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

Dom Helder
CENTRO UNIVERSITÁRIO

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.

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

O PERIGO DA FALTA DE FISCALIZAÇÃO DA IA E O DIREITO À PRIVACIDADE

THE DANGER OF A LACK OF IA MONITORING AND THE RIGHT TO PRIVACY

Sarah Brito e Souza

Resumo

A IA tem seu início datado no século XX, com o fim de propiciar maior praticidade em determinadas funções. Todavia, no cenário atual, há o distanciamento desses objetivos, sendo essa questão o objeto de estudo dessa dissertação, que é pautada no método dedutivo. Dessa forma, foram realizadas pesquisas sobre a temática, mediante diversas fontes e materiais. Diante disso, concluiu-se que o tema não somente impacta no âmbito jurídico, mas também no social.

Palavras-chave: Ia, Violação, Vazamento

Abstract/Resumen/Résumé

IA began in the 20th century with the aim of making certain functions more practical. However, in the current scenario, there is a move away from these objectives, and this issue is the object of study of this dissertation, which is based on the deductive method. Research was therefore carried out on the subject, using various sources and materials. As a result, it was concluded that the issue not only has an impact on the legal sphere, but also on the social sphere.

Keywords/Palabras-claves/Mots-clés: Ia, Violation, Leakage

1 Considerações Iniciais

O direito à privacidade é um dos direitos fundamentais mais essenciais e pode ter um aspecto positivo e negativo. O direito à privacidade, como um direito positivo, é aquele no qual há a exigência de que o Estado proteja a privacidade dos brasileiros, por exemplo, evitando o vazamento de seus dados. Já no âmbito negativo, cabe explicar que se trata do dever do Estado de não interferir em certas esferas da vida pessoal, bem como o dever dele de criar meios para evitar a interferência de terceiros em aspectos pessoais e privados de sua vida. Ademais, salienta-se que tal direito está contemplado em inúmeras legislações e normas, como: no art. 5°, no inciso X, da CF/88; no art.21º, do CC/2002; na Lei 13.709/2018 (LGPD) e no art.12º da DUDH.

A IA é um sistema que, através da identificação de padrões, pode realizar tarefas, como cálculos, pesquisas e criação de imagens, mas ela tende a errar na maioria das vezes, conforme dados do CJR (2025), em que se afirma que as "IAs tendem a errar em 60% das buscas por citações de notícias". Ela também pode ser dividida em genérica e especialista, sendo a primeira aquela na qual há a realização de várias tarefas, com menor complexidade, como o próprio ChatGPT, já a segunda é aquela na qual há a realização de tarefas complexas que exigem algoritmos mais sofisticados, como o AlphaFold (ferramenta usada para auxiliar na produção de medicamentos e que já é sinônimo de avanço na área farmacêutica).

Todavia, apesar dessas normas e dos benefícios fornecidos por esses sistemas, a violação do direito à privacidade tem se tornado frequente, principalmente através do uso de IA por seres humanos e por sistemas autônomos sem supervisão humana, até mesmo contra pessoas jurídicas, comprova-se tal afirmação por meio de dados do G1 (2025), nos quais se indica que houve o atentado a 60% dos dados de empresas em decorrência de IA' s de mercado.

A presente dissertação visa compreender de maneira clara e significativa o quão grave é a presente situação de falta de cumprimento das normas da LGPD no uso da IA, bem como compreender o impacto disso ao nível social e jurídico, para tal fim foi empregada uma metodologia direcionada para pesquisa qualitativa, descritiva e explicativa, bem como o método dedutivo.

Ademais, pretende-se evidenciar também a falta de fiscalização efetiva frente a essas ferramentas e mostrar a pertinência de se ampliar as fiscalizações a elas e de se ter uma maior transparência com os seus usuários sobre o uso de dados deles, a fim de haver uma segurança maior para os indivíduos e empresas e o real cumprimento da norma mencionada anteriormente.

2 (A Falta do) Direito à Privacidade e a IA

Em primeira análise, deve-se afirmar que a IA traz muitas vantagens consigo, como a verificação de informações de forma rápida, contudo isso não omite os prejuízos que ela tem trazido, como um dos problemas da sociedade, que acontecem na era tecnológica: a violação do direito à privacidade. Corrobora-se tal afirmação por meio do caso que ocorreu em BH, com jovens que tiveram fotos íntimas falsas, feitas por IA, publicadas em redes sociais por colegas de colégio, neste ano (G1, 2025). Ou seja, além de passarem pelo constrangimento de serem expostas em redes sociais com fotos desse tipo, ainda eram fotos falsas, que uma IA, que deveria ajudar no desenvolvimento de pesquisas, fez.

Sendo assim, nota-se a violação a esse direito, mas o empecilho não é só esse, visto que, conforme estudo feito pela FGV, publicado no jornal "O Globo", em 2025, a maioria desses sistemas não cumpre requisitos mínimos exigidos pela LGPD, conforme afirma Juliana Causin, sobre IA' s específicas:

> O DeepSeek e o Grok apresentam os piores resultados, ao falharem em mais da metade das exigências. Além de não disponibilizarem a política de privacidade em português, a ferramenta chinesa e a IA do bilionário Elon Musk, que roda no X, também não apontam de maneira clara quais são os direitos dos usuários, não explicam medidas adotadas para proteger dados pessoais, nem mencionam bases legais para raspagem e uso de dados disponíveis publicamente.
>
> Ferramenta de inteligência artificial mais popular entre os brasileiros, o ChatGPT descumpre cinco dos quatorze parâmetros. Assim como Grok e DeepSeek, o sistema da OpenAI também não lista, de forma clara, os direitos dos titulares previstos na LGPD, nem especifica quais medidas de segurança são adotadas para proteger os dados tratados.

Em segunda análise, o caso citado acima não se trata de algo isolado, mas sim de um cenário crescente, tendo em vista que o caso acima ocorreu em 2025, mas em 2024, um evento semelhante ocorreu: em Cuiabá, após alunos de uma escola fazerem fotos íntimas falsas, por meio de programa de IA, de sua professora e as publicarem. Evidencia-se que, no período de um ano, praticamente, não houve nenhuma medida para evitar que outra pessoa fosse alvo desse crime.

Outro alerta a ser feito é o de que, à medida que o tempo passa, essas IA' s tendem a avançar e ser quase imperceptível diferenciar uma imagem, vídeo ou áudio falso, de um real. Assim, é importante impor limites, conforme os critérios legais, das funções que uma IA pode exercer.

Ademais, podem-se citar outros casos mais específicos, como os informados no G1 (2025):

- “Uma multinacional do ramo do agronegócio teve seus planos de expansão vazados por uma IA de análise de mercado não regulada; ”
- “O vazamento de um medicamento novo por uma IA que simula cenários; ”
- “O vazamento de dados de 240 mil clientes de um e-commerce através de uma ferramenta de marketing automation (meio de agilizar a comunicação entre cliente e empresas).”

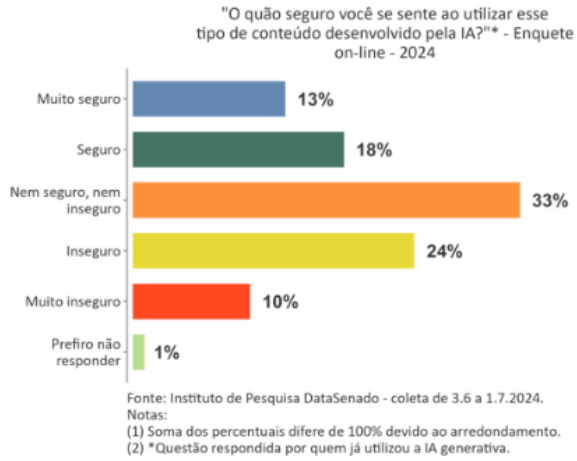
Logo, percebe-se a urgência do debate desse assunto, não só para evitar que outros sejam vítimas desse crime, mas também para zelar pelo cumprimento de uma lei que existe desde 2018.

3 Uma Análise da (Falta da) Fiscalização das IA’ s

Com base em dados do ITSEC (2024), nota-se que há um cenário de insegurança frente à disponibilização de dados de usuários, tanto para pessoas comuns quanto por empresas de grande porte, pois “79% dessas ferramentas não atendem às normas brasileiras de proteção de dados”.

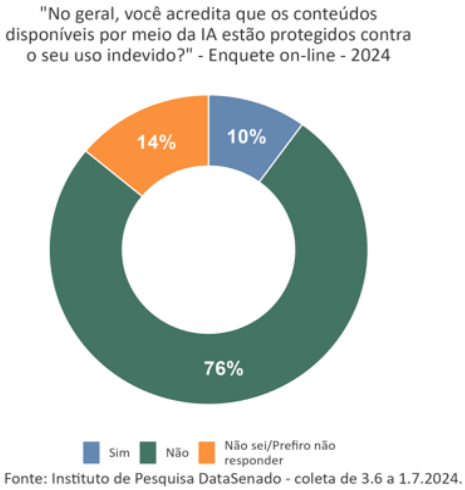
Sob essa óptica, salienta-se que a sensação de insegurança está presente na própria população brasileira, fato comprovado por pesquisa do Senado, exposto nos gráficos abaixo:

Figura 1: Opinião das pessoas em relação à segurança ao usar conteúdos feitos por IA’ s.



Fonte: Senado, 2024.

Figura 2: Opinião das pessoas sobre a proteção feita por IA' s para evitar uso indevido de seus conteúdos.



Fonte: Senado, 2024.

A partir da análise destes percentuais, aponta-se que não há um nível de confiança por parte dos usuários de IA' s no que concerne à segurança delas, tal fato está vinculado a novidade dessas ferramentas no dia a dia, pois ainda é desconhecido pela maior parte da população os diversos usos que podem ser atribuídos a elas. Além disso, também tem o fato de que não se foi ensinado como usá-las de modo seguro e funcional, simplesmente foi inserido na vida dos brasileiros.

Outrossim, também há a questão de que não há tanta transparência por parte das empresas que criam essas ferramentas, quanto ao que elas usam de dados e quanto ao que não usam, nem quanto ao que fica ou não armazenado de dado do computador ou celular do usuário, tampouco a veracidade de informações que elas disponibilizam e se existem dados pessoais disponibilizados na ferramenta que serão compartilhados com outros usuários.

Desse modo, é imprescindível analisar também as causas desses vazamentos, as quais são: "credenciais comprometidas (16%), *phishing* (15%), configuração incorreta da nuvem (12%) e ataques internos (7%)" (FECOMÉRCIO, 2025). No que se refere às credenciais comprometidas, trata-se de acessos indevidos a informações pessoais e podem atingir tanto senhas quanto usuários de login, e assim, criminosos podem acessar contas, conectar em aplicativos bancários e realizar outros crimes. Já o phishing é a falsa aparência de se tratar de uma empresa confiável e costuma ser feito via e-mails informando vagas de empregos ou até mesmo informando débitos indevidos na sua conta.

As configurações incorretas de compartilhamento da nuvem envolvem: cessão de permissões de acesso exageradas, pois pode permitir que outros usuários acessem dados seus; não realizar a mudança de senha depois da instalação inicial e não criptografar ou usar autenticação em 2 fatores em certos arquivos. Já os ataques internos são aqueles realizados por

pessoas que fazem ou já fizeram parte da cadeia produtiva da empresa e podem ocorrer de forma acidental (ao clicar em um link falso ou indevido) ou de forma proposital, com o intuito de prejudicar a empresa.

As consequências de vazamento de dados por IA' s são muito sérias e podem prejudicar desde a pessoa física até a pessoa jurídica. Na questão da pessoa física, essa situação pode: permitir que criminosos acessem suas contas bancárias e façam saques; expor detalhes da sua vida privada; permitir que criminosos acessem dados de seus familiares e dados de seus notebooks ou smartphones.

Já para as pessoas jurídicas, os danos são mais severos, posto que caso haja comprovação de que a empresa foi omissa quanto a LGPD, ela poderá ser condenada a uma sanção pelo seu descumprimento; pode também responder judicialmente aos clientes ou aos funcionários; a empresa pode ficar exposta aos outros concorrentes dependendo de qual dado foi vazado e a empresa pode sofrer impactos financeiros, pois esse cenário enfraquece a relação entre cliente e empresa.

4 Considerações finais

Desse modo, percebe-se que, no contexto atual, há uma falta de cumprimento eficaz da LGPD, tal como foi comprovado por dados acima, bem como através dos casos de vítimas que foram alvos do uso incorreto de IA' s.

Por conseguinte, afirma-se que a solução para a problemática está atrelada a fiscalização efetiva a essas ferramentas, bem como a uma rigidez maior frente aos critérios que elas devem cumprir, a fim de que as pessoas possam usá-las sem sentir medo quanto ao vazamento de seus dados e sem se preocupar com a criação de imagens falsas delas, bem como para cuidar de um direito que é tão importante e impacta tanto a vida das pessoas.

Referências

ALUNOS são expulsos após usar inteligência artificial para criar nudes falsos de professora e colegas em escola particular de Cuiabá. **G1**, 2024. Disponível em: https://g1.globo.com/mt/mato-grosso/noticia/2024/09/25/alunos-sao-expulsos-apos-usar-inteligencia-artificial-para-criar-nudes-falsos-de-professora-e-colegas-em-escola-particular-de-cuiaba.ghtml. Acesso em: 11 jul. 2025.

CAUSIN, Juliana. Do ChatGPT ao Grok, nenhuma IA cumpre exigências mínimas da lei brasileira de proteção de dados. **O Globo**, 2025. Disponível em: https://oglobo.globo.com/economia/tecnologia/noticia/2025/04/03/do-chatgpt-ao-grok-nenhuma-ia-cumpre-exigencias-minimas-da-lei-brasileira-de-protecao-de-dados.ghtml. Acesso em: 11 jul. 2025.

FREITAS, Felipe. IAs erram dados de notícias em mais de 60% do tempo. **Tecnoblog**, 2025. Disponível em: https://tecnoblog.net/noticias/pesquisa-mostra-que-chatbots-estao-errados-em-60-do-tempo/. Acesso em: 11 jul. 2025.

HIRATA, Alessandro. Direito à privacidade. **Enciclopédia jurídica da PUCSP**, 2017. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade. Acesso em: 11 jul. 2025.

MAIORIA é favorável à regulamentação de reparação de danos contra o uso indevido da inteligência artificial. **Senado**, 2025. Disponível em: https://www12.senado.leg.br/institucional/datasenado/publicacaodatasenado?id=maioria-e-favoravel-a-regulamentacao-de-reparacao-de-danos-contra-o-uso-indevido-da-inteligencia-artificial. Acesso em: 11 jul. 2025.

NASCIMENTO, Luana. IAs genéricas X especialistas. **Prezi**, 2025. Disponível em: https://prezi.com/p/b4ahp6om2r9b/ias-genericas-x-especialistas/. Acesso em: 11 jul. 2025.

VAINZOF, Rony. Vazamento de dados pessoais, LGPD e a visão do Supremo Tribunal de Justiça. **Fecomércio**, 2025. Disponível em: ttps://www.fecomercio.com.br/noticia/vazamento-de-dados-pessoais-lgpd-e-a-visao-do-supremo-tribunal-de-justica. Acesso em: 11 jul. 2025.

VAZAMENTOS de dados: a ameaça silenciosa das IAs genéricas na empresas. **G1**, 2025. Disponível em: https://g1.globo.com/pr/parana/especial-publicitario/bw8/noticia/2025/03/14/vazamentos-de-dados-a-ameaca-silenciosa-das-ias-genericas-na-empresas.ghtml. Acesso em: 11 jul. 2025.

VAZAMENTO de Dados: saiba os riscos e como se proteger. **Spc**, [s.d.]. Disponível em: https://www.spcbrasil.org.br/blog/vazamento-de-dados. Acesso em: 11 jul. 2025.

ZUBA, Fernando; GURGEL Luis. Estudantes denunciam que tiveram imagens íntimas criadas por IA e compartilhadas em colégio de BH. **G1**, 2025. Disponível em: https://g1.globo.com/mg/minas-gerais/noticia/2025/06/04/estudantes-manipulacao-vazamento-imagens-intimas-ia-colegio-bh.ghtml. Acesso em: 11 jul. 2025.