

**III CONGRESSO INTERNACIONAL
DE DIREITO, POLÍTICAS PÚBLICAS,
TECNOLOGIA E INTERNET**

DIREITO PENAL E CIBERCRIMES I

D598

Direito penal e cibercrimes I [Recurso eletrônico on-line] organização III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet: Faculdade de Direito de Franca – Franca;

Coordenadores: Clóvis Alberto Volpe Filho, Helen Cristina de Almeida e Lucas Gonçalves da Silva – Franca: Faculdade de Direito de Franca, 2025.

Inclui bibliografia

ISBN: 978-65-5274-370-1

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

Tema: Governança, regulação e o futuro da inteligência artificial.

1. Direito. 2. Políticas Públicas. 3. Tecnologia. 4. Internet. I. III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet (1:2025 : Franca, SP).

CDU: 34

III CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

DIREITO PENAL E CIBERCRIMES I

Apresentação

Entre os dias 30 de setembro e 3 de outubro de 2025, a Faculdade de Direito de Franca recebeu o III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet. O evento reuniu acadêmicos, profissionais, pesquisadores e estudantes, promovendo o debate interdisciplinar sobre o impacto das inovações tecnológicas no campo jurídico e nas políticas públicas. A programação envolveu Grupos de Trabalho (GTs) organizados para aprofundar temas específicos, abordando desde o acesso à justiça até as complexidades da regulação tecnológica, com ênfase na adaptação do sistema jurídico aos avanços da inteligência artificial e da automação.

O GT 9 examina as novas fronteiras do direito penal em meio à criminalidade virtual. As comunicações abordam o uso de reconhecimento facial, deepfakes e provas digitais, destacando riscos à privacidade e à integridade processual. O grupo busca construir parâmetros jurídicos que assegurem a proteção de direitos fundamentais diante dos desafios tecnológicos contemporâneos.

RECONHECIMENTO FACIAL NA PERSECUÇÃO PENAL: ENTRE A (IN) EFICÁCIA TECNOLÓGICA E OS RISCOS À LIBERDADE

FACIAL RECOGNITION IN CRIMINAL PROSECUTION: BETWEEN (IN) EFFECTIVE TECHNOLOGY AND THE RISKS TO FREEDOM

**Marina De Brino Penna
Luiz Gustavo Vicente Penna
Pedro De Brino de Oliveira**

Resumo

Este artigo examina criticamente o uso de algoritmos de reconhecimento facial na fase inicial da persecução penal, inserindo-se na interseção entre Direito Penal, tecnologia e crítica social. A partir do conceito de racismo algorítmico e de referenciais como Ruha Benjamin, Baratta e Zaffaroni, denuncia-se a falácia da neutralidade tecnológica e os riscos da automação discriminatória. Argumenta-se que, sem regulação adequada, essas ferramentas reforçam a seletividade penal e violam princípios constitucionais, exigindo urgente controle democrático e jurídico das tecnologias de vigilância.

Palavras-chave: Reconhecimento facial, Racismo algorítmico, Seletividade penal, Direitos fundamentais, Regulação da ia

Abstract/Resumen/Résumé

This article offers a critical analysis of the use of facial recognition systems in the early stages of criminal prosecution, positioned at the intersection of Criminal Law, technology, and social critique. Drawing on the concept of algorithmic racism and the works of scholars such as Ruha Benjamin, Baratta, and Zaffaroni, it demonstrates how the lack of effective regulation allows ostensibly neutral technologies to reproduce historical inequalities under the guise of innovation. The study highlights the risks of automated discrimination and its incompatibility with constitutional principles, advocating for a robust, democratic regulatory framework guided by fundamental rights.

Keywords/Palabras-claves/Mots-clés: Facial recognition, Algorithmic racism, Penal selectivity, Fundamental rights, Artificial intelligence regulation

INTRODUÇÃO

Entre 30 de setembro e 3 de outubro de 2025, acontecerá o III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet, com o tema: "Governança, Regulação e o Futuro da Inteligência Artificial", visando debater os impactos da IA no direito e na sociedade, sob a ótica da ética, justiça social e proteção dos direitos fundamentais.

Neste sentido, o Grupo de Trabalho 9 (GT9), intitulado "Direito Penal e Cibercrime", propõe um espaço de debate sobre os efeitos da automação e das tecnologias de vigilância no sistema penal, com destaque para o reconhecimento facial e o chamado racismo algorítmico. Tais mecanismos, embora revestidos de uma suposta neutralidade técnica, operam em contextos sociais historicamente marcados por desigualdades estruturais.

Este artigo insere-se, assim, na interseção entre o Direito Penal, a tecnologia e a crítica social, com foco na utilização de algoritmos de identificação facial nas fases iniciais da persecução penal. A partir de evidências empíricas e referenciais teóricos — nacionais e internacionais —, investiga-se o paradoxo da técnica: instrumentos concebidos para otimizar a atuação estatal acabam por reforçar a seletividade penal, reproduzindo preconceitos históricos sob o disfarce da inovação digital.

Com base nos estudos de Ruha Benjamin, Baratta, Zaffaroni, Silvio Almeida, Jacqueline Zuboff, Ingrid Costa e Mourão, este texto critica a falácia da neutralidade tecnológica. Demonstra-se como a ausência de regulação e controle democrático sobre dados biométricos marginaliza grupos sociais. Sistemas de IA, especialmente o reconhecimento facial, não são neutros; eles herdaram preconceitos e assimetrias sociais ao serem treinados com dados historicamente enviesados.

A bibliografia utilizada evidencia que a IA, treinada com dados que refletem padrões discriminatórios, tende por automatizar e acelerar tais distorções, uma vez sendo fundamentadas especialmente em probabilidades estatísticas, convertendo a desigualdade estrutural em puro cálculo técnico. No Brasil, o cenário se torna ainda mais instável pela ausência de política pública de regulação efetiva de tais ferramentas, que inclua, por exemplo, a responsabilidade civil e penal ou diretrizes de auditabilidade, permitindo que tais tecnologias sejam implementadas sem o devido controle e desatentas à dignidade humana.

Por fim, problematiza-se os efeitos jurídicos de tais práticas tecnológicas, destacando sua incompatibilidade com os princípios constitucionais da presunção de inocência, do devido processo legal e da dignidade da pessoa humana. Desta forma, utilizando o método qualitativo de forma interdisciplinar (direito penal, direitos fundamentais e tecnologia), analisando jurisprudências, documentos oficiais e casos concretos. Assim, a pesquisa oferece crítica jurídica fundamentada, abordando os riscos do reconhecimento fácil no sistema penal brasileiro, enfatizando a necessidade de uma regulação robusta, democrática e comprometida com o Estado Democrático de Direito, que enfrente os perigos da vigilância automatizada como nova engrenagem de exclusão institucionalizada.

2. RACISMO ALGORÍTMICO E O PARADOXO DA TÉCNICA: RECONHECIMENTO FACIAL E SELETIVIDADE PENAL NA ERA DIGITAL.

2.1 - Tecnologia e Discriminação: O Reconhecimento Facial como Ferramenta de Racismo Institucionalizado

A consolidação da inteligência artificial (IA) como ferramenta de gestão estatal e comercial tem promovido profundas transformações nas formas de vigilância e controle social, especialmente através da visão computacional, ou seja, do reconhecimento facial. Apesar de avançada, evidencia a falácia da suposta neutralidade algorítmica, sendo perceptível a falta de neutralidade reproduzida por esses sistemas, uma vez sendo construídos com dados padrões enviesados que resultam em erros de identificação e abusos, sobretudo contra populações historicamente vulneráveis. Esse fenômeno é amplamente reconhecido como "racismo algorítmico".

Além disso, a ausência de critérios que incorporem as particularidades sociais, históricas e culturais desses grupos, bem como a ineficiência na construção de sistemas que considerem as especificidades locais e regionais, aprofunda ainda mais as desigualdades existentes, tornando o uso da inteligência artificial um instrumento potencial de exclusão social.

Estudos do MIT Media Lab e do NIST demonstram que a acurácia dessas tecnologias é significativamente inferior para rostos de pessoas negras, indígenas ou asiáticas, especialmente mulheres, com taxas de erro que podem ultrapassar 30% para mulheres negras, contra menos de 1% para homens brancos.

No Brasil, a situação é alarmante: dados da Rede de Observatórios da Segurança (2019) revelam que 90% das prisões baseadas em reconhecimento facial eram de pessoas negras, que representam cerca de 56% da população. Além disso, a Coding Rights (2022) aponta que mais de 75% das aquisições de tecnologias de vigilância por estados brasileiros ocorreram sem licitação ou consulta à sociedade civil, agravando o risco de abusos e violações de direitos.

Não há dúvidas de que a situação é alarmante. O uso de tecnologias de reconhecimento facial em espaços públicos, frequentemente sem consentimento, afronta diretamente preceitos constitucionais basilares: a inviolabilidade da imagem e vida privada (art. 5º, X), o devido processo legal (art. 5º, LIV) e o princípio da igualdade substancial (art. 3º, IV). Embora a LGPD reconheça dados biométricos como sensíveis, sua exclusão do âmbito da segurança pública cria uma "zona cinzenta jurídica". Essa lacuna intensifica o tratamento discriminatório de dados, sem garantias fundamentais e fiscalização eficaz, naturalizando o uso de tecnologias intrusivas sob o pretexto de proteção social, mesmo ao comprometer direitos como a igualdade e a não discriminação.

Essa ausência de regulação eficaz, contudo, não atua isoladamente: ela se alia a um problema ainda mais profundo, enraizado na própria arquitetura dos sistemas algorítmicos utilizados nesses contextos. O funcionamento da inteligência artificial — especialmente no

modelo de aprendizado supervisionado — reproduz e potencializa desigualdades sociais preexistentes, uma vez que os algoritmos são treinados com base em dados previamente rotulados por seres humanos, passando a incorporar os vieses e preconceitos de seus programadores resultando em sistemas que não apenas falham — mas falham de maneira racializada.

Ingride Coelho da Costa, Thamiris Lima de Araujo e Rosalia Maria Carvalho Mourão, no artigo intitulado "*Racismo Algorítmico: o reconhecimento facial em desconformidade aos direitos fundamentais*", ensina que a ausência de participação da população preta na criação e no desenvolvimento dessas tecnologias contribui para sua marginalização. Isso acarreta prejuízos econômicos e reforça um ciclo de exclusão que atravessa tanto os meios tradicionais quanto os digitais.

Nesse contexto, o reconhecimento facial automatizado, quando usado como critério exclusivo para atuação policial ou persecução penal, configura prova ilegítima e discriminatória, violando o devido processo legal. Tal prática estabelece uma presunção indevida de culpa, baseada em mecanismos de identificação probabilísticos e estruturalmente enviesados por marcadores raciais, reeditando digitalmente antigas técnicas de vigilância seletiva incompatíveis com um Estado Democrático de Direito.

2.2. Aprendizado de Máquina e a Reatualização da Discriminação Penal

Com o avanço das tecnologias digitais e a aplicação de sistemas de reconhecimento facial, a confiabilidade dos dados usados no treinamento desses algoritmos torna-se pertinente. O *machine learning*, principal método de aprendizado, baseia-se na análise de grandes volumes de dados para identificar padrões, trazendo, porém, desafios aos desenvolvedores em relação a curadoria e filtragem de dados, visto que a vasta quantidade de informações online impede uma verificação minuciosa de todo o conteúdo. Como consequência, a utilização de dados enviesados no treinamento de modelos de *machine learning* compromete a imparcialidade dos algoritmos. Afinal, o que se pode esperar de uma máquina cujo aprendizado é pautado por milhares de decisões preconceituosas?

Em 2019, um jovem negro de 25 anos, portador de deficiência mental, foi erroneamente identificado como assaltante por um sistema de reconhecimento facial, sendo abordado de forma violenta enquanto se dirigia ao hospital acompanhado de sua mãe. Esse episódio ilustra claramente como a qualidade dos dados utilizados no *machine learning* pode comprometer seu funcionamento, refletindo vieses estruturais presentes na própria base de dados. Esse fenômeno tem sido denominado de "racismo algorítmico", refletindo o aprendizado das máquinas a partir de dados historicamente marcados por preconceitos, resultando em práticas discriminatórias do algoritmo que, em tese, deveria operar de forma imparcial.

Percebe-se então que essa dinâmica contribui para a estigmatização e marginalização de grupos racializados, notadamente a população negra, comprometendo completamente a

suposta neutralidade da tecnologia, intensificando a vigilância de áreas periféricas e marginalizadas, muitas vezes negligenciando delitos ocorridos fora dessas regiões.

Trata-se, portanto, da automatização do racismo estrutural, disfarçada sob a aparência de neutralidade técnica. Essa distorção caracteriza o que autores denominam “dupla opacidade” ou opacidade algorítmica: de um lado, uma opacidade tecnológica, que dificulta a auditoria e a contestação dos critérios utilizados pelos sistemas de inteligência artificial — a chamada “caixa-preta algorítmica”; de outro, uma opacidade ética, marcada pela ausência de transparência institucional, de prestação de contas e de controle democrático. Nesse cenário, essa blindagem técnica contribui para a naturalização dos erros como “danos colaterais aceitáveis”, sobretudo quando afetam corpos racializados e periféricos, alimentando um ciclo vicioso de discriminação contra populações marginalizadas, gerando aumento nas prisões e ainda mais dados enviesados que serão utilizados para treinar futuros sistemas.

2.3 - Tecnologia De Vigilância E Direito Penal: Reconhecimento Facial, Racismo Estrutural E O Enfraquecimento Das Garantias Constitucionais.

O avanço das tecnologias de vigilância no campo da segurança pública tem acentuado um dos dilemas mais críticos do nosso tempo: como conciliar o uso de ferramentas tecnológicas com o respeito irrestrito aos direitos fundamentais? A recente autorização, formalizada pelo Ministério da Justiça em 30 de junho de 2025, para o uso de sistemas de IA com reconhecimento facial a distância, recoloca com urgência essa discussão no cenário jurídico nacional.

A nova norma permite a aplicação da tecnologia em investigações criminais, localização de pessoas desaparecidas, recaptura de foragidos e ações em presídios, desde que haja autorização judicial e inexistência de meios menos gravosos para a obtenção de provas. Em situações excepcionais — como flagrantes de crimes com pena superior a dois anos ou risco iminente à vida — os agentes poderão utilizar o recurso, desde que comuniquem de forma imediata o Judiciário. A diretriz abrange a Polícia Federal, Polícia Rodoviária Federal e órgãos que utilizem recursos do Fundo Nacional de Segurança Pública, com promessas de padronização, segurança informacional e prevenção a vazamentos de dados sensíveis.

Contudo, a busca por eficiência investigativa acarreta um custo democrático. A prática do reconhecimento facial no Brasil revela violações sistemáticas a garantias constitucionais, atingindo predominantemente a população negra e periférica. Levantamento da Rede de Observatórios da Segurança (2019) indica que 90% das prisões por reconhecimento facial eram de pessoas negras, com concentração de falsos positivos em estados como Bahia – líder no uso da ferramenta - e Rio de Janeiro.

Esse padrão corrobora a tese de autores como Baratta e Alexander: o sistema penal é estruturalmente seletivo, agora intensificado por aparatos tecnológicos. O reconhecimento facial, baseado em aprendizado supervisionado, ao ser alimentado por dados de entrada de contextos sociais marcados pela desigualdade racial, acaba por automatizar discriminações já naturalizadas.

A ausência de regulação penal específica agrava o cenário. A Lei nº 13.709/2018 (LGPD), ao excluir o tratamento de dados para segurança pública (art. 4º, III), cria um vácuo normativo. Essa lacuna permite a coleta e o armazenamento de dados biométricos sensíveis (art. 5º, II) sem consentimento, transparência ou controle externo, violando princípios constitucionais como o contraditório, a ampla defesa e a presunção de inocência.

Embora o Anteprojeto da LGPD Penal procure suprir essa lacuna, a tecnologia persiste em uso massivo e opaco, sem balizas democráticas, com uma composição enviesada das bases de dados, frequentemente com fotos de pessoas negras obtidas sem autorização, o que afronta a LGPD e compromissos internacionais. Denúncias contra a Polícia Civil da Bahia corroboram que esses bancos de imagens são formados, em grande parte, por fotos de indivíduos negros coletadas em abordagens policiais, redes sociais e câmeras de segurança - muitas vezes sem a devida autorização. Tais práticas não apenas ferem a LGPD, mas também violam diretrizes da OCDE e a jurisprudência da Corte Interamericana de Direitos Humanos.

Do ponto de vista técnico, o reconhecimento facial apresenta falhas significativas, com taxas de erro superiores a 90% entre pessoas negras e mulheres. Apesar disso, a tecnologia segue sendo equivocadamente utilizada como prova direta, embora a doutrina, assim como o Delegado-Geral da Polícia Civil de São Paulo, Ruy Ferraz Fontes, o reconhecimento facial não deve ser utilizado como prova isolada.

2.4 - A Ilusão Da Neutralidade Tecnológica E A Urgência De Regulação.

O reconhecimento facial cria uma falsa ilusão de neutralidade e imparcialidade tecnológica. Apesar de sua aparente objetividade, estudos internacionais, como os do Instituto Nacional de Padrões e Tecnologia dos Estados Unidos (NIST), revelam que os algoritmos desses sistemas reproduzem erros estruturais dos dados de treinamento, evidenciando um déficit de adaptação à realidade brasileira. Isso ocorre porque os sistemas mais populares são desenvolvidos em países norte americanos ou europeus cujos bancos de dados não contemplam a diversidade fenotípica do Brasil, marcada por sua miscigenação, traços mestiços e pluralidade étnica.

Essa inadequação tecnológica, somada à falta de diversidade racial nos ambientes de desenvolvimento, perpetua desigualdades. Conforme Mourão *et al.* (2022) salienta, a ausência da participação de pessoas negras no desenvolvimento de tecnologias aprofunda a marginalização digital, transformando algoritmos em instrumentos de invisibilização e criminalização. Esse cenário é agravado em polos tecnológicos - como o Vale do Silício -, onde a homogeneidade étnica de pesquisadores, majoritariamente brancos, favorece a reprodução inconsciente de vieses em projetos que deveriam ser neutros. Isso reflete uma estrutura social mais ampla, na qual a “hegemonia da brancura”, como observa Bastos (2016), impede o questionamento de privilégios e a preocupação com desvantagens impostas a outros grupos.

Consequentemente, a ausência de representatividade de perfis miscigenados nos bancos de dados originais compromete tanto não a precisão como a justiça no uso dessas

ferramentas no âmbito do processo penal. Diante dessa realidade, em um Estado Democrático de Direito, é inadmissível que a inovação seja mobilizada como instrumento de opressão e seletividade. Urge a suspensão imediata do uso indiscriminado dessa tecnologia, até que normas claras estejam em vigor, com (I) exigência de autorização judicial prévia, (II) auditorias independentes dos algoritmos, (III) controle social efetivo e (IV) total transparência sobre o ciclo de dados.

A eficiência não pode justificar a corrosão da dignidade humana. A segurança pública, para ser legítima, deve estar a serviço da cidadania — e não da reprodução automatizada do racismo de Estado.

6. Considerações Finais

A utilização do reconhecimento facial no processo penal, embora promissora, exige rigorosa regulação jurídica. Sua aplicação deve estar condicionada à existência de normas específicas, auditorias independentes e contínuas dos algoritmos, garantia de contraditório técnico e vedação expressa ao seu uso exclusivo como fundamento de medidas cautelares. A eficácia da persecução penal não pode se sobrepor às liberdades individuais nem às garantias constitucionais. Sem critérios normativos claros, essa tecnologia representa um perigoso retrocesso, capaz de aprofundar a seletividade penal e as injustiças históricas.

O crescimento da IA transferiu decisões sensíveis a sistemas algorítmicos que influenciam milhões de vidas. Contudo, a pretensa neutralidade dessas tecnologias não resiste à análise crítica. Os algoritmos replicam dinâmicas de exclusão e violência estrutural do mundo *offline*, manifestando-se no Brasil na reprodução de práticas de racialização contra a população negra.

Este trabalho demonstrou que os mecanismos de IA, quando não submetidos a regulamentações sólidas e a uma fiscalização comprometida com os direitos fundamentais, incorporam os pilares do racismo estrutural. Daí a necessidade urgente de controle público, transparência e participação social em sua formulação, desenvolvimento e aplicação. Ao abordar o conceito de racismo algorítmico com base em casos concretos, evidencia-se que, sem enfrentamento crítico e normativo, a IA deixa de ser um instrumento de progresso e passa a operar como vetor de opressão tecnológica.

Referências Bibliográficas

BARBOSA, Juliana Cesario Alvim. Tecnologia e racismo algorítmico: reconhecimento facial e seletividade penal no Brasil. **Revista Brasileira de Ciências Criminais**, São Paulo, v. 29, n. 169, p. 103–129, 2021.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF. Presidência da República. 1988. Brasília, DF: Diário Oficial da União. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 02 de jul. de 2025.

BRASIL. **Lei nº 13.709 de 14 de agosto de 2018.** Lei Geral de Proteção de Dados. 2018. Brasília, DF: Diário Oficial da União. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 02 de jul. de 2025.

CALDEIRA, José Antonio; SOBRAL, Patrícia. Tecnologias de reconhecimento facial: o racismo algorítmico como instrumento de política de segurança pública. **Direito e Política**, v. 20, n. 1, 2025.

CAVALLI, Marcelo. **A prova penal no Estado Constitucional:** limites e possibilidades. Curitiba: Juruá, 2020.

COSTA, Ingrid; ARAÚJO, Thamiris; MOURÃO, Rosalia. **O Racismo algorítmico:** o reconhecimento fácil em desconformidade aos direitos fundamentais. *Revista REASE*. 2025. v. 11. n. 5.

COIMBRA, Jéssica; Moraes, Liliane; SILVA, Adrian. **Interseções entre o racismo algoritmo, reconhecimento fácil e segurança pública no Brasil.** *Revista Jurídica do CESUPA*. 2023. v. 4. n. 2.

CNJ – Conselho Nacional de Justiça. **Relatório Técnico sobre Reconhecimento Facial e Processo Penal.** Brasília: CNJ, 2021. Disponível em: <https://www.cnj.jus.br>. Acesso em: 02 de jul. de 2025.

JUNIOR, Jânio; JORGE, Derick. **Inteligência artificial no reconhecimento facial em segurança pública:** dados sensíveis e seletividade penal. *Revista Jurídica UNICESUMAR*, Maringá, v. 23, n. 3, p. 61–85, set./dez. 2022.

LIMA, Bruna Dias Fernandes. **Racismo algorítmico:** o enviesamento tecnológico e o impacto aos direitos fundamentais no Brasil. 2022. 127 f. Dissertação (Mestrado em Direito) – Universidade Federal de Sergipe, São Cristóvão, 2022.

ONU – Human Rights Council. **Racial discrimination and emerging digital technologies:** a human rights analysis. Report of the Special Rapporteur on contemporary forms of racism. A/HRC/44/57, 2020. Disponível em: <https://www.ohchr.org/en/documents/thematic-reports/ahrc4457-racial-discrimination-and-emerging-digital-technologies-human-rights-analysis>. Acesso em: 02 de jul. de 2025.

REDE DE JUSTIÇA CRIMINAL. **Olho no lance:** como o reconhecimento facial tem sido usado para prender pessoas injustamente no Brasil. São Paulo, 2020. Disponível em: <https://www.redejusticacriminal.org.br>. Acesso em: 03 de jul. de 2025.

SILVA, Tarcízio. **O racismo algorítmico é uma espécie de atualização do racismo estrutural.** CEE/Fiocruz, 2023. Disponível em: <https://cee.fiocruz.br/?q=Tarcizio-Silva-O-racismo-algoritmico-e-uma-especie-de-atualizacao-do-racismo-estrutural>. Acesso em: 03 de jul. de 2025.

SOUZA NETO, Cléber Francisco Alves. **Reconhecimento facial e racismo algorítmico.** In: BARBOSA, Juliana Cesario (org.). *Justiça e tecnologia*. Belo Horizonte: D'Plácido, 2020.