

**AUTODETERMINAÇÃO INFORMATIVA NA ERA DA HIPEREXPOSIÇÃO:
ENTRE DIREITOS FUNDAMENTAIS E CAPITALISMO DE DADOS**

**INFORMATIONAL SELF-DETERMINATION IN THE AGE OF OVEREXPOSURE:
BETWEEN FUNDAMENTAL RIGHTS AND DATA CAPITALISM**

Recebido em: 14/05/2025

Reenviado em: 12/06/2025

Aceito em: 19/06/2025

Publicado em: 12/08/2025

Felipe Boeck Fert¹ 

Centro Universitário Facvest

Geovani Broering² 

Centro Universitário Facvest

Viviane Grassi³ 

Centro Universitário Facvest

Resumo: O presente artigo analisa a transição da privacidade para o capitalismo de vigilância na sociedade digital, destacando os desafios da autodeterminação informativa diante do crescimento tecnológico e do uso massivo de dados pessoais. Examina-se o papel central das grandes plataformas digitais na coleta, processamento e monetização de informações, gerando assimetrias de poder e ameaçando a autonomia individual. Discute-se ainda como a dinâmica digital incentiva a exposição compulsiva de dados, limitando a real capacidade de escolha dos indivíduos. A cultura da hiperexposição online, associada a mecanismos de consentimento opacos, reduz a privacidade a um modelo de vigilância voltado à extração de dados, frequentemente sem plena compreensão dos usuários. A pesquisa adota o método dedutivo-analítico, com revisão de literatura e análise de marcos regulatórios. Os resultados indicam que a expansão da vigilância digital exige o fortalecimento da governança e a redefinição de limites jurídicos para proteger a privacidade e a autodeterminação informativa. Conclui-se que o aperfeiçoamento dos instrumentos normativos, aliado à promoção de mecanismos de transparência e controle, é essencial para salvaguardar os direitos fundamentais dos indivíduos na era digital.

Palavras-chave: Autodeterminação Informativa; Privacidade Digital; Proteção de Dados; Vigilância Digital; Regulação da Tecnologia.

Abstract: This article examines the transition from privacy to surveillance capitalism within digital society, highlighting the challenges faced by informational self-determination amid technological advancements and the massive use of personal data. It explores the central role of large digital platforms in collecting, processing, and monetizing information, fostering power asymmetries and threatening individual autonomy. The study also discusses how digital environments encourage individuals to compulsively disclose their data, limiting their actual ability to make autonomous choices. The prevailing culture of online overexposure, combined with opaque consent mechanisms, reduces privacy to a surveillance model designed to extract data often without users' full awareness. Adopting a deductive-analytical method, based on a literature review and an analysis of regulatory frameworks, the study finds that the expansion of digital surveillance demands stronger governance and clearer legal boundaries to protect privacy and informational self-determination. It concludes that enhancing regulatory frameworks, along

¹ Doutor em Direito pelo Programa de Pós-Graduação em Direito da UVA, RJ. Pesquisador e Professor Universitário. Coordenador do EAD da UNIFACVEST, Lages, SC. E-mail: prof.felipe.fert@unifacvest.edu.br

² Doutor em Direito pelo Programa de Pós-Graduação em Direito da UVA, RJ. Professor Pesquisador do Programa de Pós-Graduação Stricto Sensu em Direito e Desenvolvimento Sustentável da UNIFACVEST, Lages, SC. E-mail: reitoria@unifacvest.edu.br

³ Doutora em Direito pelo Programa de Pós-Graduação em Direito da UVA, RJ. Professora Pesquisadora do Programa de Pós-Graduação Stricto Sensu em Direito e Desenvolvimento Sustentável da UNIFACVEST, Lages, SC. E-mail: prof.vivianegrassi@unifacvest.edu.br

with promoting transparency and control mechanisms, is essential to safeguarding fundamental rights in the digital age.

Keywords: Informational Self-determination; Digital Privacy; Data Protection; Digital Surveillance; Technology Regulation.

INTRODUÇÃO

O artigo examina a transição da privacidade para o capitalismo de vigilância na sociedade digital, ressaltando os desafios da autodeterminação informativa diante da crescente extração e monetização de dados pessoais. Destaca-se como a inovação tecnológica e a expansão das grandes plataformas digitais transformaram os dados em ativos econômicos centrais, intensificando práticas de coleta massiva muitas vezes opacas. O estudo aponta a necessidade urgente do debate sobre privacidade, consentimento e controle de informações na era digital.

As plataformas digitais atuam como mediadoras centrais do espaço informacional, desenvolvendo sistemas sofisticados para a coleta e utilização de dados pessoais. Essa dinâmica redefine a privacidade, pois os indivíduos cedem informações voluntariamente, mas sem real controle sobre seu uso. O modelo econômico baseado na monetização de dados intensifica a assimetria de poder entre usuários e corporações, ameaçando direitos fundamentais como a liberdade de expressão, a privacidade e a autonomia informacional.

O estudo analisa o impacto da sociedade digital na autodeterminação informativa, considerando os desafios da estrutura tecnológica contemporânea e a necessidade de um arcabouço normativo que equilibre inovação e proteção da privacidade. No contexto da Quarta Revolução Industrial, destaca-se como a convergência tecnológica e a cultura da hiperexposição reconfiguram percepções de identidade e autonomia, exigindo uma regulação jurídica crítica e adaptada às novas dinâmicas. O artigo tem como objetivo geral analisar como o capitalismo de vigilância compromete a autodeterminação informativa e identificar os desafios regulatórios para assegurar maior controle dos indivíduos sobre seus dados. São definidos três objetivos específicos: i) Investigar os mecanismos pelos quais plataformas digitais coletam e monetizam dados pessoais; ii) Analisar a ilusão do consentimento e a falta de transparência no uso de informações pessoais; e, iii) Avaliar as implicações desse modelo para a proteção da privacidade e para a governança digital.

O problema de pesquisa tem como questionamento: como a estrutura das plataformas digitais impacta a autodeterminação informativa dos usuários e em que medida o consentimento se revela um mecanismo insuficiente diante da lógica de extração de dados? A análise examina

como o *design* e as estratégias operacionais das plataformas digitais promovem a coleta massiva e opaca de informações pessoais, limitando a real autonomia dos indivíduos sobre seus dados.

O presente estudo parte da hipótese de que, apesar da aparência de controle oferecida pelas ferramentas de privacidade, os usuários não exercem autodeterminação plena sobre seus dados pessoais. O ambiente digital é orientado à maximização de lucro e à consolidação de um modelo de vigilância que compromete a liberdade individual e os direitos fundamentais. Do ponto de vista social, esse modelo de extração de dados amplia desigualdades informacionais, favorecendo grandes corporações e limitando a capacidade dos usuários de compreender e controlar sua exposição digital. A crescente dependência de serviços online reforça um cenário de vigilância contínua, no qual dados pessoais são coletados para fins preditivos, publicitários e políticos, frequentemente sem o pleno conhecimento dos titulares.

Diante desse contexto, defende-se que a governança digital deve evoluir para assegurar maior transparência e autonomia informacional, estabelecendo limites claros à exploração econômica dos dados pessoais e fortalecendo a proteção da privacidade. Para analisar essas questões, o artigo organiza-se em cinco eixos principais: a transição da privacidade para o capitalismo de vigilância; a atuação das plataformas digitais na coleta e monetização de dados; os desafios do consentimento e da autodeterminação informativa; os impactos sobre a governança digital e a regulação tecnológica; e, por fim, a necessidade de repensar o equilíbrio entre inovação tecnológica e proteção da privacidade. A metodologia adota o método dedutivo-analítico, com pesquisa bibliográfica e documental, fundamentada na análise de marcos regulatórios e estudos sobre governança digital e proteção de dados.

TUTELA JURÍDICA DE PROTEÇÃO DE DADOS

A transformação digital contemporânea insere-se no conceito de Quarta Revolução Industrial, descrito por Klaus Schwab, e caracteriza-se pela convergência entre tecnologias digitais, físicas e biológicas. Segundo Schwab (2016), a evolução tecnológica ocorre de maneira exponencial, impactando a economia e as relações sociais por meio da conectividade e do processamento massivo de dados. Nesse cenário, as redes sociais, o comércio eletrônico e demais ferramentas digitais passaram a mediar grande parte das interações humanas, expondo dados pessoais a provedores, empresas e governos, bem como a outras entidades que, de forma indevida, acessam informações para fins de monitoramento social e econômico.

A coleta de dados ocorre diariamente, tanto de forma passiva, por meio do uso de dispositivos eletrônicos como *smartphones* e *wearables*, quanto de maneira ativa, a partir das

escolhas e comportamentos dos usuários no ambiente digital. Com a expansão da computação ubíqua e da Internet das Coisas (IoT), essa tendência tende a se intensificar progressivamente.

Frequentemente, sem plena consciência, os usuários da internet disponibilizam voluntariamente seus dados a terceiros. Schwab (2016) aponta esse fenômeno como um elemento central da Quarta Revolução Industrial, no qual as plataformas digitais assumem o papel de intermediadoras globais da informação. Essas empresas operam como *gatekeepers* digitais, filtrando, organizando e monetizando dados pessoais, utilizando-os em análises preditivas e em modelos de negócio baseados no capitalismo de vigilância.

O estudo justifica-se pela necessidade de analisar a atualidade e a adequação do ordenamento jurídico brasileiro em relação à privacidade, proteção de dados e direitos fundamentais no ambiente digital. Dada a natureza transnacional da internet, adota-se uma abordagem jurídica e sociológica para compreender os desafios regulatórios e as lacunas existentes na legislação nacional. A pesquisa fundamenta-se em dispositivos como o Marco Civil da Internet, a Lei Geral de Proteção de Dados (LGPD) e o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, além de outras normativas pertinentes. No ordenamento jurídico brasileiro, a Constituição Federal prevê, nos incisos X e LXXIX do artigo 5º, a proteção da privacidade, da intimidade e dos dados pessoais, assegurando garantias contra violações que comprometam a dignidade da pessoa humana⁴.

O debate acerca da proteção de dados no Brasil teve seus primeiros contornos na década de 1990, com o Recurso Especial nº 22.337/RS⁵, no qual o ministro Ruy Rosado de Aguiar, ao julgar a matéria no Superior Tribunal de Justiça (STJ), enfatizou a necessidade de resguardar a privacidade dos cidadãos diante do crescimento dos bancos de dados informatizados. Na decisão, reconheceu-se o risco da coleta indiscriminada de informações pessoais, que, além de possibilitar a invasão da esfera privada dos indivíduos, poderia ser utilizada para fins discriminatórios e contrários à moral e ao Direito. O ministro também alertou para a crescente digitalização das interações humanas e o consequente aumento da vulnerabilidade dos cidadãos diante do armazenamento e processamento massivo de dados por meio de sistemas eletrônicos.

A preocupação com a proteção de dados já era evidente no ordenamento jurídico, embora a privacidade e a vida íntima fossem reconhecidas como direitos fundamentais pela Constituição Federal de 1988, enquanto a proteção de dados ainda estava em fase incipiente no direito brasileiro. Com o desenvolvimento tecnológico e a crescente valorização dos dados

⁴ LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. (Incluído pela Emenda Constitucional nº 115, de 2022).

⁵ STJ, Recurso Especial n. 22.337/RS, rel. Ministro Ruy Rosado de Aguiar, DJ 20/03/1995, p. 6119.

pessoais, tornou-se necessária uma proteção mais robusta. Em resposta a essa demanda, a Emenda Constitucional nº 115/2022 incluiu a proteção de dados como um direito fundamental no artigo 5º da Constituição Federal, estabelecendo que “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais”.

No âmbito econômico, as corporações e Big Techs intensificaram a exploração de dados pessoais, utilizando o legítimo interesse como base legal para sustentar modelos de negócios que antes dependiam do consentimento explícito. Schwab e Malleret (2020) apontam que a pandemia reforçou o papel dessas plataformas como intermediárias centrais da economia digital, ampliando a concentração de poder informacional e os riscos de monopólio e vigilância corporativa. Nesse contexto, a autodeterminação informativa enfrenta novos desafios, exigindo a reavaliação do equilíbrio entre inovação tecnológica, proteção da privacidade e limites à exploração econômica dos dados.

Apesar do legítimo interesse ter sido inicialmente conferido o “status de uma nova carta coringa” (Bioni, 2019, p. 364), é imperativo que se aplique um teste (LIA)⁶ para confirmar sua legitimidade, assegurando que os interesses e expectativas do titular sejam efetivamente respeitados, de modo a evitar abusos por parte das empresas controladoras. O legítimo interesse, como base para o tratamento de dados, também presente na GDPR⁷, constitui uma justificativa utilizada pelas corporações para processar grandes volumes de dados quando outras bases legais se mostram insuficientes. Segundo Bioni (2019, p. 366-367), o principal argumento para a adoção dessa hipótese na LGPD é sua capacidade de flexibilizar o tratamento em cenários de uso intensivo, evitando a inviabilidade de recorrer constantemente ao consentimento. Assim, essa base legal pode ser considerada um equilíbrio entre os direitos do titular e os interesses do controlador. Ademais, Bioni (2019, p. 387) ressalta que, além de aferir a existência de um interesse legítimo, é fundamental verificar se as expectativas legítimas e os direitos e liberdades fundamentais dos cidadãos estão sendo observados, o que torna a relação entre legítimo interesse e legítima expectativa juridicamente complexa.

Bioni (2019, p. 381) ressalta que a base legal do legítimo interesse é permeada por incertezas e, portanto, deve ser devidamente documentada. Além disso, deve apresentar

⁶ *Legitimate Interests Assessment (LIA)*, previsto no Regulamento Geral de Proteção de Dados (GDPR), é uma ferramenta utilizada para avaliar a legitimidade do interesse no tratamento de dados, ponderando os interesses do titular e da empresa, bem como a legítima expectativa do titular. Além disso, busca definir salvaguardas e mecanismos de proteção adequados. Sua principal finalidade é verificar a viabilidade do uso do interesse legítimo como base legal para o tratamento de dados.

⁷ O Regulamento Geral de Proteção de Dados (GDPR - 2016/679) é a legislação do direito europeu que regula a privacidade e a proteção de dados pessoais, sendo aplicável a todos os indivíduos na União Europeia (UE) e no Espaço Econômico Europeu (EEE).

diretrizes claras para a mitigação de riscos nos casos em que seu uso não for aplicável. Para Bioni (2019, p. 387) o fluxo informacional deve ser íntegro e adequado ao livre desenvolvimento da personalidade do titular dos dados, assegurando a proteção de seus direitos e liberdades fundamentais. O Autor continua e esclarece que esse fluxo deve permanecer sob a esfera de controle do titular, respeitando suas legítimas expectativas, com a adoção de medidas de transparência que reforcem sua participação no tratamento de suas informações, ainda que em momento posterior. Bioni (2019, p. 387) afirma que a autodeterminação informativa supera o mero consentimento no tratamento de dados, assegurando que o titular só exerça efetivo controle sobre suas informações quando estas forem tratadas de acordo com suas legítimas expectativas e de forma transparente.

A sociedade contemporânea é caracterizada pelo “dataísmo”, conceito apresentado por Yuval Harari e citado por Bioni (2019, p. 390-391), no qual a economia e as relações sociais são impulsionadas pelo fluxo contínuo de dados. Nesse contexto, empresas, governos, cidadãos e dispositivos inteligentes, especialmente com o advento da Internet das Coisas (IoT), realizam trocas de dados constantes, orientando a geração de riqueza, conhecimento e a formulação de políticas públicas em setores diversos, como saúde e assistência social.

Schwab (2016) destaca que vivemos na Revolução 4.0, onde a dataficação – conversão de eventos e comportamentos em dados digitais – se tornou o eixo central das interações econômicas e sociais. Esse processo é impulsionado pelo crescimento como Big Data, inteligência artificial, IoT e computação em nuvem, permitindo a coleta e análise massiva de informações individuais. Nesse cenário, Schwab (2016, p. 78) enfatiza a necessidade de os governos, em parceria com a sociedade civil e o setor privado, estabelecerem regras e mecanismos regulatórios que garantam justiça, competitividade, equidade, segurança e confiabilidade no ambiente digital.

O surgimento de legislações regulatórias, como a Lei Geral de Proteção de Dados (LGPD) no Brasil, representa, para Bioni (2019, p. 391), um novo contrato social, capaz de estabelecer diretrizes para um funcionamento democrático e equilibrado da sociedade digital. Sua implementação pode ter um impacto econômico, social e regulatório comparável ao do Código de Defesa do Consumidor e da Consolidação das Leis do Trabalho (CLT), reforçando a necessidade de mecanismos normativos eficazes para a proteção de dados.

A seguir, são analisados o Marco Civil da Internet, o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, a Lei Geral de Proteção de Dados (LGPD) e outras normativas essenciais à fundamentação desta pesquisa.

MARCO CIVIL DA INTERNET

O livre acesso à Internet transformou significativamente a vida humana e os padrões de comportamento, cujas consequências ainda geram perplexidade. Tomasevicius Filho (2016, p. 272) destaca que, inicialmente, acreditava-se que a rede mundial de computadores funcionaria como uma “terra sem lei”, sem restrições ou sanções, em razão da dificuldade de identificação dos usuários. No entanto, logo se constatou que o ordenamento jurídico brasileiro apresentava lacunas na repressão à criminalidade virtual. As normas penais, ligadas à soberania nacional, precisaram ser adaptadas à realidade da Internet, onde a ausência de fronteiras compromete a aplicação tradicional das regras de territorialidade. Crimes podem ser cometidos de um país contra indivíduos ou instituições em outro, tornando a Internet uma “aldeia global” em que as delimitações espaciais da aplicação da lei se tornam difusas. Vieira (2017, p. 213) adverte que os danos resultantes dessa vulnerabilidade podem ser irreparáveis, especialmente diante de riscos como a exposição de informações pessoais, o vazamento de dados e a violação da privacidade em redes sociais, que se tornaram parte essencial do cotidiano.

Diante desse cenário de insegurança jurídica e crescimento dos crimes virtuais, Tomasevicius Filho (2016, p. 273) observa que o governo brasileiro pressionou o Congresso Nacional para a aprovação de uma legislação que regulasse o uso da Internet, afastando a ideia de um espaço sem normas. Assim, foi instituído o Marco Civil da Internet, frequentemente referido como a “Constituição da Internet” – denominação imprecisa, uma vez que a rede mundial desconsidera fronteiras políticas.

A formulação de um marco regulatório para a Internet no Brasil resultou de uma parceria entre o Ministério da Justiça e a Escola de Direito do Rio de Janeiro, iniciada em 2009, culminando no Projeto de Lei nº 2126/2011. Esse projeto incorporou diversas propostas legislativas apresentadas desde 2000 e foi submetido a consultas públicas, permitindo a incorporação de sugestões ao texto final. A proposta antecedeu diversos escândalos de privacidade amplamente divulgados em 2013.

O Marco Civil da Internet foi oficialmente positivado pela Lei nº 12.965, de 23 de abril de 2014, com o objetivo de disciplinar o uso da Internet no Brasil. O projeto foi influenciado pelo artigo “Internet brasileira precisa de marco regulatório civil” (Lemos, 2007) e desenvolvido colaborativamente, em contraposição à Lei de Cibercrimes, amplamente criticada e apelidada de “AI-5 Digital” (D’Ávila, 2011). Segundo Tomasevicius Filho (2016, p. 273), três pontos foram duramente criticados nessa proposta: o risco de censura a páginas da Internet, a neutralidade da rede e a exigência de datacenters no Brasil. A tramitação do Marco Civil foi

acelerada para garantir sua promulgação antes do Encontro Multissetorial Global sobre o Futuro da Governança da Internet – Net Mundial, realizado em São Paulo nos dias 23 e 24 de abril de 2014, reunindo representantes de mais de 80 países (Casal Jr., 2014).

Dada a preocupação com eventuais restrições à liberdade de expressão, o texto final da Lei nº 12.965/2014 reforçou garantias nesse sentido. Tomasevicius Filho (2016, p. 273-274) destaca que o art. 2º consagrou a liberdade de expressão como princípio fundamental do uso da Internet, enquanto o art. 19 estabeleceu a vedação à censura. O art. 3º, inciso I, reiterou o direito à liberdade de expressão, comunicação e manifestação do pensamento, conforme previsto na Constituição Federal de 1988. Além disso, Vieira (2017, p. 208) enfatiza a importância do art. 3º ao garantir a privacidade, a inviolabilidade da intimidade e o sigilo das comunicações privadas, reafirmando direitos fundamentais já assegurados pela CF/88.

A legislação também conferiu especial atenção ao direito à privacidade, sob a ótica do Direito Civil, proibindo terceiros de acessarem indevidamente informações pessoais e assegurando o direito ao isolamento. Essa proteção foi consolidada no art. 7º, especificamente nos incisos I, II, III, VII e VIII, que estabelecem a inviolabilidade da intimidade, da vida privada e das comunicações, além da exigência de consentimento para o tratamento de dados pessoais e da necessidade de informar o usuário sobre a coleta e o armazenamento de suas informações. No mesmo sentido, o art. 10 dispõe que a guarda e a disponibilização de registros de conexão e de acesso às aplicações devem respeitar a intimidade, a vida privada, a honra e a imagem dos usuários. O art. 14 proíbe provedores de conexão de armazenarem registros de acesso às aplicações e veda a retenção de dados pessoais desnecessários à finalidade do serviço, sem o consentimento prévio do usuário.

Bioni (2019, p. 213) destaca que a privacidade e a proteção de dados pessoais são pilares fundamentais do Marco Civil da Internet, ao lado da neutralidade da rede e da liberdade de expressão, consolidando-o como um instrumento essencial na regulação do ambiente digital.

Tomasevicius Filho (2016, p. 274) destaca a preocupação do legislador com ilícitos civis e criminais cometidos na Internet. Embora a rede mundial permita a interação entre indivíduos, inclusive de forma anônima, toda ação realizada no ambiente digital pode ser registrada e rastreada, possibilitando a identificação dos usuários. Para viabilizar esse controle, o art. 13 do Marco Civil da Internet exige a guarda de registros de conexão por um ano, enquanto o art. 15 determina a retenção dos registros de acesso às aplicações por seis meses. No entanto, o acesso a essas informações para fins de investigação criminal ou reparação civil depende de autorização judicial, conforme estabelece o Marco Civil da Internet.

Para Vieira (2017, p. 208) e Tomasevicius Filho (2014, p. 162), a necessidade de um Marco Regulatório da Internet no Brasil surgiu da lacuna na proteção dos direitos da personalidade no ambiente digital. Assim, a legislação foi estruturada com base em três pilares fundamentais: liberdade de expressão, proteção à privacidade e neutralidade da rede, garantindo aos usuários a inviolabilidade da intimidade e da vida privada, bem como indenização por danos materiais ou morais decorrentes de violações.

Apesar das mudanças normativas, o Marco Civil da Internet apresenta lacunas significativas, especialmente no que tange à proteção da privacidade e à segurança dos dados pessoais armazenados em bancos de dados eletrônicos (Vieira, 2017, p. 200-214). Tomasevicius Filho (2016) critica a norma, classificando-a como uma “lei sem conteúdo normativo”, fundamentada nos princípios de abertura e colaboração, sem especificar de forma clara seu alcance e aplicação. O autor já havia apontado, anteriormente, que a legislação nasceu defasada diante dos desafios da Internet, pois a doutrina já alertava que o consentimento para o armazenamento de informações é insuficiente para garantir a proteção da privacidade online. A vulnerabilidade dos usuários decorre da assimetria de poder entre indivíduos e grandes corporações, que atuam no ambiente digital. Além disso, não há mecanismos eficazes para garantir que os dados dos usuários sejam efetivamente excluídos quando solicitado, uma vez que essas informações podem ser compartilhadas entre empresas, especialmente considerando o valor econômico agregado aos dados pessoais (Tomasevicius Filho, 2014, p. 163).

O Marco Civil da Internet também alterou a responsabilidade dos provedores de aplicações ao reduzir sua obrigação de vigilância sobre conteúdos publicados por usuários. Anteriormente, o art. 942 do Código Civil determinava a responsabilidade solidária, permitindo que a vítima acionasse tanto o autor da infração quanto o provedor simultaneamente. Esse sistema exigia que os provedores disponibilizassem canais de denúncia para a remoção de conteúdos ilícitos. Tal entendimento permanece vigente no Superior Tribunal de Justiça (STJ) (Tomasevicius Filho, 2016, p. 282). No que se refere às violações de direitos, Vieira (2017, p. 213) ressalta que a maior parte dos litígios envolve exposição indevida da privacidade em redes sociais, como a divulgação não autorizada de fotos e vídeos íntimos, frequentemente tratados como danos morais pelo Judiciário.

Outro desafio enfrentado pelo Marco Civil da Internet refere-se à sua eficácia no cenário internacional. Tomasevicius Filho (2016, p. 279) argumenta que, dada a ausência de legislação similar em outros países, sua aplicação se torna limitada, sendo ingênuo presumir que uma norma nacional possa oferecer soluções globais. O próprio modelo da Internet permite que

violações de direitos ocorram em qualquer parte do mundo, fora do alcance da jurisdição brasileira. Vieira (2017, p. 209-210) reforça essa limitação, apontando que grandes plataformas digitais, motores de busca, provedores de e-mails e redes sociais estão sediados, majoritariamente, nos Estados Unidos, sem representações no Brasil. Dessa forma, a aplicação da legislação brasileira se torna inviável, visto que a privacidade das comunicações deve ser protegida, e o acesso a informações de usuários só pode ocorrer mediante autorização judicial. Tomasevicius Filho (2016, p. 276-277) reconhece a intenção positiva dos legisladores ao criar um marco regulatório para a Internet, mas destaca que, quando a infração ocorre fora do território nacional, a aplicabilidade da lei é comprometida, pois o Brasil não possui jurisdição sobre empresas estrangeiras.

REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

O Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, instituído pela Regulamento (UE) 2016/679, visa assegurar a privacidade e a proteção de dados dos cidadãos da União Europeia (UE) e do Espaço Econômico Europeu (EEE). Assinado em abril de 2016 e implementado em maio de 2018, tem como objetivos garantir maior controle dos cidadãos sobre seus dados pessoais e uniformizar as legislações europeias sobre o tema, revogando a Diretiva 95/46/CE.

Ribas e Guerra (2020, p. 75) ressaltam que o GDPR extrapola as fronteiras da União Europeia, alcançando empresas estrangeiras que coletam dados de cidadãos europeus para oferta de produtos e serviços. Deste modo, corporações transnacionais, inclusive empresas brasileiras, estão sujeitas à sua aplicação caso operem dentro da UE.

A normatização introduzida pelo GDPR representou uma transformação conceitual, atribuindo à privacidade um valor essencial e preventivo (Ribas; Guerra, 2020, p. 75-76). Seus princípios incluem livre consentimento, finalidade e adequação do uso de dados, boa-fé e não discriminação, tornando-se referência para a Lei Geral de Proteção de Dados (LGPD) no Brasil.

Zuboff (2019, p. 481-482) destaca que o GDPR trouxe novas esperanças para a proteção da privacidade, exigindo que as empresas justifiquem suas práticas de tratamento de dados e se diferenciando do modelo norte-americano. Entre suas diretrizes estão a notificação obrigatória de violações, a limitação do consentimento como base legal e o direito ao apagamento de dados, além da previsão de sanções. A autora ressalta que o GDPR pode representar um desafio ao capitalismo de vigilância, desde que haja uma aplicação ativa e contínua por parte dos cidadãos (Zuboff, 2019, p. 485). Para Ribas e Guerra (2020, p. 76) a regulação responde à crescente

valorização dos dados, considerados “o recurso mais valioso do mundo”. Seu propósito é limitar práticas abusivas na coleta e processamento de dados, garantindo transparência e controle aos usuários. Doneda (2021, p. 342) observa que a exigência de consentimento pode gerar inconveniências, mas acredita que os benefícios superam as dificuldades. Schwab (2016) destaca que a Quarta Revolução Industrial intensificou o uso de algoritmos e inteligência artificial, que influenciam decisões sociais, econômicas e políticas por meio da personalização de conteúdo.

Outro aspecto inovador do GDPR é a restrição à tomada de decisões automatizadas, protegendo a autonomia e a personalidade dos titulares de dados (Ribas; Guerra, 2020, p. 77). Com o crescimento e desenvolvimento da inteligência artificial e do aprendizado de máquinas, há preocupações sobre a defasagem das legislações, que podem se tornar obsoletas rapidamente.

Zuboff (2019, p. 485) menciona a antropóloga Laura Nader para afirmar que a eficácia do GDPR dependerá da mobilização social e judicial. A experiência do direito ao esquecimento demonstra que progressos regulatórios só se consolidam por meio da ação coletiva e institucional. Assim, tanto o GDPR quanto a LGPD no Brasil só terão impacto real se forem interpretados e aplicados de maneira consistente nos tribunais.

A abrangência do GDPR no Brasil decorre do fato de que sua aplicação se estende a qualquer empresa que processe ou armazene dados de cidadãos europeus (Ribas; Guerra, 2020, p. 78). Segundo Polido *et al.* (2018, p. 16 *apud* Ribas; Guerra, 2020, p. 78), a regulação se aplica a três situações: (i) quando o operador e o responsável possuem estabelecimento na UE; (ii) quando o operador está fora da UE, mas presta serviços a entidades dentro do bloco europeu; e (iii) quando o operador se encontra na UE, ainda que o responsável pelos dados, esteja fora do território europeu.

Dado o contexto global da economia digital, torna-se essencial que países externos à UE adotem legislações compatíveis com o GDPR. Doneda (2021, p. 257-258) argumenta que uma regulação desalinhada dos padrões internacionais pode isolar juridicamente uma nação, enquanto normas frágeis podem comprometer a proteção global de dados. Para Reidenberg (*apud* Doneda, 2021, p. 259-261), a criação de um tratado internacional sobre proteção de dados seria essencial para viabilizar o comércio eletrônico entre nações. No entanto, há o risco de que a eficácia extraterritorial do GDPR represente uma ameaça à soberania de outros países.

Por fim, Zuboff (2019, p. 486-487) ressalta que apenas o tempo dirá se o GDPR será capaz de restringir o mercado de dados e previsões comportamentais, ou se o capitalismo de

vigilância continuará em êxito. A seguir, será abordada a Lei Geral de Proteção de Dados (LGPD), inspirada no GDPR e adaptada ao contexto brasileiro.

LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados (LGPD) estabelece diretrizes para o tratamento de dados pessoais e sensíveis, assegurando direitos fundamentais, como autodeterminação informativa, liberdade de expressão e privacidade. Além disso, regulamenta a proteção dos dados pessoais nas operações de tratamento, conforme os incisos X e LXXIX do artigo 5º da Constituição Federal. A proteção de dados no Brasil desenvolveu-se de forma fragmentada, fundamentando-se na Constituição Federal, Lei de Acesso à Informação, Marco Civil da Internet, GDPR, Código Civil, Código de Defesa do Consumidor, entre outras normativas. Essa diversidade regulatória resultava em lacunas, ausência de padrões, opacidade no tratamento de dados e falta de responsabilização, o que Bioni (2019, p. 149) descreve como uma “colcha de retalhos”. A LGPD surgiu para uniformizar e aprimorar a regulamentação da proteção de dados, garantindo transparência, segurança e direitos aos titulares. Inspirada no GDPR, sua aplicação abrange pessoas físicas e jurídicas que realizam tratamento de dados com finalidade econômica no Brasil, independentemente da nacionalidade do titular, localização da sede da empresa ou do armazenamento dos dados. Conforme o artigo 3º da LGPD, a legislação se aplica quando: (i) o tratamento ocorre no território nacional; (ii) envolve oferta de bens ou serviços no Brasil; (iii) os dados foram coletados no país.

Entre os principais objetivos da LGPD está a transparência na relação entre titulares e controladores de dados. Tomasevicius Filho (2014, p. 166) já apontava a dificuldade de controle sobre informações pessoais, pois, em muitos casos, os titulares não sabem como seus dados são utilizados. A LGPD define dados pessoais como qualquer informação relacionada a uma pessoa natural identificada ou identificável, enquanto dados pessoais sensíveis incluem informações sobre origem racial, convicção religiosa, opinião política, saúde, vida sexual, dados genéticos e biométricos. Essa distinção visa prevenir discriminações e fortalecer a proteção da privacidade (Bioni, 2019, p. 348-349).

A LGPD estrutura-se em 11 princípios fundamentais, como boa-fé, finalidade, adequação, transparência, segurança e não discriminação, conforme disposto no artigo 6º. O artigo 7º estabelece as bases legais para o tratamento de dados, incluindo o consentimento do titular, cumprimento de obrigação legal, execução de contratos, proteção da vida, tutela da saúde, exercício de direitos, interesse legítimo do controlador e proteção do crédito.

A LGPD estabelece a anonimização e a pseudonimização como medidas de proteção de dados pessoais, impedindo ou restringindo a associação das informações a indivíduos. Grandes empresas já possuem tecnologia para adotar essas práticas. A eficácia da LGPD depende da atuação da ANPD, responsável pela fiscalização e aplicação de sanções, que incluem multas de até 2% do faturamento, limitadas a R\$ 50 milhões, além da suspensão e bloqueio do tratamento de dados. Vazamentos de dados, como os casos da Uber (2016), *Facebook-Cambridge Analytica* (2016), Banco Inter (2018) e diversos incidentes monitorados pela *Information Is Beautiful* (2022), ilustram a necessidade de medidas rígidas para proteção da privacidade.

A LGPD reforça o direito à autodeterminação informativa, permitindo que titulares solicitem acesso, correção e exclusão de seus dados. Essa proteção, mais ampla e célere que o *habeas data*, encontra aplicação prática na maior transparência dos sistemas de score de crédito, conforme exemplificado por O'Neil (2020). A LGPD, no entanto, pode ser considerado como o primeiro passo na proteção de dados no Brasil, alinhando-se ao cenário global de regulação digital. Sua efetividade depende da adoção de boas práticas, da fiscalização e da conscientização dos cidadãos sobre seus direitos. O estudo prossegue com a análise de outras normativas relacionadas à tutela da privacidade e da autodeterminação informativa.

NORMATIVAS COMPLEMENTARES SOBRE PROTEÇÃO DE DADOS

A Constituição Federal de 1988 estabeleceu a proteção à intimidade e à vida privada no artigo 5º, e, com a Emenda Constitucional nº 115 de 2022, reconheceu a proteção de dados pessoais como direito fundamental. A efetivação dessas garantias, porém, demandou a criação de legislações específicas.

Entre as normativas que influenciaram a construção da LGPD, destacam-se o Código de Defesa do Consumidor (CDC), que assegura o direito à informação e à transparência no tratamento de dados pessoais, e a Lei do Cadastro Positivo (Lei nº 12.414/2011), que regulamenta a coleta de informações sobre histórico de crédito. A Lei de Acesso à Informação (LAI – Lei nº 12.527/2011) estabelece diretrizes para a transparência na administração pública, incluindo regras para proteção de dados pessoais. No campo penal, a Lei Carolina Dieckmann (Lei nº 12.737/2012) criminaliza a invasão de dispositivos eletrônicos e o vazamento de informações privadas sem consentimento. Contudo, Tomasevicius Filho (2015, p. 161) considera que suas penalidades brandas a tornam de caráter meramente simbólico.

Além das legislações nacionais, documentos internacionais influenciaram a regulamentação da proteção de dados. A Declaração Universal dos Direitos Humanos (1948) e

a Convenção Europeia dos Direitos do Homem (1950) garantem a inviolabilidade da vida privada. A Diretiva de Proteção de Dados da União Europeia (1995) estabeleceu princípios como consentimento informado e direito de acesso a informações pessoais, tornando-se referência para o GDPR e a LGPD. A Convenção 108 do Conselho da Europa (1981) foi pioneira na regulamentação da proteção de dados automatizados. Nos Estados Unidos, a HIPAA (1996) impôs normas de sigilo para informações de saúde.

A evolução da tutela jurídica da privacidade reflete o impacto das transformações tecnológicas, como destaca Schwab (2016) ao afirmar que a Quarta Revolução Industrial exige novos modelos regulatórios, pois as leis tradicionais são insuficientes para os desafios do ambiente digital. Doneda (2010, p. 18) corrobora essa visão, enfatizando a necessidade de equilibrar a inovação tecnológica com a proteção dos dados pessoais.

Portanto, a proteção da privacidade e dos dados pessoais deve acompanhar a evolução tecnológica, para garantir segurança jurídica, transparência e direitos fundamentais na era digital.

AUTODETERMINAÇÃO INFORMATIVA NA SOCIEDADE DIGITAL

A autodeterminação informativa na sociedade digital é analisada a partir da evolução do conceito de privacidade e da cessão de dados pessoais em redes sociais, comércio eletrônico e plataformas digitais. O texto traça um panorama sobre o desenvolvimento da Internet e explora questões de vigilância e proteção de dados. Em diálogo com a obra 1984, de George Orwell, reflete-se sobre como o contexto tecnológico e jurídico contemporâneo pode reproduzir ou evitar um cenário de supressão da privacidade. Faleiros, Lima e Callegari (2016, p. 102) destacam a importância de definir limites do direito à privacidade, tanto para coibir abusos de grandes corporações e do Estado quanto para analisar a exposição voluntária dos indivíduos nas redes sociais, mediada pelos smartphones como teletelas modernas. O objetivo é proteger os direitos de personalidade e os direitos fundamentais. Doneda (2021, p. 79) pontua que a personalidade não é um direito, mas um status dentro dos direitos de personalidade, garantindo ao indivíduo sua própria autodeterminação. Cristóvão e Silva (2021, p. 88) enfatizam que a tecnologia é indispensável ao desenvolvimento social, sendo parte essencial das infraestruturas de vigilância, sejam elas utilizadas por regimes totalitários ou não.

Com base nesses elementos, torna-se essencial compreender o funcionamento da autodeterminação informativa e sua proteção no ordenamento jurídico. Desta forma, se iniciará

análise da evolução da Internet e das redes sociais digitais, posteriormente na autodeterminação informativa na sociedade digital e nas implicações da cessão da privacidade.

A INTERNET, REDES SOCIAIS E A SOCIEDADE DIGITAL

Neste ensaio, a Internet, as redes sociais digitais e a sociedade digital são analisadas sob uma perspectiva sociológica, destacando seu impacto no século XXI e a relação com a autodeterminação informativa. A Internet surgiu em 1969 com a ARPAnet e evoluiu com o desenvolvimento de protocolos como TCP/IP e DNS, possibilitou a criação da *World Wide Web*. A partir da década de 1990, transformou a comunicação e a troca de informações. A popularização da Internet intensificou-se com o surgimento das redes sociais digitais, que modificaram as dinâmicas de sociabilidade e acesso à informação.

Canavilhas (2010, p. 390) destaca que redes como *Blogger* (1999), *Facebook* (2004), *YouTube* (2005) e *Twitter* (2006) consolidaram um novo modelo de comunicação, em que os usuários deixaram de ser meros receptores passivos para se tornarem criadores e disseminadores de conteúdo. Essa mudança alterou a forma de consumo de informação, tornando a comunicação horizontal e interativa.

A análise de Castells (2000) enfatiza a relevância da arquitetura das interações sociais na era digital, evidenciando como a conectividade global possibilita tanto a inclusão quanto a vigilância. Nesse contexto, a sociedade digital se aproxima da lógica de controle descrita por Orwell em 1984, na qual o Ministério da Verdade reescreve a realidade conforme os interesses do poder. A coleta massiva de dados e o fornecimento voluntário de informações pelos indivíduos geram novas formas de vigilância, em que a própria sociedade contribui para sua supervisão e monitoramento.

Segundo Fialho (2014, p. 10-11), as redes sociais digitais estruturam-se como redes de comunicação simbólicas, definindo novos padrões de organização, interação e influência sobre política e economia. Contudo, Dugnani (2021, p. 11-12) argumenta que a lógica algorítmica gera “bolhas informacionais”, limitando o acesso a perspectivas divergentes e criando ambientes homogêneos que reforçam ideias preexistentes.

Evangelista e De Miranda (2018, p. 45) aponta que o ser humano passou a ser percebido como um processador de informações, tornando-se um fornecedor contínuo de dados para grandes corporações. Han (2018) descreve esse fenômeno como um “exame digital”, no qual a necessidade de exposição e validação social faz com que indivíduos forneçam voluntariamente suas informações, muitas vezes sem consciência plena dos impactos dessa

cessão de dados. O fenômeno de modulação de comportamento, descrito por Bauman e Lyon (2014), reforça a preocupação com a veracidade da informação e a manipulação algorítmica, ecoando os alertas de Orwell sobre a reescrita da realidade pelo poder dominante. O trecho de 1984 citado a seguir ilustra essa preocupação: "Se o Partido era capaz de meter a mão no passado e afirmar que esta ou aquela ocorrência jamais acontecera - sem dúvida isso era mais aterrorizante do que a mera tortura ou a morte" (Orwell, 2009, p. 47).

Nesse cenário, a autodeterminação informativa torna-se fundamental para garantir o direito à privacidade e à proteção de dados. Como destaca Tomasevicius Filho (2016, p. 271), a digitalização das relações humanas transformou não apenas a forma de comunicação, mas também a forma como os dados pessoais são tratados e utilizados. O desenvolvimento da sociedade digital e o crescente armazenamento de informações pessoais geram desafios jurídicos que demandam regulação e mecanismos eficazes de proteção de dados, como os estabelecidos pela Lei Geral de Proteção de Dados (LGPD).

A seguir, serão analisados os aspectos jurídicos da autodeterminação informativa, essenciais para garantir que a privacidade e os direitos dos indivíduos sejam preservados em um ambiente digital cada vez mais sofisticado.

AUTODETERMINAÇÃO INFORMATIVA E PRIVACIDADE

O conceito deriva do direito de personalidade, especialmente da privacidade, sendo consolidado pelo Tribunal Constitucional Alemão e positivado na Diretiva 95/46/CE da União Europeia, com influências da doutrina norte-americana de Alan Westin, desde a década de 1970 (Doneda, 2021, p. 171-177). A autodeterminação informativa confere ao indivíduo o controle sobre seus próprios dados, determinando quando, como e em quais limites terceiros podem utilizá-los. No entanto, Willemijn (2020) questiona a fragilidade do consentimento como único mecanismo de proteção, destacando a necessidade de aculturação digital para que os cidadãos compreendam o alcance da cessão de suas informações.

A proteção de dados pessoais é um direito essencial à personalidade, sendo reconhecida como instrumental para o livre desenvolvimento individual e a dignidade humana (Bioni, 2019, p. 134). Dados pessoais, conforme Mulholland (2018, p. 171), consistem em informações que identificam a pessoa e devem ser resguardados, distinguindo-se de dados impessoais ou de informações que não configuram um vínculo direto com o titular.

A privacidade informacional, classificada como novo direito da personalidade, não se limita à confidencialidade da vida íntima, mas inclui o direito de conhecer e controlar quais

informações estão sendo armazenadas e utilizadas (Doneda, 2021, p. 130). Assim, a privacidade moderna não se reduz ao “direito de ser deixado só”, mas sim à autonomia sobre os próprios dados, alinhando-se ao princípio da autodeterminação informativa (Rodotà, 2008, p. 92).

Historicamente, a noção de privacidade foi amplamente debatida. O clássico estudo *The Right to Privacy*, de Samuel Warren e Louis Brandeis, influenciou a responsabilidade civil na proteção da intimidade, conforme Tomasevicius Filho (2014, p. 142). Já Westin (1968, p. 24-25) concebe a privacidade como um equilíbrio entre anonimato e participação social, reconhecendo que a vigilância imposta por normas coletivas pode limitar essa liberdade. Com a ascensão tecnológica, a disseminação de dados sensíveis tornou-se uma ameaça constante à privacidade, e que exigem regulamentações para garantir o controle sobre o fluxo dessas informações (Mulholland, 2018, p. 172-173).

O Código Civil Brasileiro (art. 21) protege a vida privada, mas a concepção tradicional de privacidade já não reflete a realidade digital, e assim, exige novos instrumentos jurídicos para assegurar a transparência e o controle sobre os dados pessoais (Lewicki, 2003; Rodotà, 2008; Solove, 2008). No contexto do Estado Democrático de Direito, a autodeterminação informativa emerge como um direito fundamental, confere ao indivíduo o poder de decidir sobre a utilização de seus dados, para garantir sua dignidade e liberdade (Mulholland, 2012, p. 3; 2018, p. 169-170).

A Quarta Revolução Industrial impõe desafios à governança digital. Schwab (2016) adverte que o desenvolvimento tecnológico é exponencial, enquanto a regulação caminha de forma linear, permite que grandes plataformas explorem lacunas normativas para ampliar sua influência sobre os dados pessoais. Esse cenário evidencia a necessidade de modelos regulatórios que equilibrem inovação e proteção de direitos fundamentais.

A pandemia de COVID-19 expôs os conflitos entre privacidade e interesse público, ao permitir que órgãos de saúde processassem dados pessoais sem consentimento explícito, com justificativa sanitária. Schwab e Mallaret (2020) destacam que esse episódio acelerou a transformação digital, ampliando a vigilância estatal e corporativa e intensificando o debate sobre os limites da autodeterminação informativa. Bioni (2019) defende que o controle de dados deve superar o consentimento, permitindo que os titulares definam critérios de uso, pois a ausência desse controle pode levar a discriminação algorítmica e comprometer a liberdade e a dignidade humana. Esse direito, quando não respeitado, pode gerar discriminações algorítmicas e modular comportamentos, comprometendo não apenas a privacidade, mas também a liberdade e a dignidade da pessoa humana.

O direito à privacidade encontra respaldo em diversos documentos internacionais, desde a Declaração Universal dos Direitos Humanos (1948) até tratados como a Convenção Europeia dos Direitos Humanos (1950) e o Pacto de São José da Costa Rica (1969). No Brasil, Vieira (2017, p. 199-200) distingue a esfera íntima, que deve permanecer inviolável, da esfera social, onde determinados dados podem ser acessados e divulgados publicamente, respeitados os limites legais. O direito ao esquecimento, derivado do *Right to be let alone*, é objeto de intensos debates jurídicos. No julgamento do Recurso Extraordinário nº 1010606, o Supremo Tribunal Federal declarou sua incompatibilidade com a Constituição, afirmando que o tempo não justifica a censura de fatos verídicos, embora tenha reconhecido a possibilidade de responsabilização por abusos na exposição de informações pessoais. Na terceira década do século XXI, Cristóvão e Silva (2021, p. 89) alertam para a crescente banalização da privacidade, impulsionada por tecnologias de reconhecimento facial e rastreamento digital. A vigilância massiva aproxima-se do cenário descrito na obra 1984, de Orwell, em que o Partido Interno detinha controle absoluto sobre os cidadãos.

A superexposição nas redes sociais compromete a privacidade, uma vez que os próprios usuários compartilham dados sensíveis sem plena consciência das consequências. Luz e Max (2017, p. 09) destacam que ferramentas como status e lives intensificam esse fenômeno, gerando um banco de dados involuntário alimentado pelos próprios indivíduos. Zuboff (2019, p. 183) adverte que a coleta massiva de informações pessoais viabiliza a imposição de padrões de comportamento e ajustes de conduta, minando a autonomia individual e representando uma ameaça à democracia. A autodeterminação informativa, portanto, excede a questão do consentimento e se impõe como elemento essencial para assegurar a liberdade e a dignidade na era digital (Bioni, 2019, p. 400).

Evangelista e De Miranda (2018, p. 70) observam que, na sociedade digital, a pressão para adesão às plataformas torna a privacidade um privilégio restrito. Defendem que a autodeterminação informativa deve ser reconhecida como um direito fundamental, cuja efetivação requer um arcabouço regulatório capaz de limitar abusos na exploração de dados e equilibrar inovação e proteção dos indivíduos.

AUTODETERMINAÇÃO INFORMATIVA E A CESSÃO DE PRIVACIDADE NAS REDES SOCIAIS

Partindo da figura metafísica do “Grande Irmão” de Orwell para o ciberespaço das redes sociais, argumenta-se que a privacidade se tornou um conceito fluido, cujo limite entre o público e o privado é cada vez mais difícil de determinar.

A disseminação das tecnologias digitais propiciou uma conexão constante, diluindo as barreiras entre o que é privado e público (Arata Júnior, 2003). Stancioli (2010) diferencia a autonomia da pessoa natural em ceder voluntariamente parte de sua privacidade da perda definitiva da titularidade desse direito. O Código Civil Brasileiro (Brasil, 2002) estabelece que os direitos da personalidade são intransmissíveis e irrenunciáveis, mas seu exercício pode ser relativizado conforme o contexto social.

A privacidade, antes pautada no sigilo e controle individual sobre informações, foi ressignificada como um elemento de circulação e exposição (Doneda, 2021). Em redes sociais, os indivíduos voluntariamente compartilham aspectos de suas vidas cotidianas, muitas vezes em busca de reconhecimento e engajamento (Couto, 2015). Han (2017) aponta que a sociedade contemporânea valoriza a exibição constante, transformando a identidade do sujeito em mercadoria.

O fenômeno da superexposição impulsiona a construção de uma “sociedade do espetáculo”, na qual a presença digital se torna essencial para a existência social (Debord, 2007). Essa coação à visibilidade reduz a privacidade a um conceito ultrapassado, transformando-a em um privilégio raramente exercido (Bauman; Lyon, 2014).

A cessão da privacidade também se manifesta na adesão às políticas de privacidade das plataformas digitais, muitas vezes sem plena consciência dos usuários. Zuboff (2019) demonstra que a maioria dos indivíduos consente rapidamente com os termos de uso, sem compreensão real dos impactos da coleta e compartilhamento de seus dados. A partir da leitura de Bauman e Lyon (2014), argumenta-se que a exposição digital não apenas compromete a privacidade individual, mas também reforça um modelo de vigilância massiva.

A conectividade obrigatória redefine a socialização, impondo a necessidade de visibilidade constante e reduzindo o espaço para a intimidade. Han (2017) observa que a ausência de exposição equivale à inexistência, gerando pressão para a autopromoção contínua. O impulso para compartilhar detalhes da vida pessoal cria um paradigma, no qual a privacidade se torna um bem negociável em troca de interação e reconhecimento social (Couto, 2015).

O paradoxo da privacidade na era digital está na contradição entre a reivindicação de direitos individuais e a renúncia voluntária à intimidade. Vieira (2017) alerta para os riscos da superexposição, especialmente o arrependimento tardio pela divulgação excessiva de dados

peçoais. No cenário de crescente transparência digital, Han (2017) enfatiza que a eliminação do espaço privado compromete a liberdade individual e a autenticidade das relações interpessoais.

Na sociedade digital, a autodeterminação informativa está profundamente vinculada à cessão da privacidade, muitas vezes inconsciente. A vigilância digital e a cultura da exposição desafiam a autonomia individual, enquanto o capitalismo de vigilância transforma a privacidade em um fator de exclusão social, obrigando os indivíduos a negociarem sua intimidade para manterem sua visibilidade no espaço público digital.

CONSIDERAÇÕES FINAIS

A pesquisa evidenciou que, na era da hiperexposição digital, a autodeterminação informativa encontra-se gravemente comprometida pela lógica de extração massiva de dados promovida pelas plataformas digitais. A hipótese inicial, de que o consentimento não garante controle efetivo dos usuários sobre seus dados pessoais, foi confirmada pela análise crítica do modelo atual, que se baseia na coleta opaca e no uso preditivo de informações, intensificando assimetrias de poder e vulnerabilizando direitos fundamentais.

Em síntese, constatou-se que as plataformas digitais coletam e monetizam dados por meio de mecanismos opacos, tornando o consentimento ineficaz e comprometendo a privacidade, a liberdade e a governança dos dados, o que demanda uma nova regulação que equilibre inovação e proteção de direitos. A problemática central – sobre como a estrutura das plataformas digitais impacta a autodeterminação informativa e em que medida o consentimento se revela um mecanismo insuficiente – foi enfrentada por meio de revisão teórica e análise das normativas vigentes. Constatou-se que, apesar dos avanços trazidos pela Lei Geral de Proteção de Dados e por instrumentos regulatórios internacionais, o arcabouço jurídico ainda se mostra limitado diante da velocidade das transformações tecnológicas e do poder concentrado das grandes corporações digitais.

A autodeterminação informativa deve ser entendida como um pilar da cidadania digital, exigindo fortalecimento regulatório, educação digital e mecanismos de controle que assegurem a privacidade como um direito efetivo em um cenário marcado por desequilíbrios de poder e fluxos constantes de dados. É preciso estabelecer um novo modelo de governança digital que garanta o controle dos indivíduos sobre seus dados e assegure a privacidade como um direito universal. Para isso, são essenciais políticas de fiscalização, educação digital e conscientização,

com a colaboração de sociedade civil, setor privado e órgãos reguladores na criação de um ambiente digital mais justo e seguro.

A construção desse modelo passa pela revisão das relações entre usuários, plataformas e Estado, garantindo que a privacidade não se torne um privilégio, mas um direito efetivo na era digital.

REFERÊNCIAS

ARATA JUNIOR, Seiiti. Novos desafios à privacidade: os círculos sociais e as redes sociais (social networks). **Saúde Ética & Justiça**, v. 8, n. 1-2, p. 44-56, 2003. Disponível em: <https://www.revistas.usp.br/sej/article/view/42299/49563>. Acesso em: 13 maio 2024.

BAUMAN, Zygmunt. LYON, David. **Vigilância líquida**. Tradução: Carlos Alberto Medeiros. Rio de Janeiro: Jorge Zahar. 2014.

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

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal: Centro Gráfico, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 13 jun. 2024.

BRASIL. **Decreto nº 678 de novembro de 1992**. Promulga a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 22 de novembro de 1969. Brasília, DF: Presidência da República, 09 de novembro de 1992. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/d0678.htm. Acesso em: 13 maio 2024.

BRASIL. **Lei nº 10.406 de 10 de janeiro de 2002**. Institui o Código Civil. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm. Acesso em: 13 maio 2024.

BRASIL. **Lei nº 12.414 de 09 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, DF: Presidência da República, 09 de junho de 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 13 maio 2024.

BRASIL. **Lei nº 12.527 de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal (Lei de Acesso à Informação). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 10 maio 2024.

BRASIL. **Lei nº 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 14 de agosto de 2018. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 03 maio 2024.

CANAVILHAS, João. Do gatekeeping ao gatewatcher: o papel das redes sociais no ecossistema mediático. In: **Trabalho apresentado no II Congresso Internacional de Comunicación**. 2010. Disponível em <https://campus.usal.es/~comunicacion3punto0/comunicaciones/061.pdf>. Acesso em: 19 out. 2024.

CASAL JR, Marcello. Encontro em SP reúne 80 países para debater governança da internet. 23/04/2014 - **Agência Brasil**. Disponível em <https://agenciabrasil.ebc.com.br/geral/noticia/2014-04/encontro-em-sp-reune-80-paises-para-debater-governanca-da-internet>. Acesso em: 03 jan. 2025.

CASTELLS, Manuel. **A era da informação: economia, sociedade e cultura**. São Paulo: Paz e Terra, 2000.

CONSELHO DA EUROPA. **Convenção 108 +**: Convenção para a proteção das pessoas relativamente ao tratamento de dados de carácter pessoal. 128.ª sessão do Comité de Ministros, Elsinore, 18 de maio de 2018. Disponível em: <https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2>. Acesso em: 1 mar. 2025.

COUTO, Edvaldo. Educação e redes sociais digitais: privacidade, intimidade inventada e incitação à visibilidade. **Em Aberto**, v. 28, n. 94, 2015. Disponível em: <http://emaberto.inep.gov.br/ojs3/index.php/emaberto/article/view/3052/2787>. Acesso em: 13 maio de 2024.

COUNCIL OF EUROPE. **Convenção Europeia dos Direitos do Homem**. Roma, 4 de novembro de 1950. Disponível em <https://www.echr.coe.int/documents/conventionpor.pdf>. Acesso em: 02 mar. 2024.

CRISTÓVÃO, Adriano; SILVA, Bruno. Nineteen Eighty-Four: um diálogo entre a ficção e a contemporaneidade. **Rotura-Revista de Comunicação, Cultura e Artes**, n. 2, p. 87-91, 2021. Disponível em: <https://publicacoes.ciac.pt/index.php/rotura/article/view/66/25>. Acesso em: 13 abr. 2025.

D'ÁVILA, Manuela. O AI-5 Digital e as Razões Para o #Meganão. **UOL - Congresso em Foco** 01/08/2011. Disponível em <https://congressoemfoco.uol.com.br/reportagem/o-ai-5-digital-e-as-razoes-para-o-meganao/>. Acesso em: 16 nov. 2022.

DEBORD, Guy. **A sociedade do espetáculo**. Contraponto. 1ª Edição. 2007.

DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia**. Escola Nacional de Defesa do Consumidor. Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3 ed. São Paulo: Thomson Reuters Brasil, 2021.

DUGNANI, Patricio. Massificação e Internetilização: duas faces da mesma moeda no processo de alienação pelos meios de comunicação. **Revista Observatório**, v. 7, n. 4, 2021. Disponível em: <https://sistemas.uft.edu.br/periodicos/index.php/observatorio/article/view/11578>. Acesso em: 19 out. 2024.

ESTADOS UNIDOS. **Lei de Portabilidade e Responsabilidade de Seguro de Saúde (HIPAA) de 1996**. Disponível em: <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>. Acesso em: 01 mar. 2023

EVANGELISTA, Rafael; DE MIRANDA, Danilo Santos. **Para além das máquinas de adorável graça**: Cultura hacker, cibernética e democracia. Edições Sesc, 2018.

FALEIROS, Thaísa Haber; LIMA, Lucas Ferreira Mazete; CALLEGARI, Milena Caetano Cunha. Reflexões Sobre as Redes Sociais a Partir da Obra “1984” de George Orwell: Contribuições para o Ensino do Direito. **Revista Profissão Docente**, v. 16, n. 35, 2016. DOI: <https://doi.org/10.31496/rpd.v16i35.1130>.

FIALHO, Joaquim. Análise de redes sociais: princípios, linguagem e estratégias de ação na gestão do conhecimento. **Perspectivas em Gestão & Conhecimento**, João Pessoa, v. 4, Número Especial, p. 9-26, out. 2014. Disponível em <https://periodicos.ufpb.br/index.php/pgc/article/view/20881/11745>. Acesso em: 19 out. 2024.

HAN, Byung Chul. **Infocracia**: digitalização e a crise da democracia; tradução de Gabriel S. Philipson. Petrópolis, RJ: Vozes, 2022.

HAN, Byung-Chul. **No enxame**: perspectivas do digital. Editora Vozes Limitada, 2018.

HAN, Byung-Chul. **Sociedade da transparência**. Tradução de Enio Giachini. RJ: Editora Vozes, 2017.

INFORMATION IS BEAUTIFUL. **World's Biggest Data Breaches & Hacks**. 2022. Disponível em: <https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>. Acesso em: 06 mar. 2023.

LEMOS, Ronaldo. Internet brasileira precisa de marco regulatório civil. **UOL - Notícias - Tecnologia**. 2007. Disponível em <https://tecnologia.uol.com.br/ultnot/2007/05/22/ult4213u98.jhtml>. Acesso em: 11 nov. 2024.

LEWICKI, Bruno. **A privacidade da pessoa humana no ambiente de trabalho**. Rio de Janeiro: Renovar, 2003.

LUZ, Edson Belau da; MAX, Cristiano. Comportamento digital e o Whatsapp. In: INTERCOM – SOCIEDADE BRASILEIRA DE ESTUDOS INTERDISCIPLINARES DA COMUNICAÇÃO. XVIII Congresso de Ciências da Comunicação na Região Sul, 2017, Caxias do Sul, RS. **Anais [...]**. Caxias do Sul, 15 a 17 jun. 2017. Disponível em: <http://portalintercom.org.br/anais/sul2017/resumos/R55-0619-1.pdf>. Acesso em: 10 nov. 2024.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). **Revista de**

Direitos e Garantias Fundamentais, v. 19, n. 3, p. 159-180, 2018. Disponível em: <https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603/pdf>. Acesso em: 13 maio 2024.

MULHOLLAND, Caitlin. O direito de não saber como decorrência do direito à intimidade. Comentário ao REsp 1.195.995. **Civilistica.com** - Revista Eletrônica de Direito Civil, v. 1, p. 1, 2012. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/27/15>. Acesso em: 13 maio 2024.

O'NEIL, Cathy. **Algoritmos de destruição em massa**: como o big data aumenta a desigualdade e ameaça à democracia. Tradução Rafael Abraham. 1. ed. Santo André, SP: Editora Rua do Sabão, 2020.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos de 1948**. Disponível em: <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>. Acesso em: 08 ago. 2024.

ORWELL, George. **1984**. São Paulo. Companhia das Letras, 2009.

RIBAS, Brenno Henrique de Oliveira; GUERRA, Carolinne Cardoso. O impacto do Regulamento Geral de Proteção de Dados Pessoais da União Europeia no Brasil. In: VEIGA, Fábio da Silva; et al. (Org.). **Governança e Direitos Fundamentais**. São Paulo: Instituto Iberoamericano de Estudos Jurídicos, 2020. p. 75-83.

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

SCHWAB, Klaus. **A quarta revolução industrial**. tradução Daniel Moreira Miranda. - São Paulo: Edipro, 2016.

SCHWAB, Klaus; MALLERET, Thierry. COVID-19: **O grande reset**. Tradução de Rafael Godinho. 1. ed. São Paulo: Vide Editorial, 2020.

SOLOVE, Daniel J. **Understanding Privacy**. Cambridge: Harvard University Press, 2008.

STANCIOLI, Brunello. **Renúncia ao exercício de direitos da personalidade**. Belo Horizonte: Del Rey, 2010.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Recurso Especial n. 22.337/RS**, rel. Ministro Ruy Rosado de Aguiar, DJ 20/03/1995, p. 6119.

SUPREMO TRIBUNAL FEDERAL. **Recurso Extraordinário nº 1010606**. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5091603>. Acesso em: 05 set. 2024.

TOMASEVICIUS FILHO, Eduardo. Em direção a um novo 1984? A tutela da vida privada entre a invasão de privacidade e a privacidade renunciada. **Revista da Faculdade de Direito**, Universidade de São Paulo, v. 109, p. 129-169, 2014. Disponível em: <https://www.revistas.usp.br/rfdusp/article/view/89230>. Acesso em: 13 maio 2024.

TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estudos Avançados**, v. 30, p. 269-285, 2016. Disponível em

<https://www.scielo.br/j/ea/a/n87YsBGnphdHHBSMpCK7zSN/abstract/?lang=pt>. Acesso em: 11 nov. 2024.

UNIÃO EUROPEIA. **Diretiva 95/46/CE**. 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. Diário Oficial das Comunidades Europeias, Luxemburgo, 23 nov. 1995. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TX/T/?uri=CELEX%3A31995L0046>. Acesso em: 1 mar. 2023.

VIEIRA, Waleska Duque Estrada. A privacidade no ambiente cibernético: Direito fundamental do usuário. **Revista da ESMESC**, v. 24, n. 30, p. 197-217, 2017. Disponível em: <https://revista.esmesc.org.br/re/article/view/167>. Acesso em: 13 maio 2024.

WESTIN, Alan F. Privacy and freedom. **Washington and Lee Law Review**, v. 25, n. 1, p. 166, 1968. Disponível em: <https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20/>. Acesso em: 13 maio 2024.

WILLEMIN, Andrea. Aspectos gerais da Lei Geral de Proteção de Dados: a atuação do Poder Público. Escola Superior do MPSP. **Youtube**. Transmitido em 11 de setembro de 2020. Disponível em: <https://www.youtube.com/watch?v=p7DLJWEq24U>. Acesso em: 23 maio 2024.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**. Editora Intrínseca, 2021.

ZUBOFF, Shoshana. Big Other: Capitalismo de Vigilância e Perspectivas para uma Civilização de Informação. In. BRUNO, Fernanda *et al.* (Ed.). **Tecnopolíticas da vigilância: perspectivas da margem**. Boitempo Editorial, 2019.