# II ENCONTRO NACIONAL DE DIREITO DO FUTURO - II ENDIF

## INTELIGÊNCIA ARTIFICIAL, DIREITO E REGULAÇÃO I

I61
Inteligência artificial, direito e regulação I [Recurso eletrônico on-line] organização II Encontro Nacional de Direito do Futuro: Escola Superior Dom Helder Câmara – Belo Horizonte;

Coordenadores: Marco Antônio Sousa Alves e Fernanda dos Santos Rodrigues Silva – Belo Horizonte: Escola Superior Dom Helder Câmara - ESDHC, 2025.

Inclui bibliografia
ISBN: 978-65-5274-403-6
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

Dom Helder
CENTRO UNIVERSITÁRIO

# II ENCONTRO NACIONAL DE DIREITO DO FUTURO - II ENDIF

## INTELIGÊNCIA ARTIFICIAL, DIREITO E REGULAÇÃO I

## 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.

Registramos, 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

# DA SUPERFÍCIE AO SUBMUNDO: ANÁLISE DA POSSÍVEL NORMALIZAÇÃO DOS VAZAMENTOS MASSIVOS DE DADOS PESSOAIS NA INTERNET E O ESVAZIAMENTO DA PROTEÇÃO DIGITAL NO BRASIL

# FROM THE SURFACE TO THE UNDERWORLD: ANALYSIS OF THE POSSIBLE NORMALIZATION OF MASSIVE LEAKS OF PERSONAL DATA ON THE INTERNET AND THE EMPTYING OF DIGITAL PROTECTION IN BRAZIL

**Maria Luisa Moreira Da Silva**
**Marcus Vinícius Nogueira Rebouças**

**Resumo**

Este trabalho analisa a possível normalização dos vazamentos de dados pessoais na internet, destacando a conivência de empresas privadas e a fragilidade do controle normativo no Brasil. Apesar das legislações recentes sobre proteção de dados, há lacunas entre sua existência formal e aplicação efetiva. A comercialização recorrente de informações sensíveis, inclusive na dark web, evidencia vulnerabilidade informacional e impunidade. Com metodologia bibliográfica e documental, e abordagem qualitativa, o estudo busca compreender os impactos sociais, jurídicos e institucionais da exposição de dados e os desafios à responsabilização civil.

**Palavras-chave:** Privacidade digital, Proteção de dados, Responsabilização civil, Vazamento de dados pessoais

**Abstract/Resumen/Résumé**

This paper analyzes the possible normalization of personal data leaks on the internet, highlighting the connivance of private companies and the fragility of regulatory control in Brazil. Despite recent legislation on data protection, there are gaps between its formal existence and effective application. The recurring commercialization of sensitive information, including on the dark web, highlights informational vulnerability and impunity. Using bibliographic and documentary methodology, and a qualitative approach, the study seeks to understand the social, legal and institutional impacts of data exposure and the challenges to civil liability.

**Keywords/Palabras-claves/Mots-clés:** Digital privacy, Data protection, Civil liability, Leakage of personal data

**INTRODUÇÃO:**

O presente trabalho visa analisar a normalização, no âmbito social, jurídico e institucional, dos recorrentes vazamentos de dados pessoais na internet, com foco na atuação de empresas privadas e na fragilidade do controle normativo. Nesse cenário, estabelece-se um espaço fértil para a prática de crimes cibernéticos, omissão de dados e comercialização indevida de informações sensíveis, revelando a ineficácia dos instrumentos de proteção até então implementados. Embora as legislações voltadas à proteção de dados sejam recentes, nota-se uma lacuna entre sua existência formal e a efetividade na contenção dessas práticas. A relação intrínseca entre redes de comercialização de dados e a marginalização dos usuários evidencia o esvaziamento de propostas voltadas ao controle e à fiscalização, o que fragiliza a proteção digital e dificulta a consolidação de políticas públicas eficientes. As empresas, ainda que formalmente responsáveis pela gestão das informações, por vezes participam da sua exposição ou venda, direta ou indiretamente. Soma-se a isso o uso da *dark web*, não apenas como canal de venda de dados sensíveis, mas como instrumento de vigilância e controle sobre a vida digital dos usuários. A metodologia adotada baseia-se em estudo bibliográfico, análise documental e legislativa, com abordagem qualitativa. O objetivo é compreender os impactos sociais, políticos e institucionais decorrentes do vazamento de dados, especialmente quanto à responsabilização civil e à vulnerabilidade informacional dos usuários, que, muitas vezes, sequer compreendem seus direitos ou sabem como reagir diante da violação de sua privacidade.

**OBJETIVOS:**

O propósito deste trabalho é analisar a relação entre o vazamento de dados tratados por empresas privadas e as recorrentes condutas de omissão, conivência ou participação direta dessas instituições na comercialização indevida de informações sensíveis. Busca-se também compreender as fragilidades enfrentadas pelos usuários, que rotineiramente têm seus dados solicitados, expostos ou utilizados de forma indevida, sendo vítimas de golpes e crimes digitais. Por fim, pretende-se avaliar os impactos sociais da exposição informacional, com destaque para a marginalização dos usuários diante da ineficácia institucional no combate a tais práticas.

**METODOLOGIA:**

A metodologia aplicada neste trabalho é de natureza bibliográfica e documental, envolvendo a leitura e análise de livros, doutrinas e artigos relacionados à temática proposta.

Além disso, a pesquisa adota uma abordagem qualitativa, com o propósito de avaliar argumentos e evidências relevantes para a construção do estudo.

**DESENVOLVIMENTO:**

O tratamento de dados pessoais sensíveis está diretamente relacionado à violação da esfera íntima do indivíduo, sobretudo quando esses dados são utilizados sem consentimento e resultam em danos morais. Esses danos se caracterizam pela afetação subjetiva, pessoal e psicológica do titular dos dados, sendo agravados pela exposição indevida das suas informações.

A responsabilização civil, nesse contexto, assume caráter objetivo, conforme previsto no artigo 42 da Lei Geral de Proteção de Dados Pessoais - LGPD - (Brasil2, 2018). Nesse tipo de responsabilidade, não se exige a demonstração de culpa do agente, bastando a comprovação do dano e do nexo de causalidade. No entanto, a própria LGPD prevê hipóteses excludentes, o que tem permitido às empresas alegarem, muitas vezes com êxito, que o vazamento decorreu de ação de terceiros, buscando assim afastar sua responsabilidade.

A Emenda Constitucional n°115/2022, no artigo 5°, LXXIX, da Constituição Federal, a proteção dos dados pessoais entre os direitos e garantias fundamentais. Essa inclusão consolida a competência privativa da União para legislar sobre a privacidade e proteção de dados (Brasil1, 2022). Entretanto, essa proteção ainda não foi plenamente internalizada ao observar

Além disso, observa-se um comportamento social de aceitação e comodidade diante da exposição de dados. A população, em geral, desconhece seus direitos e limita-se a tentar reparar prejuízos por meio da contestação de compras ou transações indevidas, sem questionar a origem da violação. As empresas, por sua vez, tratam os dados como objetos de troca, desconsiderando o seu caráter sensível e a necessidade de proteção.

Bauman (2014) menciona que esse processo de objetificação do indivíduo, em que os dados pessoais passam a ser não apenas instrumentos de vigilância, mas também de poder e controle. A marginalização do sujeito se dá justamente quando ele perde o domínio sobre suas informações, tornando-se vulnerável a sistemas que o manipulam, silenciam e expõem.

Do ponto de vista jurisprudencial, observa-se um padrão preocupante: empresas frequentemente alegam que os vazamentos ocorreram por responsabilidade de terceiros — como hackers ou falhas externas — e não por falha própria. Tal argumento vem sendo acolhido por decisões judiciais, com base no Código Civil, que admite a exclusão de responsabilidade quando o dano decorre exclusivamente de fato de terceiro (Brasil4, 2002).

Contudo, é necessário observar que, diante da LGPD e do Código de Defesa do Consumidor (CDC), esse argumento exige análise específica, caso a caso, sobretudo considerando a relação de confiança entre o titular dos dados e a empresa que os armazena.

Mesmo com a previsão legal da responsabilização objetiva, as empresas continuam utilizando o CDC e o Código Civil como formas de minimizar sua responsabilização, o que revela uma prática de fuga institucional. Isso é ainda mais preocupante quando se constata que os próprios dados compartilhados voluntariamente pelos usuários — como nome completo, CPF, RG, data e local de nascimento, preferências pessoais — são classificados por decisões judiciais como "não sensíveis", ignorando o fato de que tais informações, uma vez expostas, adquirem caráter sensível por sua capacidade de gerar risco, discriminação ou dano.

Segundo Couto (2022), há uma incongruência entre o que se entende por dado sensível na prática judicial e os efeitos reais da exposição dessas informações. Muitas decisões não reconhecem a gravidade de tais vazamentos, dificultando a reparação e ampliando a sensação de impunidade.

Além disso, a LGPD enfatiza a prevenção como medida essencial. Lima (2024) destaca que a prevenção é um dever imposto às empresas e aos agentes de tratamento de dados, exigindo a adoção de mecanismos de segurança para evitar a ocorrência de danos. A negligência nesse sentido configura falha grave, especialmente quando combinada com vazamentos decorrentes de ataques cibernéticos, falhas sistêmicas ou omissão institucional.

Outro marco importante é o Marco Civil da Internet (Lei nº 12.965/2014), que também traz princípios de proteção à privacidade, mas esbarra, na prática, na dificuldade de rastrear responsáveis e na limitação das ferramentas legais tradicionais, sobretudo diante da velocidade e volume das infrações digitais (Brasil3, 2014).

Dessa forma, embora haja um arcabouço legal que regulamenta a proteção de dados no Brasil, o que se percebe na prática é a fragilidade da aplicação desses instrumentos. Os dados pessoais seguem sendo expostos, comercializados e tratados como mercadoria, ao passo que os mecanismos de responsabilização permanecem frágeis, permitindo a perpetuação de práticas abusivas sob uma falsa aparência de legalidade.

## RESULTADOS E DISCUSSÕES:

Constata-se um padrão consolidado de impunidade nas alegações das empresas quanto à responsabilidade por vazamentos de dados pessoais. A justificativa recorrente é a atuação de terceiros, o que transfere a responsabilidade para fora das estruturas empresariais, blindando-as juridicamente. No entanto, a realidade mostra que os dados da população são

tratados como mercadoria de troca — coletados, armazenados e vendidos como ativos econômicos. Trata-se de uma dinâmica que ultrapassa falhas pontuais e revela uma lógica sistematizada de dominação informacional.

No plano social, vive-se a naturalização da exposição informacional. As pessoas, em sua maioria, não questionam os mecanismos por trás da coleta de seus dados. Isso se dá pela falsa sensação de segurança construída a partir de contratos de adesão, termos de uso extensos e linguagem técnica que mascaram cláusulas permissivas de comercialização. A confiança do usuário é instrumentalizada pelas empresas, que se utilizam de brechas legais, falta de fiscalização e omissão institucional para ampliar seu domínio sobre as informações pessoais.

Essa estrutura de manipulação tem na *dark web* sua expressão mais agressiva. Segundo Jesus Filho (2024), a *dark web* atua como um ecossistema de disseminação de dados ilícitos, valendo-se de links maliciosos, engenharia social e mecanismos de rastreamento para controlar, manipular e comercializar informações sensíveis. O que começa com o próprio usuário fornecendo dados de forma passiva — muitas vezes sem consciência do alcance disso — termina em um ciclo de vigilância, monetização e violação.

Essa realidade demonstra uma hierarquia informacional em que os usuários se tornam alvos manipuláveis, enquanto as empresas exercem um poder estrutural sustentado por tecnologia, contratos e omissões jurídicas. Quando a responsabilização é exigida judicialmente, muitas vezes as decisões acolhem as alegações empresariais de ausência de culpa, invocando o Código Civil para justificar a exclusão da responsabilidade com base em fatos atribuídos a terceiros. Ainda assim, as informações foram, de início, disponibilizadas pelas próprias empresas, que têm obrigação legal de protegê-las.

Essa omissão ganha contornos de estrutura criminosa. Como você mencionou, há indícios de que funcionários internos, conscientemente ou não, repassam dados a terceiros. Isso desenha uma engrenagem de mercado ilícito que, embora disfarçada de legalidade, funciona à semelhança de organizações criminosas — com canais, fluxos, agentes e beneficiários. A sociedade, nesse processo, encontra-se aprisionada em uma espécie de ciclo de inércia informacional, no qual os riscos — como fraudes, falsidade ideológica, chantagens e danos morais — são sistematicamente ignorados.

Ainda que existam leis como a LGPD e o Marco Civil da Internet, a ausência de rigor na fiscalização e a conivência institucional — seja por lentidão judicial, seja por interpretações que desqualificam a gravidade dos dados vazados — reforçam esse sistema de impunidade. Conforme alertado por Borges (2021, p. 11), “os dados pessoais são coletados e analisados de maneira automática pela inteligência do programa sob a justificativa de que as

informações dos usuários são necessárias para melhorar sua experiência". Tal discurso serve como álibi técnico para legitimar uma prática de vigilância contínua e lucrativa, baseada na dependência tecnológica e na submissão informacional.

As empresas se beneficiam da ausência de regulação firme e da falta de adequação estrutural para responder criminal ou civilmente pelos danos causados. Elas transformam os dados dos usuários em fontes de renda e controle. Com o avanço das tecnologias, especialmente a inteligência artificial, as redes sociais e os aplicativos de uso cotidiano, o usuário é induzido a se expor continuamente. Torna-se, assim, um sujeito desprovido de autonomia, entregue a sistemas que o monitoram, preveem seus comportamentos e o moldam conforme interesses econômicos.

Nesse sentido, os vazamentos de dados deixam de ser incidentes isolados para se tornarem expressão de uma estrutura sustentada pela permissividade jurídica, pela ignorância coletiva e por um modelo digital centrado na exploração do usuário. A marginalização informacional é real, estrutural e sistêmica. A sociedade, ao não reagir, apenas perpetua o ciclo. E, como você apontou com exatidão, talvez só se perceba a gravidade dessa violação quando as consequências se tornarem insuportáveis, como em contextos de exceção, golpes ou crises institucionais — lembrando o efeito de inércia social que precedeu momentos históricos graves, como o golpe de Collor de Mello.

**CONCLUSÃO**:

A realidade digital contemporânea revela uma distopia informacional, na qual dados pessoais são veiculados, comercializados e manipulados sob o pretexto da legalidade, enquanto se perpetua a impunidade institucional. As estruturas jurídicas, ao generalizarem a responsabilidade das empresas e acolherem argumentos frágeis sobre a culpa de terceiros, acabam por esvaziar o sentido de proteção da intimidade e da privacidade.

Mesmo com a vigência de marcos legais como o Código Civil, o Código de Defesa do Consumidor e a Lei Geral de Proteção de Dados (LGPD), a atuação do Judiciário demonstra ineficácia e, por vezes, conivência com a lógica de exploração digital. A consequência é a perpetuação de práticas abusivas, legitimadas por contratos de adesão e políticas opacas que não garantem qualquer controle real ao titular dos dados.

Portanto, não basta a existência formal de leis. É necessária a reformulação crítica e prática dos mecanismos de responsabilização e fiscalização, com vistas à proteção efetiva do usuário e ao enfrentamento da mercantilização da informação. Sem isso, seguirá a falsa

aparência de legalidade que encobre um sistema de exploração estrutural, no qual o sujeito é reduzido a um dado, e a dignidade é substituída por algoritmos de lucro.

**REFERÊNCIAS:**


BAUMAN, Zygmunt. **Vigilancia líquida**. Editora Schwarcz-Companhia das Letras, 2014.

BORGES, Maria Emília Orrico Pinheiro. **Os direitos da personalidade e a privacidade na era digital.** 2021.

BRASIL1. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022.** Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. [S. l.], 10 fev. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 8 jul. 2025.

BRASIL2. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). [S. l.], 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 8 jul. 2025.

BRASIL3. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União: seção 1, Brasília, DF, ano 151, n. 78, p. 1, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 8 jul. 2025.

BRASIL4. **Lei nº 10.406, de 10 de janeiro de 2002.** Institui o Código Civil. Diário Oficial da União: Brasília, DF, 10 jan. 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 8 jul. 2025.

COUTO, J. H. O. Vazamentos de dados e dano moral ’in re ipsa’: comentários ao Agravo em Recurso Especial nº 2.130.619/SP. **Revista IBERC**, Belo Horizonte, v. 6, n. 2, p. 171–188, 2023. DOI: 10.37963/iberc.v6i2.258. Disponível em: https://revistaiberc.responsabilidadecivil.org/iberc/article/view/258. Acesso em: 8 jul. 2025.

JESUS FILHO, Sebastião Alves de et al. **Identificação de posts maliciosos na dark web utilizando Aprendizado de Máquina Supervisionado.** 2024

LIMA, G. F. de, & Bandeira, L. S. de O. A (IM)POSSIBILIDADE DO RECONHECIMENTO DO DANO PRESUMIDO POR VAZAMENTO DE DADOS PESSOAIS. **Revista Contemporânea**, *4*(10), e6145. 2024. https://doi.org/10.56083/RCV4N10-095