REDE DE PESQUISA EM GOVERNANÇA DA INTERNET

Anais do Encontro Anual da Rede de Pesquisa em Governança da Internet

Maio de 2025

VIII ENCONTRO DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET - REDE 2025

FICHA TÉCNICA

ANAIS DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET-VOL. 8, ISSN 2675-1690

Editora
Kimberly Anastácio

Autoras (es)
Amanda Cunha e Mello Smith Martins
Bianca Galvão Marques
Carla Alessandra Marques
Cinthia Obladen de Almendra Freitas
Diná Santana Santos
Elizabeth Machado Veloso
João Pedro Bueno Ghizelini
José Humberto Fazano Filho
Pietra Milani Bizerril
Tatiana Nascimento Heim
Thiago Novaes

O VIII Encontro da Rede de Pesquisa em Governança da Internet e a publicação dos Anais resultantes deste encontro receberam apoio de: Comitê Gestor da Internet no Brasil - CGI.br, Internet Society - Capítulo Brasil e do Programa de Pós-graduação em Ciências Sociais da Universidade Estadual de Campinas (Unicamp), através de recursos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES).

PRIVACIDADE, INTELIGÊNCIA ARTIFICIAL E REGULAÇÃO

Elizabeth Machado Veloso

SUMÁRIO

PRIVACIDADE, INTELIGÊNCIA ARTIFICIAL E REGULAÇÃO

Elizabeth Machado Veloso[1]

RESUMO

Este artigo investiga as razões pelas quais leis de privacidade têm enfrentado dificuldades para proteger de forma efetiva a privacidade de indivíduos e instituições, sobretudo diante da rápida expansão da inteligência artificial. Com base no conceito de endogeneidade legal de Edelman (2016), argumenta-se que os símbolos de conformidade superficial — como treinamentos, auditorias formais e políticas de privacidade genéricas — estão sendo equivocadamente tratados como provas de cumprimento efetivo das normas. Por meio de revisão bibliográfica e análise crítica, o artigo contextualiza essa falha em um cenário global marcado por práticas abusivas no uso de dados por redes sociais, aplicativos e plataformas digitais. A conclusão é que a aplicação meramente simbólica da legislação compromete a proteção prometida ao consumidor, sendo necessária uma abordagem normativa mais substantiva, coerente com a realidade tecnológica e social.

PALAVRAS-CHAVE

proteção de dados; lei de privacidade; endogeneidade legal; redes sociais; inteligência artificial.

ABSTRACT

This article investigates the reasons why privacy laws face difficulties in effectively protecting the privacy of individuals and institutions, especially in the context of the rapid expansion of artificial intelligence. Based on the concept of legal endogeneity developed by Edelman (2016), the article argues that superficial compliance symbols—such as training programs, formal audits, and generic privacy policies—are being mistakenly interpreted as genuine compliance with privacy law requirements. Through a literature review and critical analysis, the article contextualizes this failure within a global landscape marked by abusive practices in data usage by social media, apps, and digital

[1] Doutora em Ciências da Comunicação pela Universidade do Minho, em Braga, Portugal; mestre em Políticas Públicas pela Universidade de Westminster, em Londres, Inglaterra; Consultora Legislativa da Câmara dos Deputados na área de Comunicação, Informática e Ciência e Tecnologia; apresentou o Programa Papo de Futuro na Rádio Câmara e na TV Câmara; colunista do site Congresso em Foco. E-mail: beth.veloso1@gmail.com.

platforms. The conclusion is that the symbolic application of legislation undermines the promise of consumer protection, highlighting the need for a more substantive approach that aligns with technological and social realities.

KEY WORDS
data protection; privacy law; legal endogeneity; social media; artificial intelligence.

INTRODUÇÃO

A Inteligência Artificial (IA) emergiu como um dos temas mais sensíveis e complexos da era digital, reconfigurando as fronteiras entre o público e o privado, e desafiando as normas tradicionais de regulação. Sua expansão massiva, impulsionada pelo acesso quase irrestrito a dados pessoais, tem levantado sérias questões sobre a eficácia das leis de proteção de dados. Como afirma Zuboff (2019), vivemos sob a lógica do capitalismo de vigilância, no qual os dados pessoais são sistematicamente explorados por empresas e governos, com ou sem consentimento consciente dos usuários.

Dados da Organização das Nações Unidas (UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, 2023) apontam que 75% dos países pesquisados possuem legislações para proteção de dados pessoais. No entanto, paradoxalmente, os dados nunca estiveram tão expostos e vulneráveis: os incidentes de vazamentos aumentaram em 20% entre 2022 e 2023 (HARVARD BUSINESS REVIEW, 2024). Essa contradição revela uma tensão entre a promessa normativa das leis e sua implementação concreta no cotidiano digital. A inteligência artificial, ao depender da coleta massiva de dados para treinar seus modelos, amplia essa contradição ao máximo.

OBJETIVOS

Este artigo busca analisar criticamente a efetividade das leis de proteção de dados no contexto contemporâneo e discutir os limites práticos de sua implementação. Propõe-se a demonstrar que há uma dissonância entre o discurso jurídico de proteção e a realidade do extrativismo digital, impulsionado por modelos de negócios baseados em dados.

Argumenta-se que o formalismo regulatório se confunde com proteção real, fragilizando os direitos dos cidadãos. Para isso, serão abordadas: a endogeneidade legal (EDELMAN, 2016), a falácia do consentimento informado, os limites das estruturas de enforcement e a ausência de uma arquitetura normativa orientada por valores de justiça e dignidade.

A pesquisa desenvolvida fundamenta-se em revisão bibliográfica e documental, analisando obras de autores consagrados como Zuboff, Edelman, Doneda, Waldman e DeNardis, além de relatórios técnicos da ANPD, CGI.br, ONU, e dados de vazamentos e incidentes reais. A análise teórica é complementada por estudos de caso, como os de comercialização de dados pessoais pela Serasa (DISTRITO FEDERAL, 2021) e do Facebook/Cambridge Analytica (2018), com ênfase nos impactos sobre o direito à privacidade e à autodeterminação informativa.

Este estudo articula distintas abordagens para compreender o fracasso regulatório. Zuboff (2019): capitalismo de vigilância e transformação do sujeito em fonte de valor informacional. Edelman (2016): endogeneidade legal e o uso simbólico das normas pelas próprias corporações reguladas. Waldman (2020): promessa falha das leis de privacidade diante de uma arquitetura digital orientada para o extrativismo. Doneda (2021): proteção de dados como extensão da dignidade humana. Marques (2023): privacidade projetada como arranjo socioeconômico e tecnológico. DeNardis (2014): governança da infraestrutura da internet como fator estruturante da política de dados.

A necessidade deste estudo emerge da constatação de que o aparato legal atual é insuficiente frente aos desafios impostos pela economia digital e pelas plataformas de IA. O consentimento se tornou um dispositivo disfuncional, e as obrigações legais frequentemente são neutralizadas por estratégias formais de conformidade. No plano normativo, tramita no Congresso Nacional um conjunto de proposições sobre IA e proteção de dados, mas ainda carecem de densidade técnica e de mecanismos de enforcement robustos. O Substitutivo ao Projeto de Lei 2338/2023, aprovado no Senado Federal em dezembro de 2024, representa um avanço, mas permanece aquém do necessário para enfrentar os dilemas estruturais da vigilância algorítmica.

A Lei Geral de Proteção de Dados (LGPD) foi promulgada com o propósito de limitar a coleta, uso e disseminação de dados pessoais no Brasil. No entanto, sua eficácia é profundamente questionável. É possível observar, na prática, que a lei se transformou em um instrumento simbólico — uma fachada de conformidade — sem alterar o cerne de uma cultura de extrativismo de dados que já permeia o ambiente digital.

O EXTRATIVISMO DE DADOS COMO CULTURA DOMINANTE

Shoshana Zuboff (2019) cunhou o conceito de capitalismo de vigilância ao apontar que as corporações tratam dados pessoais como um recurso natural a ser

explorado, coletado e monetizado. Esse extrativismo se sustenta em infraestruturas que, embora legalmente conformes, operam segundo uma lógica predatória. A LGPD introduziu obrigações como consentimento explícito, relatórios e auditorias, mas essas exigências muitas vezes se limitam a práticas superficiais — “checklists” que são cumpridos apenas para cumprir a lei, sem modificar o funcionamento real das plataformas.

Segundo Gadoni Canaan (2023), ao replicar o modelo GDPR, a LGPD estimulou investimentos em tecnologias de proteção de dados, mas os principais ganhos econômicos foram apropriados por grandes empresas ocidentais, em detrimento da inovação local. Ou seja: houve reforço institucional da lei, mas isso não se traduziu em mudanças estruturais.

O design das plataformas está calibrado para que o usuário acate o consentimento sem compreendê-lo — opt-out camuflado em botões mínimos, políticas extensas e caixas pré-marcadas que viram meras formalidades legais. Isso reforça o que Ari Ezra Waldman (2020) chama de “falsa aparência de conformidade”: aparentam estar em conformidade, mas, na prática, continuam a explorar livremente os dados dos usuários.

Esse consentimento é enganoso: o usuário escolhe, mas sem informação ou transparência verdadeira. As políticas de privacidade são técnicas, complexas e irreais para leitura comum. O resultado é uma transferência da responsabilidade para o indivíduo, como se a proteção dependesse exclusivamente de sua ação e compreensão (FERREIRA et al., 2021).

PRIVACIDADE PROJETADA E VIDA PRIVADA

O trabalho de Daniel Marques (2023) aponta uma distinção crucial entre privacidade projetada e privacidade tradicional. A primeira refere-se ao conceito que contempla privacidade como fenômeno emergente da interação entre tecnologias, dispositivos e contextos, indo além da simples proteção de dados. Já a segunda, privacidade tradicional, diz respeito à esfera privada, o direito constitucional de ter partes da vida excluídas do domínio público.

Enquanto a LGPD foca no âmbito formal — consentimentos, relatórios e auditoria — a privacidade projetada requer uma abordagem sistêmica, que engloba desde os dispositivos (como smart speakers) até o uso real dos dados em contextos diversos. Lauren Edelman (2016) denominou esse fenômeno de endogeneidade legal: empresas adotam medidas superficiais que simulam conformidade, mas não alteram cultura, va-

lores ou práticas operacionais. Isso fragiliza a atuação da LGPD, transformando-a em formalismo jurídico, enquanto a prática contradiz a letra da lei.

A falta de uma cultura de proteção de dados e a ausência de sanções eficazes agravam o problema. Segundo críticos, a regulamentação cria uma sensação enganosa de proteção — os cidadãos acreditam estar protegidos enquanto as plataformas mantêm extração massiva de dados sem punição (CGI.br, 2022).

IA, COLETA MASSIVA E CUSTO REGULATÓRIO

A inteligência artificial demanda volumes massivos de dados para funcionar conforme expectativas dos usuários. Naturalmente, isso reforça a lógica de extrativismo. E o usuário, em geral, aceita essa troca: comodidade e personalização em troca de dados pessoais.

Contudo, esse custo regulatório se agrava quando se considera que a coleta independe do uso apenas em redes sociais: acontece em e-commerce, sistemas de localização (GPS), buscadores, serviços de streaming, aplicativos de saúde e crédito. A rede mundial de computadores se desdobra em várias camadas: redes sociais; plataformas de serviços; provedores de infraestrutura (ISPs, nuvens, CDNs); sistemas de vigilância governamental; e Internet das Coisas (IoT).

Todas essas camadas ameaçam diretamente valores constitucionais consagrados na Constituição Federal de 1988, como a privacidade (art. 5º, inciso X), a intimidade (art. 5º, inciso X), a dignidade da pessoa humana (art. 1º, inciso III) e a autodeterminação informativa — esta última como direito implícito derivado dos princípios da liberdade e da proteção da vida privada. A vulnerabilidade a vazamentos e fraudes, associada à arquitetura técnica de coleta indiscriminada de dados, configura grave risco à realização plena desses direitos fundamentais no ambiente digital.

Casos emblemáticos evidenciam a fragilidade estrutural da proteção de dados pessoais, mesmo após a promulgação da LGPD. Em janeiro de 2021, o vazamento de dados na internet expôs informações pessoais de mais de 220 milhões de brasileiros — incluindo CPF, endereço, renda presumida e até perfis de redes sociais — em um dos maiores incidentes de segurança da história do país (G1, 2021). A falha evidenciou a ausência de mecanismos técnicos robustos e o baixo grau de transparência na resposta institucional à violação. Apesar da gravidade, o episódio não resultou em sanções proporcionais às empresas envolvidas.

Outro caso marcante foi o escândalo internacional da Cambridge Analytica, revelado em 2018, que demonstrou como dados de usuários do Facebook foram utilizados de forma indevida para fins de microdirecionamento político. A empresa coletou, sem consentimento adequado, informações de cerca de 87 milhões de perfis para influenciar processos eleitorais, como o Brexit e a eleição presidencial dos EUA em 2016 (CADWALLADR & GRAHAM-HARRISON, 2018). O caso expôs globalmente os riscos de uso político e comercial dos dados pessoais por plataformas digitais sem fiscalização pública efetiva.

Relatórios da Controladoria-Geral da União (CGU, 2022) e do Ministério Público Federal apontam que, apesar da existência da LGPD, o país ainda carece de uma cultura institucional de proteção de dados. As ações fiscalizatórias são esparsas, as sanções são morosas e, frequentemente, limitam-se a advertências ou recomendações. A ANPD, embora formalmente constituída, ainda enfrenta desafios de estrutura, autonomia e efetividade.

No setor de design e interfaces, análises técnicas identificam que os termos de uso das plataformas digitais permanecem ilegíveis, de difícil compreensão e incompatíveis com os princípios da transparência e da autodeterminação informativa exigidos pela legislação brasileira (FERREIRA et al., 2021). No setor de design e interfaces, análises evidenciam que os termos de uso são ilegíveis, ilegítimos e em desacordo com as diretrizes legais e de usabilidade recomendadas (FERREIRA et al., 2021).

ANÁLISE À LUZ DO PL 2.338/2023 (REGULAÇÃO DE IA)

O PL 2.338/2023 foi aprovado pelo Senado em 10 de dezembro de 2024, por um substitutivo do senador Eduardo Gomes (PL-TO), após tramitação conduzida por uma comissão de juristas presidida por Ricardo Villas Bôas Cuevas e o então presidente Rodrigo Pacheco. Entre as propostas relevantes, estão a classificação de sistemas de alto risco – inclui IA em áreas sensíveis como recrutamento, biometria e serviços públicos, exigindo avaliação de impacto algorítmico realizada por equipes multidisciplinares; direitos das pessoas afetadas – garante acesso à informação, correção de vieses, revisão humana e não-discriminação pelos sistemas de IA.

O projeto de lei em questão também traz a proibição de sistemas de risco excessivo – veda autômatos de manipulação comportamental, armas autônomas e exploração de vulnerabilidades; autorização restrita para reconhecimento facial somente

em contextos criminais; Criação do SIA – institui o Sistema Nacional de Regulação e Governança da IA, sob coordenação da ANPD, responsável pela classificação de risco, normatização e fiscalização; governança e boas práticas – estabelece obrigações para avaliações de risco, auditorias, transparência de bancos de dados e eficiência energética em IA generativa.

Complementarmente, a ANPD em seu relatório preliminar (ANPD, 2023) sugere que o texto elimine lacunas de interface com a LGPD, especialmente no caso de sandboxes regulatórios. Sandboxes regulatórios são ambientes controlados, criados por autoridades reguladoras, nos quais empresas podem testar produtos, serviços ou modelos de negócio inovadores sob supervisão institucional e com flexibilização de determinadas normas. O objetivo é estimular a inovação — especialmente em setores de alta complexidade técnica, como fintechs, inteligência artificial, blockchain e saúde digital — sem comprometer a proteção aos usuários ou a estabilidade do mercado.

O PL fortalece a lógica de accountability prevista na LGPD, classificando o uso de dados por sistemas de risco. O direito à explicação humana amplia o chamado "direito à explicação" da GDPR, até então pouco efetivado na LGPD. A centralização da competência pela ANPD, que agora passa a abarcar também fiscalização de IA, atende às lacunas técnicas apontadas previamente.

Apesar dos avanços, replicam-se os riscos já identificados com a LGPD: avaliações de risco são relativamente facultativas para sistemas de baixo risco, o que pode esvaziar o princípio de governança proativa (COALIZÃO DIREITOS NA REDE, LAPIN, 2023); emendas no Senado removeram requisitos de integridade informacional entre critérios de avaliação, evidenciando diluição das normas; não ficou claro que as sanções propostas sejam eficazes ou dissuasórias, o que reproduz o cenário de enforcement fraco, já observado na LGPD.

Assim, mantém-se a lógica da endogeneidade legal (EDELMAN, 2016) — regulação que simbolicamente aparenta ser forte, mas que pode falhar na modificação de práticas corporativas. Dessa forma, o PL busca convergir LGPD e regulação de IA, centrando-se na ANPD e na proteção de direitos fundamentais. Contudo, sua efetividade dependerá de: supervisão técnica institucional robusta; transparência real dos processos de classificação de risco; independência política e autonomia da ANPD; sensibilização cultural para a privacidade projetada (MARQUES, 2023) — isto é, conceber dados pessoais como extensão da pessoa humana.

Sem essas medidas, há o risco de transformar mais uma norma em fachada protetiva, sem romper com a estrutura do capitalismo de vigilância.

CONSIDERAÇÕES FINAIS

A LGPD representa um avanço formal no ordenamento jurídico brasileiro ao estabelecer princípios e normas para a proteção de dados pessoais. No entanto, ela ainda não foi capaz de desmontar a lógica estrutural do capitalismo de vigilância, que se apoia na coleta massiva e no uso opaco de dados para fins comerciais, políticos e de controle social. A cultura de extrativismo informacional, a arquitetura predatória das plataformas digitais e a fragilidade dos mecanismos de fiscalização dificultam a efetividade da lei. O consentimento, frequentemente obtido de forma simbólica e sem real compreensão, pouco contribui para a proteção do usuário. O design das plataformas, por sua vez, é pensado para induzir a coleta constante de dados, e a abordagem da privacidade projetada segue sendo marginalizada nas práticas institucionais (MARQUES, 2023).

Para que a LGPD realmente cumpra seu propósito, é necessário compreendê-la como expressão de um direito fundamental vivo e dinâmico, cuja eficácia depende não apenas da existência formal da norma, mas da criação de um ecossistema institucional, tecnológico e educativo voltado à proteção efetiva dos dados pessoais. Isso exige que a proteção de dados seja integrada desde o design das tecnologias, incorporando os princípios de "privacy by design" e "privacy by default". Também é imprescindível promover uma cultura regulatória robusta, com fiscalização ativa, aplicação de sanções dissuasórias e autonomia plena da ANPD.

O consentimento do usuário deve ser requalificado, exigindo-se que as interfaces sejam claras, acessíveis e alinhadas com os princípios da autodeterminação informativa. A transparência algorítmica precisa ser assegurada, com a obrigatoriedade de explicabilidade nas decisões automatizadas, conforme previsto no debate europeu sobre o "direito à explicação". Além disso, é fundamental fomentar a pesquisa e o desenvolvimento de soluções tecnológicas nacionais, de forma a garantir soberania digital e reduzir a dependência de grandes corporações transnacionais.

Nesse sentido, recomenda-se uma ação coordenada do Estado, do setor privado e da sociedade civil, voltada à construção de políticas públicas estruturantes que assegurem não apenas a proteção legal, mas também a proteção substantiva

dos dados pessoais. A dignidade da pessoa humana, a privacidade, a liberdade e a intimidade, previstos na Constituição Federal de 1988, devem ser reafirmados como princípios orientadores da era digital. Sem esse comprometimento institucional e social, seguiremos trocando a privacidade por comodidades tecnológicas e normalizando a erosão de direitos fundamentais no cotidiano digital.

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS – ANPD. **Análise preliminar do Projeto de Lei nº 2 338/2023, que dispõe sobre o uso da Inteligência Artificial**. Brasília: ANPD, 6 jul. 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-analise-preliminar-do-projeto-de-lei-no-2338-2023-que-dispoe-sobre-o-uso-da-inteligencia-artificial. Acesso em: 10 jul. 2025.

BONAVIDES, Paulo. **Curso de Direito Constitucional.** 35. ed. Salvador: Malheiros, 2020. 880 p.

CADWALLADR, Carole; GRAHAM-HARRISON, Emma. Revealed: 50 million **Facebook profiles harvested for Cambridge Analytica in major data breach.** The Guardian, 17 mar. 2018. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Acesso em: 20 jul. 2025.

COALIZÃO DIREITOS NA REDE; LAPIN. **Nota Técnica: PL 2338/2023 – Diretrizes para a regulação de Inteligência Artificial no Brasil**. [S. l.], 29 nov. 2024. Disponível em: https://direitosnarede.org.br/wp-content/uploads/2023/08/Nota-tecnica-PL-que-regula-a-IA.pdf. Acesso em: 13 jul. 2025.

CONTROLADORIA-GERAL DA UNIÃO – CGU. **Parecer CONJUR nº 177/2024**. Disponível em: https://repositorio.cgu.gov.br/bitstream/1/93365/1/Parecer_177_2024_CONJUR_CGU_AGU_tarjamento.pdf. Acesso em: 15 jul. 2025.

DENARDIS, Laura. **The global war for internet governance.** New Haven: Yale University Press, 2014. 320 p.

DONEDA, Danilo. **Da privacidade à proteção de dados**. 3. ed. São Paulo: Revista dos Tribunais, 2021.

EDELMAN, Lauren B. **Working law: courts, corporations, and symbolic civil rights.** Chicago: University of Chicago Press, 2016. 312 p.

FERREIRA, Juliano Cordeiro; PINHEIRO, Kerr Oliveira; MARQUES, Daniel Moreno Góis Rabêlo. **Termos de uso e políticas de privacidade das redes sociais on-line: uma análise sob a perspectiva do Direito à Informação.** Informação & Informação, Londrina, v. 26, n. 2, p. 307–328, maio/ago. 2021. Disponível em: https://repositorio.ufmg.br/bitstream/1843/51720/2/Termos%20de%20uso%20e%20pol%C3%ADticas%20de%20privacidade%20das%20redes%20sociais%20on-line.pdf?utm_source=chatgpt.com. Acesso em: 10 jul. 2025.

G1. **Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber**. [S. l.], 28 jan. 2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml. Acesso em: 15 jul. 2025.

GADONI CANAAN, **Renan. The effects on local innovation arising from replicating the GDPR into the Brazilian General Data Protection Law.** Internet Policy Review, v. 12, n. 1, fev. 2023. DOI: 10.14763/2023.1.1686. Disponível em: https://doi.org/10.14763/2023.1.1686. Acesso em: 20 jul. 2025.

HARVARD BUSINESS REVIEW. **Why data breaches spiked in 2023**. Boston: Harvard Business Publishing, 22 fev. 2024. Disponível em: https://hbr.org/2024/02/why-data-breaches-spiked-in-2023. Acesso em: 15 jul. 2025.

MARQUES, Daniel Góis Rabêlo. **Privacidade projetada, plataformas digitais e o sujeito-dado**: um estudo de caso dos problemas contemporâneos de privacidade a partir dos *smart speakers*. 2023. Tese (Doutorado em Comunicação e Cultura Contemporâneas) – Faculdade de Comunicação, Universidade Federal da Bahia, Salvador, 2023. Disponível em: https://repositorio.ufba.br/handle/ri/37284. Acesso em: 8 jul. 2025.

MARTÍNEZ DEVIA, Andrea. **La inteligencia artificial, el Big Data y la era digital: ¿una amenaza para los datos personales?.** Revista la Propiedad Inmaterial, Bogotá, n. 27, p. 5-23, enero/junio 2019. Disponível em: https://doi.org/10.18601/16571959.n27.01. Acesso em: 14 jan. 2025.

SENADO FEDERAL. Plenário. **Marco da inteligência artificial é aprovado em Plenário.** Brasília, 10 dez. 2024. Disponível em: https://www12.senado.leg.br/noticias/videos/2024/12/marco-da-inteligencia-artificial-e-aprovado-em-plenario-e-vai-a-camara. Acesso em: 20 jul. 2025.

DISTRITO FEDERAL (Distrito Federal). Tribunal de Justiça do Distrito Federal e dos Territórios. **LGPD: Justiça determina que Serasa deixe de comercializar dados pessoais**. Brasília, 20 jul. 2021. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/noticias/2021/julho/lgpd-justica-determina-que-serasa-deixe-de-comercializar-dados-pessoais. Acesso em: 15 jul. 2025.

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT (UNCTAD). **Data protection and privacy legislation worldwide**. Geneva: UNCTAD, 2023. Disponível em: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide. Acesso em: 14 jul. 2025.

WALDMAN, Ari Ezra. **Privacy law's false promise.** Washington University Law Review, Washington D.C, v. 97, n. 3, p. 773-834, 2020. Disponível em: https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=6386&context=law_lawreview. Acesso em: 14 jan. 2025.

ZUBOFF, Shoshana. **The age of surveillance capitalism: the fight for a human future at the new frontier of power.** New York: Public Affairs, 2019. 704 p.