# A PORTARIA MJSP 961/2025 E OS LIMITES CONSTITUCIONAIS AO USO DA INTELIGÊNCIA ARTIFICIAL NA SEGURANÇA PÚBLICA

## *MJSP ORDINANCE 961/2025 AND THE CONSTITUTIONAL LIMITS ON THE USE OF ARTIFICIAL INTELLIGENCE IN PUBLIC SECURITY*

**Bruno Cavalcante Leitão Santos**[1]
Centro Universitário Cesmac, Cesmac, Brasil
brunoleitao.adv@hotmail.com

**Francisco de Assis de França Júnior**[2]
Centro Universitário Cesmac, Cesmac, Brasil
francajuniordireito@gmail.com

DOI: https://doi.org/10.5281/zenodo.17624181

**Resumo:** O artigo analisa criticamente a Portaria do Ministério da Justiça e Segurança Pública (MJSP) 961/2025, que impõe diretrizes para o uso de tecnologias da informação em segurança pública, com destaque às vedações do art. 11 como mecanismos de proteção de direitos fundamentais. O problema de pesquisa consiste em verificar até que ponto tais vedações vinculam estados e municípios, especialmente quando utilizam recursos federais para adoção de tecnologias baseadas em inteligência artificial (IA) na segurança pública. Parte-se da hipótese de que, embora a Portaria tenha aplicação direta apenas na esfera federal, suas diretrizes funcionam como parâmetro normativo e constitucional para políticas locais, sobretudo em temas relacionados à proteção de dados e direitos fundamentais. Adota-se abordagem hipotético-dedutiva, com pesquisa documental e bibliográfica. Os resultados indicam que a Portaria, embora restrita à esfera federal, alinha-se às diretrizes internacionais sobre regulação da IA e oferece parâmetros interpretativos para a constitucionalidade de políticas de segurança pública.

**Palavras-chave:** inteligência artificial; controle de riscos; segurança pública; competência constitucional; proteção de dados.

**Abstract:** The article critically analyzes Ordinance 961/2025 of the Brazilian Ministry of Justice and Public Security (MJSP), which establishes guidelines for the use of information technologies in public security, with emphasis on Article 11 prohibitions as mechanisms for protecting fundamental rights. The research problem consists of verifying the extent to which such restrictions bind states and municipalities, especially when they use federal funds to adopt artificial intelligence-based technologies in public security. The starting point is the hypothesis that, although the Ordinance applies directly only at the federal level, its guidelines function as a normative and constitutional parameter for local policies, especially on issues related to data protection and fundamental rights. A hypothetical-deductive approach is adopted, supported by documentary and literature review. The findings indicate that, although formally restricted to the federal sphere, the Ordinance aligns with international artificial intelligence regulatory frameworks and provides interpretive guidance for assessing the constitutionality of public security policies.

**Keywords:** artificial intelligence; risk control; public security; constitutional competence; data protection.

### 1. Introdução

O avanço acelerado das tecnologias digitais, especialmente as que se utilizam de inteligência artificial (IA), tem impactado as práticas de segurança pública no Brasil. A adoção de sistemas automatizados para fins de investigação criminal e inteligência, muitas vezes impulsionada por promessas de eficiência e predição, ocorre em um cenário de baixa regulamentação e escassa transparência.

Nesse contexto, a Portaria do Ministério da Justiça e Segurança Pública (MJSP) 961, de 24 de junho de 2025, surge como uma clara tentativa de controle institucional, impondo diretrizes para o uso das tecnologias na segurança pública.

[1] Doutor e Pós-Doutorando em Direito pela PUCRS. Líder do Grupo de Pesquisa Sistema Penal, Democracia e Direitos Humanos pelo Cesmac e, pesquisador dos Grupos de Estudos e Pesquisa em Direito e Inteligência Artificial pela PUCRS. Professor de Direito Penal no Centro Universitário Cesmac (https://ror.org/03rzfjh59) – Maceió/AL. Advogado. ORCID: https://orcid.org/0000-0001-7556-2348. Currículo Lattes: http://lattes.cnpq.br/9699629460607799. Instagram: @brunoleitaoadv.

[2] Pós-doutor em Ciências Criminais pela PUCRS. Doutor e Mestre em Direito pela Faculdade de Direito da Universidade de Coimbra, Portugal. Pós-graduado em Psicologia Jurídica e em Ciências Penais. Professor de Direito Penal e Criminologia no Centro Universitário Cesmac (https://ror.org/03rzfjh59) – Maceió/AL. Advogado. ORCID: https://orcid.org/0000-0002-6958-920X. Currículo Lattes: http://lattes.cnpq.br/2739102277898461. Instagram: @franciscofrancajr.

Assim, o presente artigo analisa criticamente os efeitos jurídicos do ato, com especial atenção às vedações contidas no art. 11, §1º, que proíbem práticas como a vigilância massiva, a discriminação algorítmica e a identificação remota sem respaldo legal, de maneira que a problemática que orientou a pesquisa foi exatamente a que segue: até que ponto as vedações do art. 11 da Portaria MJSP 961/2025 vinculam estados e municípios, especialmente quando utilizam recursos federais na adoção de tecnologias com IA em segurança pública?

Diante disso, parte-se da hipótese de que, embora a Portaria tenha aplicação direta apenas aos órgãos da União, suas diretrizes podem funcionar como parâmetro normativo e constitucional para políticas locais, sobretudo em temas como a proteção de dados e os direitos fundamentais.

O objeto da pesquisa consiste na análise das vedações do art. 11 da Portaria MJSP 961/2025 como parâmetro normativo de proteção de direitos fundamentais e de limitação da autonomia dos entes federativos na adoção de tecnologias baseadas em IA.

O tema, portanto, é relevante, uma vez que decorre da necessidade de compatibilizar a autonomia dos entes federativos com os princípios constitucionais que regem o uso de tecnologias sensíveis na persecução penal, como a legalidade, a proporcionalidade e a auditabilidade. A proteção de dados pessoais, alçada ao status de direito fundamental (CF, art. 5º, LXXIX), impõe ao Estado o dever de controlar o uso de sistemas opacos e invasivos, sob pena de legitimar práticas típicas do que se pode chamar de capitalismo de vigilância (**Zuboff**, 2020), marcado pela extração preditiva de comportamentos e pela erosão das garantias individuais.

Por fim, como método, adota-se uma abordagem hipotético-dedutiva, com base em pesquisa documental e bibliográfica nacional e internacional nas áreas do Direito Constitucional, da Segurança Pública e da teoria dos dados pessoais. Busca-se, com isso, oferecer análise crítica sobre os limites da autonomia regulatória dos estados e os caminhos para a construção de uma governança federativa responsável em matéria de tecnologias aplicadas à segurança pública.

## 2. Diretrizes da Portaria MJSP 961/2025 para o uso de IA pela Segurança Pública

A aplicação de tecnologias de informação e comunicação na segurança pública, especialmente da IA, tem avançado sem parâmetros regulatórios claros, gerando riscos significativos à privacidade, à igualdade e ao devido processo legal. Em resposta às preocupações conhecidas, a Portaria MJSP 961/2025 (**Brasil**, 2025) impôs diretrizes voltadas à mitigação de inúmeros riscos, com fundamento no art. 87 da Constituição Federal e na Lei 13.675/2018 (**Brasil**, 2018), que organiza o Sistema Único de Segurança Pública.

Essa Portaria é orientada pelo respeito aos direitos e às garantias fundamentais, atrelado a princípios como inviolabilidade da intimidade, devido processo legal, proporcionalidade, transparência, prestação de contas e proteção de dados pessoais (art. 2º), alinhando-se às diretrizes internacionais de governança responsável da IA, como as propostas pela União Europeia (2024), **Organização das Nações Unidas para a Educação, a Ciência e a Cultura** (2023) e **Organização para a Cooperação e Desenvolvimento Econômico** (2019). O art. 3º da Portaria exige avaliação prévia dos riscos e estabelece no art. 10, parágrafo único, que, quando houver possibilidade de lesão a direitos fundamentais, os resultados algorítmicos devem ser revisados por humanos, exigindo-se uma supervisão (**Brasil**, 2025b).

O ponto mais sensível do ato aqui enfocado, no entanto, está no art. 11, §1º, que veda práticas como vigilância massiva, discriminação algorítmica, coleta e monitoramento indiscriminado, e identificação biométrica remota em tempo real sem respaldo legal. A razão de ser dessas vedações é evidente: trata-se de salvaguardar direitos constitucionais como a dignidade da pessoa humana, a proteção de dados pessoais, a privacidade e a proporcionalidade no exercício do poder estatal. Ao impor tais limites, a Portaria responde à crítica de que sistemas algorítmicos, quando opacos, tendem a operar como caixas-pretas imunes à contestação (**Pasquale**, 2015), ameaçando pilares do devido processo legal.

A importância prática desse dispositivo é justamente limitar usos abusivos de tecnologias de alto risco, evitando que a identificação biométrica em massa ou o monitoramento indiscriminado consolidem uma lógica de suspeição permanente e de expansão punitiva automatizada. Ao exigir autorização judicial prévia ou hipóteses excepcionais, a Portaria garante um mecanismo de controle democrático sobre ferramentas que, em mãos desreguladas, poderiam corroer liberdades públicas e fomentar um Estado de vigilância.

As permissões excepcionais previstas — busca de vítimas ou desaparecidos, flagrante de crimes graves, recaptura de presos e cumprimento de mandados judiciais — justificam-se por razões de elevado interesse público. Nesses casos, a intervenção tecnológica não se destina à vigilância generalizada, mas à proteção imediata da vida, da integridade física ou ao cumprimento de decisões judiciais. Justamente por isso, devem ser interpretadas de forma restritiva e aplicadas com rigor, de modo a evitar a banalização das exceções. A coleta de dados biométricos é especialmente sensível, pois permite rastreamento contínuo de indivíduos e pode viabilizar formas de controle incompatíveis com democracia (**Zuboff**, 2020).

Não obstante, o dispositivo pode enfrentar críticas quanto à sua efetividade prática. A ausência de mecanismos de sanção para entes que descumpram a vedação sem recorrer a recursos federais, bem como o risco de interpretação ampliativa das exceções, revelam limites importantes da Portaria e demonstram que seu alcance normativo ainda é restrito

A relevância prática das vedações do art. 11 para vedar seu uso indiscriminado é confirmada por dados do relatório da Defensoria Pública da União e do Centro de Estudos de Segurança e Cidadania (**Nunes *et al.***, 2025), que mapeou 337 projetos ativos de reconhecimento facial no Brasil, alcançando 81 milhões de pessoas. Na Bahia, 90% das prisões em 2019 com uso da tecnologia recaíram sobre pessoas negras, em grande parte por crimes sem violência, revelando seletividade penal. Em Aracaju e Salvador, a aplicação em festas populares resultou em prisões divulgadas como exitosas, mas sem transparência sobre algoritmos ou listas de procurados. O estudo ainda registrou prisões indevidas por falsos positivos e investimentos superiores a R$ 160 milhões sem comprovação de eficácia.

A Portaria, portanto, embora não seja uma "bala de prata" diante de todas as preocupações com o uso da IA em segurança pública, representa um passo relevante quando explicita alguns dos limites normativos e reforça o dever estatal de garantir a autodeterminação informacional (**Doneda**, 2019). Sua inspiração em abordagens regulatórias baseadas em risco — como as defendidas pela Unesco — aponta para a urgência de um marco jurídico sólido que seja capaz de equilibrar inovação tecnológica com a proteção de direitos fundamentais.

## 3. Vigilância algorítmica e controle federativo: a Portaria MJSP 961/2025 como parâmetro

Após examinar o conteúdo normativo da Portaria MJSP 961/2025 e suas vedações centrais, passa-se à análise de seus efeitos sobre os entes federativos, com foco na vinculação decorrente do uso de recursos públicos e nos riscos associados à vigilância algorítmica. Seu art. 1º, §2º, vincula estados, Distrito Federal e municípios às diretrizes da norma sempre que utilizarem recursos do Fundo Nacional de Segurança Pública ou do Fundo Penitenciário Nacional para aquisição de tecnologias de informação.

Essa previsão levanta debate sobre sua natureza jurídica: trata-se apenas de uma condição para repasse de verbas ou de uma tentativa de imposição normativa de alcance geral? Ainda que sua obrigatoriedade formal se restrinja ao uso de recursos federais, o conteúdo da Portaria projeta-se como parâmetro relevante para o controle da constitucionalidade de políticas locais, sobretudo em temas que envolvem direitos fundamentais.

Essa técnica de indução normativa, contudo, revela fragilidade, pois a observância da Portaria pode ser facilmente contornada por financiamento com recursos próprios de estados e municípios, ou pela iniciativa privada, o que limita o alcance prático de suas balizas protetivas.

A atuação normativa da União é compatível com o modelo cooperativo de repartição de competências previsto nos arts. 22, 24 e 144 da CF/88. Nesse arranjo, cabe à União a edição de normas gerais, sem prejuízo de os entes subnacionais adotarem regras mais protetivas. A recente Arguição de Descumprimento de Preceito Fundamental 1.143 (**Brasil**, 2024a), atualmente em julgamento no Supremo Tribunal Federal, ilustra esse cenário ao apontar a omissão legislativa quanto ao uso estatal de programas de monitoramento remoto e intrusão em dispositivos digitais. A Corte, em sua audiência pública (**Brasil**, 2024b), destacou que o uso dessas ferramentas exige previsão legal específica, proporcionalidade estrita e salvaguardas eficazes — requisitos reforçados pelo art. 11 da Portaria.

Na prática, ao condicionar o financiamento federal à observância dessas balizas, a Portaria funciona como mecanismo de indução normativa e de padronização mínima para a proteção de dados e a supervisão humana em decisões algorítmicas.

Esse papel ganha destaque diante da difusão de práticas de mineração de dados que transforma o cidadão em objeto de predição e controle algorítmico. Tecnologias como reconhecimento facial, drones com câmeras inteligentes e *softwares* preditivos são implementadas em larga escala sem filtros legais adequados. Agrava-se esse risco com iniciativas federais de criação de uma nuvem soberana, cuja infraestrutura envolve empresas privadas como a Huawei (**Brasil**, 2025a). Tal parceria amplia o risco de opacidade no tratamento de dados públicos, reforçando o temor de que o Estado se torne ele próprio vetor de vigilância, conforme o diagnóstico de **Zuboff** (2020).

Além disso, segundo **Gloeckner e Giacomolli** (2023), o uso da IA em segurança pública opera uma expansão punitiva silenciosa, estatística e opaca, fundada em inferências algorítmicas que classificam indivíduos por padrões históricos enviesados, tensionando os princípios da presunção de inocência e da intervenção mínima do Estado penal. A racionalidade punitiva por antecipação, reforçada por tecnologias preditivas, desloca a responsabilização penal do sujeito de direito para categorias probabilísticas impessoais, em dissonância com o modelo de garantismo penal proposto por **Ferrajoli** (2014), que exige decisões fundadas em racionalidade jurídica e epistêmica.

A ausência de verificabilidade que caracterizam muitos sistemas algorítmicos comprometem o controle democrático sobre decisões automatizadas, contribuindo para o que **Pasquale** (2015) denominou "sociedade da caixa preta". Nesse ambiente, escolhas decisórias escapam à supervisão institucional e ao escrutínio público, agravando o risco de expansão do Direito Penal por meio de uma lógica de antecipação e suspeição generalizada.

Como alerta **Silva Sánchez** (2011), esse deslocamento do foco da punição do fato concreto para categorias de risco cria um modelo de Direito Penal de autor, que se agrava com as classificações estatísticas geradas por tecnologias preditivas. Tais classificações constroem perfis impessoais com base em dados históricos enviesados, minando os princípios da pessoalidade e da presunção de inocência. Em reforço à preocupação de Silva Sanchez, **Ferrajoli** (2014) sustenta que o exercício legítimo do poder punitivo deve estar submetido à racionalidade jurídica e epistêmica, o que é incompatível com decisões automatizadas carentes de explicabilidade e verificabilidade.

Diante disso, a Portaria MJSP 961/2025 — ainda que limitada a iniciativas com financiamento federal — deve ser compreendida como instrumento normativo de contenção e orientação constitucional. Suas vedações, especialmente quanto à vigilância massiva e à identificação biométrica remota sem respaldo legal, oferecem balizas que podem e devem ser adotadas pelos entes subnacionais para assegurar a legalidade e a proporcionalidade no uso de tecnologias de segurança.

## 4. Federalismo, autodeterminação informacional e interpretação constitucional da Portaria MJSP 961/2025

Diante dos riscos normativos e das implicações federativas discutidas, importa agora aprofundar o exame dos fundamentos constitucionais que legitimam — e limitam — a atuação da União e dos estados no uso de tecnologias algorítmicas em segurança pública. A União detém competência privativa para legislar sobre normas gerais de segurança pública (**Brasil**, 1988, art. 22, XXI e XXII), cabendo aos estados suplementarem-nas (art. 24, I e IX), em um modelo de responsabilidade compartilhada (art. 144).

A vinculação prevista no art. 1º, §2º, condiciona a observância da Portaria ao uso de recursos federais (**Brasil**, 2025b), conferindo-lhe eficácia normativa indireta. Ainda que não obrigue automaticamente os estados, suas diretrizes funcionam como parâmetro constitucional interpretativo, sobretudo por envolverem direitos fundamentais.

Esse entendimento ganha força com o reconhecimento da proteção de dados pessoais como direito fundamental autônomo (Emenda Constitucional 115/2022), já afirmado pelo Supremo Tribunal Federal na Ação Direta de Inconstitucionalidade 6387 (**Brasil**, 2020), que vedou o compartilhamento irrestrito de dados sensíveis. A autodeterminação informacional torna-se, nesse contexto, pressuposto normativo da dignidade humana (**Doneda**, 2019).

A regulamentação da IA deve, assim, assegurar transparência, supervisão humana e controle democrático. A ausência desses elementos contribui para opacidade dos mecanismos decisórios e riscos sistêmicos à liberdade. Do mesmo modo, a lógica extrativista de captura comportamental descrita por **Zuboff** (2020) desafia os limites constitucionais da legalidade e proporcionalidade.

A Portaria funciona, nesse cenário, como instrumento normativo de contenção e antecipação de riscos. Ainda que não substitua uma lei geral sobre IA, pode orientar a elaboração de normas federativas harmônicas com os princípios da dignidade humana, finalidade legítima e proteção de dados.

**Sarlet e Saavedra** (2020) sustentam que a proteção de dados constitui condição para o livre desenvolvimento da personalidade, exigindo explicabilidade algorítmica e controle sobre fluxos informacionais. Complementarmente, a proteção da dignidade humana, da liberdade e da autodeterminação informacional permite uma interpretação extensiva do art. 5º da Constituição Federal, a partir de uma hermenêutica aberta à atualização normativa frente às transformações tecnológicas (**Barroso**, 2012; **Hoffmann-Riem**, 2022; **Sarlet**, 2012). Tal perspectiva fundamenta não apenas a vedação de práticas incompatíveis com a proteção de dados aqui discutida, mas também a privacidade mental e a supervisão humana em sistemas decisórios automatizados, mesmo antes da existência de normas legisladas específicas sobre o tema (**Santos**, 2025).

## 5. Considerações finais

A análise da Portaria MJSP 961/2025 permite concluir que, embora sua aplicação imediata esteja vinculada ao uso de recursos federais por órgãos de segurança pública, suas diretrizes transcendem o aspecto orçamentário e se projetam como parâmetro normativo interpretativo para a constitucionalidade de políticas de vigilância nos âmbitos estadual e municipal. Responde-se, assim, à pergunta central do artigo: ainda que não haja imposição automática aos entes subnacionais, a Portaria opera como um marco orientador relevante, capaz de limitar práticas incompatíveis com os direitos fundamentais assegurados pela Constituição Federal.

Os principais achados demonstram que a norma avança ao estabelecer vedações claras a práticas como a vigilância massiva, o monitoramento contínuo e a identificação remota sem previsão legal, alinhando-se às exigências de legalidade, proporcionalidade, transparência e supervisão humana. Tais vedações respondem não apenas às demandas internas de proteção constitucional, mas também a diretrizes normativas internacionais e pela jurisprudência constitucional comparada.

Reconhece-se, porém, que a Portaria não está isenta de desafios, sobretudo pela ausência de força vinculante direta em relação a entes subnacionais e pela dependência de regulamentações complementares, o que relativiza sua eficácia prática.

A discussão revelou, ainda, que o uso da IA na segurança pública, se não regulamentado com rigor, pode operar uma expansão punitiva silenciosa e estatística, em tensão com os princípios da presunção de inocência e da intervenção mínima do direito penal. Ao oferecer um conjunto de balizas regulatórias que buscam limitar o *jus puniendi* algorítmico, a Portaria representa um passo importante na contenção dos riscos associados à adoção de tecnologias opacas e potencialmente discriminatórias.

Não se trata de demonizar a IA, mas de reconhecer que seu uso em segurança pública exige balizas normativas que garantam proporcionalidade, explicabilidade e supervisão humana, sob pena de erosão dos direitos fundamentais.

Do ponto de vista jurídico, a Portaria se insere em um contexto de afirmação da autodeterminação informacional como direito fundamental, reforçando a ideia de que a dignidade da pessoa humana e a liberdade não podem ser relativizadas diante de promessas de eficiência algorítmica. Em termos hermenêuticos, sua aplicação deve ser lida à luz de uma interpretação constitucional protetiva, que reconhece balizas normativas já existentes mesmo na ausência de legislação específica.

Diante desse cenário, a consolidação de um marco legal nacional sobre IA torna-se imperativa. Esse arcabouço deverá garantir a auditabilidade, contestabilidade e responsabilização no uso de algoritmos, impedindo os riscos de uma sociedade da caixa-preta ou a perpetuação da lógica extrativista do capitalismo de vigilância (**Zuboff**, 2020), sobretudo quando impulsionada por parcerias público-privadas que transferem a infraestrutura estatal de dados a corporações transnacionais.

Somente com regulação transparente e centrada nos direitos fundamentais será possível assegurar que o futuro digital não se torne uma nova forma de opressão, mas sim um prolongamento da cidadania constitucional e da promessa democrática.

## Informações adicionais e declarações dos autores (integridade científica)

**Declaração de conflito de interesses:** os autores confirmam que não há conflitos de interesses na condução desta pesquisa e na redação deste artigo. **Declaração de autoria:** somente os pesquisadores que cumprem os requisitos de autoria deste artigo são listados como autores; todos os coautores são totalmente responsáveis por este trabalho em sua totalidade.

**Declaração de originalidade:** os autores garantiram que o texto aqui publicado não foi publicado anteriormente em nenhum outro recurso e que futuras republicações somente ocorrerão com a indicação expressa da referência desta publicação original; eles também atestam que não há plágio de terceiros ou autoplágio.

### Como citar (ABNT Brasil)

SANTOS, Bruno Cavalcante Leitão; FRANÇA JÚNIOR, Francisco de Assis de. A Portaria MJSP 961/2025 e os limites constitucionais ao uso da inteligência artificial na segurança pública. *Boletim IBCCRIM*, São Paulo, v. 33, n. 397, p. 18-21, 2025. DOI: 10.5281/zenodo.17624181. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/2227. Acesso em: 1 nov. 2025.

### Referências

BARROSO, Luís Roberto. *Interpretação e aplicação da Constituição*. 7. ed. São Paulo: Saraiva, 2012.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil*. Brasília: Senado Federal, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 1 jul. 2025.

BRASIL. *Lei nº 13.675, de 11 de junho de 2018*. Disciplina a organização e o funcionamento dos órgãos responsáveis pela segurança pública. Brasília: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13675.htm. Acesso em: 1 jul. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. MGI apresenta iniciativas do Governo Digital brasileiro em evento internacional de Inteligência Artificial e Nuvens de Governo. *Gov.br*, 4 abr. 2025a. Disponível em: https://www.gov.br/governodigitalEGD/pt-br/noticias/mgi-apresenta-iniciativas-do-governo-digital-brasileiro-em-evento-internacional-de-inteligencia-artificial-e-nuvens-de-governo. Acesso em: 23 jun. 2025.

BRASIL. Ministério da Justiça e Segurança Pública. *Portaria MJSP Nº 961, de 24 de junho de 2025*. Brasília: MJSP, 2025b. Disponível em: https://dspace.mj.gov.br/bitstream/1/15324/2/PRT_GM_2025_961.html. Acesso em: 1 jul. 2025.

BRASIL. Supremo Tribunal Federal. *Arguição de Descumprimento de Preceito Fundamental n. 1.143*. Rel. Min. Cristiano Zanin, 16 jun. 2024a. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6900814. Acesso em: 23 jun. 2025.

BRASIL. Supremo Tribunal Federal. *Medida Cautelar na Ação Direta de Inconstitucionalidade 6837*. MP 954/2020. 24 abr. 2020. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf. Acesso em: 3 jul. 2025.

BRASIL. Supremo Tribunal Federal. STF debate limites e riscos de ferramentas de monitoramento secreto de dispositivos eletrônicos. *Portal do STF*, 10 jun. 2024b. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=546557&ori=1. Acesso em: 23 jun. 2025.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Revista dos Tribunais, 2019.

FERRAJOLI, Luigi. *Direito e razão*: teoria do garantismo penal. 4. ed. Tradução: Ana Paula Zomer Sica *et al*. São Paulo: Revista dos Tribunais, 2014.

GLOECKNER, Ricardo; GIACOMOLLI, Felipe. Problemas jurídico penais associados ao uso de inteligência artificial na fase preliminar do processo penal. *In*: SARLET, Gabrielle Bezerra Sales *et al.* (org.). *Inteligência artificial e Direito*. Porto Alegre: Fundação Fênix, 2023. p. 245-264.

HOFFMANN-RIEM, Wolfgang. *Teoria geral do direito digital*: transformação digital: desafios para o direito. 2. ed. Rio de Janeiro: Forense, 2022.

NUNES, Pablo *et al*. *Mapeando a vigilância biométrica*: levantamento nacional sobre o uso do reconhecimento facial na segurança pública. Rio de Janeiro: CESeC; DPU, 2025.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. *Recommendation of the Council on Artificial Intelligence*. Paris: OCDE, 2019. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. Acesso em: 30 jun. 2025.

PASQUALE, Frank. *The black box society*: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

SANTOS, Bruno Cavalcante Leitão. Integração de neurotecnologias e inteligência artificial: implicações para a proteção dos neurodireitos como direitos fundamentais. *Revista Jurídica da Presidência*, Brasília, v. 27, n. 141, p. 194-222, 2025. https://doi.org/10.20499/2236-3645.RJP2025v27e141-3227

SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais*: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 11. ed. Porto Alegre: Livraria do Advogado, 2012.

SARLET, Ingo Wolfgang; SAAVEDRA, Giovani Agostini. Fundamentos jusfilosóficos e âmbito de proteção do direito fundamental à proteção de dados pessoais. *Revista de Direito Público*, Brasília, v. 17, n. 93, p. 33-57, maio/jun. 2020. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/4315. Acesso em: 23 jun. 2025.

SILVA SÁNCHEZ, Jesús María. *A expansão do Direito Penal*: aspectos da política criminal nas sociedades pós-industriais. 2. ed. São Paulo: RT, 2011.

UNESCO. *Consultation paper on AI regulation emerging approaches across the world*. Geneva: UNESCO, 2024. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000390979. Acesso em: 1 jul. 2025.

UNIÃO EUROPEIA. Parlamento Europeu. *Sessão de 16 de abril de 2024 que cria regras harmonizadas em matéria de inteligência artificial* [...]. Regulamento da Inteligência Artificial. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_PT.pdf. Acesso em: 21 jun. 2025.

ZUBOFF, Shoshana. *A era do capitalismo de vigilância*: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2020.

Recebido: 5 ago. 2025. Aprovado: 25 ago. 2025. Última versão dos autores: 8 set. 2025.