



O FIM DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS NA DATAFICAÇÃO DE TUDO¹

THE END OF THE RIGHT TO PERSONAL DATA PROTECTION IN THE DATAFICATION OF EVERYTHING

João Pedro Seefeldt Pessoa²
Têmis Limberger³

RESUMO

Este artigo analisa criticamente a evolução e eficácia do direito à proteção de dados pessoais no contexto do capitalismo de vigilância e da dataficação generalizada. Adotando uma abordagem fenomenológico-hermenêutica e método monográfico, o estudo examina a trajetória histórica e normativa da proteção de dados, desde as primeiras discussões sobre privacidade até os marcos regulatórios contemporâneos. A pesquisa revela que, apesar dos avanços significativos representados por legislações como o RGPD e a LGPD, os modelos regulatórios atuais mostram-se insuficientes para salvaguardar efetivamente os direitos e liberdades individuais frente aos desafios da economia digital. A análise expõe contradições fundamentais entre os princípios de proteção de dados e a lógica do capitalismo de vigilância, evidenciando como conceitos como consentimento e finalidade tornam-se problemáticos em um contexto de assimetria informacional e exploração contínua de dados. Conclui-se que uma proteção efetiva de dados pessoais no futuro digital exigirá uma abordagem holística e ética, que transcenda as limitações das regulações atuais e promova uma redefinição fundamental da relação entre tecnologia, privacidade e autonomia individual.

Palavras-chave: Capitalismo de vigilância; Dataficação; Proteção de dados pessoais.

ABSTRACT

This article critically analyzes the evolution and effectiveness of the right to personal data protection in the context of surveillance capitalism and widespread datafication. Adopting a phenomenological-hermeneutic approach and monographic method, the study examines the historical and normative trajectory of data protection, from the earliest privacy discussions to contemporary regulatory frameworks. The research reveals that, despite significant advances represented by legislation such as the GDPR and LGPD, current regulatory models prove insufficient to effectively safeguard individual rights and freedoms in the face of digital economy challenges. The analysis exposes fundamental contradictions between data protection principles and the logic of surveillance capitalism, highlighting how concepts such as consent and purpose become problematic in a context of informational asymmetry and continuous data exploitation. It concludes that effective personal data protection in the digital future will require a holistic and ethical approach that transcends the limitations of current regulations and promotes a fundamental redefinition of the relationship between technology, privacy, and individual autonomy.

Keywords: Datafication; Personal data protection; Surveillance capitalism.

¹ O presente artigo científico foi subvencionado pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001

² Doutorando em Direito pela Universidade do Vale do Rio dos Sinos - UNISINOS (CAPES/PROEX). Mestre em Direito pela Universidade Federal de Santa Maria - UFSM. E-mail: jpseefeldt@gmail.com. Currículo Lattes: <http://lattes.cnpq.br/3238221565472756>. Orcid ID: <https://orcid.org/0000-0003-1974-0247>.

³ Pós-Doutora em Direito pela Universidade de Sevilha. Doutora em Direito pela Universidade Pompeu Fabra. Mestra em Direito pela Universidade Federal do Rio Grande do Sul. E-mail: temisl@unisinis.br. Currículo Lattes: <http://lattes.cnpq.br/4818791232370274>. Orcid ID: <https://orcid.org/0000-0003-0670-583X>.



INTRODUÇÃO

A proteção de dados pessoais emergiu como um dos temas mais prementes e complexos do século XXI, refletindo as profundas transformações sociais, econômicas e tecnológicas trazidas pela era digital. Desde as primeiras discussões sobre privacidade no final do século XIX até os atuais debates sobre o capitalismo de vigilância, a evolução deste campo reflete não apenas mudanças tecnológicas, mas também transformações fundamentais na forma como concebemos identidade, autonomia e direitos individuais em um mundo cada vez mais datafocado.

Diante deste cenário, emerge uma questão fundamental: em que medida os modelos regulatórios atuais de proteção de dados pessoais são capazes de salvaguardar efetivamente os direitos e liberdades individuais no contexto do capitalismo de vigilância e da dataficação generalizada? Esta problemática se desdobra em questionamentos sobre a adequação dos princípios e direitos estabelecidos, a eficácia dos mecanismos de *enforcement*, e a própria concepção de privacidade e autonomia individual subjacente a estes modelos regulatórios.

O objetivo geral deste artigo é analisar criticamente a evolução, o estado atual e as perspectivas futuras do direito à proteção de dados pessoais, avaliando sua eficácia e limitações no contexto da economia digital contemporânea. Como objetivos específicos, busca-se: (1) examinar a evolução histórica e normativa do direito à proteção de dados pessoais, desde suas origens até as legislações contemporâneas; e (2) avaliar criticamente os princípios, direitos e modelos regulatórios atuais de proteção de dados pessoais frente aos desafios impostos pelo capitalismo de vigilância e a dataficação generalizada.

Este estudo adota uma metodologia de abordagem fenomenológico-hermenêutica, buscando compreender o fenômeno da proteção de dados pessoais em sua complexidade e contexto histórico-social. O método de procedimento empregado é o monográfico, focalizando a análise aprofundada do tema específico da proteção de dados. As técnicas de pesquisa baseiam-se principalmente na documentação indireta, através da revisão bibliográfica de fontes doutrinárias, legislativas e jurisprudenciais relevantes para o tema.

A primeira seção traça a evolução histórica e normativa do direito à proteção de dados pessoais, abordando desde as primeiras discussões sobre privacidade até o desenvolvimento das legislações contemporâneas. A segunda seção oferece uma análise crítica dos modelos regulatórios atuais, examinando suas limitações e contradições no contexto do capitalismo de vigilância, e discutindo os desafios futuros e a necessidade de uma abordagem holística e ética para a proteção de dados no século XXI.



1 DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS

O conceito de privacidade tem evoluído significativamente desde o final do século XIX, refletindo as mudanças sociais e tecnológicas de cada época. O marco crucial nessa evolução foi a publicação do artigo *The Right to Privacy* por Samuel Warren e Louis Brandeis em 1890. Motivados por experiências pessoais de exposição pública excessiva, os autores propuseram uma abordagem inovadora, argumentando que a proteção da privacidade deveria basear-se na noção de personalidade inviolável, transcendendo o mero direito à propriedade. Esta perspectiva ampliou consideravelmente o escopo da proteção da privacidade, considerando aspectos intrínsecos à identidade e dignidade da pessoa⁴.

Os autores alertaram que novas tecnologias, como máquinas fotográficas instantâneas, estavam invadindo o espaço privado, exigindo um novo nível de proteção legal. Na década de 1960, o debate sobre privacidade nos Estados Unidos se intensificou com o surgimento da tecnologia informática, deslocando-se para a proteção dos dados pessoais e as formas de tratamento das informações. Projetos como o *National Data Center* levantaram preocupações sobre os riscos do processamento automatizado de dados para a privacidade e a liberdade individual, o que culminou na aprovação de legislações importantes, como o *Fair Credit Reporting Act* de 1970 e o *Privacy Act* de 1974, que estabeleceram princípios fundamentais para o tratamento de dados pessoais.

O relatório *Records, Computers and the Rights of Citizens* de 1973 propôs a adoção de *Fair Information Practice Principles*, sugerindo a implementação de uma normativa federal sobre proteção de dados pessoais⁵. Embora os Estados Unidos tenham optado por uma abordagem de autorregulamentação setorial, esses desenvolvimentos influenciaram significativamente o debate global sobre privacidade e proteção de dados, estabelecendo as bases para futuras regulamentações em todo o mundo.

A evolução normativa europeia em matéria de proteção de dados pessoais teve seu marco inicial em 1970, com a promulgação da Lei de Proteção de Dados de Hesse na

⁴ BRANDEIS, Louis. WARREN, Samuel. The right to privacy. In: *Harvard Law Review*, v. IV, n. 5, dez., 1890. Disponível em: <http://faculty.uml.edu/sgallagher/brandeisprivacy.htm>. Acesso em: 1 ago. 2024.

⁵ ESTADOS UNIDOS DA AMÉRICA. Departamento de Saúde, Educação e Bem-Estar dos Estados Unidos. *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*. Washington D.C.: U.S. Department of Health, Education & Welfare, 1973. Disponível em: <https://www.justice.gov/opcl/docs/rec-com-rights.pdf>. Acesso em: 2 ago. 2024.



Alemanha⁶. Esta legislação pioneira estabeleceu princípios fundamentais como a necessidade de autorização para o tratamento de dados pessoais, medidas de segurança técnica, dever de confidencialidade e a criação de uma autoridade independente de fiscalização. A lei de Hesse representou uma mudança significativa de perspectiva, inaugurando um modelo normativo autônomo para a proteção de dados pessoais em resposta aos desafios impostos pelas novas tecnologias de processamento de informações.

Nesse contexto, um marco crucial na evolução normativa europeia ocorreu em 1983, quando o Tribunal Constitucional Federal Alemão proferiu uma decisão histórica sobre a Lei do Recenseamento de População⁷. Neste julgamento, o Tribunal reconheceu a existência de um direito fundamental à autodeterminação informativa, derivado do direito geral de personalidade e da dignidade da pessoa humana. Esta decisão estabeleceu que os indivíduos têm o direito de decidir por si mesmos quando e dentro de quais limites os fatos pessoais de sua vida podem ser revelados, destacando a importância do controle individual sobre os dados pessoais em uma era de processamento automatizado de informações⁸.

A decisão do Tribunal Constitucional Federal Alemão teve um impacto profundo na concepção de proteção de dados na Europa. O conceito de autodeterminação informativa passou a ser entendido como um direito fundamental, essencial para o livre desenvolvimento da personalidade em condições modernas de processamento de dados. Esta interpretação influenciou significativamente o desenvolvimento de legislações subsequentes, tanto na Alemanha quanto em outros países europeus, estabelecendo as bases para uma abordagem mais abrangente e centrada no indivíduo em relação à proteção de dados pessoais⁹.

A evolução normativa europeia culminou na adoção de instrumentos supranacionais de proteção de dados. A Convenção 108 do Conselho da Europa, assinada em 1981, foi o primeiro instrumento internacional juridicamente vinculativo no domínio da proteção de

⁶ HESSE. *Hessisches Datenschutzgesetz*. Hesse: Gesetz-und Verordnungsblatt für das Land Hessen Teil I (GVBl, II 300-10), 1970. Disponível em:

<https://starweb.hessen.de/cache/GVBL/1970/00041.pdf>. Acesso em: 2 ago. 2024.

⁷ MARTINS, Leonardo. *Tribunal Constitucional Federal Alemão: decisões anotadas sobre direitos fundamentais*. Volume 1: Dignidade humana, livre desenvolvimento da personalidade, direito fundamental à vida e à integridade física, igualdade. São Paulo: Konrad-Adenauer Stiftung - KAS, 2016, p. 58. Disponível em: https://www.kas.de/c/document_library/get_file?uuid=4f4eb811-9fa5-baeb-c4ce-996458b70230&groupId=268877. Acesso em: 5 ago. 2024.

⁸ LIMBERGER, Têmis. *Cibertransparência informação pública em rede: a virtualidade e suas repercussões na realidade*. Porto Alegre: Livraria do Advogado, 2017.

⁹ PÉREZ LUÑO, Antonio Enrique. *Los derechos en la sociedad tecnológica*. Madri: Editorial Universitas, S.A., 2012.



dados¹⁰. A evolução internacional da proteção de dados pessoais ganhou impulso significativo com a publicação das Diretrizes sobre Proteção da Privacidade e Fluxo de Dados Transfronteiriços pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE) em 1980¹¹. Estas diretrizes estabeleceram princípios fundamentais como limitação da coleta, qualidade dos dados, especificação da finalidade, limitação de uso, segurança, transparência, participação individual e responsabilização.

No contexto europeu, a Diretiva 95/46/CE, adotada em 1995, representou um marco importante na harmonização das leis de proteção de dados entre os Estados-membros da União Europeia. Esta diretiva estabeleceu padrões comuns para o tratamento de dados pessoais, introduzindo conceitos como consentimento informado, direitos dos titulares dos dados e a necessidade de autoridades de supervisão independentes. No entanto, com o avanço das tecnologias digitais e a crescente complexidade dos fluxos de dados transfronteiriços, tornou-se evidente a necessidade de uma regulamentação mais robusta e uniforme¹².

Em resposta a esses desafios, o Regulamento Geral de Proteção de Dados (RGPD) foi aprovado pelo Parlamento Europeu em 2016, entrando em vigor em maio de 2018. O RGPD representa uma evolução significativa no cenário internacional de proteção de dados, estabelecendo um conjunto abrangente e uniforme de regras diretamente aplicáveis em todos os Estados-membros da UE. O regulamento fortalece significativamente os direitos dos titulares dos dados, introduzindo conceitos como o direito à portabilidade dos dados e o direito ao esquecimento, além de impor obrigações mais rigorosas aos controladores e processadores de dados¹³.

¹⁰ CONSELHO DA EUROPA. **Convenção nº 108, do Conselho da Europa, para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais**. Estrasburgo: Conselho da Europa, 1981. Disponível em: <https://rm.coe.int/1680078b37>. Acesso em: 5 ago. 2024.

¹¹ ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**. Paris: OCDE, 1980. Disponível em: <https://www.oecd.org/sti/ieconomy/oecdguidelinesonthe protectionof privacyandtransborderflows of personaldata.htm>. Acesso em: 10 ago. 2024.

¹² UNIÃO EUROPEIA. Parlamento Europeu. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados**. Luxemburgo: Jornal Oficial da União Europeia, 1995. Disponível em: <http://data.europa.eu/eli/dir/1995/46/oj>. Acesso em: 5 ago. 2024.

¹³ UNIÃO EUROPEIA. Parlamento Europeu. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Bruxelas: Jornal Oficial da União Europeia, 2016. Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 5 ago. 2024.



Uma das inovações mais significativas do RGPD é sua aplicação extraterritorial, que estende sua jurisdição para além das fronteiras da UE. O regulamento se aplica a qualquer organização que processe dados de residentes da UE, independentemente de onde a organização esteja localizada. Isso teve um impacto global, levando empresas e organizações em todo o mundo a reavaliar e adaptar suas práticas de tratamento de dados para cumprir com os padrões do RGPD. Além disso, o regulamento introduziu sanções substancialmente mais elevadas para violações, reforçando ainda mais seu impacto e influência internacionais.

Por sua vez, o direito à proteção de dados pessoais no Brasil teve seu marco inicial com a Constituição Federal de 1988, que estabeleceu garantias fundamentais relacionadas à inviolabilidade da intimidade, da vida privada e do sigilo das comunicações¹⁴. Ao longo dos anos seguintes, diversas leis abordaram aspectos específicos da proteção de dados, como o Código de Defesa do Consumidor (1990), a Lei do Habeas Data (1997) e o Marco Civil da Internet (2014). No entanto, a ausência de uma legislação abrangente e específica sobre proteção de dados pessoais tornava-se cada vez mais evidente, especialmente diante dos avanços tecnológicos e da crescente importância dos dados na economia digital.

O desenvolvimento da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil começou efetivamente em 2012, com a tramitação do Projeto de Lei nº 4.060/2012 na Câmara dos Deputados¹⁵. Este processo legislativo foi influenciado por discussões internacionais, particularmente o desenvolvimento do Regulamento Geral de Proteção de Dados (RGPD) na União Europeia. Em 2018, após um longo período de debates e consultas públicas, a Lei nº 13.709 foi finalmente sancionada, estabelecendo a LGPD como o marco regulatório brasileiro para a proteção de dados pessoais¹⁶.

A LGPD, fortemente inspirada no RGPD europeu, introduziu um conjunto abrangente de princípios, direitos e obrigações para o tratamento de dados pessoais no Brasil. A lei estabelece dez princípios fundamentais, incluindo finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização. Além disso, a LGPD fortalece significativamente os direitos dos titulares

¹⁴ BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 7 ago. 2024.

¹⁵ BRASIL. Câmara dos Deputados. **Projeto de Lei nº 4.060, de 13 de junho de 2012**. Dispõe sobre o tratamento de dados pessoais e dá outras providências. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>. Acesso em: 7 ago. 2024.

¹⁶ BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Diário Oficial da União, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 7 ago. 2024.



dos dados, garantindo, entre outros, o direito de acesso, retificação, exclusão e portabilidade dos dados pessoais.

A implementação da LGPD representou um desafio significativo para organizações públicas e privadas no Brasil, exigindo uma mudança cultural e operacional na forma como os dados pessoais são tratados. A lei estabeleceu um período de adaptação, com sua entrada em vigor ocorrendo em setembro de 2020, exceto para as sanções administrativas, que passaram a vigorar em agosto de 2021. Em 2022, a importância da proteção de dados pessoais no ordenamento jurídico brasileiro foi ainda mais reforçada com a aprovação da Emenda Constitucional nº 115, que incluiu o direito à proteção de dados pessoais no rol de direitos fundamentais da Constituição Federal¹⁷. Esta evolução normativa posicionou o Brasil entre os países com legislações mais avançadas em matéria de proteção de dados pessoais, alinhando-se às melhores práticas internacionais e estabelecendo um novo paradigma para o tratamento de dados no país.

Assim, o direito à proteção de dados pessoais reflete uma mudança paradigmática significativa, afastando-se do enfoque tradicional do sigilo e avançando em direção à circulação e controle da informação pelo titular. Esta nova perspectiva reconhece o direito à proteção de dados pessoais como um direito fundamental autônomo, essencial para assegurar a dignidade humana e o livre desenvolvimento da personalidade no contexto das tecnologias de informação e comunicação¹⁸. A abordagem contemporânea busca equilibrar a necessidade de inovação e desenvolvimento econômico com a proteção efetiva dos direitos dos titulares dos dados¹⁹.

Os modelos regulatórios atuais estabelecem um conjunto de princípios que orientam o tratamento de dados pessoais, dentre eles os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização. O princípio da finalidade, por exemplo, exige que os dados sejam coletados para propósitos específicos, explícitos e legítimos, enquanto o princípio da necessidade limita a coleta ao mínimo necessário para atingir os objetivos pretendidos.

¹⁷ 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: Diário Oficial da União, 2022. Disponível em:

https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 7 ago. 2024.

¹⁸ DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: RT, 2019.

¹⁹ RODOTÀ, Stefano. **A vida na sociedade de vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008.



As bases legais para o tratamento de dados pessoais constituem outro elemento crucial da doutrina atual da privacidade. Embora o consentimento do titular seja frequentemente considerado a base legal mais reconhecida, os modelos regulatórios contemporâneos reconhecem outras justificativas legítimas para o processamento de dados. Estas podem incluir o cumprimento de obrigações legais, a execução de contratos, a proteção de interesses vitais do titular ou de terceiros, o atendimento a interesses legítimos do controlador ou de terceiros, e a realização de tarefas de interesse público.

A doutrina atual também enfatiza a importância dos direitos dos titulares dos dados, que incluem o acesso às informações pessoais, a retificação de dados incorretos, a exclusão de dados em determinadas circunstâncias (também conhecido como direito ao esquecimento), a portabilidade dos dados e o direito de oposição ao processamento, dentre outros. Além disso, há um reconhecimento crescente da necessidade de proteger os indivíduos contra decisões automatizadas que possam ter impactos significativos em suas vidas, garantindo o direito à revisão humana de tais decisões.

No entanto, à medida que avançamos para uma era de dataficação intensiva, onde praticamente todos os aspectos da vida humana são convertidos em dados, surgem novos desafios e questionamentos. Nesse contexto, a próxima seção explorará como a proteção de dados pessoais se posiciona diante desses desafios contemporâneos, avaliando sua eficácia e as possíveis adaptações necessárias para garantir a tutela dos direitos fundamentais em um cenário de dataficação generalizada.

2 O DIREITO À PROTEÇÃO DE DADOS PESSOAIS NA DATAFICAÇÃO DE TUDO

O capitalismo de vigilância emerge como uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais de extração, previsão e vendas. Este modelo, inicialmente desenvolvido por empresas como a Google, baseia-se na descoberta do superávit comportamental - a ideia de que os dados gerados pelos usuários, mesmo aqueles aparentemente sem uso imediato, podem ser extremamente valiosos quando analisados em larga escala. Esta lógica transformou as interações digitais



dos usuários em novas commodities, processadas e analisadas para gerar previsões comportamentais que são vendidas em um novo tipo de mercado global²⁰.

A dataficação de tudo, fenômeno central neste novo paradigma econômico, refere-se à conversão de aspectos cada vez mais amplos da vida cotidiana em dados quantificáveis²¹. Este processo é impulsionado pela proliferação de dispositivos conectados e plataformas digitais que coletam e processam dados continuamente, transformando cada interação humana em uma oportunidade de extração de valor. A ubiquidade da coleta de dados cria um ambiente onde a vigilância é constante e a atenção dos usuários é continuamente capturada, eliminando distinções tradicionais entre tempo de trabalho e lazer, público e privado²².

O capitalismo de vigilância opera através de técnicas sofisticadas de manipulação comportamental, como a personalização extrema da comunicação digital, arquiteturas de escolha e engajamento baseado em emoções fortes, incluindo o ódio. Estas estratégias visam não apenas prever, mas também moldar ativamente o comportamento dos usuários, criando um ciclo de *feedback* onde as ações dos indivíduos são continuamente monitoradas, analisadas e influenciadas. A eficácia dessas técnicas reside em sua capacidade de operar de maneira invisível e contínua, aproveitando-se da assimetria de poder e conhecimento entre as plataformas e os usuários²³.

O conceito de homem-caramujo digital ilustra como os indivíduos carregam consigo, constantemente, os instrumentos de sua própria vigilância, numa forma de autoexploração²⁴. Esta vigilância internalizada leva a uma forma de autocontrole, onde os indivíduos modulam seu próprio comportamento em resposta à consciência constante de estarem sendo observados e analisados. A rendição à inevitabilidade da vigilância digital resulta em uma forma de servidão voluntária informacional, onde a participação na vida digital contemporânea é vista como um custo inevitável²⁵.

²⁰ ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder**. Rio de Janeiro: Intrínseca, 2019.

²¹ WOLFGANG, Hoffmann-Riem. **Teoria geral do direito digital: transformação digital e desafios para o Direito**. 2. ed. São Paulo: Grupo Gen | Forense, 2021.

²² MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big data: a revolution that will transform how we live, work, and think**. Boston: Houghton Mifflin Harcourt, 2013.

²³ VAN DIJCK, José; POELL, Thomas; DE WAAL, Martijn. **The platform society: public values in a connective world**. Oxônia: Oxford University Press, 2018.

²⁴ BAUMAN, Zygmunt. **Vigilância líquida: diálogos com David Lyon**. Rio de Janeiro: Jorge Zahar, 2013.

²⁵ PESSOA, João Pedro Seefeldt. **O Efeito Orwell na sociedade em rede: cibersegurança, regime global de vigilância social e direito à privacidade no século XXI**. Porto Alegre: Fi, 2020. Disponível em: <https://www.editorafi.org/073orwell>. Acesso em: 31 jul. 2024



As *big techs*, como *Google*, *Facebook*, *Amazon* e outras, emergiram como os principais atores deste novo cenário econômico, exercendo um poder sem precedentes que transcende fronteiras nacionais e desafia estruturas regulatórias tradicionais²⁶. A capacidade de operar como sujeitos globais, impondo seus próprios padrões e normas sociais, levanta questões críticas sobre monopólio, concorrência e o futuro da democracia. A concentração de poder econômico e informacional nas mãos dessas corporações não apenas intensifica desigualdades existentes, mas também engendra novas formas de disparidade social, econômica e informacional, cujos impactos se fazem sentir de maneira particularmente relevante em contextos de crise global²⁷.

Os modelos regulatórios de proteção de dados pessoais, embora concebidos com a intenção de salvaguardar os direitos dos indivíduos, acabam, na verdade, expandindo e legitimando o próprio capitalismo de dados²⁸. Estas regulações, propostas no contexto do recrudescimento de um sistema econômico baseado na exploração de informações e do fenômeno da dataficação de tudo, falham em abordar adequadamente as implicações mais amplas dessa nova ordem econômica. Ao estabelecerem parâmetros para o tratamento legal de dados pessoais, estas normas inadvertidamente normalizam e institucionalizam práticas de vigilância e exploração informacional.

Uma crítica fundamental ao direito à proteção de dados pessoais reside na própria definição de “dados pessoais” adotada pelos modelos regulatórios atuais. Esta abordagem limitada ignora o fato de que o capitalismo de dados opera eficientemente com uma gama muito mais ampla de informações. Dados anonimizados, pseudoanonimizados, sintéticos, abertos, ínfimos, agregados, contextuais, comportamentais, sensoriais e públicos, entre outros, são utilizados para alimentar algoritmos e gerar valor, mesmo que não identifiquem diretamente um indivíduo²⁹.

Curiosamente, os atuais marcos regulatórios de proteção de dados pessoais incorporam, em sua essência, a noção de que é necessário garantir o livre fluxo dessas informações. Essa abordagem, que se alinha perfeitamente com as aspirações da economia baseada em dados, entra em conflito direto com a ideia de que os indivíduos devem ter controle real sobre suas próprias informações.

²⁶ MOROZOV, Evgeny. **Big Tech**: a ascensão dos dados e a morte da política. São Paulo: Ubu, 2018.

²⁷ SRNICEK, Nick. **Platform Capitalism**. Cambridge: Polity Press, 2016.

²⁸ ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2019.

²⁹ O DILEMA das redes. Direção de Jeff Orlowski. Roteiro: Davis Coombe; Vickie Curtis; Jeff Orlowski. [S.L]: Netflix Inc., 2020. (89 min.), son., color. Legendado



A crença de que sistemas mais eficientes, incluindo os sistemas sociais, dependem de um maior volume de dados em circulação, é fundamentalmente incompatível com uma proteção genuína da privacidade em um mundo onde tudo está sendo convertido em dados. Esta inconsistência fundamental nas atuais estruturas regulatórias acaba por promover a exploração desenfreada de dados, em vez de oferecer uma proteção efetiva aos direitos individuais³⁰.

O consentimento, pilar central do sistema de proteção de dados, transforma-se em uma falácia diante da assimetria informacional e da complexidade dos processos de tratamento de dados. O indivíduo, confrontado com extensas políticas de privacidade e termos de uso frequentemente incompreensíveis, vê-se forçado a aquiescer com práticas de coleta e processamento de dados como condição para a participação na vida digital³¹. Esta realidade transmuta o consentimento de um ato de autodeterminação em uma mera formalidade burocrática, esvaziando-o de seu propósito original de empoderamento do titular dos dados.

A tendência das regulações atuais de tratarem os dados como uma *commodity* que pode ser livremente comercializada, desde que certas salvaguardas estejam em vigor, ignora o fato de que os dados pessoais estão intrinsecamente ligados à personalidade e à dignidade humana. Esta visão mercantilista dos dados pessoais falha em reconhecer as implicações éticas e sociais profundas da comercialização irrestrita de informações pessoais, que vão muito além das considerações puramente econômicas ou legais. Ao fazê-lo, as regulações atuais correm o risco de legitimar um sistema que reduz a experiência humana a meros ativos informacionais a serem explorados economicamente³².

Os princípios de finalidade, adequação e necessidade, pilares fundamentais da proteção de dados pessoais, mostram-se incompatíveis com a realidade do capitalismo de vigilância e da dataficação generalizada. A lógica do *big data* e da inteligência artificial, que valoriza a descoberta de correlações inesperadas e usos não previstos inicialmente, colide frontalmente com a ideia de limitar o tratamento a propósitos específicos e predeterminados³³.

³⁰ CRARY, Jonathan. **Terra arrasada: além da era digital, rumo a um mundo pós-capitalista**. São Paulo: Ubu, 2023.

³¹ SUJEITO a termos e condições. Direção de Cullen Hoback. Nova Iorque: Variance Films; Hyrax Films, 2013. (80 min.), son., color.

³² ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder**. Rio de Janeiro: Intrínseca, 2019.

³³ MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big data: a revolution that will transform how we live, work, and think**. Boston: Houghton Mifflin Harcourt, 2013.



A noção de adequação torna-se fluida em um cenário onde a análise exploratória de dados é a norma, e o princípio da necessidade é constantemente desafiado pela lógica da acumulação infinita de informações, característica central do capitalismo de dados. Neste contexto, os direitos de confirmação da existência de tratamento e de informação sobre compartilhamento tornam-se praticamente inócuos, dada a ubiquidade e a complexidade das operações de processamento de dados.

Os princípios de livre acesso, qualidade dos dados e transparência, assim como os direitos correlatos de acesso, correção e informação, são sistematicamente minados pela opacidade intrínseca aos processos algorítmicos e pela proteção conferida aos segredos comerciais. A complexidade dos sistemas de inteligência artificial e aprendizado de máquina cria barreiras quase intransponíveis para o efetivo exercício desses direitos pelos titulares³⁴.

Mesmo quando as informações são disponibilizadas, a vastidão e a natureza técnica dos dados tornam praticamente impossível para o cidadão comum compreender efetivamente como suas informações estão sendo utilizadas e quais são as implicações desse uso. A qualidade e a correção dos dados tornam-se conceitos fluidos em um contexto onde a informação é constantemente reprocessada e recontextualizada, muitas vezes sem o conhecimento ou consentimento do titular.

Os princípios de segurança e prevenção, embora cruciais, revelam-se promessas vazias diante da recorrência e da magnitude dos incidentes de vazamento de dados. A incompatibilidade entre as práticas de segurança e a voracidade do capitalismo de dados resulta em um cenário de vulnerabilidade crônica, onde a proteção efetiva dos dados pessoais torna-se uma exceção, não a regra.

Neste panorama, os direitos de anonimização, bloqueio e eliminação dos dados enfrentam desafios significativos, haja vista que a natureza difusa e interconectada dos dados no ecossistema digital torna a eliminação efetiva uma tarefa quase impossível, questionando a própria viabilidade do direito ao esquecimento. Além disso, as técnicas de re-identificação cada vez mais sofisticadas colocam em xeque a eficácia real dos processos de anonimização.

A não discriminação é sistematicamente desafiada pelos vieses algorítmicos e pelo fenômeno do racismo algorítmico, com a opacidade dos sistemas de IA tornando extremamente difícil identificar e corrigir práticas discriminatórias embutidas nos processos automatizados de tomada de decisão. A natureza agregada e inferencial de muitos dados valiosos torna o conceito de portabilidade problemático, questionando como transferir

³⁴ MOROZOV, Evgeny. **Big Tech: a ascensão dos dados e a morte da política**. São Paulo: Ubu, 2018.



insights gerados por algoritmos proprietários ou perfis comportamentais construídos ao longo do tempo.

Os princípios de responsabilização e prestação de contas revelam-se inadequados no contexto da economia digital contemporânea. A assimetria informacional entre os titulares dos dados e as corporações que os coletam, aliada à ubiquidade da coleta de dados no cotidiano digital, torna o conceito praticamente uma ficção jurídica. A responsabilização efetiva das corporações torna-se um desafio diante da complexidade das cadeias de processamento de dados e da natureza transnacional das operações, com as sanções muitas vezes sendo tratadas como meros custos operacionais pelas grandes empresas de tecnologia³⁵.

O avanço acelerado de tecnologias emergentes e inovações disruptivas no campo da informação e comunicação apresenta desafios significativos para os modelos regulatórios de proteção de dados pessoais. A velocidade com que novas tecnologias são desenvolvidas e implementadas frequentemente ultrapassa a capacidade dos legisladores e reguladores de compreenderem plenamente suas implicações e de formularem respostas normativas adequadas.

Esta defasagem temporal entre inovação tecnológica e adaptação regulatória cria lacunas significativas na proteção efetiva dos direitos dos titulares de dados, permitindo a exploração de zonas cinzentas normativas por atores mal-intencionados ou oportunistas. Projetos envolvendo inteligência artificial avançada, internet das coisas, computação quântica e tecnologias de realidade aumentada e virtual, por exemplo, têm o potencial de redefinir completamente as noções tradicionais de privacidade e controle sobre dados pessoais.

A normalização dessas práticas de vigilância em massa no espaço público ameaça direitos fundamentais à privacidade e à liberdade de movimento, bem como cria as condições para um controle social sem precedentes, potencialmente levando a formas sutis, mas profundas, de discriminação e exclusão social baseadas em perfis comportamentais gerados algoritmicamente. Ademais, o desenvolvimento de tecnologias de interface cérebro-computador e a crescente sofisticação de técnicas de dados neurais representam uma fronteira preocupante na intersecção entre tecnologia e privacidade³⁶.

³⁵ SILVEIRA, Sérgio Amadeu da. A hipótese do colonialismo de dados e o neoliberalismo. In: CASSINO, João Francisco; SOUZA, Joyce; SILVEIRA, Sérgio Amadeu da. (Org.). **Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal**. São Paulo: Autonomia literária, 2021, pp. 33-52.

³⁶ HARARI, Yuval Noah. **Homo deus: uma breve história do amanhã**. São Paulo: Schwarcz, 2015.



Os modelos regulatórios atuais de proteção de dados pessoais, ao falharem em abordar efetivamente os desafios impostos pelo capitalismo de vigilância, comprometem a privacidade individual, mas também representam uma ameaça significativa à própria democracia. A concentração massiva de dados nas mãos de grandes corporações tecnológicas, combinada com a capacidade de manipulação comportamental em larga escala, cria um desequilíbrio de poder sem precedentes entre essas entidades e os cidadãos comuns, facilitando a manipulação da opinião pública, a interferência em processos eleitorais e a erosão do discurso público informado, pilares fundamentais de uma sociedade democrática.

Diante desses desafios, torna-se evidente a necessidade de uma visão holística e ética que transcenda as abordagens regulatórias convencionais focadas exclusivamente em dados pessoais identificáveis. É imperativo reconhecer que a proteção da privacidade no contexto digital contemporâneo requer uma compreensão mais ampla dos impactos sociais, psicológicos e éticos das tecnologias de informação e comunicação³⁷.

Isso implica em desenvolver *frameworks* regulatórios que respondam a tecnologias específicas e que estabeleçam princípios éticos fundamentais capazes de guiar o desenvolvimento e a implementação de inovações tecnológicas de maneira alinhada com valores humanos e direitos fundamentais³⁸. Esta abordagem holística deve visar a promoção ativa de um ecossistema digital que respeite a dignidade humana, fomente a autonomia individual e promova o bem-estar coletivo, reconhecendo que a proteção de dados no futuro digital requer uma redefinição fundamental de nossa relação com a tecnologia.

CONCLUSÃO

A proteção de dados pessoais emerge como um desafio crucial no cenário digital, marcado pela ubiquidade da coleta e processamento de informações e pelo surgimento de novas formas de exploração econômica baseadas na vigilância e manipulação comportamental. Este artigo buscou examinar criticamente a evolução e o estado atual do direito à proteção de dados pessoais, questionando em que medida os modelos regulatórios vigentes são capazes de salvaguardar efetivamente os direitos e liberdades individuais no contexto do capitalismo de vigilância e da dataficação generalizada.

³⁷ BERARDI, Franco. **Depois do futuro**. São Paulo: Ubu, 2019.

³⁸ CRARY, Jonathan. **Terra arrasada: além da era digital, rumo a um mundo pós-capitalista**. São Paulo: Ubu, 2023.



A análise histórica e normativa apresentada revelou uma trajetória complexa, desde as primeiras articulações sobre o direito à privacidade até o desenvolvimento de marcos regulatórios abrangentes como o RGPD e a LGPD. Esta evolução reflete não apenas avanços tecnológicos, mas também mudanças fundamentais na compreensão da privacidade e da autonomia individual na era digital. O desenvolvimento de princípios, direitos e mecanismos de proteção específicos para dados pessoais representa um esforço significativo para adaptar o arcabouço jurídico às realidades da sociedade da informação.

Ainda, percebem-se profundas contradições e limitações dos modelos regulatórios atuais frente aos desafios impostos pelo capitalismo de vigilância. Desvelou-se como conceitos fundamentais, como consentimento e finalidade, tornam-se problemáticos em um contexto de assimetria informacional e exploração contínua de dados. Além disso, a seção destacou como as próprias regulações, ao legitimarem certas práticas de coleta e processamento de dados, podem inadvertidamente facilitar a expansão de um sistema econômico baseado na vigilância e na modulação comportamental.

Em resposta à questão central da pesquisa, conclui-se que os modelos regulatórios atuais de proteção de dados pessoais, embora representem um avanço significativo, mostram-se insuficientes para salvaguardar efetivamente os direitos e liberdades individuais no contexto do capitalismo de vigilância. A incompatibilidade fundamental entre a lógica de acumulação e exploração de dados característica da economia digital contemporânea e os princípios de limitação e controle individual sobre informações pessoais revela as limitações intrínsecas da abordagem regulatória vigente.

Diante deste cenário, torna-se evidente a necessidade de uma revisão profunda não apenas dos mecanismos regulatórios específicos, mas da própria concepção de privacidade na era digital. Talvez, a abordagem verdadeiramente eficaz para a proteção de dados pessoais no futuro exigirá uma visão holística e ética, que transcenda as limitações das regulações focadas exclusivamente em dados pessoais identificáveis. Isso implica no desenvolvimento de *frameworks* que abordem os impactos sociais, psicológicos e éticos mais amplos das tecnologias de informação e comunicação, considerando uma redefinição fundamental de nossa relação com a tecnologia e uma reafirmação dos valores humanos como centro do desenvolvimento tecnológico.

REFERÊNCIAS

BAUMAN, Zygmunt. *Vigilância líquida: diálogos com David Lyon*. Rio de Janeiro: Jorge Zahar, 2013.



BERARDI, Franco. **Depois do futuro**. São Paulo: Ubu, 2019.

BRANDEIS, Louis. WARREN, Samuel. The right to privacy. In: **Harvard Law Review**, v. IV, n. 5, dez., 1890. Disponível em: <http://faculty.uml.edu/sgallagher/brandeisprivacy.htm>. Acesso em: 1 ago. 2024.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 4.060, de 13 de junho de 2012**. Dispõe sobre o tratamento de dados pessoais e dá outras providências. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>. Acesso em: 7 ago. 2024.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 7 ago. 2024.

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: Diário Oficial da União, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 7 ago. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Diário Oficial da União, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 7 ago. 2024.

CONSELHO DA EUROPA. **Convenção nº 108, do Conselho da Europa, para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais**. Estrasburgo: Conselho da Europa, 1981. Disponível em: <https://rm.coe.int/1680078b37>. Acesso em: 5 ago. 2024.

CRARY, Jonathan. **Terra arrasada: além da era digital, rumo a um mundo pós-capitalista**. São Paulo: Ubu, 2023.

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

ESTADOS UNIDOS DA AMÉRICA. Departamento de Saúde, Educação e Bem-Estar dos Estados Unidos. **Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems**. Washington D.C.: U.S. Department of Health, Education & Welfare, 1973. Disponível em: <https://www.justice.gov/opcl/docs/rec-com-rights.pdf>. Acesso em: 2 ago. 2024.

HARARI, Yuval Noah. **Homo deus: uma breve história do amanhã**. São Paulo: Schwarcz, 2015.

HESSE. **Hessisches Datenschutzgesetz**. Hesse: Gesetz-und Verordnungsblatt für das Land Hessen Teil I (GVBl, II 300-10), 1970. Disponível em: <https://starweb.hessen.de/cache/GVBL/1970/00041.pdf>. Acesso em: 2 ago. 2024.

LIMBERGER, Têmis. **Cibertransparência informação pública em rede: a virtualidade e suas repercussões na realidade**. Porto Alegre: Livraria do Advogado, 2017.

MARTINS, Leonardo. **Tribunal Constitucional Federal Alemão: decisões anotadas sobre direitos fundamentais**. Volume 1: Dignidade humana, livre desenvolvimento da personalidade, direito fundamental à vida e à integridade física, igualdade. São Paulo: Konrad-Adenauer Stiftung - KAS, 2016, p. 58. Disponível em: https://www.kas.de/c/document_library/get_file?uuid=4f4eb811-9fa5-baeb-c4ce-996458b70230&groupId=268877. Acesso em: 5 ago. 2024.



MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big data: a revolution that will transform how we live, work, and think.** Boston: Houghton Mifflin Harcourt, 2013.

MOROZOV, Evgeny. **Big Tech: a ascensão dos dados e a morte da política.** São Paulo: Ubu, 2018.

O DILEMA das redes. Direção de Jeff Orlowski. Roteiro: Davis Coombe; Vickie Curtis; Jeff Orlowski. [S.L]: Netflix Inc., 2020. (89 min.), son., color. Legendado

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.** Paris: OCDE, 1980. Disponível em: <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsfpersonaldata.htm>. Acesso em: 10 ago. 2024.

PÉREZ LUÑO, Antonio Enrique. **Los derechos en la sociedad tecnológica.** Madri: Editorial Universitas, S.A., 2012.

PESSOA, João Pedro Seefeldt. **O Efeito Orwell na sociedade em rede: cibersegurança, regime global de vigilância social e direito à privacidade no século XXI.** Porto Alegre: Fi, 2020. Disponível em: <https://www.editorafi.org/073orwell>. Acesso em: 31 jul. 2024

RODOTÀ, Stefano. **A vida na sociedade de vigilância: a privacidade hoje.** Rio de Janeiro: Renovar, 2008.

SILVEIRA, Sérgio Amadeu da. A hipótese do colonialismo de dados e o neoliberalismo. In: CASSINO, João Francisco; SOUZA, Joyce; SILVEIRA, Sérgio Amadeu da. (Org.). **Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal.** São Paulo: Autonomia literária, 2021, pp. 33-52.

SRNICEK, Nick. **Platform Capitalism.** Cambridge: Polity Press, 2016,

SUJEITO a termos e condições. Direção de Cullen Hoback. Nova Iorque: Variance Films; Hyrax Films, 2013. (80 min.), son., color.

UNIÃO EUROPEIA. Parlamento Europeu. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.** Luxemburgo: Jornal Oficial da União Europeia, 1995. Disponível em: <http://data.europa.eu/eli/dir/1995/46/oj>. Acesso em: 5 ago. 2024.

UNIÃO EUROPEIA. Parlamento Europeu. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).** Bruxelas: Jornal Oficial da União Europeia, 2016. Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 5 ago. 2024.

VAN DIJCK, José; POELL, Thomas; DE WAAL, Martijn. **The platform society: public values in a connective world.** Oxônia: Oxford University Press, 2018.

WOLFGANG, Hoffmann-Riem. **Teoria geral do direito digital: transformação digital e desafios para o Direito.** 2. ed. São Paulo: Grupo Gen | Forense, 2021.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder.** Rio de Janeiro: Intrínseca, 2019.