IX ENCONTRO VIRTUAL DO CONPEDI

INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL

I61

Internet: dinâmicas da segurança pública internacional [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Tatiana Stroppa; Valter Moura do Carmo – Florianópolis: CONPEDI, 2026.

Inclui bibliografia
ISBN: 978-65-5274-568-2
Modo de acesso: www.conpedi.org.br em publicações
Tema: Constituição, Processo e Justiça Social: o papel da jurisdição constitucional na efetivação de direitos

2. Internet. 3. Segurança pública internacional. IX Encontro Virtual do CONPEDI (2: 2026: Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

IX ENCONTRO VIRTUAL DO CONPEDI

INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL

Apresentação

Apresentação

O IX Encontro Virtual do CONPEDI, realizado entre os dias 22 e 26 de junho de 2026, reafirmou o compromisso da entidade com a promoção da pesquisa jurídica de excelência, reunindo pesquisadoras, pesquisadores, docentes, discentes e profissionais do Direito de diversas instituições brasileiras e estrangeiras em um espaço dedicado ao debate científico e à difusão do conhecimento. Nesta edição, cujo tema foi "Constituição, Processo e Justiça Social: o papel da jurisdição constitucional na efetivação de direitos", o evento proporcionou reflexões sobre os desafios contemporâneos enfrentados pelo Estado, pelas instituições e pela sociedade na concretização dos direitos fundamentais.

Inserido nesse contexto, o Grupo de Trabalho Internet: Dinâmicas da Segurança Pública e Internacional I, coordenado por Tatiana Stroppa e Valter Moura do Carmo, proporcionou um ambiente de diálogo interdisciplinar acerca de alguns dos mais relevantes desafios decorrentes da transformação digital. As discussões evidenciaram que o desenvolvimento das tecnologias da informação, da inteligência artificial e dos sistemas algorítmicos tem produzido impactos significativos sobre a segurança pública, a proteção nacional e internacional dos direitos humanos, a tutela dos direitos da personalidade e a própria conformação do Estado Democrático de Direito. Partindo desse diagnóstico, as reflexões avançaram pela análise de como equilibrar a necessária atuação estatal diante das mudanças promovidas pelas e nas plataformas digitais, dinâmicas que impõem ao Direito a necessidade de constante atualização de seus instrumentos normativos e interpretativos.

3. ECA Digital (Lei 15.211/2025): Governança, Lacunas Normativas e Justiça Interseccional na Proteção da Infância em Ambientes Digitais, de Lizeth Nataly Delgado Villota, Thaís Agnoletti Alcova e Fernando de Brito Alves;

4. O Combate ao Crime de Pornografia Infantil e o Uso de Ronda Virtual: uma Leitura a partir da Jurisprudência do Superior Tribunal de Justiça, de Henrique Bassi da Silva e Gustavo Henrique de Andrade Cordeiro;

5. Proteção de Dados Pessoais e Regulação Digital: Reflexões sobre a ANPD e as Big Techs, de Márcia Haydée Porto de Carvalho, Alexsandro José Rabelo França e Pedro Bergê Cutrim Filho;

6. Tecnificação da Violência Sexual Infantil: a Mercantilização dos Robôs Sexuais, de Isabel Borderes Motta e Jacqueline Valadares da Silva Alckmim; e

7. Violência Psicológica contra a Mulher em Ambientes Digitais: Revitimização Algorítmica e a (In)Suficiência da Resposta Jurisdicional Brasileira, de Hudson Luiz França Mancilha e Vivianne Rigoldi.

Em conjunto, os artigos demonstram que as questões relacionadas à internet e às tecnologias digitais ultrapassam os limites tradicionais dos diversos ramos do Direito, exigindo abordagens capazes de integrar perspectivas oriundas do Direito Constitucional, do Direito Digital, do Direito Penal, da proteção de dados pessoais, dos direitos humanos e da regulação econômica. Ao mesmo tempo, evidenciam que a construção de mecanismos jurídicos aptos a compatibilizar inovação tecnológica, segurança pública e proteção dos direitos fundamentais constitui uma das agendas mais relevantes da pesquisa jurídica contemporânea e que exigirá o comprometimento não apenas dos Estados, mas das próprias plataformas digitais, grupos de interesse, sociedade civil e da comunidade acadêmica na busca de modos para vivenciar

Espera-se que os estudos ora publicados contribuam para o aprofundamento das reflexões acerca das relações entre tecnologia, segurança pública, segurança internacional e direitos fundamentais, estimulando novas pesquisas e fortalecendo o desenvolvimento desse importante campo de investigação jurídica.

Boa leitura!

Profa. Dra. Tatiana Stroppa

Centro Universitário de Bauru - Instituição Toledo de Ensino

Prof. Dr. Valter Moura do Carmo

Escola Superior da Magistratura Tocantinense (ESMAT)

ACCOUNTABILITY E INTELIGÊNCIA ARTIFICIAL: PERSPECTIVA COMPARADA ENTRE BRASIL E UNIÃO EUROPEIA SOBRE O USO DO RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA.

ACCOUNTABILITY AND ARTIFICIAL INTELLIGENCE: A COMPARATIVE PERSPECTIVE BETWEEN BRAZIL AND THE EUROPEAN UNION ON THE USE OF FACIAL RECOGNITION IN PUBLIC SECURITY.

Ana Beatriz Casado Gentil [1]
Stephanny Resende De Melo [2]

Resumo

O presente artigo busca analisar o uso do reconhecimento facial na segurança pública, especificamente acerca da necessidade de efetiva accountability nos regimes regulatórios do Brasil e da União Europeia, visto que a expansão das tecnologias de inteligência artificial no setor público amplia riscos de responsabilidade civil frágil. Nesse contexto, o objetivo geral do estudo é analisar se o regime de responsabilidade civil brasileiro é suficiente para assegurar accountability por danos causados pela utilização do reconhecimento facial na segurança pública. Como objetivos específicos, busca-se revisar a literatura especializada sobre o tema, analisar os parâmetros normativos nos dois contextos e comparar os ordenamentos identificando lacunas regulatórias e propondo complementações. Para isso, a metodologia utilizada é uma análise bibliográfica e documental, com abordagem comparativa entre os cenários examinados. A pesquisa concluiu que o Brasil ainda carece de um sistema normativo mais especializado, enquanto a U.E. apresenta uma estrutura regulatória mais consistente e robusta. Assim, conclui-se que a consolidação de um regime regulatório satisfativo depende da adoção de mecanismos de accountability efetivos.

Palavras-chave: Reconhecimento facial, Inteligência artificial, Accountability, Brasil, União europeia

Abstract/Resumen/Résumé

This article aims to analyze the use of facial recognition in public security, specifically

objectives include reviewing the specialized literature on the subject, analyzing the normative parameters in both contexts, and comparing the legal systems, identifying regulatory gaps and proposing additions. To this end, the methodology used is a bibliographic and documentary analysis, with a comparative approach between the scenarios examined. The research concluded that Brazil still lacks a more specialized normative system, while the EU presents a more consistent and robust regulatory structure. Thus, it concludes that the consolidation of a satisfactory regulatory regime depends on the adoption of effective accountability mechanisms.

Keywords/Palabras-claves/Mots-clés: Facial recognition, Artificial intelligence, Accountability, Brazil, European union

1 INTRODUÇÃO

A utilização de sistemas de Inteligência Artificial (I.A.) na segurança pública tem aumentado o debate jurídico sobre responsabilidade, transparência e proteção dos direitos humanos, especialmente, quando essas tecnologias operam com ferramentas de reconhecimento facial e produzem decisões com potencial de atingir a liberdade, a privacidade e a igualdade dos indivíduos. Por conta do uso crescente desses sistemas por agentes públicos e pela participação de agentes privados em seu desenvolvimento, surge a necessidade de definir com maior precisão quem é o responsável por danos decorrentes de falhas, vieses ou usos indevidos desta tecnologia.

No Brasil, esse debate ganha destaque diante da ausência de um marco regulatório consolidado e da contínua incerteza quanto à suficiência da legislação vigente acerca da responsabilidade para enfrentar danos produzidos por sistemas algorítmicos de grande complexidade. Embora o ordenamento jurídico brasileiro possua instrumentos gerais de proteção da personalidade, da privacidade e da não discriminação, bem como prevendo responsabilidade por atos lesivos, não possui nenhuma lei específica que regulamente o uso da I.A. em âmbito nacional, permanecendo, assim, a dúvida se tais mecanismos são suficientes para assegurar efetiva *accoutability* em casos de erros biométricos, falsos positivos e discriminação algorítmica, por exemplo.

Essa problemática se torna ainda mais relevante quando observada em comparação com a União Europeia (U.E.), que avançou na construção de um modelo regulatório baseado em riscos por meio do AI Act, estabelecendo proibições e obrigações para determinadas aplicações da inteligência artificial, inclusive envolvendo a biometria. Nesse sentido, o regulamento europeu passou a proibir certos usos considerados incompatíveis com direitos fundamentais e prevê controle mais rígido sobre sistemas de alto risco, oferecendo parâmetros relevantes para avaliar as insuficiências e as possibilidades de melhoria do modelo brasileiro.

Diante desse cenário, o problema de pesquisa que orienta este estudo é: o regime de responsabilidade civil brasileiro, baseado em normas gerais de proteção de dados e princípios constitucionais, revela-se suficiente para assegurar *accountability* efetiva pelos danos causados por sistemas de reconhecimento facial na segurança pública, considerando os riscos específicos inerentes a essa tecnologia?

Nesse contexto, o presente artigo tem como objetivo geral analisar se o regime de responsabilidade civil brasileiro é suficiente para assegurar *accountability* pelos danos causados por sistemas de reconhecimento facial empregados na segurança pública. Como

objetivos específicos, busca-se: (a) revisar a literatura especializada sobre sistemas de inteligência artificial, especialmente sobre o uso de reconhecimento facial na segurança pública, bem como acerca da *accountability*; (b) mapear os parâmetros legislativos atualmente disponíveis no ordenamento brasileiro e na União Europeia acerca da responsabilidade pelo uso desses sistemas; e, por fim, (c) comparar os ordenamentos normativos brasileiro e europeu, identificando lacunas regulatórias e propondo complementações legislativas no intuito de fortalecer a *accountability* algorítmica no contexto nacional.

A metodologia apresenta uma pesquisa de abordagem qualitativa, de natureza básica, com procedimentos bibliográfico e documental, a partir de seleção de livros e textos científico-acadêmicos em bases de dados, tais como Google Acadêmico e Scielo, mediante descritores como "Reconhecimento Facial", "Inteligência Artificial", "Dados Biométricos" e "Privacidade de Dados".

2 FUNDAMENTOS TEÓRICOS PARA A REGULAÇÃO DO RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA

A inteligência artificial por ser compreendida como a capacidade de dispositivos eletrônicos de operar de forma semelhante ao raciocínio humano, considerando variáveis, tomando decisões e resolvendo problemas (Pereira e Oliveira, 2024). No setor estatal, sistemas algorítmicos passaram a ser utilizados para apoiar ou automatizar processos, inclusive na área da segurança pública, com a promessa de aumentar eficiência, reduzir custos e ampliar a capacidade operacional do Estado. A expansão dessa tecnologia, contudo, não pode ser analisada apenas sob a ótica da inovação tecnológica visto que o uso de sistema de I.A. pelo poder público interfere diretamente com garantias fundamentais, sobretudo quando inserida em contextos de vigilância estatal (Duarte, Nunes e Lima, 2023).

Na área da segurança pública, em especial, o uso de sistema de inteligência artificial é inserido em uma lógica de governança de dados na qual ferramentas digitais são utilizadas para identificar padrões, rastrear comportamentos, estimar riscos e subsidiar decisões (Grossi, 2025). Ao mesmo tempo que a adoção dessa tecnologia é vista como um passo à modernidade, também cresce a preocupação com o fato de que esses sistemas podem produzir danos, operar com baixa transparência e dificultar o controle sobre como e onde essa tecnologia está presente. É nesse cenário que a inteligência artificial passa a ocupar posição central no debate sobre segurança pública na atualidade.

Entre as diversas aplicações da I.A. está o reconhecimento facial, que pode ser conceituados como uma tecnologia biométrica que opera por meio de algoritmos capazes de analisar imagens capturadas por câmeras e, também, extrair representações matemáticas de características específicas do rosto, como o formato do nariz ou a distância entre os olhos de um indivíduo, gerando um padrão facial único que pode ser comparado a bancos de dados já existentes (Costa; Kremer, 2022). Dessa forma, pessoas podem ser identificadas e comparadas a bancos de dados quase instantaneamente, entretanto, sem que tenham sido informadas ou que tenha permitido tal ação.

Assim, não se trata de simples registro de imagem, mas de análise de dados biométricos que converte características físicas em padrões digitais comparáveis, permitindo que o sistema relacione uma pessoa a um registro anteriormente captado. Dessa forma, apesar de apresentado como ferramenta de modernização e eficiência, o aumento no uso dessa tecnologia acentua um cenário de vigilância estatal e incerteza quanto à proteção de direitos fundamentais, como a privacidade e a intimidade (Meireles, 2020).

Nesse contexto, importa destacar que estudos e relatórios apontam que sistemas biométricos podem apresentar falsos positivos e falsos negativos, além de desempenho desigual conforme perfil de gênero, de raça e baseado na qualidade das imagens utilizadas (Meissner e Brigham, 2001). No âmbito da segurança pública, tais falhas não se limitam às estatísticas, elas podem resultar em vigilância indevida, suspeição injustificada e até restrições ilegítimas à liberdade de pessoas incorretamente identificadas. Nesse sentido, cabe trazer como demonstrativo um estudo realizado a partir de relatos da aplicação do reconhecimento facial no estado da Bahia, especificamente em Feira de Santana, durante o Carnaval de 2019, onde foram utilizados sistemas com tecnologia biométrica, contudo foi detectada uma taxa de eficiência inferior a 4% (Belli, Gaspar e Zingales, 2024).

Diante disso, observa-se como o debate jurídico sobre essas tecnologias se relaciona com as discussões sobre proteção de dados, privacidade e, principalmente, responsabilidade. Quando o uso de tecnologias de I.A. ocorre sem critérios de transparência, sem controle externo adequado e sem mecanismos claros de questionamento e contestação por partes de pessoas afetadas, resta demonstrada a necessidade de aprimoramento no sistema regulatório vigente no país.

No cenário internacional, a União Europeia ao estruturar o Regulamento (UE) 2024/1689, conhecido como AI Act (ou, em português, Ato da I.A.), buscou estabelecer um marco jurídico abrangente para a inteligência artificial, adotando uma lógica baseada em níveis de riscos e reconhecendo as diversas aplicações da I.A., incluindo as ligadas à dados

biométricos (Instituto de Tecnologia & Sociedade, 2024). Esse movimento regulatório evidencia que a questão da tecnologia de reconhecimento facial não se limita a sua utilidade, mas também a necessidade de disciplinar juridicamente seu uso em atividades tanto no âmbito privado como no âmbito governamental. É neste ponto que o debate sobre reconhecimento facial se relaciona ao debate sobre responsabilidade civil e *accountability*.

Accountability, termo oriundo da língua inglesa diante a ausência de uma expressão, em língua portuguesa, que consiga refletir a abrangência do conceito, está intrinsecamente ligada à transparência e a mecanismos ou estruturas de supervisão (Szkudlarek e Fachin, 2025). Nesse sentido, políticas de *accountability* buscam assegurar que aqueles envolvidos na construção, contratação e utilização de sistemas algorítmicos possam ser efetivamente responsabilizados pelos impactos que possam ocorrer. Esse conceito envolve, essencialmente, uma obrigação legal e ética de um indivíduo ou organização de prestar contas de suas atividades, aceitar a responsabilidade por elas e divulgar os seus resultados de forma transparente (Koene *et al.,* 2019).

Dessa forma, *accountability* não é apenas a existência de responsabilidade jurídica após o dano, mas também envolve mecanismos de supervisão, explicabilidade, possibilidade de contestação e, principalmente, transparência pública. Neste tópico, o Centro de de Estudos de Segurança e Cidadania (CESeC), junto a Defensoria Pública da União (DPU), realizou, em 2025, uma pesquisa acerca da utilização de tecnologias de reconhecimento facial pelas polícias brasileiras, segundo o qual entre os 23 estado brasileiros que se manifestaram, 26% deles não forneceram documentos detalhados, como contratos e valores, alegando “sigilo operacional” (Nunes *et al.*, 2025).

Nesse cenário em que sistemas de identificação biométrica não apenas reconhecem indivíduos, mas também contribuem com decisões que podem afetar liberdades fundamentais, a ausência de uma verdadeira *accountability* compromete a efetividade da responsabilidade em relação aos agentes envolvidos. Com base nisso, resta evidente que o uso de sistemas de reconhecimento facial na segurança pública, não se limita ao plano técnico de otimização operacional, mas representa um problema legislativo de grande relevância.

A literatura especializada no tema, portanto, demonstra que sistemas biométricos não apenas aumentam riscos de erros e discriminações, mas também desafiam os mecanismos tradicionais de controle e responsabilização, exigindo, assim, uma noção ampliada de *accountability*. Diante disso, torna-se necessária a análise comparada entre o sistema normativo brasileiro e o europeu, revelando tanto as insuficiências de ambos os regimes quanto às possibilidades de aprimoramento mútuo.

3 REFERÊNCIAS NORMATIVAS APLICÁVEIS AO RECONHECIMENTO FACIAL

3.1 Parâmetros Normativos no Brasil

A análise da responsabilidade por danos decorrentes do uso de sistemas de reconhecimento facial na segurança pública exige, no Brasil, a consideração de uma base normativa fragmentada, composta por normas constitucionais, civis e de proteção de dados. Devido a inexistência de legislação nacional específica sobre o tema, a utilização dessa tecnologia pelo setor público tem sido regulada, majoritariamente, por iniciativas estaduais, como nos estados do Ceará, a Lei nº 16.873/2019 (Ceará, 2019) e de Minas Gerais, a Lei nº 21.737/2015 (Minas Gerais, 2015), ambas abordando a implementação de sistemas de reconhecimento facial em determinados espaços públicos (Francisco, Hurel e Rielli, 2020).

Nesse contexto, importa destacar que, no Brasil, os entes federados possuem competência para legislar sobre o uso de sistemas de reconhecimento facial para fins de segurança pública. O governo federal, por sua vez, fica responsável de estabelecer, por meio de leis, limites e regras gerais sobre o tema (Ceia e Teffé, 2021). Através dessa possibilidade, os estados, bem como o Distrito Federal, podem atender às necessidades específicas de suas próprias localidades.

Em nível constitucional, o tema encontra respaldo na importância da dignidade da pessoa humana, conforme art. 1°, inciso III, da Constituição Federal de 1988 (Brasil, 1988), e na proteção dos direitos fundamentais à intimidade, à vida privada, à honra e à imagem, previstos no art. 5º, inciso X, da CF/88 (Brasil, 1988). Nesse sentido, o uso do reconhecimento facial pelo poder público, sobretudo em contextos de policiamento e vigilância, afronta diretamente essas esferas jurídicas, uma vez que envolve monitoramento de pessoas em espaços públicos, coleta e tratamento de características biométricas e possibilidade de abordagem estatal fundada em decisões automatizadas (Pereira; Oliveira, 2024).

Em nível infraconstitucional, a responsabilidade civil representa um dos principais instrumentos para enfrentar danos causados por falhas ou usos indevidos de sistemas de I.A.. Nesse sentido, o Código Civil estabelece o dever geral de reparar violações que causem danos materiais ou morais a terceiros. Entretanto, no contexto específico da tecnologia de identificação biométrica, a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, assume papel de destaque, uma vez que essa tecnologia opera com dados biométricos sensíveis. Nesse viés, a LGPD define como dado pessoal sensível o dado biométrico vinculado a uma pessoa natural e estabelece que a disciplina da proteção de dados

tem por objetivo proteger os direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade (Brasil, 2018).

Contudo, cabe destacar, logo de início, que o art. 4º da LGPD determina que esta lei não se aplica ao tratamento de dados pessoais realizado para fins de segurança pública, defesa nacional, segurança do Estado e investigação e repressão de infrações penais, prevendo que essas hipóteses deverão ser disciplinadas por legislação específica (Brasil, 2018). Essa ressalva gera uma lacuna regulatória relevante, pois limita a atuação da proteção jurídica sobre os dados pessoais sensíveis justamente em um contexto estratégico. Tal brecha aumenta ainda mais a preocupação com a ausência de transparência e controle sobre o uso de I.A. na segurança pública (Grossi, 2025).

Por outro lado, a LGPD estabelece princípios que dialogam com a noção de *accountability*, como finalidade, necessidade, adequação, prevenção, não discriminação, prestação de contas, transparência e responsabilização. Esses fundamentos se mostram relevantes no contexto do uso de sistemas de reconhecimento facial, pois exigem que o tratamento de dados se dê para finalidades legítimas, com limitações ao necessário, proteção contra abusos e capacidade de explicabilidade. Dessa forma, a LGPD assume papel central na contenção dos riscos associados à opacidade dos algoritmos, ao exigir, por exemplo, a disponibilização de informações claras sobre os critérios utilizados em decisões automatizadas que afetem os titulares de dados (Grossi, 2025).

Além disso, dentre as principais formas de garantir a *accountability* presentes na LGPD, vale destacar o que essa norma disciplina acerca de revisões de decisões automatizadas. O art. 20 desta lei assegura ao titular o direito de solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, bem como o acesso a informações claras e adequadas sobre os critérios e procedimentos utilizados (Brasil, 2018). Assim, esse dispositivo configura um instrumento essencial de *accountability*, à medida que estabelece a possibilidade de explicabilidade e revisão humana em decisões automatizadas.

Em conjunto com as normas vigentes citadas, a base normativa brasileira sobre inteligência artificial na segurança pública é marcada por um processo legislativo ainda em formação. Nesse contexto, o Projeto de Lei nº 2.338/2023 (Brasil, 2023), de autoria do Senador Rodrigo Pacheco, ocupa lugar de destaque por ser a principal proposta sobre o tema. Importa ressaltar que essa proposição foi criada a partir de uma inspiração na legislação da União Europeia (Melo, 2024), buscando definir normas gerais, em âmbito nacional, para o desenvolvimento, a implementação e o uso responsável de sistemas de I.A. no Brasil.

A proposta insere a inteligência artificial no campo da governança baseada em risco, da proteção de direitos fundamentais, da supervisão regulatória e da definição de deveres para diferentes agentes da cadeia tecnológica (Paulino, 2024). Vale destacar que o art. 15 do projeto de lei estabelece ressalvas ao uso da identificação biométrica à distância em ambientes públicos, apenas permitindo esta prática quando houver previsão em lei federal específica, mediante autorização judicial e nos casos de persecução penal individualizada de crimes com pena superior a dois anos, busca de desaparecidos ou flagrante delito (Brasil, 2023).

Dessa forma, o projeto de lei além de introduzir o conceito de altos riscos ao direito civil brasileiro (Melo, 2024), o dispositivo mencionado demonstra um compromisso com a proteção dos direitos fundamentais e representa um passo à frente para garantir a *accountability* necessária no ordenamento brasileiro. Assim, a relevância do PL 2338/2023 no cenário legislativo do país decorre menos de seu valor normativo atual, já que se trata ainda de um projeto de lei, e mais de sua capacidade de revelar a direção do debate institucional brasileiro.

3.2 Parâmetros Normativos na União Europeia

No cenário europeu, vale destacar, de início, que existem diversos documentos normativos acerca da proteção de dados, incluindo regulamentos e diretrizes sobre o tema. Dentre eles, pode-se citar o Regulamento Geral de Proteção de Dados (RGPD), que é constantemente tratada como a lei de privacidade e segurança mais rigorosa do mundo, impondo obrigações à organizações em qualquer lugar desde que atuem ou coletem dados de pessoas na União Europeia (Conselho da União Europeia, 2024). Contudo, a RGPD não aborda de forma direta as particularidades da inteligência artificial, sendo necessário, para este estudo, focar na normativa sucessora deste regulamento.

Na U.E., portanto, a disciplina normativa acerca do uso da inteligência artificial, inclusive na segurança pública, é o AI Act, marco jurídico apresentado pela própria União Europeia, que busca enfrentar os riscos inerentes a sistemas de I.A. e regulamentar sua utilização. Considerado o primeiro marco regulatório mundial sobre inteligência artificial, o AI Act foi proposto pela Comissão Europeia em 2021 como resposta aos riscos sistêmicos identificados em sistemas algorítmicos e sua elaboração contou com um amplo processo de consulta pública (Conselho da União Europeia, 2025). Além disso, o regulamento visa padronizar as estratégias regulatórias entre os Estados-Membros, visto que a supervisão

regulatória autônoma poderia gerar riscos à integração regional característica da U.E. (Melo; Souza; Vasco e Reis, 2022).

A estrutura normativa do A.I. Act baseia-se na classificação por risco associados a utilizações específicas da I.A, classificando-os em 4 níveis de risco, bem como estabelecendo regras diferentes para cada. As categorias são: (i) risco inaceitável, configuram práticas proibidas; (ii) risco elevado, sistemas sujeitos a obrigações reforçadas; (iii) risco limitado, exige transparência básica; e (iv) risco mínimo ou nulo, basta autorregulação voluntária. Cabe ressaltar que a execução prevista no AI Act combina governança nacional e da comunidade europeia visto que os Estados-Membros designam autoridades responsáveis pela avaliação de conformidade, notificação e fiscalização, sob a supervisão da Comissão Europeia (Conselho da União Europeia, 2025).

Na área da segurança pública, o AI Act foca especialmente nas aplicações de execução da lei *(law enforcement)*, reconhecendo o potencial lesivo dessa tecnologia sobre os direitos fundamentais. Os arts. 5º e 6º proíbem práticas de risco inaceitável, incluindo o uso de sistemas de identificação biométrica remota em tempo real em espaços públicos para fins de aplicação da lei, salvo exceções como combate ao terrorismo ou busca por pessoas desaparecidas, mediante, ainda, autorização judicial (Conselho da União Europeia, 2025). Esses dispositivos refletem a preocupação europeia com vigilância em massa e violação da privacidade em espaços de uso comum, contexto no qual o reconhecimento facial tradicionalmente é utilizado.

Nesse contexto, aqueles sistemas biométricos que não são proibidos se encontram classificados como de alto risco pelo AI Act, sujeito a obrigações rigorosas como avaliações de conformidade, gestão de riscos, alta qualidade dos dados de treinamento, supervisão humana e transparência efetiva (Nunes e Neta, 2024). Essas medidas visam minimizar erros como falsos positivos, opacidade decisória e discriminação algorítmica, riscos inerentes a sistemas de reconhecimento facial, principalmente quando utilizados no âmbito da segurança pública.

Diante disso, é possível perceber como AI Act incorpora a *accountability* através dessa sistemática, impondo obrigações e exigências específicas aos fornecedores, executores e usuários de sistemas de alto risco, incluindo os biométricos e de execução de lei. Em síntese, os fornecedores devem manter sistemas de qualidade (art. 17), elaborar documentação detalhada (art. 11), realizar avaliações contínuas (art. 19) e registrar sistemas em base central da U.E., enquanto os usuários respondem pela supervisão humana efetiva (art. 14), monitoramento de desempenho e comunicação transparente aos afetados (Conselho

da União Europeia, 2025). Essa divisão de responsabilidades institucionaliza a prestação de contas ao longo de todo o ciclo de vida do sistema, desde o desenvolvimento, a implantação e a operação, demonstrando a devida *accountability*.

Portanto, o AI Act configura um marco regulatório que dispõe de classificações, exigências e proibições específicas para as diversas utilidades da inteligência artificial. No contexto da segurança pública, destaca-se a busca pelo equilíbrio entre utilidade operacional e preservação de liberdades fundamentais através de transparência ativa, supervisão humana obrigatória e controle independente (Nunes e Neta, 2024). Assim, estabelece padrões consolidadas e verificáveis de *accountability* algorítmica, envolvendo a prevenção, rastreabilidade e responsabilização ao longo do ciclo de vida inteiros do sistema em questão

4 REGULAÇÃO DO RECONHECIMENTO FACIAL EM PERSPECTIVA COMPARADA: BRASIL E U.E.

A comparação entre os ordenamentos jurídicos do Brasil e da União Europeia revela contrastes importantes na abordagem à *accountability* de sistemas de reconhecimento facial na segurança pública. O paralelo entre esses dois cenários se torna ainda mais relevante à medida que ambos enfrentam o mesmo desafio regulatório, mas o encaram de formas diferentes. De um lado a U.E. desenvolveu um regulamento específico e orientado por riscos, e de outro, o Brasil ainda lida com o tema por meio de um conjunto fragmentado de normas constitucionais, civis e de proteção de dados, sem lei específica em âmbito nacional. A presente análise permite, portanto, avaliar o nível de *accountability* algorítmica, destacando possibilidades de aprimoramento para o regime regulatório brasileiro.

A *accountability* deve ser compreendida como um fenômeno multidimensional, que abrange diferentes áreas, como a técnica, a procedimental e a institucional. No caso da segurança pública, esse conceito se torna ainda mais relevante porque as tecnologias de reconhecimento facial operam com dados biométricos sensíveis. Não se trata, portanto, apenas de responsabilizar alguém depois da ocorrência de um dano, mas de construir uma base normativa em que o uso de sistema de identificação biométrica seja juridicamente inteligível, controlável e compatível com os limites da Democracia (Ceia e Teffé, 2021).

Diante disso, a análise comparativa entre Brasil e União Europeia é útil para identificar em que medida cada ordenamento consegue transformar o uso do reconhecimento facial em prática efetivamente sujeita à explicabilidade e a prestação de contas. Para isso, a tabela a seguir sintetiza os principais contrastes normativos entre Brasil e U.E. no tratamento da *accountability* para uso estatal de reconhecimento facial.

Quadro 1 - Análise Comparada

Aspecto	**Brasil**	**União Europeia**
Base Normativa	AI Act - Trata especificamente sobre Inteligência Artificial.	Constituição, Código Civil e LGPD - Não trata especificamente sobre Inteligência Artificial.
Reconhecimento Facial	O uso de sistemas biométricos na segurança pública recebe tratamento restritivo, com proibições e exigências reforçadas para hipóteses permitidas.	Não há disciplina específica e uniforme em âmbito federal sobre o tema.
Lógica Regulatória	Abordagem preventiva e orientada à gestão de riscos.	Abordagem reativa, baseada em controle posterior e responsabilização eventual.
Accountability	Há maior densidade normativa para controle, supervisão, documentação e responsabilização dos agentes envolvidos.	A *accountability* depende de interpretação de normas gerais e de posterior judicialização ou controle administrativo difuso.

Fonte: Elaboração própria (2026)

De início, cabe destacar os pontos fortes do modelo europeu, destacando o fato de que a União Europeia trata o reconhecimento facial com uma estratégia regulatória mais ampla de governança da I.A.. Essa abordagem fortalece a *accountability* visto que não trata essa tecnologia como uma questão isolada, mas como uma prática sujeita a parâmetros jurídicos prévios, controle institucional e avaliações (Madiega e Midlebrath, 2021). O AI Act, busca se preocupar não só com a reparação de danos posteriores, mas também com o próprio ato de utilizar essa tecnologia, estabelecendo limites e obrigações que procuram reduzir a opacidade e minimizar usos incompatíveis com direitos fundamentais.

Outro aspecto positivo do modelo europeu é que ele incorpora, de modo explícito, a preocupação com a compatibilidade entre inovação tecnológica e proteção de direitos (Madiega e Midlebrath, 2021). No contexto do reconhecimento facial, especialmente para execução da lei *(law enforcement)*, isso fica demonstrado na adoção de restrições severas, na previsão de hipóteses excepcionais de uso e na exigência de salvaguardas adicionais para práticas consideradas particularmente sensíveis. Em termos de *accountability*, isso significa que o ordenamento europeu entende que a tecnologia do reconhecimento facial deve ser sempre justificada e submetida à regulação legal, justamente por seu potencial de afetar privacidade, liberdade e igualdade.

Partindo agora para a análise do caso brasileiro, apesar da ausência de um marco legal nacional específico, há aspectos positivos que merecem ser considerados. O primeiro deles reside na existência de uma base constitucional e infraconstitucional sólida de proteção de direitos, formada, sobretudo, pela dignidade da pessoa humana, pelos direitos à intimidade, à vida privada, à honra e à imagem, pela tutela dos dados pessoais e pelo regime geral da responsabilidade civil. A LGPD, mesmo que não se aplicando a segurança pública, ao classificar os dados biométricos como sensíveis e ao estabelecer princípios como finalidade, necessidade, adequação, transparência e não discriminação, também oferece instrumentos importantes para enquadrar juridicamente o uso do reconhecimento facial.

Ainda que esses elementos não formem uma regulamentação própria e sólida, eles fornecem fundamentos relevantes para contenção do poder estatal e para a formulação de pretensões de responsabilização diante de usos abusivos, discriminatórios ou desproporcionais da tecnologia. Além disso, outro elemento que merece ser considerado entre os pontos fortes do caso brasileiro é a dimensão federativa da regulação, que abre espaço para maior experimentação normativa pelos estados.

Na ausência de um marco federal consolidado sobre reconhecimento facial na segurança pública, a existência de legislações estaduais permite que os entes federados adaptem os princípios gerais do ordenamento jurídico às suas particularidades locais, consideradas suas capacidades institucionais, seus contextos operacionais e suas necessidades administrativas (Francisco, Hurel e Rielli, 2020). Isso pode favorecer respostas regulatórias mais ajustadas à realidade local e contribuir para o desenvolvimento gradual de parâmetros concretos de uso da tecnologia. Essa potencialidade, evidentemente, não elimina os riscos da fragmentação, mas revela que o federalismo também pode operar como campo de aprendizado regulatório e de acomodação prática entre princípios gerais e realidades locais.

Porém, também deve-se considerar os pontos fracos de ambos os modelos. No caso europeu, o regulamento mantém uma vedação geral ao uso de sistemas de reconhecimento facial em tempo real, mas abre exceções que, na prática, podem ampliar a margem de atuação das autoridades e esvaziar a força da proibição (Zulehner, 2024). A existência de exceções no campo de execução da lei, somada ao certo grau de complexidade do próprio sistema regulatório, pode reduzir a clareza e a uniformidade da aplicação das proteções, especialmente na prática administrativa dos Estados-Membros.

Dessa forma, mesmo em um cenário normativo aparentemente mais sofisticado, a efetividade da *accountability* depende não apenas do texto regulatório, mas da capacidade institucional de interpretação, fiscalização e de garantia na implementação das normas. Também vale destacar que a densidade normativa exige elevados níveis de coordenação administrativa, conhecimento técnico e capacidade institucional para produzir seus efeitos concretos.

Em consequência, a *accountability* europeia, embora mais bem estruturada, ainda depende de um esforço contínuo de harmonização, fiscalização e tradução prática das exigências legais para o cotidiano das autoridades públicas e dos operadores dos sistemas (Erdogan, 2024). Isso demonstra que a sofisticação regulatória, por si só, não garante automaticamente o controle efetivo da tecnologia, ainda que constitua passo decisivo nessa direção.

No Brasil, por outro lado, as fragilidades são mais evidentes. A principal delas consiste justamente na ausência de uma norma federal específica para o reconhecimento facial na segurança pública. Na prática, isso cria um cenário em que a expansão do uso da tecnologia não é acompanhada por normas uniformes sobre hipóteses de cabimento, critérios de necessidade e proporcionalidade, transparência pública, retenção de dados, revisão de decisões e mecanismos específicos de controle (Picolo e Rachid, 2022). Diante disso, o resultado é um regime de *accountability* fraco, no qual a responsabilização ocorre após a violação, sem mecanismos de prevenção.

Além da fragmentação normativa, observa-se que os cidadãos brasileiros frequentemente desconhecem quando estão sendo monitorados, quais bases de dados são utilizadas, quem exerce o controle sobre o sistema e quais mecanismos estão disponíveis para contestar eventuais erros ou exigir correções (Araújo, Cardoso e Paula, 2021). Soma-se a isso o fato de que os sistemas de reconhecimento facial operam com margens relevantes de imprecisão e vieses algorítmicos, circunstâncias que agravam significativamente os riscos de lesão a direitos fundamentais. Desse modo, em vez de um controle preventivo robusto, o

Brasil ainda se apoia em um regime que normaliza a expansão da vigilância biométrica sem impor proteções suficientes à privacidade, à igualdade e ao devido processo.

À luz dessa comparação, é possível identificar também um espaço de convergência normativa entre os dois modelos. A União Europeia poderia aproveitar da experiência brasileira no tocante a dimensão federativa da regulação, que permite maior experimentação institucional e adaptação das regras às realidades locais, sem prejuízo da observância de princípios gerais de proteção de direitos.

Por sua vez, o Brasil poderia incorporar do modelo europeu uma estrutura regulatória mais preventiva, com definição clara de hipóteses de uso, mecanismos de avaliação de risco, salvaguardas procedimentais e deveres específicos de transparência e responsabilização. Nesse sentido, a comparação não se limita a apontar diferenças, mas revela possibilidades de aprendizado recíproco capazes de contribuir para a construção de um regime mais equilibrado e eficaz de *accountability* no uso do reconhecimento facial.

5 CONCLUSÃO

O presente trabalho demonstrou que a aplicação de sistemas de inteligência artificial na área da segurança pública vem crescendo nos últimos anos, acompanhada de um amplo debate regulatório. Os riscos associados ao uso de tecnologias biométricas, mostram que, especialmente no contexto de vigilância em massa, existe uma necessidade de regulamentação jurídica robusta e específica às particularidades desses sistemas, a fim de mitigar situações de erros biométricos e discriminação algoritimica. Nesse contexto, a noção de *accountability* se torna ainda mais relevante, envolvendo deveres de prestação de contas, transparência e explicabilidade.

Diante disso, a análise comparada entre os regimes regulatórios no Brasil e na União Europeia buscou identificar lacunas legislativas e propor complementações, no intuito de fortalecer a *accountability* algorítmica, principalmente no contexto nacional. No caso europeu, a partir do estudo do AI Act, restou demonstrada uma lógica regulatória robusta, focada em prevenção e baseada em riscos, prezando pela contenção, supervisão e responsabilização, porém, não é isenta de fragilidades. No Brasil, foi possível perceber uma fragmentação regulatória ainda persistente, inexistindo regulamentação nacional e específica sobre o tema, apenas normas constitucionais, civis e de proteção de dados, que juntas podem ser utilizadas para disciplinar a matéria, entretanto, sem enfrentar com precisão os desafios próprios da vigilância biométrica.

Conclui-se, portanto, que a consolidação de um arcabouço regulatório adequado para disciplinar o uso do reconhecimento facial na área da segurança pública depende necessariamente da superação da fragmentação normativa e seu caráter reativo que predomina no Brasil. A efetividade da *accountability*, nesse cenário, pressupõe não só a definição de limites ao uso dessa tecnologia, mas também a exigência de critérios de transparência, explicabilidade, controle institucional e responsabilização. Assim, não se trata apenas de permitir ou proibir a utilização de sistemas de I.A., como o reconhecimento facial, mas sim assegurar que o seu uso seja submetido a mecanismos efetivos de prestação de contas capazes de prevenir violações aos direitos humanos.

REFERÊNCIAS

ARAÚJO, Romulo de Aguiar; CARDOSO, Naiara Deperon; PAULA, Amanda Marcélia de. Regulação e uso do reconhecimento facial na segurança pública do Brasil. **Revista de Doutrina Jur.**, Brasília, DF, v. 112, e021009, 2021. Disponível em: https://revistajuridica.tjdft.jus.br/rdj/article/view/734/135. Acesso em: 11 maio 2026.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidente da República, [2016]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acesso em 13 maio 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm (planalto.gov.br in Bing). Acesso em: 05 maio 2026.

BRASIL. **Projeto de Lei n° 2338 de 2023.** Dispõe sobre o uso da Inteligência Artificial. Senado Federal, Brasília, DF, 03 maio 2023. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em: 11 maio 2026.

BELLI, L.; GASPAR, W. B.; ZINGALES, N. Regulating facial recognition in Brazil: legal and policy perspectives. In: MATULIONYTE, R.; ZALNIERIUTE, M. (Ed.). **The Cambridge handbook of facial recognition in the modern state.** Cambridge, Cambridge University Press, 2024. p. 228-241. Disponível em: https://www.cambridge.org/core/books/cambridge-handbook-of-facial-recognition-in-the-modern-state/regulating-facial-recognition-in-brazil/CEEA7751492156D1FFE96E029CB014AD. Acesso em: 12 maio 2026.

CEARÁ. **Lei nº 16.873, de 10 de maio de 2019**. Dispõe sobre o comércio e consumo de bebida alcoólica em estádios e arenas desportivas no estado do ceará e define penalidades pelo descumprimento às normas de comercialização. Fortaleza. Disponível em: https://www2.al.ce.gov.br/legislativo/legislacao5/leis2019/16873.htm. Acesso em 09 maio 2026.

CEIA, Eleonora; TEFFÉ, Chiara Spadaccini de. Facial recognition and public security in the city of Rio de Janeiro: a critical analysis in the perspective of federative competences and fundamental rights. **IUS PUBLICUM Network Review**, 2021. Disponível em: https://www.ius-publicum.com/repository/uploads/10_06_2022_17_13_5_IusPublicum_FACIAL-RECOGNITION-AND-PUBLIC-SECURITY-IN-THE-CITY-OF-RIO-DE-JANEIRO–.pdf

CONSELHO DA UNIÃO EUROPEIA. **Regulamento Inteligência Artificial.** Bruxelas, 2025. Disponível em: https://www.consilium.europa.eu/pt/policies/artificial-intelligence/. Acesso em: 06 maio 2026.

CONSELHO DA UNIÃO EUROPEIA. **Regulamento Geral sobre a Proteção de Dados.** Bruxelas, 2024. Disponível em: https://www.consilium.europa.eu/pt/policies/data-protection-regulation/#gdpr. Acesso em: 12 maio 2026.

COSTA, Ramon Silva; KREMER, Bianca. Inteligência artificial e discriminação: desafios e perspectivas para a proteção de grupos vulneráveis frente às tecnologias de reconhecimento facial. **Revista Brasileira de Direitos Fundamentais & Justiça**, Belo Horizonte, v. 16, n. 1, out. 2022.

DUARTE, Daniel Edler; NUNES, Pablo; LIMA, Thallita G. L. **Panorama Estudos de Vigilância.** Rio de Janeiro: CESeC, 2023. (Coleção Panorama).

ERDOGAN, Irmak. Diving into the Iceberg: Establishing Transparency in AI for Law Enforcement. **European Papers**, Vol. 9, 2024, No 3, pp. 956-977, ISSN 2499-8249 - doi: 10.15166/2499-8249/794. Disponível em: https://www.europeanpapers.eu/system/files/pdf_version/EP_eJ_2024_3_SS1_3_Irmak_Erdogan_00794.pdf. Acesso em: 10 maio 2026.

FRANCISCO, Pedro Augusto P.; HUREL, Louise Marie; RIELLI, Mariana Marques. Regulação do reconhecimento facial no setor público: avaliação de experiências internacionais. Rio de Janeiro: Instituto Igarapé; **Data Privacy Brasil Research**, jun. 2020. Disponível em: https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regulação-do-reconhecimento-facial-no-setor-público.pdf.

GROSSI, Alexandre Viezzer. A aplicação da inteligência artificial na segurança pública brasileira: O caso de São Paulo e a análise do PL nº 2338/2023. **Revista PPC: Políticas públicas e cidades**, Ponta Grossa, v. 37, n. 1, 2025.

INSTITUTO DE TECNOLOGIA E SOCIEDADE. **Como regular a inteligência artificial?** Expandindo os horizontes de análise para além da União Europeia. Rio de Janeiro: Instituto de Tecnologia e Sociedade, 2024. Relatório técnico.

KOENE, Ansgar. et al. **Regulating facial recognition in the EU**. Bruxelas, 2019. European Parliamentary Research Service. Disponível em: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf. Acesso em: 9 maio 2026.

MADIEG, Tambiama; MILDEBRATH, Hendrik. **Regulating facial recognition in the EU**. Bruxelas, 2021. European Parliamentary Research Service. Disponível em: https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf. Acesso em: 10 maio 2026.

MEIRELES, Adriana Veloso. **Algoritmos, privacidade e democracia:** ou como o privado nunca foi tão político como no século XXI. Orientador: Luis Felipe Miguel. 2020. Tese (Doutorado em Ciências Políticas) – Universidade de Brasília, Brasília, 2020.

MEISSNER, Christian A.; BRIGHAM, John C. Thirty years of investigating the own-race bias in memory for faces: a meta-analytic review. **Psychology, Public Policy, and Law,** v. 7, n. 1, p. 3-35, 2001. DOI: 10.1037/1076-8971.7.1.3.

MELO, Ana Karolina Acris; SOUZA, Jéssica C.; VASCO, Amanda Corrêa; REIS, Breno Salomon. **Regulação da Inteligência Artificial: Benchmarking internacional de políticas públicas.** Brasília: Escola Nacional de Administração Pública – ENAP. Diretoria de Altos Estudos – EvEx, 2022.

MELO, Gustavo da Silva. Inteligência Artificial e responsabilidade civil: uma análise do anteprojeto do Marco Legal da Inteligência Artificial e do Projeto de Lei 2338/2023. **Revista IBERC,** Belo Horizonte, v. 7, n. 1, p. 49–65, 2024. DOI: 10.37963/iberc.v7i1.271. Disponível em: https://revista.iberc.org.br/iberc/article/view/271. Acesso em: 12 maio. 2026.

MELO, Stephanny Resende de. **E quando o suspeito for você?** Reconhecimento facial na segurança pública. São Paulo: Editora Dialética, 2024.

MINAS GERAIS. **Lei nº 21.737 de 05 de agosto de 2025.** Dispõe sobre a comercialização e o consumo de bebida alcoólica nos estádios de futebol localizados no Estado e dá outras providências. Belo Horizonte. Disponível em: https://www.almg.gov.br/legislacao-mineira/texto/LEI/21737/2015/. Acesso em: 09 maio 2026.

NUNES, Pablo et al. **Mapeando a vigilância biométrica** [livro eletrônico]: levantamento nacional sobre o uso do reconhecimento facial na segurança pública. Rio de Janeiro: CESeC, 2025. Disponível em: https://direitoshumanos.dpu.def.br/wp-content/uploads/2025/05/CESeC__DPU_Mapeando_a_vigilancia_biometrica.pdf. Acesso em: 12 maio 2026.

NUNES, Lorena de Almeida; NETA, Ainah Hohenfeld Angelini. Marco Regulatório da Inteligência Artificial: Análise do AI ACT da União Europeia no Tocante a Privacidade e Proteção dos Dados Pessoais. **Revista de Direito UNIFACS** - Debate Virtual, Salvador, n. 293, 2024. Disponível em: https://revistas.unifacs.br/index.php/redu/article/viewFile/9279/5266.

PAULINO, Thiago Junior. **Responsabilidade civil por atos de inteligência artificial:** desafios e perspectivas no direito brasileiro. Trabalho de Conclusão de Curso (Graduação em Direito) - Faculdade Nacional de Direito, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2024.

PEREIRA, Sara Matias Ferrari; OLIVEIRA, Tarsis Barreto. O uso da inteligência artificial no direito penal e seus reflexos sobre os direitos fundamentais da não discriminação e da privacidade. **Revista do Instituto de Direito Constitucional e Cidadania**, Londrina, v. 9, n. 1, p. 99, jan./jun. 2024.

PICOLO, Cynthia; RACHID, Raquel. **Principles on facial recognition technologies:** a response by Laboratory of Public Policy and Internet to Global Privacy Assembly. Brasília: Laboratory of Public Policy and Internet, 2022. Disponível em:https://lapin.org.br/wp-content/uploads/2022/07/GPA-final.pdf. Acesso em: 11 maio 2026.

SZKUDLAREK, A. L.; FACHIN, M. G. O dever de accountability algorítmica sob a Convenção Americana sobre Direitos Humanos. **Revista de Direitos Humanos e Desenvolvimento Social,** v. 6, e 2516093, 2025. DOI: https://doi.org/10.24220/2675-9160v6a2025e16093.

ZULEHNER, Bruno. EU Artificial Intelligence Act: Regulating the Use of Facial Recognition Technologies in Publicly Accessible Spaces. Stanford-Vienna European Union **Law Working Paper.** No. 91, 2024.