

IX ENCONTRO VIRTUAL DO CONPEDI

DIREITOS E GARANTIAS FUNDAMENTAIS I

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria - CONPEDI

Presidente - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - FMU - São Paulo

Diretor Executivo - Prof. Dr. Orides Mezzaroba - UFSC - Santa Catarina

Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa - Pará

Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG - Goiás

Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos - Rio Grande do Sul

Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio - Rio de Janeiro

Vice-presidente Nordeste - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

Representante Discente: Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

Conselho Fiscal:

Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão

Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais

Prof. Dr. Valter Moura do Carmo - UFERSA - Rio Grande do Norte

Prof. Dr. Fernando Passos - UNIARA - São Paulo

Prof. Dr. Edinilson Donisete Machado - UNIVEM/UENP - São Paulo

Secretarias

Relações Institucionais:

Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná

Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia

Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal

Comunicação:

Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina

Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul

Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe

Relações Internacionais para o Continente Americano:

Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do sul

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão

Prof. Dr. Felipe Chiarello de Souza Pinto - UPM - São Paulo

Relações Internacionais para os demais Continentes:

Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará

Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul

Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI - Santa Catarina

Educação Jurídica

Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba - PR

Prof. Dr. Rubens Beçak - USP - SP

Profa. Dra. Livia Gaigher Bosio Campello - UFMS - MS

Eventos:

Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo

Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina

Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

Comissão Especial

Prof. Dr. João Marcelo de Lima Assafim - UFRJ - RJ

Profa. Dra. Maria Creusa De Araújo Borges - UFPB - PB

Prof. Dr. Antônio Carlos Diniz Murta - Fumec - MG

Prof. Dr. Rogério Borba - UNIFACVEST - SC

D597

Direitos e garantias fundamentais I [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Eudes Vitor Bezerra; Viviane Coêlho de Séllos Knoerr; Andre Pires Gontijo – Florianópolis: CONPEDI, 2026.

Inclui bibliografia

ISBN: 978-65-5274-584-2

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. Direitos. 3. Garantias fundamentais. 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

DIREITOS E GARANTIAS FUNDAMENTAIS I

Apresentação

Honrados, apresentamos os trabalhos defendidos durante o IX Encontro Virtual do CONPEDI, no âmbito do GT 48 - Direito e Garantias Fundamentais. Temas variados, envolvendo os desafios para proteção e compreensão dos direitos fundamentais na contemporaneidade foram abordados e agora trazidos para o leitor.

Mariana Oliveira de Sá realizou duas pesquisas. A primeira pesquisa sobre o Critério Hermenêutico para avaliação, onde buscou explorar como o efeito inibidor fortalece a democracia e estendeu para a necessidade de ponderação em suas aplicações. A segunda pesquisa sobre Violência Estrutural no BRASIL como Mecanismo de Aprofundamento das Desigualdades Sociais das Minorias, debruçou-se sobre o impacto desigual da violência estrutural nas minorias e concluiu questionando a necessidade de extensão do conceito de violência.

Kenza Borges, no artigo A proteção jurídica da cultura em um País de diversidade cultural e desigualdades estruturais, analisou que a proteção da cultura no Direito brasileiro, examinando o arcabouço normativo destinado à tutela da diversidade cultural e sua efetividade em um contexto de profundas desigualdades sociais. Concluiu que a mera existência de normas não é suficiente para garantir a democratização da cultura em uma sociedade caracterizada pelas desigualdades sociais.

Lucas Gonçalves da Silva e Leandro Sousa Vieira, no ensaio A Anonimização de Dados Sensíveis e Soberania Tecnológica no Sistema Judiciário Brasileiro, exploraram a utilização de softwares de código fechado pelo Poder Judiciário, destacando que, embora não haja

simultaneamente, protege as garantias fundamentais, concluiu defendendo a ampliação e o fomento dessa regulação para fortalecer a proteção dos direitos fundamentais previstos na Constituição Federal de 1988.

Gil Cesar Costa de Paula, realizou duas pesquisas. A pesquisa inicial focou na Jurisprudência e precedentes como instrumentos das garantias dos direitos fundamentais, em que o objetivo era compreender a diversidade de julgados proferidos por magistrados e tribunais distintos, com foco para os precedentes do STF sobre racismo e homofobia. Na pesquisa subsequente sobre Tratados Internacionais de Direitos Humanos, analisou como opera a aplicação dos tratados internacionais de direitos humanos no ordenamento jurídico brasileiro. Com foco na discussão acerca da natureza supralegal dos tratados internacionais que não foram aprovados pelo rito qualificado previsto na Constituição Federal, à luz do entendimento consolidado pelo Ministro Gilmar Mendes no Supremo Tribunal Federal.

Marcos Leite Garcia escreveu dois artigos. O primeiro Polemica De Não Considerar A Propriedade Como Direito Fundamental, onde argumenta que a propriedade foi considerada direito fundamental em determinado contexto histórico, mas que na contemporaneidade essa fundamentação não mais se sustenta, todavia não se confunde com o direito à moradia, este sim considerado fundamental e expresse na Constituição. Usou como referências FERRAJOLI e a Revolução Francesa como marco inicial da relativização da propriedade, adendo especial a Revolução vez que a relativização foi por via de uma revolução burguesa, e não socialista. No segundo artigo sobre a Dignidade da Pessoa Humana, usou como base a obra do Prof. Gregório Barbas (professor e deputado), sustentou no artigo que a dignidade da pessoa humana constitui o ponto de partida e de chegada dos direitos fundamentais. Destacou, ainda, que a dignidade pode ser violada tanto antes quanto depois de sua positivação jurídica, especialmente quando não há efetividade normativa. Considerou também a possibilidade de o Amor ser considerado um direito fundamental, todavia questionando como sua exigibilidade poderia ser operacionalizada no ordenamento jurídico brasileiro.

contexto estadunidense. Abordou o uso da cultura como instrumento de proteção dos direitos dos migrantes diante das políticas anti-imigração da atual administração Trump. Argumentou na pesquisa que os migrantes são frequentemente utilizados como bodes expiatórios, especialmente os latino-americanos, e que o Reggaeton funciona como instrumento de resistência cultural e decolonial.

Veronica Corrêa Silva e Cristina Veloso de Castro ensaio Cannabis medicinal e direitos fundamentais: análise comparativa entre Brasil e Itália, buscaram realizar uma análise legislativa, das resoluções do CFM e da regulamentação da ANVISA destacando as barreiras regulatórias e a necessidade de judicialização para assegurar a efetividade dos direitos fundamentais.

Amanda Gomes Seguins e Márcia Haydée Porto de Carvalho no artigo intitulado Contenção jurisprudencial do habeas corpus, discutiram o enfraquecimento da tutela da liberdade de locomoção decorrente da contenção jurisprudencial do habeas corpus, bem como a possibilidade de compreender essa limitação como um mecanismo de proteção voltado à racionalização do sistema recursal e à preservação da finalidade constitucional do remédio.

Ana Paula Nunes Borba e Paulo Roberto Gomes Junior e Roberto da Freiria Estevão no estudo Desindexação e direito ao esquecimento, exploraram a distinção entre a desindexação e o direito ao esquecimento, tendo como principal referência o Tema 786 do Supremo Tribunal Federal, cuja tese firmou o entendimento de que o direito ao esquecimento é incompatível com a Constituição Federal de 1988. Também foi abordada a orientação do Superior Tribunal de Justiça no sentido de que a remoção de conteúdo na internet exige a indicação da URL específica. A análise foi desenvolvida à luz da teoria dos direitos fundamentais de Robert Alexy. A Conclusão final foi que a desindexação e o direito ao esquecimento constituem institutos jurídicos distintos, sendo possível a aplicação da desindexação, desde que observados os requisitos estabelecidos pela jurisprudência do Superior Tribunal de Justiça.

da incapacidade da Corte Estadunidense de superar desigualdades raciais, tendo, em diversas ocasiões, atuado como perpetuadora dessas desigualdades. A pesquisa utilizou como referência o entendimento sintetizado na expressão “iguais, porém diferentes”. Sustentou que a desigualdade racial constitui um elemento estrutural da sociedade em estudo, a qual, após o período da escravidão, passou a adotar um regime institucionalizado de segregação racial, evidenciando a permanência de mecanismos de discriminação e exclusão mesmo após a abolição da escravidão.

Clara Angélica Gonçalves Cavalcanti Dias e Hellen Crystian Prado na pesquisa *Etarismo e os Desafios Jurídicos para Efetivação da Proteção da Pessoa Idosa no Brasil*, abordaram a concepção de etarismo, realizaram uma análise jurisprudencial e legislativa e com enfoque no Estatuto do Idoso, argumentando que o etarismo é fundamento estrutural e não situacional, percebendo em diversas situações da vida cotidiana. Concluiu que a responsabilização de ser do Estado e da sociedade.

Cinthia Karla Flores da Silveira e Célia de Oliveira de Santana no estudo sobre o ECA Digital – Lei n.º 15.211, identificaram lacunas estruturais relacionadas à fiscalização, especialmente quanto à ausência de definição clara da autoridade fiscalizadora, à autoidentificação da criança, à concentração das sanções no Poder Judiciário e à insuficiência de mecanismos de cooperação internacional, concluindo, portanto, que há a necessidade de questionamento acerca da nova lei e do aperfeiçoamento das fragilidades evidenciadas.

Déa Carla Pereira Nery na pesquisa intitulada *o Reconhecimento facial e seletividade penal*, onde sustentou que as plataformas de reconhecimento não são neutras na identificação de suspeitos, observando-se recorrência de erros especificamente em relação à população negra.

Fausy Vieira Salomão e Luana Bernardi Coelho de Oliveira na pesquisa sobre a Efetividade da liberdade religiosa e racismo institucional, discutiram acerca da burocratização do racismo. Colocaram como estudo de caso a questão da proibição dos cultos religiosos de

Prof. Dr. André Pires Gontijo - UNIEURO

**RECONHECIMENTO FACIAL, SELETIVIDADE PENAL E DEVIDO PROCESSO:
RISCOS ALGORÍTMICOS E PROTEÇÃO DE GARANTIAS FUNDAMENTAIS NO
SISTEMA DE JUSTIÇA CRIMINAL BRASILEIRO.**

**FACIAL RECOGNITION, CRIMINAL SELECTIVITY AND DUE PROCESS:
ALGORITHMIC RISKS AND THE PROTECTION OF FUNDAMENTAL
GUARANTEES IN THE BRAZILIAN CRIMINAL JUSTICE SYSTEM.**

Dea Carla Pereira Nery

Resumo

A expansão do reconhecimento facial na segurança pública brasileira tem sido acompanhada por um discurso de eficiência, modernização e neutralidade tecnológica. Todavia, a incorporação desse recurso ao sistema de justiça criminal suscita questionamentos relevantes sobre discriminação algorítmica, seletividade penal, opacidade decisória e erosão de direitos fundamentais. O presente artigo investiga de que modo o uso do reconhecimento facial, no contexto da perseguição penal, pode aprofundar padrões históricos de controle seletivo e comprometer garantias estruturantes do Estado Democrático de Direito. O problema de pesquisa consiste em verificar se a promessa de maior eficácia investigativa se sustenta diante dos riscos de falsos positivos, vieses raciais e fragilização do devido processo legal. Parte-se da hipótese de que, em um sistema penal historicamente seletivo, a automação da identificação de suspeitos tende a reproduzir e intensificar desigualdades preexistentes, sobretudo contra populações negras, pobres e periféricas. A metodologia é qualitativa, de natureza exploratória e crítico-dogmática, desenvolvida por meio de revisão bibliográfica, análise documental e exame de referências normativas nacionais e internacionais. Conclui-se que o reconhecimento facial, em seu atual estágio de utilização na segurança pública brasileira, não pode ser tratado como instrumento neutro de prova ou investigação. Ao contrário, sua adoção desregulada amplia riscos de prisões injustas, dificulta o exercício do contraditório, compromete a proteção de dados pessoais e exige parâmetros regulatórios rigorosos, com transparência, auditoria independente, supervisão humana qualificada e controle judicial estrito.

guarantees of the Democratic Rule of Law. The research problem is to assess whether the promise of greater investigative efficiency can withstand the risks of false positives, racial bias, and the weakening of due process of law. The central hypothesis is that, within a historically selective criminal justice system, the automation of suspect identification tends to reproduce and intensify pre-existing inequalities, especially against Black, poor, and peripheral populations. The methodology is qualitative, exploratory, and critical-dogmatic, based on bibliographical review, documentary analysis, and the examination of national and international legal references. The article concludes that facial recognition, at its current stage of use in Brazilian public security, cannot be treated as a neutral investigative or evidentiary tool. On the contrary, its unregulated adoption increases the risk of wrongful arrests, hinders adversarial defense, compromises personal data protection, and demands strict regulatory standards, including transparency, independent auditing, meaningful human oversight, and rigorous judicial review.

Keywords/Palabras-claves/Mots-clés: Facial recognition, Criminal selectivity, Due process of law, Algorithmic surveillance, Fundamental rights

1 INTRODUÇÃO

A presença crescente de sistemas de inteligência artificial no campo da segurança pública tem alterado, de maneira profunda, as formas de vigilância, identificação e intervenção estatal sobre os indivíduos. Entre essas tecnologias, o reconhecimento facial ocupa posição central, tanto pela promessa de ganho operacional quanto pelo potencial de reconfigurar as fronteiras entre liberdade, privacidade e poder punitivo. Em diversas cidades brasileiras, sua adoção tem sido apresentada como resposta técnica à criminalidade, sobretudo em ambientes de grande circulação, como vias públicas, eventos, estações de transporte e equipamentos urbanos monitorados por câmeras.

Esse processo, contudo, não pode ser examinado apenas sob a ótica da inovação administrativa ou da eficiência policial. A literatura crítica tem demonstrado que tecnologias algorítmicas não são neutras. Elas dependem de bases de dados, critérios de programação, escolhas institucionais e contextos de implementação que refletem assimetrias sociais já existentes. Por essa razão, quando sistemas de reconhecimento facial são incorporados a uma estrutura penal historicamente seletiva, marcada por desigualdades raciais, territoriais e socioeconômicas, surge o risco de que a automação reforce padrões discriminatórios sob a aparência de objetividade técnica.

O problema de pesquisa que orienta este estudo consiste em investigar de que modo o uso do reconhecimento facial no âmbito da segurança pública e da justiça criminal contribui para aprofundar a seletividade penal e comprometer garantias fundamentais. A questão central pode ser formulada nos seguintes termos: a adoção dessa tecnologia, apresentada como instrumento de maior precisão investigativa, é compatível com o devido processo legal, a presunção de inocência, a igualdade e a proteção de dados pessoais em um Estado Democrático de Direito?

A hipótese desenvolvida é a de que o reconhecimento facial, longe de representar mecanismo puramente técnico de identificação, tende a reproduzir e intensificar padrões históricos de vigilância seletiva, sobretudo quando utilizado em contextos de baixa transparência, ausência de auditoria independente e fragilidade regulatória. Em outras palavras, inserido em um sistema penal que já incide de forma desproporcional sobre pessoas negras, pobres e periféricas, o recurso algorítmico não corrige distorções; ao contrário, pode automatizá-las, ampliando o risco de abordagens abusivas, constrangimentos ilegítimos e prisões injustas.

O objetivo geral do artigo é analisar criticamente os impactos do reconhecimento facial sobre a seletividade penal e as garantias fundamentais no sistema de justiça criminal brasileiro. Como objetivos específicos, pretende-se: examinar o funcionamento dessa tecnologia e sua inserção no paradigma da vigilância algorítmica; discutir os vieses algorítmicos e seus efeitos na produção de suspeição penal; avaliar os reflexos do reconhecimento facial sobre o devido processo legal, a presunção de inocência, a igualdade e a proteção de dados pessoais; e, por fim, indicar limites normativos e parâmetros regulatórios compatíveis com a ordem constitucional brasileira.

A metodologia adotada é qualitativa, de caráter exploratório e crítico-dogmático. O estudo foi desenvolvido mediante revisão bibliográfica interdisciplinar, com diálogo entre criminologia crítica, teoria do controle social, direito constitucional, direito processual penal e estudos sobre governança algorítmica. Também se procedeu à análise documental de materiais institucionais e normativos, com destaque para a Constituição da República, a Lei Geral de Proteção de Dados Pessoais, o relatório do Grupo de Trabalho do Conselho Nacional de Justiça sobre reconhecimento de pessoas, a Portaria MJSP nº 961/2025 e o debate legislativo em torno do Projeto de Lei nº 2.338/2023. No plano comparado, consideram-se ainda referências internacionais sobre vieses demográficos e restrições regulatórias à identificação biométrica remota em espaços públicos.

A relevância do tema decorre de uma dupla circunstância. De um lado, a expansão do reconhecimento facial avança em ritmo superior ao amadurecimento dos controles jurídicos e institucionais capazes de conter abusos. De outro, as consequências de erros ou vieses produzidos por essa tecnologia não se limitam à esfera abstrata da inovação, mas alcançam diretamente a liberdade, a honra, a imagem e a dignidade das pessoas submetidas à atuação estatal. Nessa medida, discutir reconhecimento facial não significa apenas discutir tecnologia; significa discutir quais limites a democracia impõe ao poder de vigiar, classificar e punir.

A exposição está organizada em quatro seções analíticas, além desta introdução e das considerações finais. Na primeira, examina-se o reconhecimento facial como instrumento de vigilância algorítmica e de ampliação do controle social. Na segunda, discute-se a relação entre viés algorítmico e seletividade penal, com ênfase no contexto brasileiro. Na terceira, analisam-se os impactos sobre garantias fundamentais, especialmente devido processo, presunção de

inocência, igualdade e proteção de dados pessoais. Na quarta, apresentam-se limites jurídicos e parâmetros regulatórios para o uso dessa tecnologia na segurança pública.

2 RECONHECIMENTO FACIAL E VIGILÂNCIA ALGORÍTMICA NA SEGURANÇA PÚBLICA

O reconhecimento facial pode ser descrito, em termos gerais, como um conjunto de técnicas computacionais voltadas à identificação ou verificação de identidade por meio da comparação de traços biométricos faciais. Em sua operação ordinária, o sistema detecta uma face em imagem ou vídeo, extrai pontos de referência, converte esses elementos em um padrão matemático e compara o resultado com bases de imagens previamente armazenadas. Caso a correspondência ultrapasse determinado limiar probabilístico, o sistema emite um alerta de identificação. Embora essa descrição sugira objetividade e precisão, ela oculta decisões técnicas e institucionais determinantes, como a qualidade das imagens captadas, a composição da base de treinamento, os critérios de correspondência e os protocolos adotados após a geração do resultado.

A dimensão jurídica do problema emerge precisamente porque o reconhecimento facial não atua em vazio social. Inserido na infraestrutura urbana, ele converte câmeras de monitoramento em dispositivos de identificação contínua, aptos a rastrear deslocamentos, seleccionar suspeitos e produzir bancos de dados sensíveis em larga escala. O que antes era, em muitos casos, mera captação passiva de imagens transforma-se em vigilância biométrica ativa. A diferença é substancial: o foco deixa de ser apenas o registro de fatos passados e passa a incluir a filtragem permanente de pessoas em circulação.

Esse cenário se enquadra no paradigma da vigilância algorítmica, caracterizado pela coleta automatizada de dados, pelo processamento massivo de informações pessoais e pela classificação de indivíduos com base em padrões inferidos por sistemas computacionais. A vigilância, nesse contexto, torna-se mais capilar, menos visível e mais difícil de contestar. Em vez de depender de observação humana contínua, opera por meio de infraestruturas técnicas que monitoram populações inteiras e produzem alertas de risco ou suspeição em tempo real.

Sob a perspectiva criminológica, essa transformação altera a própria racionalidade do controle social. O espaço público tende a deixar de ser ambiente de anonimato relativo para converter-se em território de rastreabilidade permanente. A consequência não é apenas tecnológica, mas político-jurídica: ao expandir a capacidade estatal de observar e classificar indivíduos, o reconhecimento facial favorece formas preventivas e atuariais de controle, nas quais

o foco recai menos sobre o fato concretamente praticado e mais sobre a antecipação de riscos, a gestão de probabilidades e a identificação automatizada de perfis considerados suspeitos.

A retórica institucional que acompanha a difusão dessa tecnologia costuma enfatizar três promessas centrais: rapidez, precisão e eficiência. Afirmar-se que o reconhecimento facial contribuiria para localizar foragidos, prevenir delitos, apoiar investigações e otimizar recursos humanos. Ocorre que essas promessas, quando não submetidas a testes públicos e independentes, podem funcionar como estratégia de legitimação política de instrumentos intrusivos. A ausência de evidências robustas sobre efetividade, aliada à baixa transparência contratual e técnica, dificulta a avaliação democrática do custo jurídico e social dessa escolha.

No Brasil, essa preocupação mostra-se especialmente relevante. Mapeamentos recentes indicam a disseminação de tecnologias de reconhecimento facial em diferentes órgãos de segurança e justiça, frequentemente sem critérios claros de governança, transparência ou prestação de contas. O debate público, por sua vez, nem sempre acompanha a velocidade da implementação. Em muitos casos, a tecnologia é adquirida e operacionalizada antes mesmo da definição de protocolos consistentes de auditoria, explicabilidade, preservação da cadeia de custódia e acesso da defesa às informações técnicas necessárias à impugnação do resultado produzido.

A opacidade constitui, aliás, um dos pontos mais sensíveis da matéria. Muitos desses sistemas são desenvolvidos por empresas privadas e protegidos por segredo comercial, o que dificulta o acesso a informações relativas ao banco de treinamento, às métricas reais de erro, ao funcionamento interno do algoritmo e aos fatores que produziram determinada correspondência. Quando a atuação estatal se apoia em tecnologias cuja inteligibilidade é restrita a fornecedores ou especialistas, surge uma tensão evidente com os princípios da publicidade administrativa, da motivação dos atos estatais e do controle jurisdicional efetivo.

Também não se pode ignorar a dimensão econômica e política dessa expansão. A vigilância biométrica se insere em um ecossistema mais amplo de mercantilização de dados e oferta de soluções de segurança por atores privados. Isso cria incentivos institucionais para a incorporação de tecnologias cada vez mais invasivas, muitas vezes justificadas por narrativas de modernização, mas desvinculadas de avaliação séria sobre impactos distributivos e constitucionais. A tecnologia, assim, deixa de ser mera ferramenta operacional e passa a integrar um modelo de gestão da segurança orientado por predição, classificação e rastreamento massivo.

Nesse contexto, o reconhecimento facial não deve ser entendido como simples aperfeiçoamento instrumental do policiamento. Trata-se, antes, de mecanismo que reordena a forma de exercício do poder de polícia, deslocando-o para um terreno em que a suspeita pode ser acionada por probabilidades algorítmicas, por correspondências estatísticas e por critérios técnicos pouco acessíveis ao escrutínio público. Essa constatação é decisiva para compreender por que a discussão sobre reconhecimento facial exige abordagem jurídica e democrática mais rigorosa do que aquela normalmente reservada a meras inovações administrativas.

3 VIÉS ALGORÍTMICO E SELETIVIDADE PENAL NO CONTEXTO BRASILEIRO

A seletividade penal constitui traço estrutural do sistema de justiça criminal. A criminologia crítica há décadas evidencia que o poder punitivo não incide de maneira uniforme sobre todos os grupos sociais, mas se concentra, com maior intensidade, sobre segmentos historicamente vulnerabilizados. No Brasil, essa seletividade apresenta forte dimensão racial, territorial e classista, atingindo de modo desproporcional pessoas negras, pobres e periféricas. Esse dado de realidade é indispensável para qualquer avaliação sobre o impacto de tecnologias de identificação automatizada.

Em tese, poderia parecer que o uso de algoritmos reduziria a arbitrariedade humana e contribuiria para decisões mais imparciais. No entanto, esse argumento desconsidera que sistemas algorítmicos são treinados e avaliados a partir de bases de dados socialmente produzidas. Se os dados de origem refletem padrões históricos de desigualdade, a automação tende a reproduzir tais padrões. Em vez de eliminar vieses, a tecnologia pode codificá-los, amplificá-los e revesti-los de aparência técnica.

Estudos internacionais já apontaram diferenças de desempenho em sistemas de reconhecimento facial conforme raça, sexo e idade, com impactos relevantes nas taxas de falsos positivos e falsos negativos. No campo da segurança pública, tais distorções adquirem gravidade singular, porque um erro de identificação não representa mero inconveniente estatístico: pode desencadear abordagem policial, condução coercitiva, constrangimento público, prisão cautelar ou mesmo condenação injusta quando inserido em cadeias probatórias frágeis.

No caso brasileiro, o problema assume contornos ainda mais agudos. O sistema penal nacional opera em ambiente de racismo estrutural e de histórica naturalização da suspeição sobre determinados corpos e territórios. Quando o reconhecimento facial é implementado em áreas periféricas, terminais de transporte ou eventos populares, ele não amplia a vigilância de forma

neutra; amplia, em grande medida, a vigilância sobre populações já mais expostas ao controle estatal. A seletividade, portanto, não se manifesta apenas no algoritmo em si, mas também no desenho institucional de sua implantação.

Há, nesse ponto, uma dimensão espacial relevante. A distribuição desigual de câmeras e sistemas de monitoramento em áreas urbanas tende a reforçar circuitos de observação sobre regiões socialmente marcadas pela pobreza e pela presença majoritária de população negra. A consequência é um ciclo de retroalimentação: mais vigilância nesses locais produz mais abordagens e registros; esses registros alimentam bancos de dados criminais; tais bancos, por sua vez, influenciam futuras identificações, aprofundando a incidência do controle sobre os mesmos grupos. A seletividade penal passa, assim, a ser reproduzida em linguagem algorítmica.

Esse fenômeno dialoga com a crítica ao chamado viés de automação. Uma vez emitido o alerta pelo sistema, agentes públicos podem atribuir ao resultado elevado grau de confiabilidade, reduzindo o espaço para verificação crítica e aumentando a probabilidade de que a atuação policial se oriente por uma confiança excessiva na máquina. A autoridade simbólica do algoritmo tende a converter uma hipótese de correspondência em quase certeza prática, mesmo quando o sistema opera com margens significativas de erro ou em condições inadequadas de imagem, iluminação e resolução.

Além disso, é necessário considerar a composição dos bancos de dados utilizados para comparação biométrica. Quando bases estatais se formam a partir de registros produzidos por um sistema penal previamente seletivo, elas não constituem espelho neutro da população, mas repositório assimétrico de pessoas já mais expostas à intervenção criminal. A base de comparação, portanto, já carrega o peso histórico das desigualdades punitivas. O resultado é que o algoritmo pode funcionar como mecanismo de estabilização e reprodução de discriminações anteriores, e não como corretivo.

A literatura e os relatórios institucionais brasileiros sobre reconhecimento de pessoas reforçam esse diagnóstico. Dados difundidos no debate público e institucional apontam que os erros de reconhecimento e as condenações injustas atingem majoritariamente pessoas negras, evidenciando que a falha probatória não se distribui aleatoriamente. Trata-se de um dado central: quando o erro tem padrão racializado, ele deixa de ser simples imperfeição técnica para revelar problema estrutural de justiça, igualdade e legitimidade democrática.

Nesse sentido, o reconhecimento facial não deve ser examinado apenas como tecnologia de identificação, mas como dispositivo de produção de suspeição penal. Seu uso em segurança pública interfere na definição prática de quem será observado, abordado, parado e investigado. Ao selecionar rostos, comparar bases e emitir alertas, o sistema participa da construção institucional da figura do suspeito. Em sociedades profundamente desiguais, isso significa participar da reatualização de hierarquias raciais e sociais que historicamente orientam o controle penal.

A consequência teórica e normativa dessa análise é decisiva. Se a seletividade penal já constitui dado estrutural do sistema de justiça criminal, qualquer inovação tecnológica deve ser avaliada não apenas por sua suposta eficácia, mas por sua capacidade de agravar ou mitigar assimetrias. No caso do reconhecimento facial, os indícios apontam para um cenário de agravamento. A automação da vigilância, em vez de neutralizar desigualdades, tende a sofisticar a seletividade por meio de procedimentos opacos, distribuídos e permanentemente legitimados por um discurso de precisão científica.

4 RECONHECIMENTO FACIAL E VIOLAÇÕES DE GARANTIAS FUNDAMENTAIS

A expansão do reconhecimento facial na segurança pública repercute diretamente sobre um conjunto de garantias que estruturam o Estado Democrático de Direito. O ponto não reside apenas em saber se a tecnologia funciona com maior ou menor precisão, mas em verificar se sua lógica de operação é compatível com os parâmetros constitucionais que limitam a atuação punitiva do Estado. A resposta exige examinar, de forma articulada, o devido processo legal, a presunção de inocência, a igualdade, a proteção de dados pessoais e a própria admissibilidade da prova produzida ou influenciada por sistemas algorítmicos.

O devido processo legal é afetado, em primeiro lugar, pela opacidade dos sistemas utilizados. Não há contraditório efetivo quando a defesa não consegue compreender os critérios que levaram à identificação, tampouco acessar de modo amplo os dados necessários à contestação do resultado. Se o sistema opera como caixa-preta, protegido por sigilo técnico ou comercial, a parte acusada não dispõe dos meios mínimos para impugnar a confiabilidade da correspondência, a adequação da base utilizada, a taxa real de erro ou as condições concretas da captação. Nessa hipótese, a assimetria informacional entre acusação e defesa compromete o conteúdo substancial da ampla defesa.

A presunção de inocência também sofre abalo relevante. Em ambientes monitorados por reconhecimento facial, todos os transeuntes passam a ser permanentemente comparados com bases criminais ou investigativas, como se a circulação no espaço público autorizasse, por si só, uma triagem biométrica contínua. A lógica implícita é a de que qualquer pessoa pode ser tratada como suspeita até que o sistema deixe de apontá-la como coincidência relevante. A inversão é grave: em vez de a atuação estatal depender de indícios concretos e individualizados, a suspeição emerge de varredura generalizada e automatizada.

No plano da igualdade, o problema decorre da combinação entre vieses de desempenho e padrões seletivos de implementação. Se determinados grupos estão mais sujeitos a erros de identificação, abordagens e constrangimentos, há violação do dever estatal de tratamento isonômico. O princípio da igualdade não é compatível com tecnologias que, na prática, concentram riscos mais intensos sobre pessoas negras, periféricas e socialmente vulneráveis. Nesses casos, a desigualdade deixa de ser efeito colateral e passa a integrar o próprio modo de funcionamento da política de segurança.

Outra garantia diretamente implicada é a proteção de dados pessoais, especialmente em sua vertente de tutela dos dados sensíveis. A biometria facial constitui informação singular, permanente e intensamente identificadora. Diferentemente de senhas ou credenciais substituíveis, o rosto não pode ser simplesmente alterado após uso indevido, vazamento ou tratamento abusivo. Por isso, sua coleta e processamento em massa exigem cautela redobrada. A transformação do corpo em chave contínua de rastreamento e classificação projeta nova forma de vulnerabilidade sobre os titulares de dados.

No ordenamento brasileiro, a proteção de dados foi alçada à condição de direito fundamental, o que reforça a necessidade de submeter qualquer tratamento biométrico a critérios estritos de necessidade, finalidade, adequação, proporcionalidade e transparência. Ainda que a LGPD preveja exceções ou regimes específicos para a segurança pública e a persecução penal, isso não autoriza espaço normativo de indiferença constitucional. Ao contrário, quanto mais sensível e intrusivo for o tratamento, mais robustas devem ser as salvaguardas legais, institucionais e procedimentais.

Também merece destaque a relação entre reconhecimento facial e prova penal. Um alerta algorítmico não equivale, por si só, a prova conclusiva de identidade. Trata-se, quando muito, de resultado probabilístico condicionado por fatores técnicos e contextuais. Transformar

essa correspondência em fundamento isolado para prisão, denúncia ou condenação representa confusão entre indício tecnológico e certeza jurídica. A prova penal, sobretudo quando afeta liberdade, deve satisfazer padrões rigorosos de confiabilidade, contraditório e corroboração. A confiança acrítica no algoritmo enfraquece essas exigências.

A cadeia de custódia da evidência digital agrava a questão. Para que um resultado de reconhecimento facial seja minimamente escrutinável, seria necessário preservar, de forma íntegra, as imagens captadas, os metadados, os registros de processamento, os parâmetros utilizados, a identificação da base consultada e os logs das intervenções humanas subsequentes. Sem esses elementos, a defesa não consegue reconstruir o itinerário técnico da identificação nem demonstrar eventuais falhas, contaminações ou manipulações. Em outras palavras, a opacidade do sistema repercute também na fragilidade da prova.

Há ainda um efeito difuso, mas relevante, sobre outras liberdades públicas. A percepção de monitoramento biométrico permanente pode produzir efeito inibidor sobre o exercício da liberdade de reunião, manifestação, circulação e expressão. Cidadãos submetidos à sensação de estarem constantemente identificáveis e rastreáveis tendem a ajustar condutas, evitar determinados espaços e moderar sua atuação pública. A vigilância biométrica, assim, não interfere apenas na persecução penal posterior; ela molda preventivamente comportamentos e restringe o ambiente democrático de exercício das liberdades.

Por todas essas razões, o reconhecimento facial desafia categorias clássicas do processo penal e do direito constitucional. Ele tensiona a exigência de motivação racional da suspeita, reconfigura a natureza da prova de identidade, amplia a distância técnica entre Estado e cidadão e projeta discriminações estruturais sobre procedimentos que deveriam ser juridicamente controláveis. Não se trata, portanto, de simples questão de eficiência administrativa, mas de um teste contemporâneo da capacidade do constitucionalismo de impor limites efetivos ao uso de tecnologias invasivas em matéria penal.

5 LIMITES NORMATIVOS E PARÂMETROS REGULATÓRIOS PARA O USO NA SEGURANÇA PÚBLICA

Diante dos riscos analisados, a questão central passa a ser a definição de limites jurídicos para o emprego do reconhecimento facial. O ponto de partida deve ser a afirmação de que, em matéria penal e de segurança pública, inovação tecnológica não pode significar suspensão tácita

de garantias constitucionais. Ao contrário, quanto maior o potencial lesivo da ferramenta, mais densa deve ser a arquitetura de controle normativo, institucional e jurisdicional.

No plano brasileiro, a Constituição da República oferece o marco decisivo. A dignidade da pessoa humana, a igualdade, a intimidade, a honra, a imagem, o devido processo legal, a ampla defesa e a presunção de inocência formam um conjunto de limites materiais que vinculam qualquer política pública de vigilância. O reconhecimento facial, portanto, somente poderia ser admitido em ambiente de estrita legalidade, controle de proporcionalidade e demonstração objetiva de necessidade. Soluções tecnológicas amplas, genéricas ou massificadas não se coadunam com esse regime constitucional de proteção reforçada.

A Lei Geral de Proteção de Dados, embora tenha ressalvas quanto ao tratamento de dados para segurança pública e persecução penal, não elimina a exigência de legislação específica e de salvaguardas adequadas. Ao contrário, a exclusão parcial do seu regime geral evidencia a urgência de um marco normativo setorial mais claro e rigoroso. A inexistência de uma disciplina abrangente para tratamento de dados na esfera penal e de segurança pública aprofunda a insegurança jurídica e favorece práticas administrativas desuniformes, muitas vezes apoiadas em contratos opacos e protocolos internos inacessíveis ao escrutínio social.

Nesse cenário, a Portaria MJSP nº 961/2025 representa tentativa relevante de estabelecer diretrizes para o uso de soluções tecnológicas em investigações criminais e inteligência de segurança pública, especialmente ao reafirmar a centralidade dos direitos fundamentais, da privacidade, da proteção de dados e do devido processo legal. Embora a portaria não resolva sozinha os problemas estruturais do reconhecimento facial, ela sinaliza que o debate regulatório já não pode prescindir de categorias como supervisão humana, governança, rastreabilidade e responsabilidade institucional.

No âmbito legislativo, o debate em torno do Projeto de Lei nº 2.338/2023 demonstra que a inteligência artificial passou a ser tratada sob lógica regulatória baseada em risco. Esse movimento é importante, mas insuficiente se não vier acompanhado de limites substantivos severos para a identificação biométrica remota em espaços públicos. A experiência internacional mostra que, justamente por afetar intensamente direitos fundamentais, esse tipo de sistema tem recebido tratamento jurídico mais restritivo, sobretudo quando voltado à atuação policial em tempo real.

Por essa razão, o primeiro parâmetro regulatório consistente é a adoção de postura de máxima cautela. Enquanto não houver demonstração pública e independente de confiabilidade técnica adequada, ausência de discriminações sistemáticas e compatibilidade com o devido processo legal, a utilização de reconhecimento facial em segurança pública deve ser limitada de forma intensa, podendo inclusive justificar moratórias ou proibições em usos massivos e indiscriminados. O argumento da urgência securitária não pode funcionar como salvo-conduto para experimentação estatal sobre direitos fundamentais.

O segundo parâmetro é a transparência robusta. Órgãos públicos devem divulgar, de forma acessível, quais sistemas utilizam, com que finalidade, quais bases de dados alimentam as comparações, quais métricas de desempenho foram aferidas, quais empresas fornecem a tecnologia e quais protocolos orientam a atuação humana após a emissão do alerta. Sem publicidade ativa e inteligível, não há controle democrático. A transparência deve alcançar tanto a contratação quanto a operação cotidiana da tecnologia.

O terceiro parâmetro consiste na auditoria independente e periódica. Sistemas de reconhecimento facial precisam ser submetidos a avaliações técnicas externas capazes de medir taxas de erro, impactos discriminatórios, deriva de desempenho e adequação dos contextos de uso. Auditorias meramente formais ou conduzidas exclusivamente pelo fornecedor não bastam. A confiabilidade da tecnologia só pode ser minimamente aceita quando testada por instâncias autônomas, com metodologia pública e possibilidade de escrutínio por comunidade científica, órgãos de controle e sociedade civil.

O quarto parâmetro é a supervisão humana qualificada. Isso significa que o alerta algorítmico não pode gerar automaticamente restrições de direitos. Toda correspondência deve ser tratada como elemento preliminar e submetida a avaliação humana crítica, devidamente capacitada para compreender margens de erro, limitações do sistema e riscos de viés de automação. Supervisão humana, porém, não pode ser meramente simbólica. Ela deve ser documentada, motivada e passível de revisão posterior.

O quinto parâmetro refere-se ao estatuto processual do resultado algorítmico. Em hipótese alguma o reconhecimento facial deve funcionar como prova isolada suficiente para fundamentar prisão cautelar, condenação ou medidas invasivas de grande intensidade. Seu eventual uso deve ser estritamente subsidiário, dependente de corroboração por outros elementos autônomos e submetido a contraditório pleno. Além disso, a defesa deve ter acesso integral aos

registros técnicos indispensáveis para impugnação da prova, inclusive logs, parâmetros, relatórios de auditoria e cadeia de custódia das imagens e processamentos.

O sexto parâmetro diz respeito à responsabilização. Danos decorrentes de falsos positivos, uso abusivo, retenção indevida de dados, vazamentos ou discriminações sistemáticas não podem ser tratados como meros acidentes operacionais. O Estado deve responder de modo efetivo por violações produzidas em nome da inovação tecnológica, inclusive com mecanismos de reparação, revisão de procedimentos, suspensão de sistemas inadequados e responsabilização administrativa dos agentes e fornecedores envolvidos.

Por fim, a regulação precisa incorporar participação social e controle externo. Políticas públicas que ampliam a capacidade de vigilância do Estado não podem ser decididas exclusivamente em arenas técnicas ou contratuais. A legitimidade democrática do uso de reconhecimento facial depende de debate público informado, de acompanhamento por órgãos de controle, defensorias, ministério público, advocacia, academia e organizações da sociedade civil. Sem essa abertura, a regulação corre o risco de se converter em mera linguagem formal de legitimação de práticas previamente consolidadas.

6 CONSIDERAÇÕES FINAIS

O desenvolvimento deste estudo permitiu demonstrar que o reconhecimento facial, quando empregado no âmbito da segurança pública e da justiça criminal, não pode ser compreendido como simples inovação neutra destinada a aprimorar a eficiência investigativa. Trata-se de tecnologia que reorganiza a produção da suspeição penal, amplia a capacidade estatal de vigilância e projeta, sobre a persecução criminal, problemas complexos de discriminação, opacidade e fragilização de direitos fundamentais.

A análise evidenciou, em primeiro lugar, que a inserção do reconhecimento facial no paradigma da vigilância algorítmica transforma o espaço público em ambiente de rastreamento contínuo, no qual a identificação biométrica deixa de ser medida excepcional e passa a operar como lógica permanente de filtragem populacional. Esse deslocamento altera a racionalidade do controle social e reforça formas preventivas de suspeição incompatíveis com a tradição garantista do processo penal democrático.

Em segundo lugar, verificou-se que os riscos do reconhecimento facial não se distribuem de forma abstrata ou uniforme. Em um sistema penal historicamente seletivo, marcado por racismo estrutural e profunda desigualdade socioespacial, a automação da identificação tende a

reproduzir e intensificar padrões de controle já dirigidos a populações negras, pobres e periféricas. O problema, portanto, não se limita a falhas técnicas isoladas. Ele reside na convergência entre viés algorítmico, desenho institucional da vigilância e estrutura seletiva do poder punitivo.

Em terceiro lugar, concluiu-se que o uso desregulado dessa tecnologia compromete garantias fundamentais centrais. A opacidade algorítmica enfraquece o contraditório e a ampla defesa; a triagem biométrica contínua tensiona a presunção de inocência; os vieses de desempenho e implementação afetam a igualdade; e o tratamento massivo de biometria impõe riscos severos à privacidade e à proteção de dados pessoais. No plano probatório, o reconhecimento facial não pode ser equiparado a meio de prova conclusivo, tampouco servir como fundamento isolado para medidas restritivas de liberdade.

A hipótese inicialmente formulada foi, assim, confirmada. Longe de corrigir as distorções do sistema penal, o reconhecimento facial tende a automatizar e sofisticar mecanismos históricos de seletividade, atribuindo-lhes aparência de precisão científica. Em razão disso, o debate jurídico sobre sua utilização deve abandonar o fascínio pela eficiência tecnológica e recentrar-se na pergunta constitucional decisiva: até que ponto uma democracia pode admitir mecanismos de vigilância biométrica que ampliam a suspeição generalizada e distribuem seus riscos de forma desigual?

A resposta proposta por este artigo é a de que o reconhecimento facial somente pode ser objeto de consideração jurídica sob regime de extrema cautela, transparência rigorosa, auditoria independente, supervisão humana significativa, contraditório pleno e controle judicial estrito. Na ausência dessas salvaguardas, sua utilização em segurança pública não representa modernização legítima, mas aprofundamento tecnicamente sofisticado do arbítrio e da desigualdade.

Em perspectiva final, o desafio posto ao direito contemporâneo não consiste em negar a existência da inovação tecnológica, mas em impedir que ela se converta em argumento de erosão das garantias construídas historicamente para conter o poder punitivo. Se a tecnologia pretende ocupar espaço na justiça criminal, deverá fazê-lo sob primazia absoluta da dignidade humana, da igualdade material e do devido processo legal. Fora desse horizonte, o reconhecimento facial deixa de ser promessa de segurança e passa a constituir risco objetivo à democracia constitucional.

REFERÊNCIAS

ARAÚJO, R. de Aguiar; CARDOSO, N. D.; et al. Regulação e uso do reconhecimento facial na segurança pública do Brasil. **Revista de Doutrina Jurídica**, Brasília, 2021.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018.

BRASIL. **Portaria MJSP nº 961, de 24 de junho de 2025**. Estabelece diretrizes sobre uso de soluções de tecnologia da informação aplicadas às atividades de investigação criminal e inteligência de segurança pública. Brasília, DF: Ministério da Justiça e Segurança Pública, 2025.

COIMBRA, J. P. M.; BARBOSA, A.; et al. Interseções entre racismo algorítmico, reconhecimento facial e segurança pública no Brasil. **Revista Direito, Políticas Públicas e Mundialização**, 2023.

CONSELHO NACIONAL DE JUSTIÇA. **Relatório do Grupo de Trabalho sobre Reconhecimento de Pessoas**. Brasília: CNJ, 2022.

DELEUZE, Gilles. **Conversações**. São Paulo: Editora 34, 1992.

FOUCAULT, Michel. **Vigiar e punir: nascimento da prisão**. Petrópolis: Vozes, 2014.

GARLAND, David. **A cultura do controle: crime e ordem social na sociedade contemporânea**. Rio de Janeiro: Revan, 2008.

GROTHER, Patrick; NGAN, Mei; HANOOKA, Kayee. **Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects**. Gaithersburg: National Institute of Standards and Technology, 2019.

HARCOURT, Bernard E. **Against prediction: profiling, policing, and punishing in an actuarial age**. Chicago: University of Chicago Press, 2007.

LIMANTÈ, Agnè. Bias in facial recognition technologies used by law enforcement: understanding the causes and searching for a way out. **Nordic Journal of Human Rights**, 2024.

NUNES, Pablo; LIMA, Thallita. Algoritmos decidem, mas quem se responsabiliza? Os riscos da adoção desregulada de tecnologias digitais na justiça criminal brasileira. **Fonte Segura**, 2025.

O'NEIL, Cathy. **Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça a democracia**. Santo André: Rua do Sabão, 2020.

PARLAMENTO EUROPEU; CONSELHO DA UNIÃO EUROPEIA. **Artificial Intelligence Act.** União Europeia, 2024.

ZAFFARONI, Eugenio Raúl. **Em busca das penas perdidas: a perda de legitimidade do sistema penal.** Rio de Janeiro: Revan, 1991.

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