

II ENCONTRO NACIONAL DE DIREITO DO FUTURO - II ENDIF

**DIREITOS HUMANOS E INTELIGÊNCIA
ARTIFICIAL**

D598

Direitos humanos e inteligência artificial [Recurso eletrônico on-line] organização II Encontro Nacional de Direito do Futuro: Escola Superior Dom Helder Câmara – Belo Horizonte;

Coordenadores: André Luiz Olivier da Silva e Wilson Engelmann– Belo Horizonte: Escola Superior Dom Helder Câmara - ESDHC, 2025.

Inclui bibliografia

ISBN: 978-65-5274-397-8

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

Tema: Justiça social e tecnológica em tempos de incerteza.

1. Direito do Futuro. 2. Justiça Social. 3. Justiça Tecnológica. I. II Encontro Nacional de Direito do Futuro (1:2025 : Belo Horizonte, MG).

CDU: 34



II ENCONTRO NACIONAL DE DIREITO DO FUTURO - II ENDIF

DIREITOS HUMANOS E INTELIGÊNCIA ARTIFICIAL

Apresentação

O II Encontro Nacional de Direito do Futuro (II ENDIF), organizado pelo Centro Universitário Dom Helder com apoio técnico do Conselho Nacional de Pesquisa e Pós-graduação em Direito – CONPEDI, reafirma-se como um espaço qualificado de produção, diálogo e circulação do conhecimento jurídico, reunindo a comunidade científica em torno de um propósito comum: pensar, com rigor metodológico e sensibilidade social, os caminhos do Direito diante das transformações que marcam o nosso tempo. Realizado nos dias 09 e 10 de outubro de 2025, em formato integralmente on-line, o evento assumiu como tema geral “Justiça social e tecnológica em tempos de incerteza”, convidando pesquisadoras e pesquisadores a enfrentar criticamente os impactos da inovação tecnológica, das novas dinâmicas sociais e das incertezas globais sobre as instituições jurídicas e os direitos fundamentais.

Nesta segunda edição, os números evidenciam a força do projeto acadêmico: 408 trabalhos submetidos, com a participação de 551 pesquisadoras e pesquisadores, provenientes de 21 Estados da Federação, culminando na organização de 31 e-books, que ora se apresentam à comunidade científica. Essa coletânea traduz, em linguagem acadêmica e compromisso público, a vitalidade de uma pesquisa jurídica que não se limita a descrever problemas, mas busca compreendê-los, explicar suas causas e projetar soluções coerentes com a Constituição, com os direitos humanos e com os desafios contemporâneos.

A publicação dos 31 e-books materializa um processo coletivo que articula pluralidade temática, densidade teórica e seriedade científica. Os textos que compõem a coletânea passaram por avaliação acadêmica orientada por critérios de qualidade e imparcialidade, com destaque para o método double blind peer review, que viabiliza a análise inominada dos trabalhos e exige o exame por, no mínimo, dois avaliadores, reduzindo subjetividades e preferências ideológicas. Essa opção metodológica é, ao mesmo tempo, um gesto de respeito à ciência e uma afirmação de que a pesquisa jurídica deve ser construída com transparência, responsabilidade e abertura ao escrutínio crítico.

O II ENDIF também se insere em uma trajetória institucional já consolidada: a primeira edição, realizada em junho de 2024, reuniu centenas de pesquisadoras e pesquisadores e resultou na publicação de uma coletânea expressiva, demonstrando que o Encontro se consolidou, desde o início, como um dos maiores eventos científicos jurídicos do país. A

continuidade do projeto, agora ampliada em escopo e capilaridade, reafirma a importância de se fortalecer ambientes acadêmicos capazes de integrar graduação e pós-graduação, formar novas gerações de pesquisadoras e pesquisadores e promover uma cultura jurídica comprometida com a realidade social.

A programação científica do evento, organizada em painéis temáticos pela manhã e Grupos de Trabalho no período da tarde, foi concebida para equilibrar reflexão teórica, debate público e socialização de pesquisas. Nos painéis, temas como inteligência artificial e direitos fundamentais, proteção ambiental no sistema interamericano, proteção de dados e herança digital foram tratados por especialistas convidados, em debates que ampliam repertórios e conectam a produção acadêmica aos dilemas concretos vividos pela sociedade.

A programação científica do II ENDIF foi estruturada em dois dias, 09 e 10 de outubro de 2025, combinando, no período da manhã, painéis temáticos com exposições de especialistas e debates, e, no período da tarde, sessões dos Grupos de Trabalho. No dia 09/10 (quinta-feira), após a abertura, às 09h, realizou-se o Painel I, dedicado aos desafios da atuação processual diante da inteligência artificial (“Inteligencia artificial y desafios de derechos fundamentales en el marco de la actuación procesal”), com exposição de Andrea Alarcón Peña (Colômbia) e debate conduzido por Caio Augusto Souza Lara. Em seguida, às 11h, ocorreu o Painel II, voltado à proteção ambiental no Sistema Interamericano, abordando a evolução da OC-23 ao novo marco da OC-32, com participação de Soledad Garcia Munoz (Espanha) e Valter Moura do Carmo como palestrantes, sob coordenação de Ricardo Stanziola Vieira. No período da tarde, das 14h às 17h, desenvolveram-se as atividades dos Grupos de Trabalho, em ambiente virtual, com apresentação e discussão das pesquisas aprovadas.

No dia 10/10 (sexta-feira), a programação manteve a organização: às 09h, foi realizado o Painel III, sobre LGPD e a importância da proteção de dados na sociedade de vigilância, com exposições de Laís Furuya e Júlia Mesquita e debate conduzido por Yuri Nathan da Costa Lannes; às 11h, ocorreu o Painel IV, dedicado ao tema da herança digital e à figura do inventariante digital, com apresentação de Felipe Assis Nakamoto e debate sob responsabilidade de Tais Mallmann Ramos. Encerrando o evento, novamente no turno da tarde, das 14h às 17h, seguiram-se as sessões dos Grupos de Trabalho on-line, consolidando o espaço de socialização, crítica acadêmica e amadurecimento das investigações apresentadas.

Ao tornar públicos estes 31 e-books, o II ENDIF reafirma uma convicção essencial: não há futuro democrático para o Direito sem pesquisa científica, sem debate qualificado e sem compromisso com a verdade metodológica. Em tempos de incerteza — tecnológica, social,

ambiental e institucional —, a pesquisa jurídica cumpre um papel civilizatório: ilumina problemas invisibilizados, questiona estruturas naturalizadas, qualifica políticas públicas, tensiona o poder com argumentos e oferece horizontes normativos mais justos.

Registrarmos, por fim, nosso reconhecimento a todas e todos que tornaram possível esta obra coletiva — autores, avaliadores, coordenadores de Grupos de Trabalho, debatedores e equipe organizadora —, bem como às instituições e redes acadêmicas que fortalecem o ecossistema da pesquisa em Direito. Que a leitura desta coletânea seja, ao mesmo tempo, um encontro com o que há de mais vivo na produção científica contemporânea e um convite a seguir construindo, com coragem intelectual e responsabilidade pública, um Direito à altura do nosso tempo.

Belo Horizonte-MG, 16 de dezembro de 2025.

Prof. Dr. Paulo Umberto Stumpf – Reitor do Centro Universitário Dom Helder

Prof. Dr. Franclim Jorge Sobral de Brito – Vice-Reitor e Pró-Reitor de Graduação do Centro Universitário Dom Helder

Prof. Dr. Caio Augusto Souza Lara – Pró-Reitor de Pesquisa do Centro Universitário Dom Helder

PRIVACIDADE E INOVAÇÃO TECNOLÓGICA: O DESCOMPASSO ENTRE A PROTEÇÃO DE DADOS E A CAPACIDADE REGULADORA DO DIREITO

PRIVACY AND TECHNOLOGICAL INNOVATION: THE MISMATCH BETWEEN DATA PROTECTION AND THE REGULATORY CAPACITY OF LAW

Bruna Ferreira Gomes

Resumo

Este trabalho analisa o descompasso entre a rápida evolução tecnológica e a capacidade regulatória do Direito, com foco na proteção da privacidade e dos dados pessoais. As inovações têm promovido novas formas de coleta e uso de informações sensíveis, muitas vezes superando os mecanismos jurídicos existentes. A partir de pesquisa bibliográfica e documental, discutem-se os desafios enfrentados pelos ordenamentos jurídicos para garantir direitos fundamentais sem comprometer a inovação. Propõe-se, ao final, uma abordagem normativa centrada na proteção por design, na proporcionalidade e na responsabilidade compartilhada entre Estado, setor privado e cidadãos como forma de enfrentamento dos riscos contemporâneos.

Palavras-chave: Privacidade, Proteção de dados, Inovação tecnológica

Abstract/Resumen/Résumé

This paper analyzes the mismatch between the rapid pace of technological advancement and the regulatory capacity of the law, with a focus on the protection of privacy and personal data. Innovations have introduced new ways of collecting and using sensitive information, often outpacing existing legal frameworks. Based on bibliographic and documentary research, the study discusses the challenges faced by legal systems in ensuring fundamental rights without hindering innovation. It concludes by proposing a normative approach centered on privacy by design, proportionality, and shared responsibility among the State, the private sector, and citizens as a way to address contemporary risks.

Keywords/Palabras-claves/Mots-clés: Privacy, Data protection, Technological innovation

INTRODUÇÃO

Vivemos em uma era de intensa digitalização, em que a coleta e o processamento de dados pessoais sustentam a nova economia, mas também impõe sérios desafios à proteção da privacidade, dado o descompasso entre a rápida evolução tecnológica e a resposta ainda reativa e fragmentada do Direito. O presente trabalho investiga como o ordenamento jurídico pode atuar de forma mais eficaz diante dessa transformação, buscando equilibrar a promoção da inovação com a salvaguarda dos direitos fundamentais. A pesquisa, de caráter qualitativo, fundamenta-se em revisão bibliográfica e documental, partindo da hipótese de que a regulação da privacidade deve ser prospectiva, dialogando com a complexidade tecnológica e responsabilizando os agentes do ecossistema digital.

2. ALGUNS ASPECTOS SOBRE A PRIVACIDADE

A privacidade tem passado por transformações significativas ao longo da história, moldada por fatores tecnológicos, culturais e jurídicos. Originalmente ligada à intimidade do lar e ao espaço físico, especialmente nas civilizações antigas, sua concepção evoluiu com a modernidade, passando a ser vista como um direito subjetivo. O marco teórico mais relevante desse processo foi a publicação de *The Right to Privacy*¹, que propôs a privacidade como um direito autônomo — o “direito de estar só”. A mistura entre o público e o privado, visível nas condições habitacionais e sociais até o século XIX, evidencia que o conceito de privacidade sempre refletiu as estruturas sociais de cada época.

Com o avanço das tecnologias, especialmente a fotografia, o jornalismo e, mais tarde, os sistemas digitais, novos desafios emergiram para a separação entre o público e o privado. Danilo Doneda² destaca que não há consenso sobre o que é privacidade ou o que constitui sua violação, justamente porque o conceito está diretamente condicionado ao estado da tecnologia vigente. Luciano Floridi³ observa que a privacidade se tornou uma questão ética central do nosso tempo, ainda que tenha sido pouco abordada em tratados filosóficos

¹WARREN, Samuel D.; BRANDEIS, Louis D. *The right to privacy*. Harvard Law Review, Cambridge, v. 4, n. 5, p. 193–220, Dec. 1890. Disponível em: <https://www.jstor.org/stable/1321160>. Acesso em: 14 maio 2025.

²DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Sequência: estudos jurídicos e políticos, Florianópolis, v. 34, n. 65, p. 19-38, jan./abr. 2013. Disponível em: <https://www.scielo.br/j/seq/a/ZNmgSYVR8kfvZGYWW7g6nJD/>. Acesso em: 04 maio 2025. p. 60.

³FLORIDI, Luciano. *The fourth revolution: How the infosphere is reshaping human reality*. OUP Oxford, 2014. p. 102.

anteriores. A chegada da era digital, portanto, impôs uma profunda reconfiguração no entendimento desse direito.

Hoje, diante da coleta massiva de dados por meio de plataformas digitais, *big data* e inteligência artificial, a privacidade ultrapassa a ideia de não intromissão para assumir o contorno de autodeterminação informacional — o poder de cada indivíduo decidir sobre o uso de seus dados pessoais. Como apontam Grassegger e Krogerus⁴, vivemos em uma sociedade onde tudo deixa rastros digitais, e esses dados são usados de formas cada vez mais sofisticadas, muitas vezes sem o conhecimento ou consentimento do usuário. Assim, a privacidade contemporânea se tornou um campo de tensão entre inovação tecnológica, interesses econômicos e a necessidade de proteção dos direitos fundamentais.

3. A PRIVACIDADE E OS DIREITOS FUNDAMENTAIS NA ERA DIGITAL

A privacidade é um direito fundamental reconhecido por diversos instrumentos jurídicos internacionais, como a Declaração Universal dos Direitos Humanos⁵ e o Pacto Internacional dos Direitos Civis e Políticos⁶, além da Constituição Federal de 1988⁷, que assegura a inviolabilidade da vida privada no Brasil. Com o avanço das tecnologias digitais, esse direito passou a demandar formas mais sofisticadas de proteção, diante de um cenário em que dados pessoais são coletados, processados e utilizados em larga escala por sistemas de inteligência artificial e pela economia digital.

⁴GRASSEGGER, Hannes; KROGERUS, Mikael. *The data that turned the world upside down*. Motherboard, 28 jan. 2017.

⁵Artigo 12º Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei. ORGANIZAÇÃO DAS NAÇÕES UNIDAS. *Declaração Universal dos Direitos Humanos*. Paris, 1948. Disponível em: <https://www.oas.org/dil/port/1948%20Declara%C3%A7%C3%A3o%20Universal%20dos%20Direitos%20Humanos.pdf>. Acesso em: 22 maio 2025.

⁶ARTIGO 17 1. Ninguém poderá ser objeto de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais às suas honra e reputação. 2. Toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas. BRASIL. *Decreto nº 592, de 6 de julho de 1992. Promulga o Pacto Internacional sobre Direitos Civis e Políticos*. Diário Oficial da União: seção 1, Brasília, DF, 7 jul. 1992. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm. Acesso em: 22 maio 2025.

⁷Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; BRASIL. *Constituição da República Federativa do Brasil de 1988*. Diário Oficial da União: seção 1, Brasília, DF, 5 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 22 maio 2025.

O uso de dados vai muito além das informações fornecidas diretamente pelos usuários, abrangendo também dados inferidos e preditivos, gerando perfis detalhados e previsões comportamentais. Esse tratamento massivo e opaco das informações, frequentemente utilizado para fins econômicos, securitários ou de controle social, impõe riscos significativos à privacidade, incluindo práticas discriminatórias e manipulação de preferências. A falta de transparência algorítmica, como aponta Frank Pasquale⁸, dificulta a contestação jurídica dessas práticas, pois os critérios utilizados para as decisões automatizadas muitas vezes são inacessíveis aos próprios afetados.

Nesse contexto, a privacidade precisa ser entendida não apenas como o direito de manter informações em sigilo, mas como autonomia informacional — a capacidade do indivíduo de controlar o destino de seus dados. Isso exige uma reconfiguração das estruturas regulatórias, com mecanismos que superem o consentimento meramente formal e garantam participação consciente dos usuários nas decisões sobre o uso de suas informações. A proteção da privacidade, portanto, torna-se elemento central na defesa da dignidade humana frente aos desafios impostos pela vigilância digital e pela assimetria entre usuários e sistemas automatizados.

4. A INOVAÇÃO TECNOLÓGICA E SEUS IMPACTOS DA PROTEÇÃO DE DADOS

A inovação tecnológica, impulsionada por *big data*, Internet das Coisas (IoT), inteligência artificial (IA), biometria e sistemas autônomos, ampliou drasticamente a capacidade de coleta e tratamento de dados pessoais. Dispositivos como celulares, assistentes virtuais, câmeras inteligentes e redes sociais operam como instrumentos contínuos de vigilância, desafiando os modelos clássicos de proteção da privacidade. A IoT, conforme definem Bruno Santos⁹ e Eduardo Magrani¹⁰, representa um ecossistema de objetos físicos conectados à internet por meio de sensores, capazes de oferecer serviços, gerar dados em tempo real e otimizar tarefas cotidianas — o que amplia oportunidades, mas também os riscos técnicos, sociais e jurídicos.

A combinação entre IA e IoT potencializa a coleta e análise de dados, permitindo a criação de perfis comportamentais altamente precisos. A IA, alimentada por informações

⁸PASQUALE, Frank. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press, 2015.

⁹SANTOS, Bruno P. et al. *Internet das Coisas: da teoria à prática*. Belo Horizonte: Departamento de Ciência da Computação, Universidade Federal de Minas Gerais, [s.d.].

¹⁰MAGRANI, Eduardo. *A internet das coisas*. Rio de Janeiro: FGV Editora, 2018. p. 20.

captadas continuamente por dispositivos conectados — como eletrodomésticos, veículos, relógios inteligentes e outros sensores — pode personalizar serviços, mas também manipular escolhas, reforçar desigualdades ou limitar oportunidades com base em inferências estatísticas. Como destaca Maria das Graças Araújo¹¹, a IA é essencial à IoT, pois transforma dados brutos em conhecimento e decisões automatizadas. No entanto, essa integração inviabiliza os limites entre o público e o privado, exigindo novas abordagens regulatórias que contemplam transparência, governança e respeito aos direitos fundamentais.

A dinâmica acelerada da inovação nem sempre incorpora a privacidade desde a concepção dos produtos (*privacy by design*¹²). Muitas empresas adotam modelos baseados em coleta extensiva de dados, com consentimentos genéricos e interfaces pouco claras, o que contribui para a naturalização da vigilância. Além disso, a utilização de algoritmos em decisões automatizadas — como crédito, triagens de currículos ou políticas públicas — introduz riscos de discriminação, especialmente quando se baseiam, direta ou indiretamente, em dados sensíveis. A ausência de transparência e de mecanismos de responsabilização (*accountability*¹³) compromete a legitimidade desses processos, exigindo um debate ético e jurídico urgente.

5. O DESCOMPASSO ENTRE O DIREITO E A TECNOLOGIA: LIMITES DA REGULAÇÃO TRADICIONAL

O Direito, tradicionalmente reativo, mostra-se insuficiente diante da velocidade das transformações tecnológicas. A complexidade dos sistemas digitais, somada à falta de previsibilidade legislativa, cria lacunas que dificultam a proteção efetiva da privacidade.

¹¹ARAÚJO, Maria das Graças; MORAES, Jorge Luiz Abreu. *Inteligência artificial na internet das coisas*. Disponível em: <http://revista.universo.edu.br/index.php?journal=1reta2&page=article&op=view&path%5B%5D=7634&path%5B%5D=3791>. Acesso em: 20 maio 2025.

¹²*Privacy by design* (é a preocupação com a privacidade dos dados desde a concepção de qualquer novo projeto ou serviço) diz respeito ao emprego de meios para se preservar a privacidade durante todo o ciclo de vida dos dados pessoais. No caso, a privacidade é base para a arquitetura dos sistemas e processos desenvolvidos, de modo a possibilitar, pelo formato disponibilizado e pelo serviço prestado, condições que permitam ao titular de dados pessoais preservar a sua privacidade e o formato em que ocorre o tratamento dos seus dados. TERRACAP. *O que é privacy by design e privacy by default?* Disponível em: <https://www.terracap.df.gov.br/index.php/listagem-faq/78-lgpd-lei-geral-de-protecao-de-dados-pessoais/196-53-o-que-e-privacy-by-design-e-privacy-by-default>. Acesso em: 20 maio 2025.

¹³*Accountability* é um termo inglês utilizado para descrever as práticas relacionadas à prestação de contas. O conceito também tem um entendimento mais amplo, sendo muitas vezes utilizado como sinônimo de controle, responsabilidade, transparência e fiscalização. CNN BRASIL. *Accountability: o que é e como aplicar nas empresas?*. São Paulo, 15 dez. 2022. Disponível em: <https://www.cnnbrasil.com.br/economia/microeconomia/o-que-e-accountability-conheca-o-termo-que-ajuda-a-epensar-direitos-e-deveres/>. Acesso em: 20 maio 2025.

Embora a LGPD¹⁴ no Brasil e o GDPR¹⁵ na União Europeia representem avanços importantes, ainda enfrentam desafios práticos, como a fiscalização limitada, a assimetria informacional entre usuários e plataformas e a dificuldade de responsabilização por decisões automatizadas e pelo uso de dados inferenciais. A criação da Autoridade Nacional de Proteção de Dados (ANPD) é um passo relevante, mas ainda não cobre de forma abrangente os riscos trazidos pela inteligência artificial e pela Internet das Coisas (IoT).

Nesse cenário, alternativas como a regulação responsável e a co-regulação ganham força, propondo normas construídas em diálogo com os setores regulados e com foco na transparência e conformidade dinâmica. A IoT e a IA, ao transformarem objetos do cotidiano em dispositivos conectados, tornam urgente o desenvolvimento de uma governança ética e jurídica que preserve os direitos fundamentais. A adoção dos Princípios Orientadores da ONU sobre Empresas e Direitos Humanos (UNGPs) surge como um referencial adequado para guiar Estados e empresas na promoção da responsabilidade compartilhada e na construção de um ecossistema digital seguro e digno. Isso inclui o dever estatal de proteger, a responsabilidade empresarial de respeitar os direitos humanos e a existência de mecanismos eficazes de reparação.

A atuação coordenada entre governos e setor privado deve incluir estratégias técnicas e políticas para garantir a segurança e a privacidade desde a concepção dos produtos (*privacy by design*). Isso envolve avaliações de risco, categorização de dispositivos conforme vulnerabilidades e disseminação no mercado, além de boas práticas no desenvolvimento de software, como atualizações contínuas, gestão de identidades e canais permanentes para notificação de falhas. Também é essencial uma estrutura normativa clara, capaz de assegurar o consentimento informado, o acesso e a exclusão de dados pessoais, além da limitação da coleta ao estritamente necessário. O setor privado, por sua vez, deve adotar compromissos explícitos com os direitos humanos, realizar due diligence e prestar contas de seus impactos.

Para enfrentar os desafios impostos pela digitalização, é imprescindível repensar os instrumentos jurídicos e incorporar a proteção de dados como elemento estrutural das tecnologias emergentes. A educação digital da população deve ser fomentada, garantindo que

¹⁴BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet)*. Diário Oficial da União: seção 1, Brasília, DF, ano 155, n. 157, p. 59-64, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 maio 2025.

¹⁵GDPR-INFO.EU. General Data Protection Regulation (GDPR). Disponível em: <https://gdpr-info.eu/>. Acesso em: 14 maio 2025.

os cidadãos conheçam seus direitos e possam exercê-los de forma consciente. Autoridades reguladoras precisam de autonomia, estrutura técnica e poder fiscalizador eficaz. A transparência dos sistemas automatizados deve ser compatível com a proteção de dados, por meio de soluções como explicação seletiva e computação segura. Por fim, a regulação deve ser orientada por riscos, proporcionalidade e responsabilidade compartilhada, com participação ativa do Estado, das empresas e da sociedade civil.

CONCLUSÃO

O presente trabalho demonstrou que o descompasso entre a velocidade da inovação tecnológica e a resposta do Direito representa um dos principais desafios contemporâneos à proteção da privacidade. Tecnologias emergentes como inteligência artificial, big data, Internet das Coisas e sistemas de vigilância automatizados operam com complexidade e opacidade, frequentemente escapando das estruturas normativas tradicionais, baseadas no consentimento formal e na responsabilização posterior ao dano. Essa realidade amplia os riscos de violações sistêmicas e silenciosas à privacidade, exigindo uma mudança de paradigma: é preciso pensar preventivamente, incorporando salvaguardas desde a concepção das tecnologias e promovendo a autodeterminação informacional como um direito central na sociedade digital.

Diante desse cenário, torna-se urgente a adoção de uma regulação jurídica prospectiva, integrada e orientada por princípios como o da proteção por design (privacy by design), que exige que a privacidade esteja presente desde o início do desenvolvimento tecnológico. Paralelamente, é fundamental investir em políticas públicas de educação digital crítica e garantir a atuação autônoma, técnica e efetiva das autoridades de proteção de dados. A cooperação internacional entre Estados, empresas e sociedade civil é igualmente indispensável para enfrentar os desafios globais da privacidade. Conclui-se que o equilíbrio entre inovação e proteção de dados não apenas é possível, mas necessário para consolidar um ecossistema digital ético, seguro e comprometido com a dignidade humana.

REFERÊNCIAS BIBLIOGRÁFICAS

- ARAÚJO**, Maria das Graças; MORAES, Jorge Luiz Abreu. *Inteligência artificial na internet das coisas.* Disponível em: <http://revista.universo.edu.br/index.php?journal=1reta2&page=article&op=view&path%5B%5D=7634&path%5B%5D=3791>. Acesso em: 20 maio 2025.

BELLI, Luca. *Uma perspectiva de direitos humanos para decriptar a ascensão da Internet das Coisas (IoT)*. Revista Brasileira de Direitos Fundamentais e Justiça, Belo Horizonte: Fórum, ano 13, n. 41, p. 157–181, jul./dez. 2019. Disponível em: <https://hdl.handle.net/20.500.12178/169014>. Acesso em: 20 maio 2025.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Diário Oficial da União: seção 1, Brasília, DF, 5 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constiticao/constituicao.htm. Acesso em: 22 maio 2025.

_____. *Decreto nº 592, de 6 de julho de 1992. Promulga o Pacto Internacional sobre Direitos Civis e Políticos*. Diário Oficial da União: seção 1, Brasília, DF, 7 jul. 1992. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm. Acesso em: 22 maio 2025.

_____. *Lei nº 13.709, de 14 de agosto de 2018*. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, ano 155, n. 157, p. 59-64, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 maio 2025.

CNN BRASIL. *Accountability: o que é e como aplicar nas empresas?*. São Paulo, 15 dez. 2022. Disponível em: <https://www.cnnbrasil.com.br/economia/macroeconomia/o-que-e-accountability-conheca-o-temo-que-ajuda-a-repensar-direitos-e-deveres/>. Acesso em: 20 maio 2025.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Sequência: estudos jurídicos e políticos, Florianópolis, v. 34, n. 65, p. 19-38, jan./abr. 2013. Disponível em: <https://www.scielo.br/j/seq/a/ZNmgSYVR8kfVZGYWW7g6nJD/>. Acesso em: 04 maio 2025.

GRASSEGGER, Hannes; KROGERUS, Mikael. *The data that turned the world upside down*. Motherboard, 28 jan. 2017.

MAGRANI, Eduardo. *A internet das coisas*. Rio de Janeiro: FGV Editora, 2018.

GDPR-INFO.EU. *General Data Protection Regulation (GDPR)*. Disponível em: <https://gdpr-info.eu/>. Acesso em: 14 maio 2025.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. *Declaração Universal dos Direitos Humanos*. Paris, 1948. Disponível em: <https://www.oas.org/dil/port/1948%20Declara%C3%A7%C3%A3o%20Universal%20dos%20Direitos%20Humanos.pdf>. Acesso em: 22 maio 2025.

PALO ALTO NETWORKS. *What Is Explainable AI (XAI)?* Disponível em: <https://www.paloaltonetworks.com/cyberpedia/explainable-ai>. Acesso em: 16 maio 2025.

PASQUALE, Frank. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press, 2015.

SANTOS, Bruno P. et al. *Internet das Coisas: da teoria à prática*. Belo Horizonte: Departamento de Ciência da Computação, Universidade Federal de Minas Gerais, [s.d.].

TERRACAP. *O que é privacy by design e privacy by default?* Disponível em: <https://www.terracap.df.gov.br/index.php/listagem-faq/78-lgpd-lei-geral-de-protecao-de-dados-pessoais/196-53-o-que-e-privacy-by-design-e-privacy-by-default>. Acesso em: 20 maio 2025.

WARREN, Samuel D.; **BRANDEIS**, Louis D. *The right to privacy*. Harvard Law Review, Cambridge, v. 4, n. 5, p. 193–220, Dec. 1890. Disponível em: <https://www.jstor.org/stable/1321160>. Acesso em: 14 maio 2025.