Direito) - Faculdade de Direito, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2022.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Regulamento Geral sobre a Proteção de Dados. Jornal Oficial da União Europeia, Luxemburgo, L 119, 4 maio 2016. Disponível em: <https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=pt>. Acesso em: 12 maio 2026.

VAN DIJCK, José. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. **Surveillance & Society**, Kingston, v. 12, n. 2, p. 197-208, 2014.

VARIAN, Hal R. Big data: new tricks for econometrics. **Journal of Economic Perspectives**, Nashville, v. 28, n. 2, p. 3-28, 2014.

VILJOEN, Salomé. A relational theory of data governance. **Yale Law Journal**, New Haven, v. 131, n. 2, p. 573-654, 2021.

YEUNG, Karen. “Hypernudge”: big data as a mode of regulation by design. **Information, Communication & Society**, London, v. 20, n. 1, p. 118-136, 2017.

ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. **Journal of Information Technology**, London, v. 30, n. 1, p. 75-89, 2015.

ZUBOFF, Shoshana. **The age of surveillance capitalism**: the fight for a human future at the new frontier of power. New York: PublicAffairs, 2019.