

VIII ENCONTRO VIRTUAL DO CONPEDI

**DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS
II**

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 Napolini - 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

Direito, governança e novas tecnologias II [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Cinthia Obladen de Almendra Freitas; Yuri Nathan da Costa Lannes. – Florianópolis: CONPEDI, 2025.

Inclui bibliografia

ISBN: 978-65-5274-156-1

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

Tema: Direito Governança e Políticas de Inclusão

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias. VIII Encontro Virtual do CONPEDI (2; 2025; Florianópolis, Brasil).

CDU: 34



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

VIII ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

Apresentação

O VIII Encontro Virtual do CONPEDI, organizado pelo CONPEDI, teve como tema central “Direito Governança e Políticas de Inclusão”. A partir dessa temática, foram promovidos intensos debates entre pesquisadores nacionais e internacionais, com apresentações de trabalhos previamente selecionados por meio de avaliação duplo-cega por pares.

Os artigos reunidos nesta publicação foram apresentados no Grupo de Trabalho “Direito, Governança e Novas Tecnologias II”, realizado no dia 27 de junho de 2025, e refletem o estado atual das pesquisas desenvolvidas por graduandos e pós-graduandos em direito em diversas instituições brasileiras. O conjunto de trabalhos revela a diversidade temática e a profundidade das discussões jurídicas contemporâneas sobre os impactos da tecnologia na sociedade.

As apresentações cobriram uma ampla gama de tópicos que envolvem a interface entre tecnologia, direito, demonstrando um panorama das preocupações acadêmicas sobre o reconhecimento facial, a inteligência artificial e os desafios ao judiciário, direitos autorais e inteligência artificial, democracia digital e pós-verdade, governo digital, políticas públicas, sociedade digital e transformação do direito privacidade, desinformação e desigualdades digitais. Com o intuito de facilitar a leitura e destacar os enfoques abordados, os trabalhos foram organizados nos seguintes eixos temáticos:

1. Reconhecimento Facial, Vigilância e Direitos Fundamentais - Este eixo concentra estudos sobre o uso da tecnologia de reconhecimento facial no contexto da segurança pública e seus impactos sobre direitos fundamentais, com ênfase em discriminação algorítmica, proteção de

Reconhecimento facial para vigilância: comparação das aplicações da inteligência artificial em eventos de massa no Brasil e em experiências internacionais (Yuri Nathan da Costa Lannes / Júlia Mesquita Ferreira / Lais Faleiros Furuya)

Reconhecimento facial e a violação de direitos fundamentais: discriminação algorítmica, vigilância em massa e a necessidade de regulação no Brasil (Bibiana Paschoalino Barbosa / Anderson Akira Yamaguchi / Ruan Ricardo Bernardo Teodoro)

2. Inteligência Artificial, Judiciário e Regulação - Este eixo analisa a aplicação da inteligência artificial no sistema de justiça e os desafios regulatórios do contexto brasileiro, com foco na governança tecnológica e nos riscos da opacidade algorítmica:

O uso da inteligência artificial no Poder Judiciário brasileiro e a Resolução do Conselho Nacional de Justiça n.º 615/2025 (Simone Stabel Daudt / Rosane Leal Da Silva / Julia Daudt Mansilha)

Inteligência artificial e a crise da regulação clássica: um estudo sobre o atual contexto regulatório brasileiro (Fernanda Sathler Rocha Franco / Luiz Felipe de Freitas Cordeiro / Marina Moretzsohn Chust Trajano)

Direito à transparência, inteligência artificial e desafios técnicos: uma análise do Projeto de Lei nº 2.338/23 (Fernanda Sathler Rocha Franco)

Opacidade algorítmica estratégica e risco sistêmico informacional nas eleições: considerações para uma governança anti-manipulação das democracias digitais (Helena Dominguez Paes Landim Bianchi / Maria Clara Giasseti Medeiros Corradini Lopes)

3. Direitos Autorais, Propriedade Intelectual e IA - Reúne pesquisas que discutem a

O uso indevido das imagens geradas pelos filtros Ghibli e a proteção do direito à imagem sob a perspectiva da Lei Geral de Proteção de Dados (LGPD) (Lilian Benchimol Ferreira / Maria Cristina Almeida Pinheiro de Lemos / Narliane Alves De Souza E Sousa)

4. Democracia Digital, Desinformação e Pós-Verdade - Trabalhos que discutem os impactos da tecnologia na propagação de fake news, movimentos ideológicos e desinformação em contextos democráticos:

Movimentos antifeministas e desinformação: quando a misoginia se propaga em fake News (Juliana Aparecida de Jesus Pires / Irineu Francisco Barreto Junior / Samyra Haydêe Dal Farra Napolini)

A sociedade do cansaço e pós-verdade: fake news sobre as urnas eletrônicas (Bruna Figueiredo Dos Santos / Zulmar Antonio Fachin)

5. Governança Digital, Políticas Públicas e Compartilhamento de Dados - Aborda o papel das políticas públicas e da governança digital no século XXI, destacando os desafios do uso de dados por entes públicos e o potencial das tecnologias no desenvolvimento social:

Governança digital e democracia no século XXI: o papel das políticas públicas na era da inteligência artificial (Daniel David Guimarães Freire)

O potencial do compartilhamento de dados entre entes federativos para o desenvolvimento de políticas públicas inteligentes (Ana Cristina Neves Valotto Postal / Paulo Cezar Dias / Rodrigo Abolis Bastos)

6. Tecnologia, Sustentabilidade e Transformação Econômica - Esse eixo reúne trabalhos sobre o impacto das inovações tecnológicas em setores como o agronegócio e as ecotecnologias, destacando aspectos de compliance, sustentabilidade e tributação:

7. Sociedade Digital, Infância e Transformações do Direito - Trabalhos que discutem os efeitos das tecnologias emergentes sobre a infância, os registros civis, a exposição digital e os reflexos no Direito Civil e registral:

A vitrine digital da infância e o papel do Direito: análise do sharenting e das iniciativas legislativas brasileiras (Ana Júlia Oliveira Machado / Bibiana Paschoalino Barbosa)

Inovações e desafios na implantação das tecnologias notariais e registrais: uma análise do e-Notariado cinco anos após sua criação (José Luiz de Moura Faleiros Júnior / Francislene Silva Da Costa Garcia / Isabela da Cunha Machado Resende)

O impacto da tecnologia na sociedade aberta: desafios e oportunidades para o Direito Civil (Viviane Ferreira Mundim / Najua Samir Asad Ghani / Patricia Maria Paes de Barros)

Treinamento de inteligência artificial e consumidores mudando marcas de seus bens em protesto político (Carlos Alberto Rohrmann)

Espera-se que esta publicação contribua para o aprofundamento dos debates sobre os desafios jurídicos da era digital, estimulando novas reflexões e a produção científica crítica e inovadora. Agradecemos a todos os pesquisadores, pareceristas e organizadores que tornaram este Grupo de Trabalho possível. Desejamos uma excelente leitura!

Cinthia Obladen de Almendra Freitas – PUC-PR

Liton Lanes Pilau Sobrinho – UNIVALI

Yuri Nathan da costa Lannes - FDF

**RECONHECIMENTO FACIAL E A VIOLAÇÃO DE DIREITOS FUNDAMENTAIS:
DISCRIMINAÇÃO ALGORÍTMICA, VIGILÂNCIA EM MASSA E A
NECESSIDADE DE REGULAÇÃO NO BRASIL**

**FACIAL RECOGNITION AND THE VIOLATION OF FUNDAMENTAL RIGHTS:
ALGORITHMIC BIAS, MASS SURVEILLANCE AND THE NEED FOR
REGULATION IN BRAZIL**

Bibiana Paschoalino Barbosa ¹
Anderson Akira Yamaguchi ²
Ruan Ricardo Bernardo Teodoro ³

Resumo

Em um cenário de rápida expansão da implementação de sistemas de Reconhecimento Facial (RF) em capitais e municípios brasileiros para fins de segurança pública, a presente pesquisa pretende investigar os seguintes problemas: qual/quais impactos o uso indiscriminado do RF na segurança pública causa nos direitos fundamentais dos indivíduos submetidos à sua atuação? Havendo impactos negativos à tutela dos direitos fundamentais, quais soluções podem ser propostas para a remediação do problema? Desse modo, valeu-se da pesquisa qualitativa, analisando artigos, notícias, livros, periódicos, leis e regulamentos, entre outras fontes, para compreender e interpretar o fenômeno do avanço do uso do Reconhecimento Facial na segurança pública. Por fim, encontrou-se que o uso indiscriminado do RF na segurança pública acarreta violações aos direitos fundamentais, resultando em altos índices de “falsos” positivos, discriminação algorítmica de grupos racializados, de gênero e LGBTQIA+, potencialização da desigualdade social e vigilância em massa, sendo que a discussão pública acerca do RF deve ser estimulada, a fim de mitigar seus efeitos negativos, incluindo a publicação de projetos de lei e normas regulamentares específicas, não somente gerais, que delimitem o uso do RF, suprimindo as lacunas legais existentes.

Palavras-chave: Reconhecimento facial, Direitos fundamentais, Discriminação algorítmica, Regulação, vigilância

Brazilian capitals and municipalities for public security purposes, this research aims to investigate the following problems: what impact does the indiscriminate use of FR in public security have on the fundamental rights of individuals subjected to its use? If there are negative impacts on the protection of fundamental rights, what solutions can be proposed to remedy the problem? Thus, qualitative research was used, analyzing articles, news, books, periodicals, laws and regulations, among other sources, to understand and interpret the phenomenon of the advancing use of Facial Recognition in public security. Finally, it was found that the indiscriminate use of FR in public security leads to violations of fundamental rights, resulting in high rates of “false” positives, algorithmic bias against racialized, gender and LGBTQIA+ groups, increased social inequality and mass surveillance, thus, public discussion about FR should be stimulated in order to mitigate its negative effects, including the publication of bills and specific regulatory standards, not just general ones, which delimit the use of FR, filling existing legal gaps.

Keywords/Palabras-claves/Mots-clés: Facial recognition, Fundamental rights, Algorithmic bias, Regulation, surveillance

INTRODUÇÃO

Modelos de vigilância como o “Panótico” de Jeremy Bentham em 1785, as “teletelas” de George Orwell em sua obra 1984, publicada em 1949, ou a vida inteira de Truman exposta em telas no longa “O Show de Truman” do diretor Peter Weir, em 1998, revelam que preocupações quanto à vigilância tem se tornado cada vez mais frequentes desde o século XVIII.

Nessa seara, identifica-se um avanço na utilização de câmeras com tecnologia de Reconhecimento Facial no espaço público com a finalidade de promover a segurança pública, sendo aplicada para os mais diversos fins: cumprimento de mandados de prisão, verificação em duas etapas com o recurso da identificação biométrica, atribuição de “scores” sociais aos membros da população, entre outros.

Dessa maneira, a rápida expansão dessa tecnologia, embora traga evidentes aumentos na eficiência dos serviços e sistemas de vigilância, evidencia alguns problemas: qual/quais impactos o uso indiscriminado do Reconhecimento Facial causa nos direitos fundamentais dos indivíduos submetidos à sua atuação? Havendo impactos negativos à tutela dos direitos fundamentais, quais soluções podem ser propostas para a remediação do problema?

Essas e outras perguntas serão analisadas no decorrer da presente pesquisa, a qual pretende averiguar em que medida as ferramentas de Reconhecimento Facial utilizadas na segurança pública violam direitos fundamentais como a liberdade de ir e vir, a igualdade, presunção de inocência e privacidade, bem como, de que modo a regulação pode ou não ser uma das respostas ao problema formulado.

Para tais objetivos, realizou-se uma pesquisa qualitativa, analisando-se artigos, notícias, livros, periódicos, leis e regulamentos, entre outras fontes, para compreender e interpretar o fenômeno do avanço do uso do Reconhecimento Facial na segurança pública, assim como, sugestões e soluções para o problema evidenciado no trabalho, desenvolvendo 3 capítulos os quais tratam sobre o que é o Reconhecimento Facial, quais os riscos seu uso indiscriminado causa às liberdades fundamentais e como e se a regulação pode ser uma das soluções para mitigar os seus efeitos.

1 O QUE É O RECONHECIMENTO FACIAL?

O reconhecimento facial configura-se como uma das mais complexas e controversas inovações tecnológicas da contemporaneidade, situando-se na interseção entre

desenvolvimento científico, segurança pública e proteção de direitos fundamentais. Afinal, o que é o reconhecimento biométrico?

A autenticação por reconhecimento biométrico é uma tecnologia que identifica pessoas com base em características físicas, como impressões digitais, reconhecimento facial, voz, íris ou palma da mão (Rzemyk, 2017, p. 249-254). É uma forma de autenticação e segurança que pode ser usada em dispositivos eletrônicos, aeroportos, caixas automáticos e outros locais.

Deste modo, o reconhecimento facial é uma modalidade biométrica de identificação ou verificação de um indivíduo a partir de características faciais. Essa tecnologia utiliza algoritmos avançados de inteligência artificial e aprendizado de máquina para analisar imagens e/ou vídeos, identificando padrões específicos do rosto humano (Marinho, 2025, p. 02-03).

Seu funcionamento ocorre em três estágios sequenciais: a captura de imagens por dispositivos óticos, processamento biométrico mediante mapeamento de pontos nodais faciais – como a distância entre os olhos, o formato do nariz e da mandíbula, criando um modelo matemático único para cada indivíduo –, e comparação com banco de dados preexistentes (Oliveira, 2025, p. 10167).

A expansão dessa tecnologia tem sido marcada por aplicações diversas, abrangendo desde a esfera privada - como sistemas de autenticação em dispositivos eletrônicos - até políticas públicas de segurança (Hermes, 2025, p. 08-09). Contudo, tal disseminação ocorre sem o necessário aprofundamento crítico sobre seus impactos sociais e jurídicos, especialmente no que concerne à potencialização de desigualdades e violação de garantias fundamentais.

No plano jurídico, a utilização do reconhecimento facial enfrenta desafios particularmente complexos no ordenamento brasileiro. Embora a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) estabeleça princípios como finalidade, adequação e necessidade para o tratamento de dados biométricos (art. 6º), a ausência de regulamentação específica cria lacunas preocupantes, especialmente quando a tecnologia é empregada por órgãos de segurança pública. Como observa Hermes (2025, p. 09-12), a combinação entre sistemas imprecisos e estruturas institucionais com histórico de discriminação racial potencializa riscos à liberdade individual e à igualdade material.

A experiência comparada revela abordagens divergentes: enquanto países como a Alemanha adotam restrições rigorosas ao reconhecimento facial em espaços públicos, o Brasil segue tendência expansionista, com pelo menos oito capitais incluindo a tecnologia em suas

políticas de segurança (Melo; Serra, 2022, p. 213-214). Essa disparidade evidencia a necessidade de um debate fundamentado sobre os limites éticos e jurídicos da tecnologia, considerando especialmente seu impacto desproporcional sobre populações vulneráveis.

Mais detalhadamente, em estudo realizado pelos professores Paulo Victor Melo e Paulo Serra, identificou-se que 15 dos 26 prefeitos de capitais brasileiras apresentaram, em seus programas de governo nas eleições municipais de 2020, propostas que envolvem o uso de tecnologias digitais na área de segurança pública, sendo que 13 desses prefeitos mencionam a instalação de câmeras de monitoramento e 8 deles apontam a utilização de tecnologias de reconhecimento facial (2022, p. 213-214).

Destaca-se que a Bahia foi um dos estados pioneiros na implantação do Reconhecimento de dados biométricos para o cumprimento de mandados de prisão. Iniciado o sistema em 2019, as 3.500 câmeras instaladas em mais de 80 cidades do estado localizaram 3.000 mil foragidos até a data de 04 de abril de 2025. (Secretaria de Segurança Pública da Bahia, 2025)

A capital paranaense, por sua vez, com uma proposta de diminuir os índices de criminalidade e fortalecer a segurança pública, lançou em 2021 o programa “Muralha Digital”, o qual previu a instalação de 1.742 câmeras em pontos da região metropolitana de Curitiba, sendo que parte das câmeras instaladas permitia o reconhecimento facial (Rede Cidade Digital, 2021).

Tal realidade, no entanto, preocupa a esfera jurídica, uma vez que a aplicação do Reconhecimento Facial (RF) “para finalidades que visem a garantia da segurança pública apresenta riscos para os direitos fundamentais do indivíduo, como a liberdade, a privacidade, a inviolabilidade da vida íntima, dentre outros aspectos” (Almeida, 2022, p. 273).

Ainda, a questão do viés algorítmico nos sistemas de reconhecimento facial representa um desafio estrutural que transcende a mera imperfeição tecnológica. Esses vieses são, na realidade, um reflexo computacional de assimetrias sociais históricas, pois os algoritmos são desenvolvidos e treinados a partir de bases de dados que frequentemente sub-representam grupos étnicos minoritários, mulheres e populações com características fenotípicas diversas (Alves, 2025, p. 07). O núcleo do problema reside no fato de que a maioria dos conjuntos de dados utilizados para treinamento desses sistemas provém predominantemente de populações caucasianas do hemisfério norte, criando um padrão de referência distorcido que marginaliza outras características faciais.

A superação desses vieses exige abordagens multidimensionais. Primeiramente, é imperativo desenvolver bancos de dados representativos que contemplem a diversidade

étnica, de gênero e fenotípica das populações. Contudo, como alertam Buolamwini e Gebru (2018, p. 12), a simples ampliação quantitativa de dados não resolve o problema - é necessário um redesenho completo dos pipelines de desenvolvimento algorítmico, incorporando perspectivas interdisciplinares que incluam especialistas em ciências sociais e direitos humanos no processo de criação tecnológica.

A supervisão humana qualificada emerge como elemento crucial nesse contexto. Mais do que uma camada adicional de verificação, trata-se de implementar mecanismos de auditoria contínua que avaliem não apenas a precisão matemática dos sistemas, mas seu impacto social diferenciado. Como propõe Silva (2022, p. 81), é necessário estabelecer comitês éticos multidisciplinares com poder de veto sobre implementações dessas tecnologias em espaços públicos, garantindo que questões de equidade tenham peso equivalente a critérios técnicos de eficiência.

Assim, embora o reconhecimento facial configure um avanço tecnológico notável com aplicações promissoras em diversos setores, sua adoção apresenta uma complexa dicotomia entre eficiência operacional e salvaguarda de direitos fundamentais. A implementação dessa tecnologia demanda um equilíbrio delicado que contemple simultaneamente o progresso técnico e a proteção de garantias individuais e coletivas, especialmente em sociedades marcadas por profundas desigualdades estruturais.

Diante desse quadro, compreende-se que o reconhecimento facial transcende sua dimensão técnica, assumindo contornos de instrumento de poder com profundas implicações sociais. Sua implementação indiscriminada, sem as devidas salvaguardas jurídicas e técnicas, tende a aprofundar assimetrias sociais e comprometer garantias fundamentais historicamente consolidadas.

Os desenvolvimentos subsequentes deste trabalho analisarão com maior profundidade como os problemas concretos decorrentes dessa tecnologia - incluindo falsos positivos, discriminação algorítmica e vigilância em massa - desafiam o ordenamento jurídico e demandam respostas regulatórias adequadas, sob pena de consolidação de um paradigma tecnológico incompatível com os princípios constitucionais de uma sociedade democrática.

2 O RECONHECIMENTO FACIAL E AS (POSSÍVEIS) AMEAÇAS AOS DIREITOS INDIVIDUAIS

Dado que os sistemas de Reconhecimento Facial (RF) evoluíram ao ponto de identificar rostos particulares no meio de multidões, essas ferramentas estão sendo a aposta

principal de prefeitos, vereadores e deputados para o combate à criminalidade e à promoção da segurança pública.

No entanto, as propostas legislativas e propaganda política em torno da RF ignoram que o uso indiscriminado dessas ferramentas acarreta a violação de direitos fundamentais, podendo infringir a liberdade de ir e vir e a presunção de inocência com resultados “falso positivos”, a igualdade com a discriminação algorítmica sistemática e a privacidade com a vigilância em massa perpetrada pelo Estado.

2.1 Falsos Positivos

Primeiramente, verifica-se que o uso indiscriminado do reconhecimento facial na segurança pública, embora justificado pela eficiência, gera violações sistemáticas a direitos fundamentais, como a privacidade, a liberdade e a igualdade, especialmente em grupos vulneráveis, devido a falhas técnicas, vieses algorítmicos e “falsos positivos”.

Um exemplo disso é o caso do jovem negro Daniel Félix, o qual foi preso em abril de 2023 após ser indiciado em inquéritos no qual sua foto foi reconhecida equivocadamente como autor de um crime que não cometeu, sendo a terceira vez que teve que provar sua inocência perante o judiciário por fatos semelhantes (Brasil de Fato, 2023).

O fato narrado demonstra a ocorrência de um resultado “falso positivo”. Isso ocorre quando o Reconhecimento Facial confunde o rosto analisado com outro rosto em sua base de dados, identificando erroneamente a pessoa em questão como outra. Tal ocorrência gera um constrangimento para a pessoa identificada pelo “falso positivo”, pois, identificada equivocadamente a pessoa pelo RF, o resultado é presumido como correto e um inocente é preso sem maiores questionamentos.

Nesse caso, o cumprimento do Mandado de Prisão pela equipe policial, antes de demonstrar eficiência, apresenta uma flagrante violação ao princípio da presunção de inocência previsto no art. 5º, LVII, da Constituição Federal: o Reconhecimento Facial, na hipótese de um “falso positivo”, torna culpada a pessoa erroneamente identificada, como no caso de Daniel, e lhe nega a possibilidade de recorrer de imediato. Sua única salvação é provar sua inocência perante a justiça, após a violação de sua liberdade fundamental.

Ressalta-se que o fato narrado não foi um evento isolado, haja visto que não é incomum resultados “falsos positivos” durante a utilização de RF. Nesse sentido, em pesquisa promovida por estudiosos da Universidade de Essex em 2019, referente à adoção de uma série de testes de reconhecimento facial pela polícia metropolitana de Londres entre 2016 e 2019, a

qual organizou uma lista de observação para buscar pessoas procuradas em espaços públicos, encontrou-se que aproximadamente 63% dos indivíduos abordados eram resultados incorretos apontados pela tecnologia facial (Fussey; Murrey, 2019, p. 11).

Não obstante, em estudo realizado pelo Instituto Nacional de Padrões e Tecnologias dos Estados Unidos em 2019, que analisa recursos de reconhecimento facial e biometria para verificação e identificação, encontrou-se que taxas de “falsos positivos” de africanos e asiáticos são maiores do que de europeus orientais, podendo essa diferença chegar a ser de até 100 vezes maior entre os países (Grother; Ngan; Hanaoka, 2019, p. 2).

Assim, se em países com sistemas de controle mais rígidos, como Reino Unido e EUA, os erros são alarmantes, no Brasil – onde a regulação é incipiente e os bancos de dados são majoritariamente compostos por perfis brancos – os riscos de discriminação tornam-se ainda mais graves.

O RF, portanto, não apenas é passível de “falsos positivos”, como também esses resultados possuem maior incidência em certos grupos e etnias, isto é, negros e asiáticos, acarretando maiores constrangimentos a uma fatia da população que já sofre historicamente discriminação, sendo esta potencializada pelas novas tecnologias, como se verá a seguir.

Dessa maneira, verifica-se que resultados “falsos positivos” apontados pelas tecnologias de RF, podem levar a prisões injustas e equivocadas, as quais cerceiam a liberdade individual dos cidadãos, especialmente de negros e asiáticos. A mera intervenção humana pós-erro é insuficiente, como demonstrado no caso do Daniel Félix, em que já houve o constrangimento e a violação de seu direito à liberdade e à presunção de inocência.

Necessita-se de uma atuação preventiva como o treinamento de algoritmos com bancos de dados representativos, a devida ratificação de um profissional humano dos resultados, a obrigatoriedade de transparência nos sistemas usados pelo Estado, mecanismos de recursos para vítimas de falsos positivos, entre outros.

2.2 Discriminação Algorítmica

O reconhecimento facial (RF) não é neutro: sua aplicação reproduz e amplifica desigualdades sociais, especialmente contra negros, mulheres, pessoas trans e outras minorias. Isso ocorre porque os algoritmos são treinados em bancos de dados homogêneos e refletem preconceitos sociais, como demonstrado anteriormente com casos emblemáticos nos EUA e Europa.

Conforme apontam os estudiosos Paulo Victor Melo e Paulo Serra, a utilização de:

tecnologias digitais como estratégia de combate à criminalidade demonstra-se como uma tendência nas políticas de segurança pública no país. Tendo em conta esta questão e considerando os crescentes casos de prisões injustas e outros erros na identificação de pessoas a partir do reconhecimento facial, faz-se necessário que a aplicação dessas tecnologias seja acompanhada por um processo de discussão e acompanhamento públicos, envolvendo os diferentes segmentos da sociedade. (2022, p. 217)

Tal processo de discussão pública sugerido justifica-se a partir do reconhecimento de que as populações socialmente vulneráveis têm sido frequentemente sujeitas à automatização de constrangimentos e violências, proporcionadas pelo uso de tecnologias, a exemplo de abordagens policiais equivocadas e de antecedentes criminais incorretamente atribuídos (Costa; Kremer, 2022, p. 150-151). Assim, é necessário, para garantir a igualdade entre os cidadãos que essas populações socialmente vulneráveis participem ativamente do debate público acerca da tecnologia de Reconhecimento Facial.

Nesse sentido, um caso emblemático que afetou majoritariamente a população negra ocorreu nos Estados Unidos com a plataforma COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*), a qual era utilizada para prever a taxa de risco de reincidência de criminosos condenados pelo Estado, a fim de auxiliar nas decisões judiciais. Criada pela Northpointe Inc., essa ferramenta estimava a taxa de reincidência de criminosos, baseando-se em dados como a estabilidade do condenado nos locais em que residia, abuso de substâncias, isolamento social, entre outros.

Não obstante o amplo uso pelo Departamento Penitenciário (*Department of Corrections*) de diversos estados norte-americanos – como Wisconsin, Washington, Colorado, etc., o que se verificou durante a aplicação dessa ferramenta foi um padrão decisório equivocado que elevava ou minimizava os riscos de reincidência de acordo com as características raciais dos réus, majorando a reincidência para pessoas negras e minimizando para pessoas brancas (Angwin, et al, 2016). Dessa forma, comparando-se com a base de dados do COMPAS, muitos criminosos acabavam sendo discriminados, reafirmando preconceitos nos resultados do programa.

O caso evidencia que algoritmos não 'aprendem' sozinhos: eles codificam discriminações históricas. Nos EUA, onde negros são desproporcionalmente criminalizados, o COMPAS reproduziu essa lógica, mascarando-a sob uma suposta objetividade técnica. No Brasil, onde 55,4% da população se declara negra (Ministério da Igualdade Racial, 2022, p. 5), a ausência de dados representativos nos sistemas de RF tende a repetir esse ciclo.

Tais situações, seja a maior incidência de falhas no Reconhecimento Facial de populações minoritárias, seja a discriminação acentuada em relação às pessoas negras em

sistemas preditivos de risco, conforme Tarcísio Silva, configuram o “racismo algorítmico”, isto é, “o modo pelo qual a disposição de tecnologias e imaginários sociotécnicos em um mundo moldado pela supremacia branca realiza a ordenação algorítmica racializada de classificação social, recursos e violência em detrimento de grupos minorizados.” (Silva, 2022, p. 81).

Outro caso relevante é a discriminação algorítmica voltada às pessoas trans e ao gênero. Nessa ótica, as tecnologias de RF apresentam altas taxas de erro quando se prestam a identificar pessoas trans, visto que os bancos de dados que alimentam os algoritmos muitas vezes não contêm imagens desses indivíduos e acabam por não identificar seus rostos por não se adequarem às características faciais consideradas “normais” pela sociedade predominantemente cisgênera (Viana, 2023, p. 23-24).

Quanto ao gênero, em pesquisa realizada por Joy Buolamwini e Timnit Gebru sobre os recursos de identificação de gênero e idade nos mecanismos de visão computacional da Face++, IBM e Microsoft, verificou-se que os maiores índices de erro das ferramentas ocorriam com mulheres, a ainda mais com mulheres negras, alcançando uma taxa de 34,7% para o algoritmo da IBM (2018, p. 9).

Identifica-se, dessa maneira, que grupos racializados e LGBTQIA+ são desproporcionalmente afetados negativamente pelos sistemas de RF, porque esses sistemas operam com parâmetros estreitos: em suas bases de dados predominam rostos masculinos, brancos e cisgêneros, os quais determinam a 'norma' e os resultados dos programas, enquanto outros corpos são lidos como 'desvios', estranhos à base de dados do sistema e ao que ele identifica como “correto” ou “normal”, revelando um *apartheid* digital desses grupos.

Seja na Europa ou no Brasil, o padrão segue o mesmo: algoritmos reforçam hierarquias sociais porque são desenvolvidos com base em grupos homogêneos, de modo que a RF não cria discriminação, mas a cristaliza em códigos. A narrativa de que existe uma neutralidade algorítmica é liquefeita quando se assume que esses sistemas:

são desenvolvidos por pessoas e podem refletir os preconceitos e estereótipos dessas pessoas. Além disso, os algoritmos muitas vezes são treinados em bancos de dados que já contêm preconceitos e desigualdades, o que pode perpetuar essas desigualdades e reforçar a discriminação. (Viana, 2023, p. 22)

Tais falhas de identificação de grupos racializados pela RF são resultado de bases de dados (*datasets*) centrados em indivíduos brancos, homens e cisgêneros, as quais reforçam o racismo algorítmico. De acordo com Joy Buolamwini e Timnit Gebru, é necessário majorar a representação demográfica e fenotípica nos bancos de dados faciais e na avaliação algorítmica

(2018, p. 12), considerando que a baixa representação facial no banco de dados da RF contribui para a não identificação de indivíduos com baixa representação nessas mesmas bases.

Logo, a segregação digital a que esses grupos minoritários estão sujeitos, viola seu direito fundamental à igualdade, transgressão esta causada pelas falhas no desenvolvimento humano das tecnologias de inteligência artificial, de modo que se torna necessário a estipulação de parâmetros, por meio de orientações técnicas e normas legais, que abranjam os grupos racializados e LGBTQIA+ durante a codificação do RF, a fim de garantir a diversidade ao tratar de dados sensíveis e da maneira que são empregados em processos automatizados por meio da inteligência artificial (Costa; Kremer, 2022, p. 160).

Além dos “falsos positivos” e da discriminação algorítmica, outra seara que afeta as liberdades individuais dos cidadãos mediante o emprego das novas tecnologias de RF é como elas podem ser utilizadas para realizar a vigilância em massa da população e extinguir a privacidade das pessoas.

2.3 Vigilância em Massa e Erosão da Privacidade

A expansão do reconhecimento facial (RF) em espaços públicos não se limita à segurança: ela consolida um regime de vigilância permanente, onde o Estado e corporações transformam corpos em dados, normalizando a violação de privacidade como preço inevitável do 'progresso'. Essa lógica, exemplificada pelo modelo chinês e pelas práticas de empresas como Meta, redefine a noção de liberdade em sociedades democráticas.

Nesse sentido, “se toda tecnologia de reconhecimento facial funcionasse perfeitamente toda vez, em toda demografia e população, preocupações sobre a vigilância, forense criminal, e rastreamento de longo prazo se manteriam” (Selinger; Leong, 2021, p. 10-11, tradução nossa), isto é, mesmo que fosse solucionado o problema da discriminação algorítmica e eliminadas as chances de falsos positivos, o direito fundamental à privacidade estaria, mais do que nunca, sob risco.

Como ilustração, um contexto que não é mais ficção científica e que assusta os países do Ocidente é a realidade da China, a qual conta com mais de 200 milhões de câmeras públicas vigiando as cidades do país. O Estado chinês emprega câmeras de monitoramento para garantir a segurança pública, as quais possuem softwares de reconhecimento facial.

Conforme afirmações de uma das empresas multibilionárias que produzem tais equipamentos – MegVii – uma única câmera é capaz de analisar mil pessoas por imagem

capturada, identificar seus rostos e verificar se algum dos indivíduos consta em lista de procurados pela justiça (Uol, 2019).

O caso chinês revela uma contradição: a vigilância é vendida como método eficiente para a redução da criminalização, ao passo que o uso indiscriminado do RF em locais públicos, mantém um estado massivo e perpétuo de monitoramento dos cidadãos, fato que leva a crer que o real objetivo por traz da tão propagandeada “promoção da segurança pública”, na realidade, é o controle político.

Nesse sentido, “O Estado é informado sobre o local que as pessoas frequentam, o tempo que passam em cada espaço e com quem se relacionam” (Almeida, 2022, p. 274), fatos que, aparentemente inofensivos, podem ser utilizados em prejuízo dos direitos fundamentais dos cidadãos, quando utilizados sem limites pelas entidades estatais, as quais podem se aproveitar para instaurar uma vigilância e controle massivos da população, violando sua liberdade de ir e vir e privacidade, como já ocorre na China sob o Partido Comunista.

Outrossim, cidades como Curitiba/PR, no contexto brasileiro, são pioneiras na implementação de câmeras de vigilâncias nos centros urbanos para a promoção de segurança pública, sem, contudo, apresentar propostas de lei e regulamentos que limitem a sua utilização a fim de evitar possíveis violações à privacidade e à liberdade dos cidadãos.

Nesse sentido os professores Camila Berlim Schneider e Pedro Fauth Manhães Miranda:

[...] os benefícios da vigilância por reconhecimento facial não justificam a limitação de direitos dos cidadãos, mesmo quando se apresenta disfarçada de política de segurança pública. Tais sistemas, da forma como estão formulados atualmente, podem avivar injustiças sociais e raciais preexistentes. (2020, p. 11)

Ademais, é possível afirmar que o modelo de vigilância no qual a sociedade hodierna está inserida não é mais o panóptico anunciado por Foucault, mas sim um paradigma atualizado dele, denominado pelo filósofo Didier Bigo como “banóptico”.

Nesse sentido, o banóptico representa a utilização das novas tecnologias biométricas, de reconhecimento facial e de predição de perfis pessoais (*profiling*) não somente para vigiar indivíduos, mas também para “banir” e prevenir que certos “indivíduos perigosos” entrem nos países, especialmente os imigrantes, a fim de proteger o bem-estar da “população normalizada” que deve ser protegida dos “estrangeiros” (Bigo, 2006, p. 63).

Ainda, a erosão da privacidade da população também é influenciada pelas narrativas disseminadas por empresas privadas – como a Meta e o Google – as quais sugerem que “se você não cometeu nenhuma ilicitude, você não tem nada a esconder”, ou que a crescente

coleta de dados pessoais e a diminuição da privacidade são eventos inevitáveis e necessários para o desenvolvimento das novas tecnologias (Véliz, Carissa, 2021, p. 92-93).

Quanto à crença de que o desenvolvimento tecnológico e a erosão da privacidade são inevitáveis, a pesquisadora Shoshana Zuboff conta que parece haver uma espécie de acordo universal entre os profissionais “experts” sobre a ideia que “tudo será conectado, conhecido e acionável em um futuro próximo” (2019, p. 222, tradução nossa), não havendo, entretanto, uma análise crítica na crença de que a vigilância e a tecnologia estarão em todo lugar.

Um exemplo disso é o filme, “O Círculo”, dirigido por James Ponsoldt, o qual retrata uma corporação fictícia chamada O Círculo que trabalha com produtos e inovações tecnológicas. Uma dessas invenções é uma câmera do tamanho de uma bolinha de gude que pode ser colocada em qualquer lugar permitindo vigilância ubíqua e perpétua de todos os seres humanos, sob o pretexto que os segredos é o que tornam os crimes possíveis, pois, se você não é responsabilizado pelo que faz, você se comportará de uma pior maneira (Camargo; Silva; Fígaro, 2021, p. 58).

Tais argumentos objetivam “normalizar” as ferramentas de vigilância que rodeiam os indivíduos a todo o momento, sejam as câmeras de reconhecimento facial, sejam os aplicativos de celulares. Logo, percebe-se que as tecnologias de Reconhecimento Facial, embora tragam benefícios à seara da persecução penal, devido à maior eficiência e celeridade em identificar indivíduos procurados pela justiça, também carregam riscos à privacidade dos cidadãos, a qual é solapada em nome da segurança pública.

3. A NECESSÁRIA REGULAÇÃO DO RECONHECIMENTO FACIAL E A PROTEÇÃO DOS DIREITOS FUNDAMENTAIS

Diante desse cenário, no qual o uso indiscriminado e irrestrito das tecnologias de Reconhecimento Facial na segurança pública acarretam violações aos direitos fundamentais de liberdade de ir e vir, à presunção de inocência, à igualdade e à privacidade, se torna necessário que a discussão pública sobre o tema encontre soluções para mitigar os efeitos danosos do RF nos direitos fundamentais de toda a população e, em especial, para os grupos étnicos particularmente afetados.

Um dos meios debatidos no espaço público para a mitigação desses efeitos é justamente a criação e aferição de limites e princípios normativos para o desenvolvimento e aplicação dessas tecnologias que respeitem os direitos individuais, como será abordado a seguir.

3.1. Regulamento Geral de Proteção de Dados da União Europeia (GDPR)

Primeiramente, como pioneira na busca de uma solução para os problemas apontados, a União Europeia publicou em 2016 a GDPR (General Data Protection Regulation, ou Regulamento Geral de Proteção de Dados da União Europeia – Regulamento UE 2016/679). Esse regulamento é um marco legal que estabelece normas rigorosas para o tratamento de dados pessoais, incluindo o uso de tecnologias como reconhecimento facial (Lorenzon, 2021, p. 41).

Como estratégia para mitigar as violações aos direitos fundamentais pela RF, em seu artigo 9, a GDPR proíbe o processamento de certos dados pessoais específicos (os quais a legislação brasileira vai definir como dados pessoais sensíveis), que incluem a biometria facial. Uma das exceções a essa proibição, é a possibilidade do uso desses dados para propósitos de segurança social, desde que aprovado por lei do Estado Membro da UE e salvaguardados os direitos fundamentais do titular:

Artigo 9. Parágrafo 2. O Parágrafo 1 não será aplicado caso se verifique um dos seguintes casos:

(b) Se o tratamento é necessário para efeitos de cumprimento das obrigações e exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados no domínio do direito do trabalho, da segurança social e da proteção social, na medida em que seja autorizado pela lei da União ou dos Estados-Membros ou por uma convenção coletiva nos termos de lei dos Estados-Membros que preveja salvaguardas adequadas dos direitos fundamentais e dos interesses do titular dos dados (tradução nossa, grifos nossos)

De plano, percebe-se que a o regulamento veda a utilização indiscriminada do tratamento de dados biométricos, haja vista a necessidade de se auferir a adequação de seu uso com a salvaguarda dos direitos fundamentais. No mesmo sentido, o Artigo 10 especifica que o processamento de dados pessoais relativos a medidas de segurança apenas pode ser realizado sob o controle da autoridade oficial ou quando aprovada por esta, com a ressalva dos direitos e liberdades dos titulares:

Artigo 10. O processamento de dados pessoais relativos a condenações criminais e crimes ou relacionados com medidas de segurança baseados no Artigo 6, devem ser realizados apenas sob o controle da autoridade oficial ou quando o processamento é autorizado por lei da União ou Estado Membro, providenciando salvaguardas apropriadas para os direitos e liberdades dos titulares dos dados. Qualquer registro abrangente de condenações criminais deve ser guardado apenas sob o controle da autoridade oficial. (tradução nossa, grifos nossos).

Nota-se, porém, que o regulamento europeu condiciona o processamento dos dados biométricos, e consequentemente o RF que utilize esses dados na área de segurança pública, a

leis locais e específicas que detalhem os limites de sua utilização, servindo apenas como parâmetro geral e ponto de partida ao apresentar os princípios que devem ser postos em prática nas regulações locais, como os princípios da transparência, legalidade, justiça, finalidade, entre outros apontados no Artigo 5.

Assim, a discussão pública sobre os limites e impactos da implementação de RF para segurança pública nos direitos fundamentais deve refletir o contexto social e histórico da população que é objeto de sua vigilância e do processamento dos dados biométricos. Sendo o Brasil o objeto do presente estudo, a diversidade étnica e os grupos racializados e LGBTQIA+ afetados negativamente por essas ferramentas, como discutido acima deve ser considerada para a solução do problema.

3.2. Regulação Brasileira

Embora a GDPR represente um avanço significativo na proteção de dados biométricos, sua eficácia depende da implementação complementar pelos Estados-membros – um desafio que expõe as limitações de modelos regulatórios descentralizados. Essa fragilidade torna-se ainda mais evidente ao analisar o cenário brasileiro, onde a ausência de uma legislação específica para o reconhecimento facial na segurança pública cria um vácuo normativo preocupante.

Enquanto a União Europeia condiciona o uso do RF a salvaguardas legais mínimas, o Brasil opera em um contexto de experimentação desregulada, no qual projetos municipais e estaduais avançam sem diretrizes claras ou mecanismos de controle – realidade que demanda uma análise crítica sobre os riscos dessa lacuna para os direitos fundamentais.

Se, por um lado, em 2018 foi publicada a Lei Geral de Proteção de Dados (Lei 13.709/2018), prevendo princípios de proteção aos direitos dos usuários que possuem seus dados pessoais processados (art. 6º) e diferenciando dados pessoais de dados pessoais sensíveis (art. 5º, incisos I e II), por outro lado, a lei não se aplica ao tratamento de dados pessoais quando realizado para fins exclusivos de segurança pública (art. 4º, III, “a”).

Embora o § 1º do mesmo artigo disponha que o tratamento de dados nos casos de segurança pública deve ser regido por lei específica, até o momento, não há um regulamento federal que aponte limites legais ao uso do RF, dando margem às capitais brasileiras, como Rio de Janeiro/RJ, Curitiba/PR e Salvador/BA, implementarem projetos de segurança pública que potencialmente violem direitos fundamentais, como exposto acima no caso do jovem

Daniel Félix, no Rio de Janeiro, que teve sua liberdade e seu direito à presunção de inocência violados por um resultado “falso positivo” do sistema de RF.

Como tentativa em andamento de contornar essa situação, trâmite na Câmara dos Deputados o PL 2.338/2023, de autoria do senador Rodrigo Pacheco (PSD/MG), aprovado no Senado em 10 de dezembro de 2024, que prevê diretrizes sobre o uso de Inteligência Artificial. Quanto ao uso de câmeras no espaço público para identificar pessoas em tempo real só será permitido nos seguintes casos:

Busca de vítimas de crimes ou pessoas desaparecidas, para recapturar fugitivos, **cumprir mandados de prisão ou medidas restritivas, investigar e reprimir crimes em flagrante nos casos de delitos cuja pena de prisão seja superior a dois anos** e instruir inquérito ou processo criminal com autorização do juiz, quando a prova não puder ser feita por outros meios (Agência Senado, 2024)

Sendo ressalvado no projeto de lei que aos cidadãos deve ser assegurado o direito à explicação e à revisão humana dos resultados dos programas de inteligência Artificial que tiverem impacto jurídico relevante em suas vidas, bem como, sendo realizada a identificação biométrica, a garantia de proteção contra a discriminação.

Do exposto, embora a propaganda política de diversas capitais e municípios brasileiros apresente a implementação do RF na segurança pública como a solução para a diminuição da criminalidade, ocorrendo a existência do cumprimento de mandados de prisão desde 2019 (na Bahia), não há a mesma diligência em criar normas e regulamentos que limitem o uso indiscriminado dessa tecnologia, tendo em vista a proteção dos direitos fundamentais e combate à discriminação algorítmica, aos “falsos positivos” e à erosão da privacidade e vigilância em massa.

A suposta “neutralidade algorítmica”, o “inevitável” avanço da tecnologia e os riscos aos direitos fundamentais, são normalizados pela aposta irrefreada dos municípios e capitais em projetos de RF na segurança pública que se aproveitam da vaguidade da lei e da falta de uma regulamentação específica que delimite claramente quando o tratamento dos dados biométricos se torna violação a direitos.

Como expõe os pesquisadores Paulo Victor Melo e Paulo Serra:

Quando os gestores mencionam “pessoas suspeitas”, quais dados são coletados para construção desses perfis? Como são construídos e compostos os bancos de dados que sustentam essas tecnologias? Quem, além da ação automatizada dos algoritmos, está por trás das câmeras de reconhecimento facial? Há mecanismos de proteção dos dados pessoais? Quais são os bancos de dados que estão sendo cruzados? Quem armazena, qualifica e indexa esses bancos de dados? A quem é garantido o acesso e a quem é negado? O que está sendo registrado? **O que são entendidas como “boas práticas” de utilização dessas tecnologias quando ainda não há legislação vigente normatizando os seus usos?** (2022, p. 217)

As perguntas incisivas levantadas por Melo e Serra expõem a falácia central por trás da implementação acrítica do reconhecimento facial no Brasil: a falsa dicotomia entre segurança e direitos fundamentais. A ausência de respostas claras para esses questionamentos revela que, mais do que uma lacuna regulatória, há uma opção política por manter na obscuridade os critérios que fundamentam essas tecnologias.

Essa opacidade não é acidental - é estrutural. Permite que, sob o manto da "neutralidade técnica", se perpetuem práticas discriminatórias já enraizadas no sistema de segurança pública, agora potencializadas pela automatização. Enquanto não houver transparência sobre a composição dos bancos de dados, os parâmetros dos algoritmos e os fluxos de acesso à informação, o reconhecimento facial continuará sendo menos uma ferramenta de segurança pública e mais um instrumento de controle social desigual, onde os erros do sistema recairão desproporcionalmente sobre os corpos já historicamente criminalizados.

A verdadeira questão que se coloca, portanto, não é se o Brasil está preparado para o reconhecimento facial, mas se o reconhecimento facial está preparado - e será obrigado a se adaptar - para lidar com a complexidade e diversidade da sociedade brasileira. Diante desse cenário, fica evidente que a LGPD, sozinha, é insuficiente para conter os abusos do Reconhecimento Facial na segurança pública.

Enquanto o Brasil não estabelecer uma legislação específica – com salvaguardas claras contra falsos positivos, vieses algorítmicos e vigilância em massa –, o uso dessa tecnologia seguirá servindo a um duplo propósito perverso: sob o discurso da eficiência na segurança, reproduzirá desigualdades estruturais e normalizará a violação sistemática de direitos fundamentais, especialmente entre populações historicamente marginalizadas. A ausência de regras precisas não é mera lacuna legal, mas uma escolha política que privilegia o controle sobre a proteção constitucional da privacidade, da igualdade e da presunção de inocência.

4. CONCLUSÃO

Do exposto, conclui-se que as tecnologias de Reconhecimento Facial aplicadas à segurança pública, em especial nos municípios e capitais brasileiras, embora em rápida expansão e embora aumentem a eficiência das atividades de vigilância e segurança, caso não balanceadas pela criação de normas e regulamentos que mitiguem seus efeitos negativos,

podem causar severos impactos às liberdades individuais de igualdade, presunção de inocência e privacidade.

Nesse sentido, por trás do discurso acerca da “neutralidade algorítmica” propagado pelos candidatos políticos e defensores da aplicação dos sistemas de RF, ocorre flagrante discriminação algorítmica, acarretando maior número de “falsos positivos”, maiores índices equivocados de reincidência criminal e altas taxas de erro na identificação de grupos racializados (negros, asiáticos), de gênero (mulheres) e LGBTQIA+.

O que se verifica no plano fático, é a potencialização das desigualdades sociais mediante o uso indiscriminado da tecnologia de RF, majorando, ainda, a vigilância em massa da população e a invasão da esfera da vida privada dos indivíduos, sob o argumento que o avanço tecnológico e a erosão da privacidade são “inevitáveis”.

Por fim, encontrou-se que a discussão pública acerca do RF deve ser estimulada, a fim de verificar os impactos e riscos que ela causa aos direitos fundamentais, incluindo, ainda, a publicação de projetos de lei e normas regulamentares específicas, a exemplo do PL 2.338/2023, não somente gerais, que delimitem o uso do RF, suprimindo as lacunas legais existentes. Assim, construir-se-á caminhos para tornar o Reconhecimento Facial menos um vilão de filme de ficção científica e mais uma ferramenta em favor do bem-estar dos brasileiros.

REFERÊNCIAS

Agência Senado. Senado aprova regulamentação da inteligência artificial; texto vai à Câmara. **Senado Notícias**. 2024. Disponível em: <https://www12.senado.leg.br/noticias/materias/2024/12/10/senado-aprova-regulamentacao-da-inteligencia-artificial-texto-vai-a-camara>. Acesso em 04 abr. 2025

ALVES, Davis Souza; CONCEIÇÃO, Márcio Magera. O reconhecimento facial comportamental na segurança pública. **RECIMA21 - Revista Científica Multidisciplinar**, Jundiaí, Brasil, v. 6, n. 1, p. e616190, 2025. DOI: 10.47820/recima21.v6i1.6190. Disponível em: <https://recima21.com.br/index.php/recima21/article/view/6190>. Acesso em: 3 abr. 2025.

ALMEIDA, Eduarda Costa. Os grandes irmãos: o uso de tecnologias de reconhecimento facial para persecução penal. **Revista Brasileira de Segurança Pública**, v. 16, n. 2, p. 264-283, 2022. Disponível em: <https://revista.forumseguranca.org.br/rbsp/article/view/1377>. Acesso em: 27 mar. 2025.

ANGWIN, Julia et al. **Machine Bias**: Investigating the algorithms that control our lives. ProPublica, 23 maio 2016. Disponível em: www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing Acesso em: 26 mar. 2025.

BRASIL, **Informe MIR - Monitoramento e avaliação - nº 3 - Edição Censo Demográfico 2022**. Secretaria de Gestão do Sistema Nacional de Promoção da Igualdade Racial – SENAPIR; Diretoria de Avaliação, Monitoramento e Gestão da Informação - Brasília-DF - Setembro de 2024. Disponível em: <https://www.gov.br/igualdaderacial/pt-br/composicao/secretaria-de-gestao-do-sistema-nacional-de-promocao-da-igualdade-racial/diretoria-de-avaliacao-monitoramento-e-gestao-da-informacao/informativos/Informe-edicao-censo-demografico2022.pdf>. Acesso: 02 abr. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: <https://www.planalto.gov.br>. Acesso em: 02 abr. 2025.

BUOLAMWINI, Joy; GEBRU; Timnit. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Conference on Fairness, Accountability, and Transparency, Proceedings of Machine. **Learning Research**, v. 81, p. 1-15, 2018. Disponível em: https://proceedings.mlr.press/v81/buolamwini18a.html?mod=article_inline&ref=akusion-ci-shi-dai-bizinesumedeia. Acesso em: 29 mar. 2025.

CAMARGO, Camila Acosta; SILVA, Gabriel de Melo Amancio da; FIGARO, Roseli. O imperativo da transparência como norma legitimadora da vigilância digital no capitalismo de dados a partir do filme O Círculo. **Fronteiras-Estudos Midiáticos**, v. 23, n. 1, p. 57-67, 2021. Disponível em: <https://repositorio.usp.br/item/003033521>. Acesso em: 01 abr. 2025.

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**, v. 16, n. 1, 2022. Disponível em: <https://dfj.emnuvens.com.br/dfj/article/view/1316>. Acesso em: 25 mar. 2025.

DE LIMA VIANA, Guilherme Manoel. DESIGUALDADE NA ERA DIGITAL: COMO A DISCRIMINAÇÃO ALGORÍTMICA AFETA OS TRANSEXUAIS. **Inova Jur**, v. 2, n. 1, 2023. Disponível em: <https://revista.uemg.br/index.php/inovajur/article/view/7534>. Acesso em: 28 mar. 2025.

FUSSEY, Peter; MURRAY, Daragh. Independent report on the London Metropolitan Police Service’s trial of live facial recognition technology. **The Human Rights, Big Data and Technology Project, University of Essex Human Rights Centre**. 2019. Disponível em: <https://repository.essex.ac.uk/24946/>. Acesso em: 21 mar. 2025.

GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee. **Face recognition vendor test (fvrt): Part 3, demographic effects**. Gaithersburg, MD: National Institute of Standards and Technology, 2019. Disponível em: <https://doi.org/10.6028/NIST.IR.8280>. Acesso em: 31 mar. 2025.

HERMES, Pedro Henrique; LEAL, Rogério Gesta. Inteligência artificial, políticas públicas e segurança pública: aproximações e sinergias para a tutela de direitos fundamentais. In: **Revista Direito UNIFACS**, Salvador, Brasil, p. 1-19, 2025. Disponível em: <https://revistas.unifacs.br/index.php/redu/article/view/9600>. Acesso em: 3 abr. 2025.

LORENZON, Laila Neves. Análise comparada entre regulamentações de dados pessoais no Brasil e na União Europeia (LGPD e GDPR) e seus respectivos instrumentos de enforcement.

Revista do Programa de Direito da União Europeia, v. 1, p. 39-52, 2021. Disponível em: <https://periodicos.fgv.br/rpdue/article/view/83423/79192>. Acesso em: 04 abr. 2025

MARINHO, Maria Edelvacy; LIMA, Julia Ferrari Oliveira; OLIVEIRA, Liziane Paixão Silva; MOREIRA, Diogo Rais. Inteligência Artificial, Tecnologias de Reconhecimento de Emoções e o Direito: Importância do princípio da qualidade dos dados como pilar no direito fundamental à proteção de dados. In: **Revista Brasileira de Direito**, Passo Fundo, Brasil, v. 20, n. 3, p. e5158, mar. 2025. DOI: <https://doi.org/10.18256/2238-0604.2024.v20i3.5158>. Disponível em: <https://seer.atitus.edu.br/index.php/revistadedireito/article/view/5158>. Acesso em: 03 abr. 2025.

MELO, Paulo Victor; SERRA, Paulo. Tecnologia de reconhecimento facial e segurança pública nas capitais brasileiras: apontamentos e problematizações. **Comunicação e sociedade**, n. 42, p. 205-220, 2022. Disponível em: <https://journals.openedition.org/cs/8111>. Acesso em: 30 mar. 2025.

OLIVEIRA, Rhuan Lima Ruiz de; REIS, Sálvio Roberto Freitas; VASCONCELOS, Rafael Oliveira. Análise e avaliação de modelos de detecção e reconhecimento facial. **REVISTA ARACÊ**, São José dos Pinhais, Brasil, v. 3, pág. 10164–10195, 2025. DOI: 10.56238/arev7n3-003. Disponível em: <https://periodicos.newsciencepubl.com/arace/article/view/3629>. Acesso em: 3 abr. 2025.

OLIVEIRA, Samuel Rodrigues de; COSTA, Ramon Silva. O uso de tecnologias de reconhecimento facial em sistemas de vigilância e suas implicações no direito à privacidade. In: **Revista de Direito, Governança e Novas Tecnologias**, Florianópolis, Brasil, v. 5, n. 2, p. 1–21, 2019. DOI: 10.26668/IndexLawJournals/2526-0049/2019.v5i2.5777. Disponível em: <https://www.indexlaw.org/index.php/revistadgnt/article/view/5777>. Acesso em: 3 abr. 2025.

Prefeitura de Curitiba. Curitiba inaugura centro de controle e lança a ‘Muralha Digital’ com mais de 1,7 mil câmeras. **Rede Cidade Digital**, 2021. Disponível em: <https://redecidadedigital.com.br/noticias/curitiba-inaugura-centro-de-controle-e-lanca-a-muralha-digital-com-mais-de-17-mil-cameras/9127>. Acesso em: 28 mar. 2025.

Redação. RJ: Jovem negro acusado por reconhecimento facial é inocentado pela terceira vez. **Brasil de Fato**. 2023. Disponível em: <https://www.brasildefato.com.br/2023/10/06/rj-jovem-negro-acusado-por-reconhecimento-facial-e-inocentado-pela-terceira-vez>. Acesso em: 20 mar. 2025.

RZEMYK, Thomas J. Biometrics in the Criminal Justice System and Society Today. In: FENNELLY, Lawrence J (Edit.). **Effective Physical Security**. 2ªed. Oxford: Butterworth-Heinemann, 2017, p. 249-254. DOI: <https://doi.org/10.1016/B978-0-12-804462-9.00010-5>. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/B9780128044629000105>. Acesso em: 02 abr. 2025.

Secretaria de Segurança Pública da Bahia. Reconhecimento Facial da SSP alcança 3 mil foragidos da Justiça na Bahia. **Secretaria de Segurança Pública da Bahia**. 2025. Disponível em: <https://ssp.ba.gov.br/2025/04/04/reconhecimento-facial-da-ssp-alcanca-3-mil-foragidos-da-justica-na-bahia/>. Acesso em: 04 abr. 2025

SELINGER, Evan; LEONG, Brenda. The ethics of facial recognition technology, in **The Oxford Handbook of Digital Ethics** ed. Carissa Véliz. Oxford Handbooks, 2021. Disponível em: <https://doi.org/10.1093/oxfordhb/9780198857815.013.32>. Acesso em: 25 mar. 2025.

SCHNEIDER, C. B.; MIRANDA, P. F. M. Vigilância Digital como instrumento de promoção da segurança pública. **Publicatio UEPG – Ciências Sociais Aplicadas**, Ponta Grossa/RS, v. 28, p. 1-14, 2020. Disponível em: <https://revistas.uepg.br/index.php/sociais/article/view/14435>. Acesso em: 31 mar. 2025.

SILVA, Tarcízio. **Racismo algorítmico**: inteligência artificial e discriminação nas redes digitais. Edições Sesc SP, 2022.

VÉLIZ, Carissa. **Privacidade é poder**. Editora Contracorrente, 2021.

ZMOGINSKI, Felipe. A sociedade mais vigiada do mundo: como a China usa o reconhecimento facial. **Uol**. 2019. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2019/01/19/a-sociedade-mais-vigiada-do-mundo-como-a-china-usa-o-reconhecimento-facial.htm?cmpid=copiaecola>. Acesso em: 22 mar. 2025.

ZUBOFF, Shoshana. **The age of surveillance capitalism**. The Fight for a Human Future at the New Frontier of Power. Public Affairs: New York. 2019.