Mapeando a Vigilância Biométrica

LEVANTAMENTO NACIONAL SOBRE O USO DO RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA

cesec

DPU
DEFENSORIA PÚBLICA DA UNIÃO

Ficha técnica

O PANÓPTICO: MONITOR DE NOVAS TECNOLOGIAS NA SEGURANÇA PÚBLICA
Um projeto do Centro de Estudos de Segurança e Cidadania (CESeC)

DEFENSORIA PÚBLICA DA UNIÃO – DPU

Equipe CESeC

COORDENAÇÃO
Julita Lemgruber
Silvia Ramos
Pablo Nunes

Equipe Panóptico

CONTATO E REDES
opanoptico.com.br
contatopanoptico@cesecseguranca.com.br
@opanopticobr (Instagram, X e Bluesky)

COORDENADOR
Pablo Nunes

COORDENADORA DE PESQUISA
Thallita G. L. Lima

PESQUISADORAS
Yasmin Rodrigues
Thaís Gonçalves Cruz

VOLUNTÁRIOS DE PESQUISA
Rodrigo Raimundo da Silva
Gabriel Leite

COORDENADOR DE COMUNICAÇÃO
Caio Brasil

ASSISTENTE DE COMUNICAÇÃO
Ana Carolina Aguiar

COORDENADOR DE DESIGN
Renato Cafuzo

DESIGNER ASSISTENTE
Rafael Lira

Defensoria Pública da União

CONTATO E REDES
dpu.def.br
ascom@dpu.def.br
@dpuoficial (Instagram e X)

DEFENSOR PÚBLICO-GERAL FEDERAL
Leonardo Cardoso de Magalhães

SUBDEFENSOR PÚBLICO-GERAL FEDERAL
Marcos Antônio Paderes Barbosa

Escola Nacional da Defensoria Pública da União

DIRETOR-GERAL
Edson Rodrigues Marques

VICE-DIRETORA GERAL
Rafaella Mikos Passos

Sobre este relatório

EQUIPE DO RELATÓRIO
Pablo Nunes (CESeC)
Gabriel Saad Travassos do Carmo (DPU/Politicrim)
Thallita Lima (CESeC)
Carolina Soares Castelliano Lucena de Castro (DPU)
Márcio Ferreira Rodrigues Pereira (DPU)
Lutiana Valadares Fernandes Barbosa (EDHIA-DPU)
Viviane Ceolin Dallasta Del Grossi (EDHIA-DPU)
Augusto Jobim do Amaral (Politicrim)

CONTRIBUIÇÃO
Grupo de pesquisa Grupo de Pesquisa Ética, Direitos Humanos e Inteligência Artificial (EDHIA) da Escola Nacional da DPU: Viviane Ceolin Dallasta del Grossi, Lutiana Valadares Fernandes Barbosa, Cynthia Picolo, Edson Prestes, Aziz Tuffi Saliba, Fernanda Alves, Diego de Oliveira Silva,Gustavo Macedo e Renan Maffei.

EDIÇÃO E REVISÃO DE TEXTO
Marília Gonçalves

COMPOSIÇÃO DE CAPA
Rafael Lira

DIAGRAMAÇÃO
Tomaz Alencar

Como citar

NUNES, Pablo et al. Mapeando a vigilância biométrica [livro eletrônico]: levantamento nacional sobre o uso do reconhecimento facial na segurança pública. Rio de Janeiro: CESeC, 2025.

Dados Internacionais de Catalogação na Publicação (CIP)

Mapeando a vigilância biométrica [livro eletrônico]: levantamento nacional sobre o uso do reconhecimento facial na segurança pública / Pablo Nunes...[et al.] ; edição Marília Gonçalves. – Rio de Janeiro : CESeC, 2025. 2,5 mb

Outros autores: Carolina Soares Castelliano Lucena de Castro, Thallita Lima, Gabriel Saad Travassos do Carmo, Márcio Ferreira Rodrigues Pereira, Lutiana Valadares Fernandes Barbosa, Viviane Ceolin Dallasta Del Grossi, Augusto Jobim do Amaral e Cynthia Picollo.
Formato: PDF
ISBN: 978-85-5969-057-6

1. Brasil. Segurança pública. 2. Reconhecimento facial - Segurança pública. I. Nunes, Pablo. II. Gonçalves, Marília. III. Título.

CDD-363.20981

Sueli Costa - Bibliotecária - CRB-8/5213
(SC Assessoria Editorial, SP, Brasil)

Índices para catálogo sistemático:
1. Segurança pública 363.20981

Sumário

Apresentação

O avanço das tecnologias de vigilância tem transformado profundamente a dinâmica da segurança pública e a relação entre o Estado e os cidadãos. Entre essas tecnologias, o reconhecimento facial vem sendo amplamente incorporado por órgãos públicos no Brasil, em processo que se iniciou com a realização dos megaeventos no país – especialmente a Copa do Mundo de Futebol, em 2014, e os Jogos Olímpicos, em 2016 – e se consolidou com a Portaria n.º 793, de 24 de outubro de 2019. Isso sem que haja um marco regulatório consolidado para disciplinar sua aplicação, garantir a transparência e assegurar a proteção dos direitos fundamentais.

A Defensoria Pública da União (DPU), no cumprimento de sua missão constitucional de promover o acesso à justiça e defender os direitos da população em situação de vulnerabilidade, tem acompanhado os impactos do uso dessas tecnologias na prática jurídica e na proteção de garantias fundamentais. São crescentes os relatos de cidadãos presos, processados ou investigados com base em dados biométricos extraídos de bancos compartilhados entre diferentes instituições, sem critérios claros de acesso, revisão ou possibilidade de contestação. O reconhecimento facial, por sua vez, vem sendo empregado em espaços públicos e eventos de grande porte, suscitando deba-

tes sobre privacidade, segurança da informação, viés discriminatório e ausência de mecanismos eficazes de controle social.

Diante desse cenário, este relatório é resultado de uma parceria entre a Defensoria Pública da União (DPU) e o Centro de Estudos de Segurança e Cidadania (CESeC), por meio do projeto *O Panóptico*, que há anos monitora a implementação de tecnologias de vigilância no Brasil. Além dessas entidades, o relatório conta com subsídios técnicos do grupo de pesquisa "Ética em Direitos Humanos e Inteligência Artificial", vinculado à Escola Nacional da DPU, e do grupo de pesquisa "Criminologia, Cultura Punitiva e Crítica Filosófica" (*Politicrim*), vinculado à PUCRS e coordenado pelo prof. Dr. Augusto Jobim do Amaral. O objetivo deste documento é oferecer um panorama abrangente sobre o uso do reconhecimento facial na segurança pública, analisando contratos firmados, valores investidos, empresas envolvidas e os padrões de transparência adotados pelos órgãos responsáveis.[1]

As preocupações com o uso dessas tecnologias não são infundadas. Estudos técnicos e jurídicos demonstram que os sistemas de reconhecimento facial ainda apresentam desafios significativos em termos de precisão, segurança e impacto sobre direitos fundamentais. Pesquisas conduzidas pelo *National Institute of Standards and Technology* (NIST) apontam que esses sistemas apresentam taxas de erro desproporcionalmente elevadas para determinados grupos populacionais, sendo de dez a cem vezes maiores para pessoas negras, indígenas e asiáticas em comparação com pessoas brancas.[2] No Brasil, investigações indicam que mais da metade das abordagens policiais motivadas por reconhecimento facial resultaram de identificações equivocadas, evidenciando o risco de prisões indevidas e reforço de padrões históricos de seletividade penal.

Além das preocupações técnicas, há desafios institucionais e normativos. Diferentes países têm adotado abordagens cautelosas quanto à implementação dessas tecnologias. Em sentido contrário, no contexto nacional, a implementação do reconhecimento facial cresce em espaços públicos e eventos de grande porte. Em São Paulo, por exemplo, um sistema foi contratado para monitoramento dos passageiros do metrô, prevendo capacidade de armazenamento e compartilhamento de imagens dos usuários, sem que houvesse plena transparência sobre o uso e a destinação dos dados coletados.[3] O uso dessas ferramentas também se estendeu a eventos como o Carnaval

1. Com objetivos correlatos, mas numa escala menor, cf. AMARAL, Augusto Jobim do; FERREIRA, Ana Gabriela. Solucionismo Tecnológico na Segurança Pública Brasileira: o caso do reconhecimento facial na Bahia. In: Sarlet et al. (orgs.). *Tecnologia e Antidiscriminação.* Londrina: Thoth, 2024, pp. 45-58.

2. GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee. *Face Recognition Vendor Test – Part 3: Demographic Effects*. National Institute of Standards and Technology, U.S. Department of Commerce. Disponível em: **doi.org/10.6028/NIST.IR.8280**. Acesso em: 26 mar. 2025.

3. SÃO PAULO. Tribunal de Justiça de São Paulo. 6ª Vara de Fazenda Pública. *Processo n. 1010667-97.2022.8.26.0053*. Decisão Liminar. Juíza Estadual Cynthia Tome. DJe n. 3473, 25 mar. 2023.

no Rio de Janeiro[4] e na Bahia[5], onde a tecnologia foi empregada sem regulamentação clara sobre as bases de dados utilizadas e os critérios de identificação adotados.

Este relatório consolida um levantamento detalhado sobre o uso da tecnologia de reconhecimento facial na segurança pública no Brasil, destacando aspectos como a contratação, os custos envolvidos, as empresas fornecedoras e as medidas de transparência associadas a esses projetos. Ao documentar as dinâmicas de implementação dessas ferramentas, busca-se contribuir para um debate qualificado e fundamentado sobre os impactos dessas tecnologias, o investimento público nessas ferramentas e a necessidade de uma política adequada baseada na defesa dos direitos humanos fundamentais.

A implementação de sistemas de vigilância deve estar alinhada aos princípios do Estado Democrático de Direito, assegurando transparência, fiscalização e respeito aos direitos fundamentais. Este relatório visa fornecer informações e reflexões essenciais para que as políticas públicas na área da segurança sejam conduzidas com responsabilidade, garantindo que o uso de novas tecnologias não comprometa garantias fundamentais nem amplifique desigualdades já existentes.

4. SOUZA, Roberta de. Carnaval do Rio terá monitoramento com reconhecimento facial e drones, divulga governo em plano de segurança. *O Globo*, Rio de Janeiro, 05 fev. 2024. Disponível em: **oglobo.globo.com/rio/carnaval/noticia/2024/02/05/carnaval-do-rio-tera-monitoramento-com-reconhecimento-facial-e-drones-divulga-governo-em-plano-de-seguranca.ghtml**. Acesso em: 26 mar. 2025.

5. GAMA, Guilherme. Reconhecimento facial: Seis foragidos da Justiça foram localizados no Carnaval de Salvador. *CNN Brasil*, São Paulo, 10 fev. 2024. Disponível em: **cnnbrasil.com.br/nacional/reconhecimento-facial-seis-foragidos-da-justica-foram-localizados-no-carnaval-de-salvador/**. Acesso em: 26 mar. 2025.

Introdução

No mundo todo, nossos rostos estão sendo mapeados. Isso tem ocorrido de formas mais diversas do que as pessoas comuns são capazes de perceber em um primeiro momento. Há indicadores de que 70% das forças policiais do mundo têm acesso a algum tipo de tecnologia de reconhecimento facial (TRF), e 60% dos países possuem reconhecimento facial em aeroportos.[6] Na Austrália, na França, no Reino Unido, na Alemanha, nos Países Baixos e nos Estados Unidos, a tecnologia é utilizada para segurança de fronteiras.[7] As TRF têm sido usadas ou testadas em operações de policiamento nacional para identificar suspeitos ou localizar pessoas desaparecidas em diversos países.[8] O reconhecimento facial está se tornando uma ferramenta cada vez mais utilizada por governos para verificação de identidade, identificação de pessoas, categorização e análise estatística.

6. BISCHOFF, Paul. Facial recognition technology (FRT): 100 countries analyzed, 8 June 2021. Disponível em: Comparitech, <***comparitech.com/blog/vpn-privacy/facial-recognition-statistics/#:~:text=Five%20countries***>. Acesso em: 24 mar. 2025.

7. *ibidem*.

8. THE GUARDIAN. Are you being scanned? How facial recognition technology follows you even as you shop. Disponível em: <***theguardian.com/technology/2019/feb/24/are-you-being-scanned-how-facial-recognition-technology-follows-you-even-as-you-shop***>. Acesso em: 5 fev. 2025; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (OPC). Police use of facial recognition technology in Canada and the way forward. Disponível em: <***priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/***>. Acesso em: 5 fev. 2025; EUROPEAN DIGITAL RIGHTS (EDRi). Italy introduces a moratorium on video surveillance systems that use facial recognition. Disponível em: ***edri.org/our-work/italy-introduces-a-moratorium-on-video-surveillance-systems-that-use-facial-recognition/***. Acesso em: 5 fev. 2025; STATEWATCH. Legal action against police facial recognition technology. Disponível em: <***statewatch.org/news/2020/september/france-legal-action-against-police-facial-recognition-technology/***>. Acesso em: 5 fev. 2025; INEWS. UK police forces testing new retrospective facial recognition that could identify criminals. Disponível em: <***inews.co.uk/news/technology/uk-police-testing-retrospective-facial-recognition-identify-criminals-1128711***>. Acesso em: 5 fev. 2025.

No Brasil, o uso tem se expandido rápida e amplamente por diversos setores. A adoção dessa tecnologia ganhou destaque em 2019, principalmente devido à Portaria n.º 793, de 24 de outubro de 2019, que estabelece a utilização de recursos do Fundo Nacional de Segurança Pública para estimular a instalação de sistemas de videomonitoramento com reconhecimento facial, inteligência artificial ou outras tecnologias similares (BRASIL, 2019). O uso generalizado de TRF, especialmente na segurança pública, é tema de grande relevância social, política e jurídica na atualidade, em vista das já numerosas demonstrações de como ele pode levar à violação de direitos humanos como privacidade, liberdade de expressão, não discriminação e reunião pacífica.[9]

Dados do projeto *O Panóptico* (CESeC) mostram que há 337 projetos ativos de reconhecimento para fins de segurança no Brasil, e aproximadamente 81 milhões (39,9% da população) de brasileiros estão potencialmente sob vigilância por câmeras de reconhecimento facial na segurança pública abrangendo todas as cinco regiões.[10] Apesar disso, esses sistemas apresentam taxas de erro significativas. Há diversos casos de prisões injustas decorrentes de falhas em TRF[11], somado ao racismo algorítmico presente nessas tecnologias, que, por exemplo, identifica bem homens brancos, mas com frequência falham no reconhecimento facial de pessoas afrodescendentes, especialmente mulheres, o que agrava ainda mais a vulnerabilidade de grupos historicamente marginalizados.[12] Diante disso, precisamos refletir cuidadosamente sobre o que nós, como sociedade, queremos que tais tecnologias promovam.[13]

Preocupações sobre o aumento do uso de TRF, especialmente em espaços públicos como aeroportos, estações de trem e ruas das cidades têm sido expressas em todo o mundo.[14] Algumas cidades como São Francisco e Oakland, nos Estados Unidos, proi-

9. Escritório do Alto Comissariado das Nações Unidas para os Direitos Humanos - ONU. A/HRC/55/60. **Protocolo modelo para que agentes responsáveis pela manutenção da ordem promovam e protejam os Direitos Humanos no contexto de manifestações pacíficas**, 31 de janeiro de 2024. Disponível em: ***ohchr.org/en/documents/legal-standards-and-guidelines/ahrc5560-model-protocol-law-enforcement-officials-promote***.

10. O PANÓPTICO. *Monitoramento do uso de reconhecimento facial no Brasil*. Disponível em: ***opanoptico.com.br***. Acesso em: 5 fev. 2025.

11. MOTTA, Júlia. **Jovem detido em jogo de futebol relata constrangimento após falha no reconhecimento facial da PM**. Revista Forum, 2024. ***revistaforum.com.br/brasil/2024/4/16/jovem-detido-em-jogo-de-futebol-relata-constrangimento-apos-falha-no-reconhecimento-facial-da-pm-157444.html***.

12. BUOLAMWINI, Joy; GEBRU, Timnit. **Gender shades: Intersectional accuracy disparities in commercial gender classifcation. In Conference on fairness, accountability and transparency** (pp. 1-15). 2018. Proceedings of Machine Learning Research. ***proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf***.

13. Matulionyte R, Zalnieriute M, eds. **The Cambridge Handbook of Facial Recognition in the Modern State**. Cambridge University Press; 2024, p. 11.

14. Sobre o tema, cf. de modo geral, AMARAL, Augusto Jobim do et al. (orgs.). *A cidade como máquina biopolítica*. Valencia: Tirant lo Blanch, 2022. Disponível em: ***idus.us.es/items/7a6cc72a-622a-4c17-ab61-bc81fae05f2e***

biram o uso de reconhecimento facial em espaços públicos.[15] A violação de direitos, os vieses discriminatórios[16] e a falta de transparência[17], explicabilidade, supervisão pública e de responsabilização estão entre as preocupações mais comuns associadas às TRF.

Falta transparência também na cadeia de suprimentos dessas tecnologias, o que foi apontado em levantamentos sobre o mercado de vigilância biométrica na América Latina. Relevantes pesquisas investigaram empresas fornecedoras desse setor para atores estatais na região, analisando seus produtos e os impactos nos direitos humanos à luz dos Princípios Orientadores da ONU sobre Empresas e Direitos Humanos (UNGP). As respostas das empresas demonstraram uma tendência a se eximir da responsabilidade por seus produtos ou transferi-la para outros atores, priorizando o atendimento aos clientes em detrimento da mitigação dos impactos sobre as pessoas afetadas.[18]

15. WIRED. 5 Years After San Francisco Banned Face Recognition, Voters Ask for More Surveillance. 2024. Disponível em: ***wired.com/story/san-francisco-banned-face-recognition-voters-ask-for-more-surveillance/#:~:text=San%20Francisco's%202019%20ban%20on,the%20city%2C%E2%80%9D%20Cagle%20says***. Acesso em: 5 fev. 2025

16. O CESeC tem monitorado o uso de reconhecimento facial na segurança pública brasileira desde o início da utilização em larga escala no Brasil, revelando que 90% das pessoas presas com o uso dessa tecnologia em 2019 eram negras, acusadas de crimes sem uso de violência.

17. LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET (LAPIN). *Vigilância automatizada: uso de reconhecimento facial pela administração pública no Brasil*. 7 jul. 2021. Disponível em: ***lapin.org.br/2021/07/07/vigilancia-automatizada-uso-de-reconhecimento-facial-pela-administracao-publica-no-brasil***. Acesso em: 5 fev. 2025; e LIMA et.al.,2024.

18. ACCESS NOW; ASOCIACIÓN POR LOS DERECHOS CIVILES; LABORATORY OF PUBLIC POLICY AND INTERNET – LAPIN; LALIBRE.NET. *Vigilância biométrica remota na América Latina: as empresas estão respeitando os direitos humanos?* 2023. Disponível em: ***accessnow.org/press-release/analysis-answers-surveillance-tech-latin-america/***. Acesso em: 5 fev. 2025.

Os riscos éticos e legais do uso de TRF levaram diversos organismos internacionais, organizações não governamentais (ONG), instituições públicas e legisladores de todo o mundo a pedir a regulação ou até mesmo a proibição ao seu uso. Em 2020, o Alto Comissariado das Nações Unidas para os Direitos Humanos, por exemplo, recomendou que os Estados nunca utilizem TRF para identificar indivíduos que participam pacificamente de assembleias. Além disso, sugeriu a imposição de moratórias sobre o uso dessa tecnologia nesses contextos, até que as autoridades competentes comprovem a conformidade com os parâmetros aplicáveis, como privacidade e proteção de dados.[19]

Organizações como a Autoridade Europeia de Proteção de Dados, o Fórum Econômico Mundial e a Interpol desenvolveram diretrizes específicas a respeito de como a tecnologia deve ser utilizada no contexto da aplicação da lei.[20] O primeiro ponto em comum já constatado é o potencial lesivo que essas tecnologias podem causar aos direitos fundamentais, notadamente para grupos em situação de vulnerabilidade social ou historicamente marginalizados.[21] As instituições destacaram a necessidade de regulação de coleta de biometria à distância.

A Anistia Internacional lançou a campanha "*Ban the Scan*", em que pede o banimento da tecnologia de reconhecimento facial. Segundo a organização, o uso de TRF para vigilância nas ruas de Nova Iorque estaria mirando pessoas negras em protestos e em seus domicílios. Já a Proposta de 2021 do Parlamento Europeu e do Conselho que Estabelece Regras Harmonizadas em Matéria de Inteligência Artificial, apesar de não banir, ressaltou que "[as] imprecisões técnicas dos sistemas de IA concebidos para a identificação biométrica à distância de pessoas singulares podem conduzir a resultados enviesados e ter efeitos discriminatórios. Esta questão é particularmente importante no que diz respeito à idade, à etnia, ao sexo ou a deficiências das pessoas".[22] O documento enfatiza que sistemas de identificação biométrica à distância, tanto em tempo real quanto diferido, apresentam risco elevado e sugere requisitos específicos referentes às capacidades de registro e à supervisão humana.

19. ALTO COMISSARIADO DAS NAÇÕES UNIDAS PARA OS DIREITOS HUMANOS. Relatório A/HRC/44/24: Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests. Nações Unidas, 2020. Disponível em: ***ohchr.org/en/documents/thematic-reports/ahrc4424-impact-new-technologies-promotion-and-protection-human-rights***. Acesso em: 5 fev. 2025.

20. WORLD ECONOMIC FORUM; UNICRI; INTERPOL; NETHERLANDS POLICE. *A policy framework for responsible limits on facial recognition*. 2022; EUROPEAN DATA PROTECTION BOARD (EDPB). *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*. Version 1, 12 maio 2022. Disponível em: ***edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf***. Acesso em: 5 fev. 2025.

21. Cf. AMARAL, Augusto Jobim do; ELESBÃO, Ana Clara Santos; DIAS, Felipe da Veiga. "Governamentalidade Algorítmica e Novas Práticas Punitivas", *Revista Derechos en Acción*, año 6, n. 20, 2021, pp. 667-698. Disponível em: ***sedici.unlp.edu.ar/handle/10915/137881***

22. DE MORAES, A. L. Z.; BARBOSA, L. V. F.; DEL GROSSI, V. C. D. Inteligência artificial e direitos humanos: aportes para um marco regulatório no Brasil, p. 19.

Sobre o potencial discriminatório, o Comitê da ONU para a Eliminação de Discriminação Racial afirmou que a utilização de TRF "para rastrear e controlar grupos demográficos específicos levanta preocupações em relação a diversos direitos humanos, incluindo o direito à privacidade, à liberdade de reunião e associação pacíficas, à liberdade de expressão e à liberdade de movimento".[23] Explica que tal tecnologia pode "perfilar pessoas com base em critérios discriminatórios, como raça, cor, origem nacional ou étnica, ou gênero", bem como ressalta que a precisão da TRF pode variar dependendo do gênero, da cor e da etnia violando o direito humano a não discriminação.[24] Em 2019, o Conselho de Direitos Humanos da ONU ressaltou como os sistemas de reconhecimento facial são falhos para reconhecer pessoas pretas e pardas e seu gênero, o que pode resultar em desumanização.[25]

No Brasil, a campanha *Tire Meu Rosto da Sua Mira* advoga pelo banimento do uso de TRF na segurança pública.[26] O projeto *O Panóptico* também acompanha e analisa os casos de uso dessa tecnologia e mantém um site atualizado mensalmente com os casos de uso de reconhecimento facial no país, disponibilizando a metodologia de monitoramento, bem como a base de dados resultante.[27]

A despeito de todo esse cenário, as soluções regulatórias estão atrasadas. Devido à controvérsia da tecnologia e aos múltiplos interesses concorrentes, ainda não há país que tenha uma estrutura legal abrangente que regule o uso de TRF. No Brasil, o anteprojeto da LGPD penal permanece sem avanços, enquanto o Projeto de Lei n.º 2338/2023, que propõe regular a inteligência artificial, foi aprovado no Senado Federal, incluindo disposições sobre o uso de sistemas biométricos na segurança pública. Embora o PL estabeleça uma proibição geral do uso de sistemas de identificação biométrica à distância e em tempo real em espaços públicos (art. 13)[28], as exceções previstas acabam funcionando, na prática, como uma autorização ampla para sua implementação. As categorias de permissões incluem investigações criminais, flagrante delito, busca por desaparecidos e recaptura de foragidos, situações que abrangem um espectro considerável de atividades da segurança pública. Dado o histórico de abusos e a falta de mecanismos eficazes de controle, essa

23. CERD/C/GC/36 Committee on the Elimination of Racial Discrimination General recommendation No. 36 (2020) on preventing and combating racial profiling by law enforcement officials.

24. ibid.

25. A/HRC/42/59. Human Rights Council Forty-second session 9–27 September 2019 Agenda item 9 Racism, racial discrimination, xenophobia and related forms of intolerance, follow-up to and implementation of the Durban Declaration and Programme of Action Report of the Working Group of Experts on People of African Descent on its twenty-third and twenty-fourth sessions.

26. Tire Meu Rosto da Sua Mira. Disponível em: ***tiremeurostodasuamira.org.br/***. Acesso em 24 mar. 2025.

27. O Panóptico. Disponível em: ***opanoptico.com.br***. Acesso em 24 mar. 2025.

28. Senado Federal. **PL 2338/2023**. ***legis.senado.leg.br/sdleg-getter/documento?dm=9865609&ts=1734649438349&rendition_principal=S&disposition=inline***.

abertura para uso acaba mantendo a possibilidade de um estado de vigilância e de violação de direitos.[29]

É neste cenário que emerge este relatório. Um cenário em que reguladores e formuladores de políticas – no Brasil e em todo o mundo – precisarão continuar avançando no debate para encontrar caminhos mais adequados e protetivos para o uso de tecnologias digitais nas atividades públicas, desenvolvendo também a capacidade de gerenciar as ameaças colocadas por essas tecnologias.[30]

Em vista disso, buscamos, aqui, oferecer um panorama abrangente sobre a implementação das tecnologias de reconhecimento facial no Brasil. Para isso, nós da Defensoria Nacional de Direitos Humanos e do CESeC enviamos às Secretarias de Segurança dos 26 estados da federação e do Distrito Federal ofícios que buscaram investigar e monitorar a adoção das TRF como política pública. Nossas perguntas abrangeram aspectos relacionados à implementação dessas tecnologias, incluindo contratos firmados, empresas contratadas, orçamento envolvido em cada projeto, finalidades declaradas, medidas de proteção de dados sensíveis e mitigação de possíveis vieses discriminatórios. É a análise dessas respostas que apresentamos neste documento.

Inicialmente, explicaremos os procedimentos adotados para a coleta e sistematização dos dados, detalhando as fontes utilizadas e os critérios empregados para avaliar

29. Sobre a emergência destes novos regimes de controle social, cf. AMARAL, Augusto Jobim do; MEDINA, Roberta. "As Máquinas De Visão Cibernéticas e o Advento De Um Novo Regime De Verdade", *Dorsal. Revista de Estudios Foucautianos*, N. 12, junio 2022, pp. 221-242. Disponível em: **revistas.cenaltes.cl/index.php/dorsal/article/view/490**. Acesso em: 24 mar. 2025.

30. Matulionyte R, Zalnieriute M, eds. **The Cambridge Handbook of Facial Recognition in the Modern State**. Cambridge University Press; 2024.

a transparência e a governança dos projetos de reconhecimento facial. Em seguida, a sistematização das respostas apresenta os principais achados da pesquisa, destacando as práticas adotadas pelos estados, os desafios encontrados e os níveis de opacidade na implementação dessas tecnologias. Essa análise evidencia um cenário marcado por assimetrias na adoção da TRF, disparidades nos modelos contratuais e ausência de padronização no monitoramento e na prestação de contas sobre o uso desses sistemas.

Com base nesse diagnóstico, o relatório aprofunda a discussão sobre os impactos sociais, jurídicos e operacionais do reconhecimento facial na segurança pública, contrastando as experiências nacionais com os modelos internacionais e apontando fragilidades normativas e institucionais que comprometem a proteção de direitos. O diagnóstico geral consolida os problemas identificados, demonstrando como a falta de regulamentação, transparência e controle externo amplia os riscos de discriminação, violações de privacidade e mau uso de recursos públicos.

Por fim, apresentamos diretrizes para o aprimoramento da governança dessas tecnologias, propondo medidas concretas que visam garantir maior transparência, *accountability* e proteção aos direitos fundamentais, incluindo a necessidade de regulamentação específica e mecanismos de fiscalização robustos. Dessa forma, o relatório não apenas sistematiza os desafios existentes, mas também busca subsidiar debates e orientar políticas públicas para o uso responsável da TRF no Brasil.

Nosso objetivo é contribuir para a consolidação de uma compreensão mais ampla dos desafios associados à utilização de tecnologias de reconhecimento facial como política pública de segurança no Brasil, com ênfase na proteção dos direitos fundamentais e na ampliação do controle social sobre essas práticas. Esperamos que este documento fomente debates e subsidie ações que promovam uma governança mais ética e inclusiva dessas tecnologias, alinhada aos princípios constitucionais e à defesa dos direitos humanos.[31]

31. Tanto como referência teórica quanto como instrumento de ampliação e aprofundamento do diagnóstico para outras dimensões correlatas, cf. AMARAL, Augusto Jobim do *et. al*... *Algoritarismos*. Valencia: Tirant lo Blanch, 2022. Disponível em: ***idus.us.es/items/499f3b92-78cc-4a94-9c5c-f0704ff724a5***

Metodologia

Realizamos esta pesquisa entre julho e dezembro de 2024. Todos os estados da federação, bem como o Distrito Federal, receberam perguntas que incluíam tópicos como: a existência de contratos ou licitações em curso, com solicitação de cópias dos documentos; o tipo de tecnologia empregada (transmissão em tempo real, comparação de fotos ou outros modelos); as finalidades específicas para as quais as imagens capturadas são utilizadas; a existência de verbas orçamentárias destinadas à implementação da tecnologia, com indicação do montante e da fonte de custeio; entre outros.

Além disso, pedimos informações sobre gestão e segurança dos dados, incluindo o ciclo da vida das imagens – quanto tempo as imagens coletadas ficam armazenadas e quais são as técnicas utilizadas para garantir sua integridade –, a possibilidade de compartilhamento com outros órgãos ou entidades privadas e a adoção de medidas para corrigir vieses discriminatórios nos algoritmos. Outras questões abordaram a necessidade do uso de dados pessoais ou sensíveis para o treinamento das ferramentas, os protocolos operacionais para abordagem de pessoas identificadas pelo sistema, os registros de prisões mediadas pela tecnologia e a produção de relatórios públicos sobre erros de identificação.

Entre os entes federativos consultados, 23 responderam dentro do prazo estabelecido para a pesquisa. Não recebemos retorno de quatro estados. As respostas fornecidas revelaram um panorama heterogêneo, marcado pela ausência de padronização técnica e operacional, bem como pela falta de protocolos que assegurem a observância dos direitos humanos fundamentais, em consonância com os princípios constitucionais estabelecidos na Constituição Federal de 1988. Os dados evidenciam questões problemáticas nos projetos e usos operacionais das tecnologias de reconhecimento facial, ressaltando a urgente necessidade de estabelecer critérios claros, protocolos padronizados e requisitos mínimos que assegurem tanto a transparência na alocação e no uso de recursos públicos destinados à contratação e gestão quanto o respeito aos direitos fundamentais.

descoberta

O que descobrimos

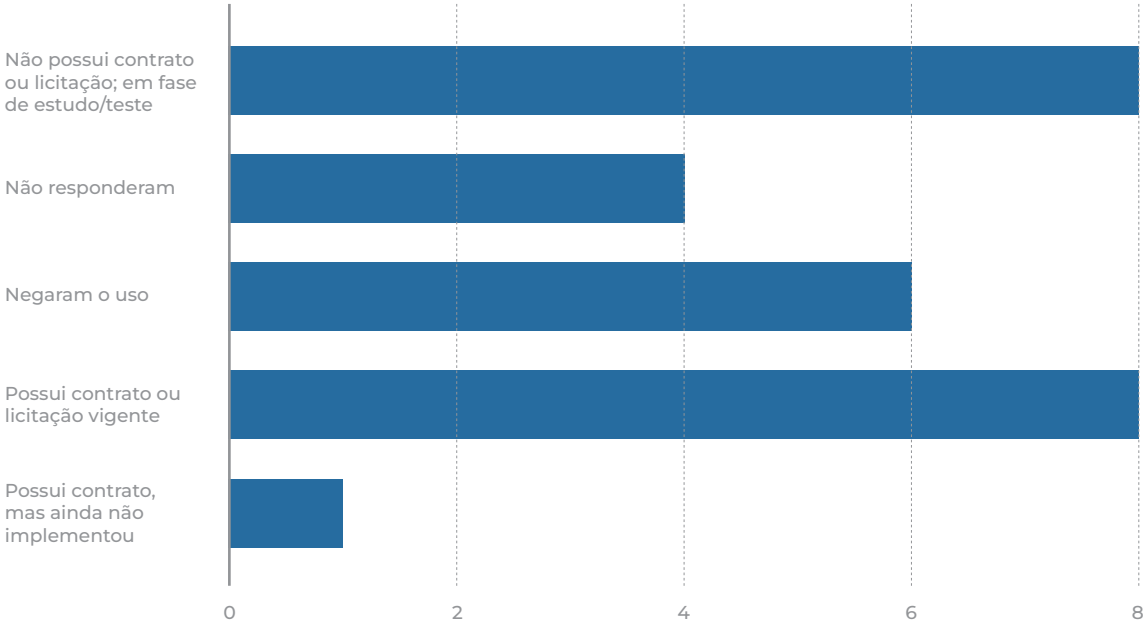
Nesta seção, apresentaremos as respostas que recebemos das Secretarias de Segurança Pública dos estados e do Distrito Federal. O objetivo desta sistematização é oferecer uma fotografia sobre as práticas e políticas relacionadas ao uso de TRF no contexto da segurança pública no Brasil.

A princípio, é preciso dizer que Amazonas, Maranhão, Paraíba e Sergipe, mesmo após reiteradas solicitações, não apresentaram qualquer retorno até a conclusão do estudo. Essa ausência de resposta compromete a plena concretização do direito constitucional de acesso à informação, previsto na Lei de Acesso à Informação (Lei n.º 12.527/2011) e derivado do princípio da publicidade constitucional.

Nossa análise sobre as respostas dos 23 demais entes federativos revela um cenário fragmentado. Seis deles negaram o uso de TRF, demonstrando uma ausência de planos concretos para implementação. Foram os casos de: Acre, Rio Grande do Norte, Rondônia, Santa Catarina, Mato Grosso do Sul e Distrito Federal. Outros oito estados já possuem contratos vigentes ou estão com processos licitatórios ativos, indicando um avanço na adoção da tecnologia. Um ponto preocupante é que, desses, seis estados possuem contratação ou licitação ativa, mas não forneceram documentos detalhados, o que compromete a transparência sobre fornecedores, finalidade e fontes de custeio.

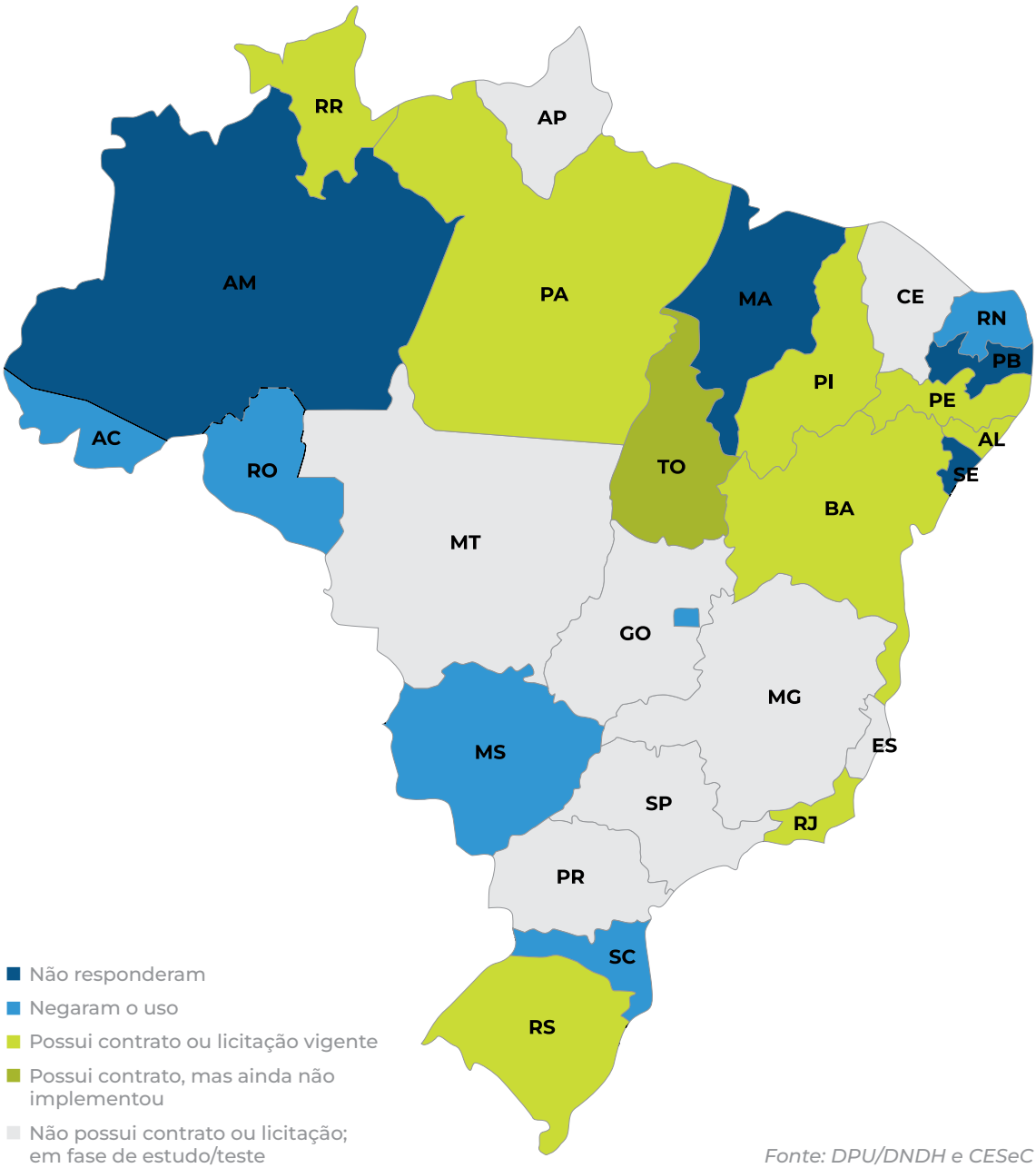
Ademais, embora existam pesquisas empíricas atestando a existência da utilização de tecnologias de reconhecimento facial para fins de policiamento por vários entes federativos do país[32], oito estados afirmaram não possuir contratos ou processos licitatórios em andamento, mas apontaram estar em fase de estudo ou teste para o uso da tecnologia. É o caso de Minas Gerais, São Paulo, Amapá, Ceará, Espírito Santo, Goiás, Mato Grosso e Paraná. Um caso específico é o de Tocantins, que já firmou contrato para o uso do reconhecimento facial, mas ainda não iniciou a implementação.

SITUAÇÃO DOS ENTES FEDERATIVOS QUANTO À TRF



Fonte: DPU/DNDH e CESeC

32. Nesse sentido, conferir, a título de exemplo, o relatório produzido em parceria entre o CESeC e o Laboratório de políticas públicas e internet (Lapin): LIMA et. al. **Vigilância por lentes opacas: mapeamento da transparência e responsabilização nos projetos de reconhecimento facial no Brasil**. Rio de Janeiro: CESeC, 2024.



Fonte: DPU/DNDH e CESeC

Os dados evidenciam um movimento crescente na adoção da tecnologia, mas também desafios significativos quanto à transparência e à justificativa da implementação. Dos estados que responderam aos ofícios, 22% não enviaram informações detalhadas, o que impede um monitoramento adequado do uso de recursos públicos, enquanto quase 30% ainda avaliam a viabilidade do sistema sem um compromisso formal. A ausência de um padrão nacional de regulamentação amplia as preocupações sobre segurança de dados e proteção à privacidade, tornando essencial o debate sobre os impactos sociais da tecnologia.

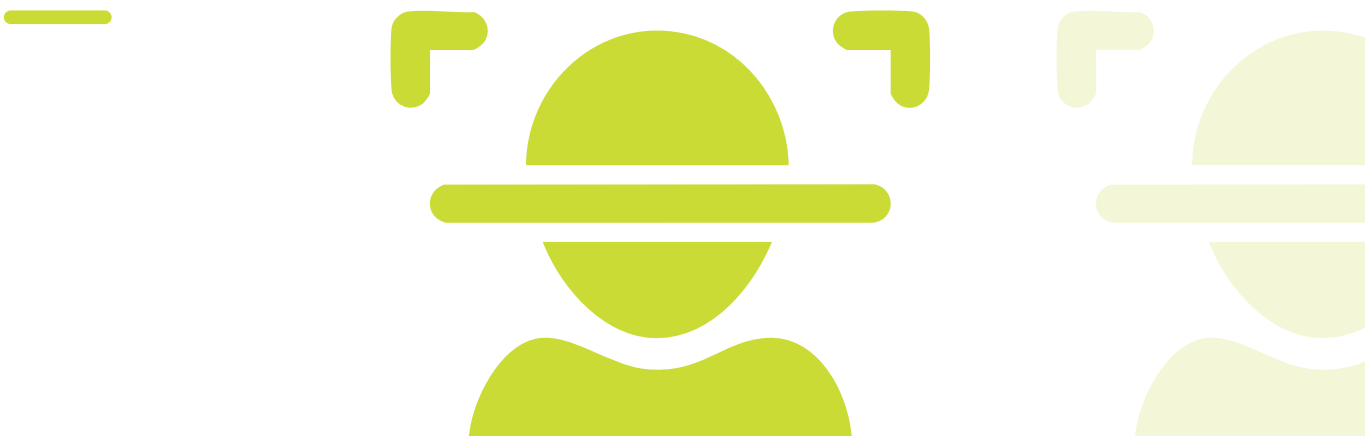
Em relação à gestão da tecnologia, 70% dos estados que já adotaram ou estudam o reconhecimento facial delegaram sua administração às Secretarias de Segurança Pública (SSP). O restante envolve outros órgãos, como a Polícia Militar, Tribunais de Justiça e institutos de identificação. Além disso, 22% dos estados confirmaram

parcerias com empresas privadas, levantando questionamentos sobre compartilhamento de dados sensíveis e segurança da informação. Vale ressaltar que, mesmo nos casos em que estados negaram o compartilhamento com empresas privadas, as licitações demonstram que foram contratadas empresas para o fornecimento do *software*, como é o caso de Pernambuco. Logo, esse número está subdimensionado em virtude da falta de compreensão de que em etapas cruciais do processo a gestão da informação passa por entes privados.

Os investimentos em TRF variam significativamente entre os estados, mas os valores disponíveis são apenas indicativos, podendo ser ainda maiores. Isso ocorre porque não foram enviados os contratos na íntegra, não há clareza se os montantes informados correspondem a valores anuais e alguns projetos não detalharam os investimentos realizados. Até o momento, mais de R$ 160 milhões já foram destinados para a implementação da tecnologia em diferentes unidades federativas. A Bahia lidera os investimentos, com um contrato de aproximadamente R$ 66 milhões, enquanto o Pará alocou R$ 20 milhões para sistemas de monitoramento. Outros estados, como Piauí e Tocantins, também registram valores expressivos: R$ 33,6 milhões e R$ 15,8 milhões, respectivamente. Por outro lado, estados como Rio Grande do Sul e Rio de Janeiro não informaram valores exatos, enquanto Minas Gerais e Mato Grosso ainda estão em fase de planejamento, com orçamentos aprovados, mas sem implementação ativa.

Outro aspecto de importante atenção são as justificativas para a adoção da TRF. A principal é o uso da tecnologia para identificação de pessoas com mandados de prisão em aberto e para o videomonitoramento e a prevenção de crimes em áreas de grande circulação. Além disso, sete dos estados relataram empregar a tecnologia para a localização de pessoas desaparecidas (Alagoas, Bahia, Rio Grande do Sul, Roraima, Pernambuco, Pará e Tocantins), utilizando bases de dados específicas e comparações em tempo real em áreas de grande circulação. Por fim, apenas um estado (Tocantins) declarou utilizar a tecnologia para identificação criminal e emissão de documentos oficiais, vinculando-se ao sistema nacional de identificação biométrica.

Além disso, é importante destacar as lacunas observadas no processo de levantamento, como a ausência de resposta por parte de alguns estados, mesmo após sucessivas tentativas de contato. Essas omissões limitam a plena compreensão do cenário nacional, mas não impedem que as informações disponíveis sirvam como base para identificar pontos críticos e propor caminhos para a criação de protocolos e políticas que levem a uma governança responsável, transparente e ética dessas tecnologias.



Os pontos críticos da adoção das TRF no Brasil

Para este relatório, selecionamos as questões mais relevantes das vinte enviadas, de modo a demonstrar os aspectos fundamentais para o entendimento das práticas e desafios associados à implementação das tecnologias de reconhecimento facial no Brasil. Os principais resultados e pontos críticos identificados são apresentados a seguir, e a íntegra das respostas está no anexo ao final do documento.

1. Problemas relacionados à transparência

Trata-se, em resumo, da ausência de informações claras, completas e acessíveis sobre o uso da tecnologia de reconhecimento facial por parte dos estados. Entre outros aspectos, a falta de transparência impede o controle social, dificulta a prestação de contas e compromete a confiança pública, violando os princípios constitucionais da publicidade e do acesso à informação.

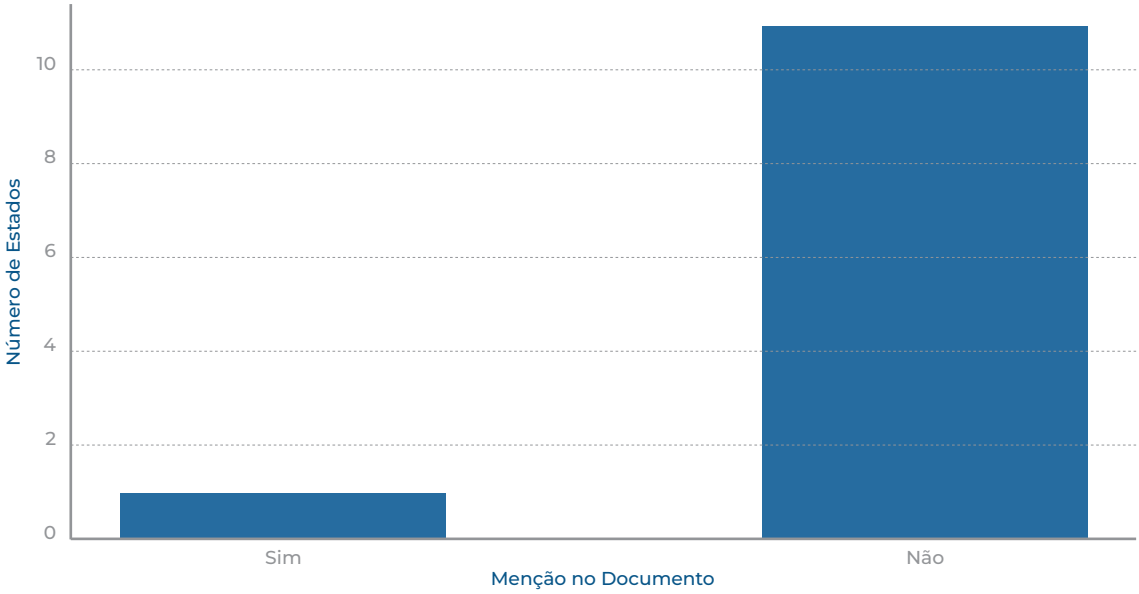
Como exemplo, podemos citar que, nas respostas fornecidas pelas Secretarias de Segurança do Rio de Janeiro, de Pernambuco, do Pará e de São Paulo, verificamos que não há qualquer aviso à população nos locais onde as câmeras de reconhecimento facial foram instaladas. Alguns estados responderam que iriam realizar essa sinalização, como Alagoas e Roraima. Na mesma linha, há casos de órgãos que se negaram a fornecer a localização exata das câmeras, alegando sigilo da informação. Ademais, em várias situações, as secretarias sequer apresentaram à DNDH o contrato relacionado à aquisição e à operação da tecnologia de reconhecimento facial. Por fim – e aqui talvez um dos pontos mais graves –, nenhum dos respondentes produz relatórios públicos avaliando a eficácia da tecnologia.

2. Falta de padronização no uso da tecnologia

Refere-se, basicamente, à ausência de diretrizes uniformes para a aplicação da tecnologia de reconhecimento facial no âmbito da segurança pública, resultando em disparidades entre os entes federativos, bem como em dificuldades na avaliação e na fiscalização da eficácia e da legalidade das abordagens policiais pautadas na referida tecnologia.

Como exemplos, podemos citar o fato de cada estado adotar um procedimento distinto na abordagem de pessoas identificadas pela tecnologia de reconhecimento facial e a falta de uma diretriz padrão para o uso da tecnologia nos Autos de Prisão em Flagrante (APF). Uma observação importante é que apenas a SSP do Rio de Janeiro afirmou fazer menção ao uso de reconhecimento facial nos APF. Os demais estados não indicaram o uso de tal referência. Essas situações podem não apenas levar a práticas discriminatórias e abusivas, mas também ameaçam os princípios constitucionais da ampla defesa e do devido processo legal.

MENÇÃO AO USO DE RECONHECIMENTO FACIAL NO AUTO DE PRISÃO OU DOCUMENTO SIMILAR



Fonte: DPU/DNDH e CESeC

3. Descumprimento às normas de proteção de dados

Um outro aspecto crítico identificado nas respostas é o manejo inadequado ou irregular de dados pessoais. Muito embora a Lei Geral de Proteção de Dados (Lei n.º 13.709/2018) excepcione a sua aplicação para fins de segurança pública, ela é expressa ao vedar o tratamento de dados com finalidade de segurança pública por pessoa jurídica de direito privado, ou seja, por empresas privadas, exceto se estiverem sob tutela de entes públicos, circunstância que deve ser objeto de informe específico à Autoridade Nacional de Proteção de Dados (ANPD), conforme art. 4º, III, 'a' c/c §2º.

Das respostas analisadas, nenhum dos estados demonstrou a efetiva comunicação à ANPD. Pernambuco, por exemplo, refere que a gestão é exclusiva do Centro Integrado de Inteligência de Defesa Social. Porém, o estado reconhece que a tecnologia opera graças a um contrato celebrado com a Empresa Pegasus Tecnologia Ltda., o que deveria conduzir ao envio de informe à ANPD – o que não ocorre.

Minas Gerais, por sua vez, informou que contrataria a empresa Clearview AI para a aquisição da ferramenta de reconhecimento facial.[33] Essa empresa, porém, foi

33. Resposta no SEI n. 7408650, Processo Administrativo n. 08170.000229/2024-80. Cf. Contrato n. 9437287, disponível em **transparencia.mg.gov.br/licitacoes-e-contratos/compras-e-contratos/comprasecontratos-filtros/5/2024/01-01-2024/31-12-2024/91/87547**. Acesso em 14.02.2025.

condenada em outros países (Suécia, França, Itália e Reino Unido, por exemplo) por coletar indiscriminadamente imagens faciais (uma média de 1,5 bilhão de imagens por mês) e violar dados pessoais de milhões de usuários na internet, utilizando-os sem consentimento para a formação de sua base.[34]

Entre outras irregularidades observadas no quadro geral das respostas, no que diz respeito à proteção dos dados, destacam-se: a coleta de dados sem fundamento jurídico claro; a ausência de consentimento informado (por exemplo, dados coletados de redes sociais); a falta de medidas que assegurem segurança, transparência e auditabilidade no tratamento desses dados; a falta de informações sobre os bancos de dados utilizados para treinar a ferramenta; e a ausência de avaliações sobre o impacto à proteção de dados (a chamada *DPIA* exigida pela LGPD). O que se percebe com base em muitas das respostas fornecidas pelas Secretarias de Segurança é um uso genérico de tecnologias de reconhecimento facial sem uma finalidade claramente definida e limitada. Vale notar que essas práticas comprometem não apenas a conformidade legal, mas também a proteção dos direitos fundamentais dos titulares de dados.

4. Incompatibilidade com princípios administrativo

Trata-se aqui da utilização, por parte dos estados, de investimentos públicos elevados em tecnologias de reconhecimento facial sem, no entanto, existir qualquer comprovação de eficiência ou justificativa para os gastos, violando, desse modo, os princípios da eficiência, economicidade e legalidade. A administração pública tem o dever de demonstrar que os investimentos realizados produzem resultados compatíveis com os custos.

Ademais, no que diz respeito à eficiência da ferramenta de reconhecimento facial para policiamento, há significativa pesquisa acadêmica indicando não apenas as diversas falhas da tecnologia, mas também o seu viés discriminatório.[35] A bem da verdade, da maneira como a tecnologia vem sendo utilizada pelos estados, tudo indica

34. GOLDENFEIN, Jake. Privacy's Loose Grip on Facial Recognition: law and the Operational Image. In: **The Cambridge Handbook of Facial Recognition in the Modern State**. Org.: Rita Matulionyte and Monika Zalnieriute. Cambridge: Cambridge University Press, 2024, p. 81. LIMANTE, Agne. Faces of War: Russia's Invasion of Ukraine and Military Use of Facial Recognition Technology. In: **The Cambridge Handbook of Facial Recognition in the Modern State**. Org.: Rita Matulionyte and Monika Zalnieriute. Cambridge: Cambridge University Press, 2024, p. 113.

35. Nesse sentido, conferir: GARVIE, Clare; BEDOYA, Alvaro M.; FRANKLE, Jonathan. **The Perpetual Line-Up: Unregulated Police Face Recognition in America**. Washington, D.C.: Georgetown Law Center on Privacy

que há uma significativa chance de a ferramenta estar aprofundando desigualdades e práticas discriminatórias.

A título de exemplo, podemos citar a falta de estudos técnicos ou dados que validem os resultados esperados e a ausência de comprovação objetiva de redução da criminalidade devido ao uso da ferramenta. Ambos os pontos ficam evidentes nas respostas aos ofícios enviados para os estados.

5. Ausência de supervisão e monitoramento

Mais um ponto crítico identificado nas respostas fornecidas pelas Secretarias de Segurança Pública foi a falta de controle efetivo sobre a aplicação da ferramenta e seus impactos, incluindo a ausência de auditorias regulares, relatórios periódicos e supervisão sobre as empresas contratadas. Como dito, nenhum estado realiza avaliações ou relatórios para verificar os impactos negativos do uso da tecnologia, como erros de identificação que podem levar a prisões indevidas ou outros danos à vida dos cidadãos. Além disso, pouco ou nenhum esforço foi identificado no sentido de realizar uma supervisão rigorosa sobre as empresas contratadas, a fim de, por exemplo, verificar a conformidade dos contratos e a eficácia do uso da tecnologia.

6. Integração ineficiente com sistemas nacionais

Refere-se às falhas na interoperabilidade entre sistemas estaduais e nacionais, comprometendo a eficácia e os objetivos das tecnologias de reconhecimento facial, reduzindo sua capacidade declarada de contribuir para a segurança pública. Nesse sentido, sem uma integração plena entre os sistemas, os investimentos na tecnologia tornam-se questionáveis, já que a falta de conexão reduz a utilidade prática pretendida.

& Technology, 2016. Disponível em: **law.georgetown.edu/privacy-technology-center/publications/the-perpetual-line-up/**. Acesso em: 10 jan. 2025. DOE, John; SMITH, Jane. **Police Use of Facial Recognition Technology and Racial Bias – An Evaluation**. *American Journal of Artificial Intelligence*, v. 7, n. 1, p. 1-13, 2023. Disponível em: **sciencepublishinggroup.com/article/10.11648.j.ajai.20230701.13**. Acesso em: 10 jan. 2025. GEORGETOWN LAW CENTER ON PRIVACY & TECHNOLOGY. **Facing Injustice: How Face Recognition Technology May Increase the Incidence of Wrongful Convictions**. Washington, D.C., 2022. Disponível em: **scholarship.law.georgetown.edu/facpub/2514/**. Acesso em: 10 jan. 2025. PERKOWITZ, Sidney. **The Bias in the Machine: Facial Recognition Technology and Racial Disparities**. *MIT Science and Engineering Research Council*, 2020. Disponível em: **mit-serc.pubpub.org/pub/bias-in-machine**. Acesso em: 10 jan. 2025.

Apesar de alguns estados alegarem usar a tecnologia de reconhecimento facial para localizar pessoas desaparecidas, por exemplo, não há evidências de integração efetiva com o Cadastro Nacional de Pessoas Desaparecidas (CNPD). Do mesmo modo, embora os estados utilizem o Banco Nacional de Mandados de Prisão (BNMP), a integração com os sistemas de reconhecimento facial varia entre os entes federativos, comprometendo a uniformidade e a eficiência da ferramenta.

7. Falta de delimitação geográfica e temporal das operações de reconhecimento

Quanto à pergunta sobre os locais onde as câmeras de reconhecimento facial foram instaladas, a resposta padrão apontou a existência de informações protegidas por sigilo. Naqueles casos em que houve uma resposta, a localização apontava para espaços de grande público de grande circulação de uma forma genérica ou em eventos de grande porte. Quanto ao tempo de armazenamento, observou-se uma heterogeneidade nas respostas, com situações de armazenamento por 24 horas (Rio Grande do Sul), 30 dias (Rio de Janeiro, Bahia e Alagoas) ou, ainda, sem delimitação até que a finalidade seja alcançada (Pernambuco).

Falta de critérios para a formação e utilização da lista de procurados

Um dos problemas graves que identificamos foi a falta de critérios objetivos e transparentes sobre a formação e a utilização da lista de procurados nas operações com tecnologia de reconhecimento facial.

Alguns estados informaram que as imagens captadas são comparadas com listas específicas compostas por dados do Banco Nacional de Monitoramento de Prisões, mantido pelo Conselho Nacional de Justiça; outros informaram a existência de um banco de mandados de prisão próprio (Rio de Janeiro), boletins de ocorrência a respeito de desaparecidos (Alagoas e Rio Grande do Sul) e listas de foragidos, procurados e desaparecidos (Pará). Como visto, há grande heterogeneidade na formação e nos critérios de escolha para a inclusão de pessoas nessas listas.

O que entendemos com base nesta pesquisa

A Constituição Federal erigiu à categoria de direitos fundamentais, entre outros, o direito à privacidade, à proteção de dados pessoais, à igualdade e à não discriminação, conforme preveem os artigos 5º, incisos X e LXXII, e o artigo 3º, inciso IV. Apesar da densidade normativa desses direitos, esta pesquisa mostrou que as políticas de segurança pública que utilizam tecnologias de reconhecimento facial estão sendo implementadas nos entes federativos sem qualquer regulamentação nacional ou tratamento homogêneo que preveja padrões mínimos e medidas efetivas para a salvaguarda de direitos.

Chama também a atenção a escassez de relatórios públicos que promovam a transparência, princípio fundamental da Administração Pública consagrado no artigo 37 da Constituição, que determina que a publicidade deve orientar os atos e políticas públicas.

Alguns países, como o Reino Unido, reconhecendo os riscos que contornam a utilização de TRF, definiram autoridades nacionais específicas para o acompanhamento da contratação e da operacionalização de equipamentos que tratem dados biométricos à distância, em tempo real ou diferido.[36] Essas autoridades são responsáveis por realizar o monitoramento, emitir opiniões e produzir relatórios sobre a compatibilidade entre o uso das tecnologias e os direitos fundamentais.

Além disso, a implementação de sistemas de reconhecimento facial nos países britânicos deve ser condicionada à lei anterior e limitada aos propósitos específicos para os quais a sua contratação foi definida.[37] Doze princípios são utilizados como bases para aferir a regularidade da TRF: i) propósito específico; ii) revisões periódicas; iii) transparência; iv) responsabilidade; v) prévia regulamentação e comunicação; vi) limitação do armazenamento; vii) restrição de acesso às imagens; viii) respeito aos padrões operacionais aprovados; ix) proteção contra uso indevido; x) auditoria regular; xi) efetividade; e xii) atualidade.[38]

Em contraste, no quadro nacional é possível notar que inexiste suporte normativo para os processos licitatórios, a contratação de empresas e a operacionalização de tecnologias de reconhecimento facial para fins de segurança pública. A excepcionalização realizada pela LGPD ainda mitiga o espectro protetivo de direitos fundamentais, sobretudo diante de um vazio de normas que regulamentem, definam responsabilidades e monitorem os gastos na contratação de empresas privadas responsáveis pela produção e operacionalização de *softwares* que capturam, armazenam e tratam imagens faciais. Esses *softwares*, em atividade no Brasil, conferem a destinação que entendem adequada sem qualquer nível de transparência e auditabilidade.

Tampouco há monitoramento sobre as taxas de acurácia das TRF, os resultados alcançados, a justificativa do gasto público, o descarte das imagens faciais ou a vedação de destinação diversa daquela contratualmente estabelecida. Cada estado tem contratado um tipo de tecnologia e um tipo de empresa, sem observância de limites materiais ou formais à captura indiscriminada das imagens faciais em locais públicos. Isso deixa todos os cidadãos vulneráveis a terem seus dados coletados e compartilhados sem que sequer saibam onde, quando ou como isso ocorre.

Podemos olhar, neste sentido, para a experiência regulatória europeia. A União Europeia, além de reconhecer que as TRF são sistemas de alto risco de tratamento de

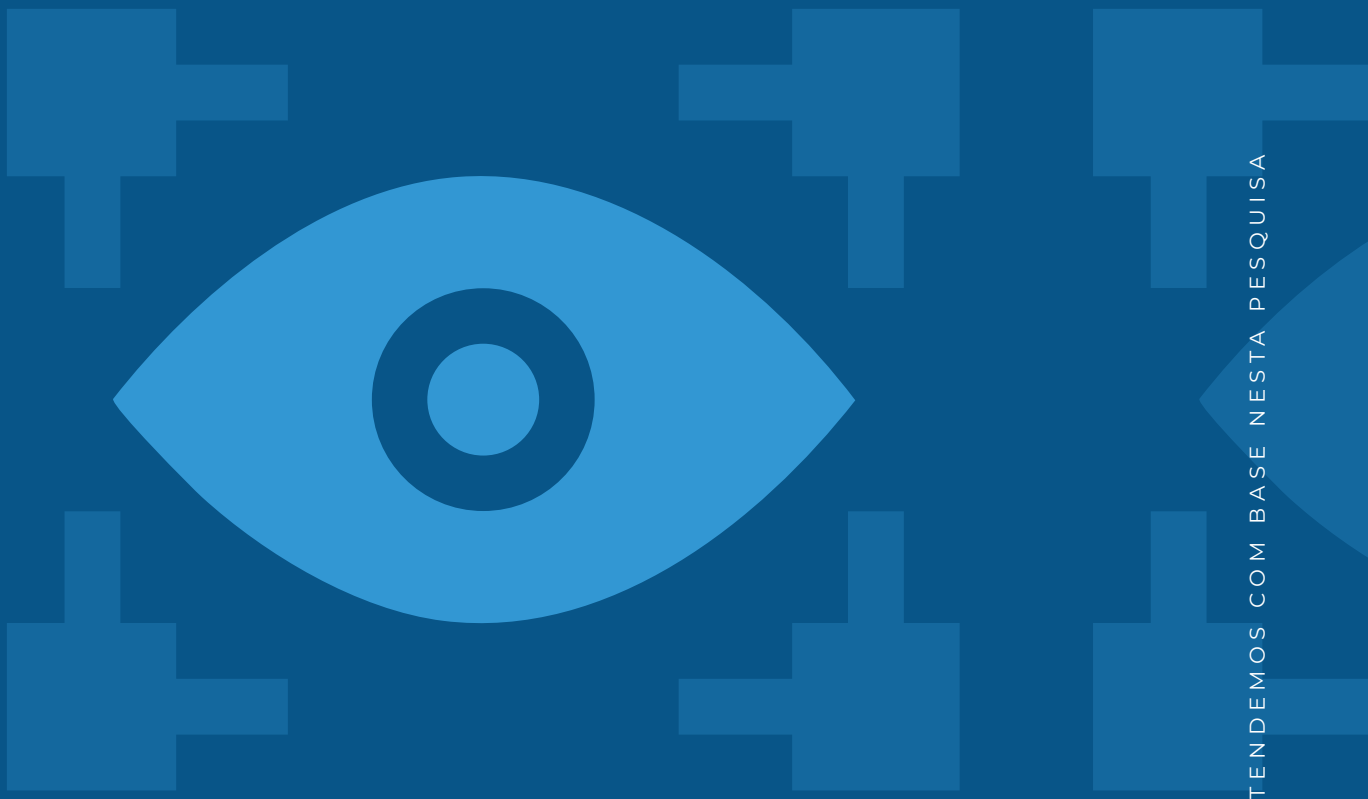
36. GENTILE, Giulia. Does Big Brother Exist? Facial Recognition Technology in the United Kingdom. In: The Cambridge Handbook of Facial Recognition in the Modern State. Org.: Rita Matulionyte and Monika Zalnieriute. Cambridge: Cambridge University Press, 2024, p. 173.

37. FUSSEY, Pete; MURRAY, Daragh. Independent report on the London Metropolitan Police service's trial of live facial recognition technology. Essex: University of Essex Repository, July, 2019.

38. REINO UNIDO. Código de Práticas sobre Sistemas de Câmeras de Vigilância. Nov. 2021. Disponível em: **gov.uk/government/publications/update-to-surveillance-camera-code** . Acesso em 13.02.2025.

dados pessoais e reafirmar a necessidade de prévia autorização legal, estabeleceu um quadro normativo em que a utilização de sistemas de identificação biométrica à distância em tempo real somente pode ocorrer para identificação de pessoa suspeita de prática de delitos com pena máxima superior a quatro anos.[39] Essa utilização deve observar a limitação geográfica e temporal, bem como ser antecedida de uma avaliação de impacto sobre os direitos fundamentais. A operacionalização de sistemas de reconhecimento facial somente poderá ocorrer também após prévia autorização judicial ou de autoridade administrativa independente.

Essas são medidas mínimas de proteção que, no curso da pesquisa, verificamos ausentes no caso brasileiro. O cenário nacional sobre reconhecimento facial implica, portanto, em uma profunda reflexão sobre a suspensão imediata da utilização desse tipo de tecnologia de reconhecimento facial até que, no processo legislativo, sejam definidas limitações, balizas ou mesmo a proibição de gastos públicos em tecnologias que não possuem justificativa suficiente de proporcionalidade entre os danos a direitos fundamentais e a efetividade que anunciam na execução de políticas de segurança pública.



39. UNIÃO EUROPEIA. Regulamento (EU) 2024/1689 do Parlamento Europeu e do Conselho. Cria regras harmonizadas em matéria de inteligência artificial. Jornal Oficial da União Europeia (PT), Série L, 12.jul. 2024.

O que propomos neste cenário

É urgente que o debate público sobre o reconhecimento facial na segurança pública seja aprofundado, com a participação da sociedade civil, de acadêmicos, de organismos internacionais e de órgãos de controle. A adoção de tecnologias com risco potencial tão alto deveria ser minimamente pautada por princípios éticos, respeito aos direitos fundamentais e garantia de transparência e *accountability*. É a este esforço que se soma o documento que apresentamos aqui.

O levantamento nacional sobre o uso do reconhecimento facial na segurança pública no Brasil revela um cenário preocupante, caracterizado pela rápida expansão dessa tecnologia sem acompanhamento regulatório, transparência ou salvaguardas adequadas aos direitos fundamentais. A ausência de um marco legal claro e a falta de protocolos padronizados para implementação e fiscalização desses sistemas colocam em risco princípios básicos do Estado Democrático de Direito, como a proteção à privacidade, à igualdade e ao devido processo legal.

Os dados obtidos evidenciam que muitos estados adotaram o reconhecimento facial sem realizar estudos técnicos que comprovem sua eficácia ou sem apresentar justificativas que sustentem o alto investimento financeiro envolvido. A falta de transparência é outro ponto crítico, com vários estados se recusando a fornecer informações básicas sobre contratos, localização de câmeras e dados de desempenho dos sistemas. Esse panorama é agravado pela inexistência de mecanismos de supervisão e auditoria, o que impede uma avaliação adequada dos impactos da tecnologia sobre a população.

Também é importante citar o risco sempre presente de discriminação algorítmica, com sistemas que apresentam taxas de erro desproporcionalmente altas para pessoas negras, indígenas e asiáticas, reforçando padrões históricos de seletividade penal e violência institucional. A falta de medidas para mitigar esses vieses, combinada com o uso indiscriminado da tecnologia, pode aprofundar ainda mais as desigualdades sociais e raciais no país.

Os dados aqui expostos dão conta de uma série de irregularidades e maus usos das tecnologias de reconhecimento facial, que afetam a proteção aos direitos fundamentais, a não discriminação, a transparência pública, a lisura na gestão do orçamento público. Chama a atenção também a falta de justificativas que fundamentam o alto investimento em tecnologias que ainda não comprovaram eficácia, em detrimento a outros serviços básicos que deveriam ser prioritários.

Esse cenário levou muitas organizações, incluindo o CESeC, a aderirem a uma campanha pedindo o banimento das tecnologias de reconhecimento facial em espaços públicos e para fins de segurança pública. Sem entrar nos méritos dessa posição, listamos aqui algumas recomendações que poderiam mitigar os problemas já sistematizados.

I. Proposição e discussão de **PROJETO DE LEI** que preveja, em âmbito nacional, as vedações, os limites e as condicionantes ao uso de tecnologias de reconhecimento facial para fins de segurança pública, estabelecendo limites claros e priorizando a proteção de direitos fundamentais, com o estabelecimento da **SUSPENSÃO DO USO** das TRF para fins de segurança pública até que haja definição em lei;

II. Na **REGULAMENTAÇÃO,** devem ser considerados quadros normativos e boas práticas que, reconhecendo a natureza de alto risco de sistemas de reconhecimento facial, abordem as seguintes medidas:

a) Desenvolvimento de **PROTOCOLOS PADRONIZADOS** de abordagem e uso do reconhecimento facial, que tragam uniformidade e garantam a transparência e o respeito ao devido processo legal;

b) Estabelecimento de **MECANISMOS DE AUDITORIA E SUPERVISÃO** independentes para fiscalizar o uso da tecnologia, garantindo a conformidade com as normas de proteção de dados e defesa dos direitos humanos;

c) **AUDITORIA** dos contratos em vigência e **TRANSPARÊNCIA** obrigatória dos novos contratos, para investigar possíveis desvios e mau uso do dinheiro público;

d) **CAPACITAÇÃO** das forças de segurança e de servidores públicos envolvidos para promover informações técnicas sobre a tecnologia e seus efeitos, bem como questões éticas e proteção de dados;

e) **GARANTIA DE INFORMAÇÃO** à população sobre o uso da tecnologia, suas implicações e maior conscientização sobre o consentimento livre e informado;

f) Desenvolvimento de **MECANISMOS QUE GARANTAM O ACESSO A BASES DE DADOS** atualizadas e íntegras, como forma de mitigar erros em relação de mandados de prisão inativos;

g) Elaboração e divulgação ampla de **RELATÓRIOS SOBRE OS IMPACTOS** do uso da tecnologia, fornecendo à população dados sobre eficiência e impactos sociais do reconhecimento facial.

III. **DELIMITAÇÃO DE CRITÉRIOS E CONDICIONANTES**, com a devida transparência e sujeito ao controle externo, para a elaboração e utilização da lista de pessoas de interesse dos órgãos policiais, com a indicação das hipóteses que justifiquem, limitação do tempo de inclusão e com a garantia do direito de petição para a retirada dos dados;

IV. Definição da necessidade de **PRÉVIA AUTORIZAÇÃO JUDICIAL** para a utilização de tecnologias de reconhecimento facial para fins de investigação, persecução ou cumprimento de mandados de prisão vinculados aos crimes que admitem o emprego desse tipo de tecnologia;

V. **IDENTIFICAÇÃO DAS EMPRESAS PRIVADAS** que atuam no planejamento, produção e operação de *softwares* de coleta, armazenamento e tratamento de dados pessoais para fins de segurança pública, cujo funcionamento deve estar atrelado a prévia autorização pela autoridade administrativa competente;

VI. Fixação de **PERÍODO MÁXIMO DE ARMAZENAMENTO** das imagens capturadas e da limitação geográfica, com o descarte imediato de imagens faciais de pessoas que não estejam na lista de interesse da polícia;

VII. Definição de limites mínimos de *score* de correspondência para a operacionalização de *softwares* de reconhecimento facial como forma de **MITIGAR OS FALSOS POSITIVOS;**

VIII. Previsão de medidas para não repetição, prevenção e reparação dos danos de pessoas e coletividades atingidas por tratamento discriminatório decorrente do emprego de tecnologias de reconhecimento facial.

Acreditamos que essas medidas trariam maior proteção aos cidadãos brasileiros, o que deveria ser um interesse de todos, especialmente dos entes públicos. É fundamental e urgente que olhemos cuidadosamente para este tema, como sociedade, para a compreensão de como nos inserimos na expansão da cultura de vigilância e como podemos reagir a ela no sentido de garantir nossos direitos básicos. Esperamos que este relatório seja um passo neste sentido.

Referências bibliográficas

A/HRC/42/59. Human Rights Council Forty-second session 9–27 September 2019 Agenda item 9 Racism, racial discrimination, xenophobia and related forms of intolerance, follow-up to and implementation of the Durban Declaration and Programme of Action Report of the Working Group of Experts on People of African Descent on its twenty-third and twenty-fourth sessions.

ACCESS NOW; ASOCIACIÓN POR LOS DERECHOS CIVILES; LABORATORY OF PUBLIC POLICY AND INTERNET – LAPIN; LALIBRE.NET. Vigilância biométrica remota na América Latina: as empresas estão respeitando os direitos humanos? 2023. Disponível em: **accessnow.org/press-release/analysis-answers-surveillance-tech-latin-america/**. Acesso em: 5 fev. 2025.

ALTO COMISSARIADO DAS NAÇÕES UNIDAS PARA OS DIREITOS HUMANOS. Relatório A/HRC/44/24: Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests. Nações Unidas, 2020. Disponível em: **ohchr.org/en/documents/thematic-reports/ahrc4424-impact-new-technologies-promotion-and-protection-human-rights**. Acesso em: 5 fev. 2025.

AMARAL, Augusto Jobim do; FERREIRA, Ana Gabriela. Solucionismo Tecnológico na Segurança Pública Brasileira: o caso do reconhecimento facial na Bahia. In: Sarlet et al. (orgs.). *Tecnologia e Antidiscriminação*. Londrina: Thoth, 2024, pp. 45-58.

AMARAL, Augusto Jobim do et al. (orgs.). *A cidade como máquina biopolítica*. Valencia: Tirant lo Blanch, 2022. Disponível em: **idus.us.es/items/7a6cc72a-622a-4c17-ab61-bc81fae05f2e**

AMARAL, Augusto Jobim do et al. (orgs.). *A cidade como máquina biopolítica*. Valencia: Tirant lo Blanch, 2022. Disponível em: **idus.us.es/items/7a6cc72a-622a-4c17-ab61-bc81fae05f2e**

AMARAL, Augusto Jobim do; ELESBÃO, Ana Clara Santos; DIAS, Felipe da Veiga. Governamentalidade Algorítmica e Novas Práticas Punitivas, *Revista Derechos en Acción*, año 6, n. 20, 2021, pp. 667-698. Disponível em: **sedici.unlp.edu.ar/handle/10915/137881**

AMARAL, Augusto Jobim do; MEDINA, Roberta. As Máquinas De Visão Cibernéticas e o Advento De Um Novo Regime De Verdade, *Dorsal. Revista de Estudios Foucautianos*, N. 12, junio 2022, pp. 221-242 . Disponível em: **revistas.cenaltes.cl/index.php/dorsal/article/view/490**

AMARAL, Augusto Jobim do *et. al.*. . *Algoritarismos*. Valencia: Tirant lo Blanch, 2022. Disponível em: **idus.us.es/items/499f3b92-78cc-4a94-9c5c-f0704ff724a5**

BISCHOFF, Paul. Facial recognition technology (FRT): 100 countries analyzed, 8 June 2021. Disponível em: Comparitech, <**comparitech.com/blog/vpn-privacy/facial-recognition-statistics/#:~:text=Five%20countries**>.

BRASIL. Ministério da Justiça e Segurança Pública. Portaria N.° 793, de 24 de outubro de 2019. Diário Oficial da União: seção 1, Brasília-DF, edição 208, p. 55, 24 de out. 2019. Disponível em: **in.gov.br/en/web/dou/-/portaria-n-793-de-24-de-outubro-de-2019-223853575**. Acesso em: 5 fev. 2025.

CERD/C/GC/36. Committee on the Elimination of Racial Discrimination General recommendation No. 36 (2020) on preventing and combating racial profiling by law enforcement officials.

DE MORAES, A. L. Z.; BARBOSA, L. V. F.; DEL GROSSI, V. C. D. Inteligência artificial e direitos humanos: aportes para um marco regulatório no Brasil.

ESCRITÓRIO DO ALTO COMISSARIADO DAS NAÇÕES UNIDAS PARA OS DIREITOS HUMANOS – ONU. A/HRC/55/60. Protocolo modelo para que agentes responsáveis pela manutenção da ordem promovam e protejam os Direitos Humanos no contexto de manifestações pacíficas. 31 jan. 2024. Disponível em: **ohchr.org/en/documents/legal-standards-and-guidelines/ahrc5560-model-protocol-law-enforcement-officials-promote**. Acesso em: 5 fev. 2025.

EUROPEAN DATA PROTECTION BOARD (EDPB). Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. Version 1, 12 maio 2022. Disponível em: **edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf**. Acesso em: 5 fev. 2025.

EUROPEAN DIGITAL RIGHTS (EDRi). Italy introduces a moratorium on video surveillance systems that use facial recognition. Disponível em: **edri.org/ourwork/italy-introduces-a-moratorium-on-video-surveillance-systems-that-use-facial-recognition/**. Acesso em: 5 fev. 2025.

FUSSEY, Pete; MURRAY, Daragh. Independent report on the London Metropolitan Police service's trial of live facial recognition technology. Essex: University of Essex Repository, July, 2019.

GENTILE, Giulia. Does Big Brother Exist? Facial Recognition Technology in the United Kingdom. In: The Cambridge Handbook of Facial Recognition in the Modern State. Org.: Rita Matulionyte and Monika Zalnieriute. Cambridge: Cambridge University Press, 2024

GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee. Face Recognition Vendor Test – Part 3: Demographic Effects. National Institute of Standards and Technology, U.S. Department of Commerce. Disponível em: **doi.org/10.6028/NIST.IR.8280**. Acesso em: 13 jun. 2024.

INEWS. UK police forces testing new retrospective facial recognition that could identify criminals. Disponível em: **inews.co.uk/news/technology/uk-police-testing-retrospective-facial-recognition-identify-criminals-1128711**. Acesso em: 5 fev. 2025.

LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET (LAPIN). Vigilância automatizada: uso de reconhecimento facial pela administração pública no Brasil. 7 jul. 2021. Disponível em: **lapin.org.br/2021/07/07/vigilancia-automatizada-uso-de-reconhecimento-facial-pela-administracao-publica-no-brasil**. Acesso em: 5 fev. 2025.

MATULIONYTE, Rita; ZALNIERIUTE, Monika. The Cambridge Handbook of Facial Recognition in the Modern State. Cambridge: Cambridge University Press, 2024.

NUNES, Pablo; LIMA, Thallita G. L.; CRUZ, Thaís G. O sertão vai virar mar: expansão do reconhecimento facial na Bahia. Rio de Janeiro: CESeC, 2023.

NUNES, Pablo; LIMA, Thallita G. L.; RODRIGUES, Yasmin. Das planícies ao planalto: como Goiás influenciou

a expansão do reconhecimento facial na segurança pública brasileira. Rio de Janeiro: CESeC, 2023.

O PANÓPTICO. Monitoramento do uso de reconhecimento facial no Brasil. Disponível em: opanoptico.com.br. Acesso em: 5 fev. 2025.

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (OPC). Police use of facial recognition technology in Canada and the way forward. Disponível em: <**priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/**>. Acesso em: 5 fev. 2025.

R(BRIDGES) VS. SOUTH WALES POLICE. Case No: C1/2019/2670. Court of Appeal (Civil Division), Royal Courts of Justice, 11 ago. 2020. Disponível em: **judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf**. Acesso em: 25 maio 2024.

SÃO PAULO. Tribunal de Justiça de São Paulo. 6ª Vara de Fazenda Pública. Processo n. 1010667-97.2022.8.26.0053. Decisão Liminar. Juíza Estadual Cynthia Tome. DJe n. 3473, 25 mar. 2023.

SCHWARTZ, Reva et al. Towards a Standard for Identifying and Managing Bias in Artificial Intelligence. National Institute of Standards and Technology, U.S. Department of Commerce. Disponível em: **doi.org/10.6028/NIST.SP.1270**. Acesso em: 13 jun. 2024.

SILVA, Tarcízio. Racismo algorítmico: inteligência artificial e discriminação nas redes digitais. São Paulo: Sesc, 2022.

SOUZA, Roberta de. Carnaval do Rio terá monitoramento com reconhecimento facial e drones, divulga governo em plano de segurança. O Globo, Rio de Janeiro, 05 fev. 2024. Disponível em: **oglobo.globo.com/rio/carnaval/noticia/2024/02/05/carnaval-do-rio-tera-monitoramento-com-reconhecimento-facial-e-drones-divulga-governo-em-plano-de-seguranca.ghtml**. Acesso em: 12 jun. 2024.

STATEWATCH. Legal action against police facial recognition technology. Disponível em: <**statewatch.org/news/2020/september/france-legal-action-against-police-facial-recognition-technology/**>. Acesso em: 5 fev. 2025.

WORLD ECONOMIC FORUM; UNICRI; INTERPOL; NETHERLANDS POLICE. A policy framework for responsible limits on facial recognition. 2022.

Anexo I: Perguntas e respostas

TABELA 1. RESPOSTAS DOS ESTADOS

ESTADO	NÚMERO DO DOCUMENTO SEI DA RESPOSTA
Acre	7460628
Alagoas	7444146 / 7460205
Amapá	7542053
Bahia	7599543 / 7599688
Ceará	7436870
Distrito Federal	7460876
Espírito Santo	7412495
Goiás	7362488
Mato Grosso	7399736
Mato Grosso do Sul	7373827
Minas Gerais	7408650
Pará	7531054
Paraná	7404149
Pernambuco	7403947
Piauí	7398593
Rio de Janeiro	7408592
Rio Grande do Norte	7362116
Rio Grande do Sul	7535513
Roraima	7528087
Santa Catarina	7391001
São Paulo	7481959
Tocantins	7370488 / 7473633

Fonte: DPU/DNDH e CESeC

1. Há algum contrato ou procedimento licitatório em curso para uso de tecnologia de reconhecimento facial no órgão? Caso positivo, favor enviar a cópia do contrato e/ou do procedimento licitatório.

2. Há utilização da tecnologia de reconhecimento facial no estado ou nos municípios? Caso positivo, qual órgão utiliza e gerencia o processamento das informações?

Os estados que declararam não possuir contrato ou procedimento licitatório em andamento para o uso de tecnologia de reconhecimento facial são: Acre, Amapá, Ceará, Distrito Federal, Espírito Santo, Goiás, Mato Grosso, Mato Grosso do Sul, Minas Gerais, Paraná, Rio Grande do Norte, Rondônia, Santa Catarina e São Paulo.

Por outro lado, alguns estados possuem contrato vigente ou procedimento licitatório em curso, mas não anexaram os documentos solicitados em suas respostas ao ofício. Estes são: Pernambuco, Piauí, Rio Grande do Sul, Rio de Janeiro, Roraima e Tocantins. Além disso, há estados que estão em fase de estudo ou teste da tecnologia, mas que ainda não possuem contrato ou processo licitatório em andamento. São eles: Amapá, Ceará, Espírito Santo, Goiás, Mato Grosso, Minas Gerais, Paraná e São Paulo.

No entanto, alguns estados declararam estar em fase de licitação para a aquisição da tecnologia, embora ela ainda não esteja sendo aplicada. Nesta situação encontram-se: Piauí e Roraima. Por fim, o estado de Tocantins informou já possuir contrato para a tecnologia de reconhecimento facial, porém ainda não tê-la implementado.

TABELA 2. CONTRATO OU PROCEDIMENTO LICITATÓRIO EM CURSO E ÓRGÃO RESPONSÁVEL

ESTADO	CONTRATO /PROCESSO	EMPRESA CONTRATADA	FINALIDADE	STATUS	FONTE DE CUSTEIO	ÓRGÃO RESPONSÁVEL
AL	SSP N° 028/2024	Teltex Tecnologia S.A.	Reconhecimento facial (implementação e operação)	Contrato em vigor, testes não iniciados	Verba estadual	Secretaria de Segurança Pública de Alagoas (SSP/AL)
BA	03/2021	Consórcio Vídeo Polícia	Serviços tecnológicos integrados de segurança pública	Contrato vigente, 60 meses	Tesouro estadual (fonte 100)	SSP-BA e supervisionado pelo Centro de Operações e Inteligência (COI)
MG	ClearView (em aquisição)	Não especificado	Processamento e análise de dados visuais	Em andamento, tecnologia não utilizada	Fesp-MG, Eixo RMVI	Não especificado.
PA	N° 108/2020-SEGUP/PA	RadioNews Comércio e Serviço de Telecomunicação e Informática LTDA	Monitoramento de desaparecidos e foragidos	Em vigor, duração de três anos	Recursos estaduais	SEGUP/PA.
PE	N° 050/2023 GAB/SDS	Pegasus Tecnologia LTDA EPP	Identificação de desaparecidos e foragidos	Em vigor, duração de três anos	Recursos estaduais	Centro Integrado de Inteligência de Defesa Social (CIIDS)
PI	00027. 000302 / 2024-65	Ainda em licitação	Captura de imagens por reconhecimento facial	Fase de licitação	Convênio estadual	Ainda em licitação
RS	N° 01/DGT/ 2021	Não informado	Localização de desaparecidos	Contrato vigente, modelo Livestream	Orçamento geral SSP/RS	Secretaria de Segurança Pública (SSP/RS)
RJ	SEI-350486/ 002133/2021	Não informado	Monitoramento em tempo real; busca de pessoas com mandados pendentes	Contrato vigente	Não especificado	Polícia Militar, TJRJ, Detran-RJ e Polícia Civil
RR	N° 98/2024 SESP/ DEPLAF/DA	Não informado	Videomonitoramento para prevenção e repressão de crimes	Em fase de implantação	Estadual (Plano Anual de Trabalho)	Ainda em licitação
TO	N° 72/2023	Griaulle LTD	Identificação criminal e localização de desaparecidos	Em fase de implantação	Convênio federal (SENASP/ MJ)	Instituto de Identificação da SSP/TO

Fonte: DPU/ DNDH e CESeC

3. Quanto ao tipo de reconhecimento facial, trata-se de modelo livestream (transmissão em tempo real à gravação), comparação de fotos em investigação ou outro modelo? Favor especificar.

TABELA 3. TIPOS DE RECONHECIMENTO FACIAL E FINALIDADE

ESTADO	MODELO UTILIZADO	FINALIDADE
Alagoas	Livestream	Comparação de imagens capturadas em tempo real com bancos de dados de foragidos, desaparecidos, pessoas vulneráveis e investigados por violência contra grupos vulneráveis.
Bahia	Comparação de fotos	Reconhecimento baseado em fotos do Banco Nacional de Mandados de Prisão.
Espírito Santo	Período de testes, planejando reconhecimento em tempo real, comparação de fotos e análise de vídeos gravados	Planejamento para atender demandas de segurança pública e investigações com tecnologia de reconhecimento facial.
Pará	Livestream	Monitoramento em tempo real em áreas de grande circulação.
Pernambuco	Livestream	Identificação de pessoas com mandados de prisão em eventos de grande porte.
Piauí	Livestream	Monitoramento em tempo real em áreas de grande circulação.
Rio Grande do Sul	Livestream	Localização de pessoas desaparecidas com câmeras instaladas em locais estratégicos.
Rio de Janeiro	Livestream e comparação de fotos	Identificação de pessoas com mandados de prisão pendentes.
Roraima	Comparação de foto com frame gravado em tempo real	Comparação de imagens capturadas com listas de pessoas procuradas e desaparecidas.
Tocantins	Comparação de fotos	Auxílio na identificação criminal e emissão de documentos de identificação.

Fonte: DPU/ DNDH e C Fonte: DPU/DNDH e CESeC ESeC

4. Existe alguma verba orçamentária destinada à implementação da tecnologia de reconhecimento facial? Caso positivo, informar o montante e a fonte de custeio.

TABELA 4. ORÇAMENTO DESTINADO A TRF E FONTE DE CUSTEIO

ESTADO	VERBA (R$)	FONTE DE CUSTEIO	OBSERVAÇÃO
Alagoas	5.839.550,76	Verba estadual	
Bahia	Aproximadamente 66 milhões	Tesouro estadual (fonte 100)	
Mato Grosso	14.000.000,00	Recursos estaduais	O Estado ainda não possui tecnologia implementada. Valor previsto no Plano Anual de Trabalho 2025, pendente de autorização do Governador.
Minas Gerais	939.480,00	Origem estadual (Fesp-MG, RMVI, Termo de Descentralização nº 07/2024, fonte 57.1)	O Estado ainda não possui tecnologia implantada, está em fase de definição e planejamento.

ESTADO	VERBA (R$)	FONTE DE CUSTEIO	OBSERVAÇÃO
Pará	20.193.510,00	Recursos estaduais	
Pernambuco	1.619.999,00	Recursos estaduais	
Piauí	33.641.819,05	Recursos estaduais	
Rio Grande do Sul	Não há verba específica	Orçamento geral SSP/RS	Custeio realizado a partir do orçamento geral da SSP/RS.
Rio de Janeiro	Existe verba, mas não foi informada	Não especificado	Informação disponível no processo público SEI-350486/002133/2021 (https://sei.rj.gov.br).
Roraima	8.397.600,00	Verba estadual; Plano Anual de Trabalho 2024 e 2025	
Tocantins	15.832.290,00	Convenio federal nº 891177/2019 (SENASP/MJ)	

Fonte: DPU/DNDH e CESeC

5. Onde as câmeras foram instaladas (solicita-se a indicação dos pontos com a localização geográfica, se possível)? O que motivou a escolha dos pontos para a instalação das câmeras?

TABELA 5. LOCALIZAÇÃO DAS CÂMERAS E MOTIVAÇÃO DA INSTALAÇÃO

ESTADO	LOCAIS DE INSTALAÇÃO	MOTIVAÇÃO
Alagoas	Locais de grande circulação de pessoas e veículos; pontos detalhados no Contrato SSP Nº 028/2024.	Detalhada no Contrato SSP Nº 028/2024.
Bahia	Pontos estratégicos da segurança pública, sem detalhamento exato.	Instrumento de prevenção ao crime com práticas eficientes de policiamento.
Espírito Santo	Imagens de câmeras de videomonitoramento existentes integradas ao CERCO INTELIGENTE; período de teste.	Não informado.
Mato Grosso	Logradouros públicos com maior concentração de pessoas; comparação com bases de dados.	Comparação de imagens com bases de dados de desaparecidos e mandados de prisão.
Pará	Belém, Castanhal, Capanema, Bragança, Santarém, Altamira, Paragominas, Marabá, Breves, Benevides e Portel; link: google.com/maps/d/viewer?mid=1eq7MilwT78T3u1vPhX3zKMiAy8cgt	Áreas de grande circulação e pontos estratégicos para segurança pública.
Paraná	Câmeras existentes do Estado usadas para testes; localização não especificada.	Uso de infraestrutura existente sem custos adicionais de hardware.
Pernambuco	Definidos pelo planejamento da Arquitetura de Reconhecimento Facial em Eventos (ARFE), sem localização fixa.	Segurança pública e monitoramento em eventos de grande porte.
Rio de Janeiro	Locais sigilosos, escolhidos com base em dados estatísticos de manchas criminais.	Baseada em dados estatísticos de manchas criminais.
Rio Grande do Sul	Porto Alegre, 20 câmeras; localização sigilosa conforme a Lei de Acesso à Informação.	Não informado.

ESTADO	LOCAIS DE INSTALAÇÃO	MOTIVAÇÃO
Roraima	Locais definidos por georreferenciamento: áreas de alta criminalidade, interseções de tráfego, pontos turísticos, etc.	Eficiência na segurança pública; prevenção e repressão de crimes.
São Paulo	Cenários específicos para validação de uso da tecnologia; testes pontuais.	Não informado.
Tocantins	Delegacias regionais, núcleos de papiloscopia e sede da SSP.	Identificação criminal e emissão de documentos oficiais.

Fonte: DPU/DNDH e CESeC

6. Para quais finalidades são utilizadas as imagens capturadas pela tecnologia de reconhecimento facial?

7. As imagens capturadas ou compartilhadas pela tecnologia de reconhecimento facial são descartadas ou ficam armazenadas em algum banco de dados? Neste segundo caso, por quanto tempo dura o armazenamento? É utilizada alguma técnica para garantir a segurança e a integridade dos bancos de dados? Qual?

TABELA 6. FINALIDADE DO USO DAS IMAGENS CAPTURADAS E TEMPO DE ARMAZENAMENTO

ESTADO	FINALIDADE DAS IMAGENS CAPTURADAS	ARMAZENAMENTO DE IMAGENS
Alagoas	Comparar imagens com bancos de dados de foragidos, desaparecidos e investigados por violência contra grupos vulneráveis.	Sim, as imagens são armazenadas por até 30 dias, sob responsabilidade da Teltex Tecnologia S.A, sem compartilhamento com outros órgãos.
Bahia	Captura de pessoas com mandado de prisão e localização de desaparecidos.	Sim, as imagens são armazenadas por até 30 dias para aprendizado da solução de IA, sendo descartadas após esse período com garantia de integridade dos dados.
Espírito Santo	Avaliar acurácia, detectar atributos faciais, analisar vieses e testar a confiabilidade do sistema durante testes. Caso aprovado, será usado para localização de desaparecidos, foragidos e investigações criminais.	A tecnologia está em teste. Caso aprovada, vídeos serão armazenados por até 30 dias, fotos por até 90 dias e metadados por até 1 ano, com segurança garantida por criptografia, controle de acesso, auditoria e monitoramento.
Mato Grosso	Comparar imagens com bases de dados de desaparecidos e mandados de prisão em aberto pela Justiça.	A tecnologia está em análise/ teste. Serão usados vários níveis de segurança, incluindo criptografia dos dados.
Pará	Busca de pessoas desaparecidas; identificação de foragidos; atendimento a solicitações de órgãos de segurança pública ou ordens judiciais.	Sim, as imagens são armazenadas por 60 dias e sobrepostas por novas imagens. Não foram especificadas técnicas de segurança.
Paraná	Auxiliar no processo de suspeita fundamentada; melhorar a segurança das equipes; localizar desaparecidos; prevenir crimes; gerenciar multidões e eventos.	Durante os testes, os dados biométricos foram processados em tempo real e retidos apenas durante a testagem, com segurança assegurada por criptografia e controle de acesso.
Pernambuco	Identificar indivíduos com mandados de prisão em aberto.	Sim, as imagens ficam armazenadas até que a finalidade de segurança pública seja alcançada. Não foram especificadas técnicas de segurança.

ESTADO	FINALIDADE DAS IMAGENS CAPTURADAS	ARMAZENAMENTO DE IMAGENS
Rio de Janeiro	Buscar pessoas com mandados de prisão pendentes.	Sim, as imagens ficam armazenadas por 30 dias. A segurança é garantida por senhas individuais e firewall NextGeneration WAF.
Rio Grande do Sul	Exclusivamente para localização de pessoas desaparecidas.	Sim, as imagens ficam armazenadas por 24 horas no Data Center PROCERGS, sendo sobrepostas diariamente com especificações técnicas de segurança.
Roraima	Prevenir e reprimir crimes; auxiliar investigações; monitorar cidadãos e veículos em áreas de maior vulnerabilidade.	Sim, as imagens são armazenadas com criptografia, controle de acesso, auditorias e testes de segurança, mas sem duração especificada.
São Paulo	Avaliar viabilidade de uso para atender às diretrizes do Sistema Único de Segurança Pública e planejamento estratégico estadual.	Não existe sistema implementado. Caso implementado, seguirá práticas estabelecidas, como termos de uso responsável e governança de dados.
Tocantins	Identificação criminal; busca por desaparecidos; emissão de documentos oficiais, como a Carteira de Identidade Nacional.	Sim, as imagens são armazenadas em banco de dados com medidas de segurança, incluindo rastreabilidade e prova eletrônica. O tempo de armazenamento não foi especificado.

Fonte: DPU/DNDH e CESeC

8. As imagens faciais capturadas são compartilhadas com algum outro órgão público ou entidade privada? Se sim, qual(is)?

TABELA 7. COMPARTILHAMENTO DAS IMAGENS

ESTADO	COMPARTILHAMENTO DE IMAGENS	COMPARAÇÃO COM LISTAS DE PROCURADOS/DESAPARECIDOS
Alagoas	Não há compartilhamento das imagens com outros órgãos ou entidades privadas.	Sim, imagens são comparadas com listas de mandados de prisão em aberto e desaparecidos. Critérios: mandados e boletins de ocorrência.
Bahia	Não há compartilhamento dos dados biométricos com entidades externas. O acesso é restrito a profissionais de segurança pública.	Sim, imagens são comparadas com bases do Banco Nacional de Mandados de Prisão e listas de desaparecidos.
Espírito Santo	Tecnologia em planejamento. Caso aprovada, as imagens poderão ser usadas em investigações e documentos oficiais, respeitando sigilo e proteção de dados.	Tecnologia em teste. Expectativa: comparação com bancos de dados da segurança pública.
Mato Grosso	Informou apenas que a tecnologia está em fase de análise e testes.	Informou apenas que a tecnologia está em fase de análise e testes.
Pará	Imagens não são compartilhadas, exceto mediante solicitação formal de órgãos de segurança pública ou determinação judicial.	Sim, comparadas com listas de dados fornecidos por órgãos de segurança. Critérios incluem nome, foto, status, e número do INFOPEN.
Paraná	Durante os testes, não houve compartilhamento de imagens faciais capturadas com outros órgãos.	Sim, durante os testes, imagens foram comparadas com listas de procurados, foragidos e desaparecidos, com dados tratados sigilosamente.
Pernambuco	Imagens faciais capturadas não são compartilhadas com outros órgãos públicos ou entidades privadas.	Sim, comparadas com a lista de pessoas procuradas do Banco Nacional de Mandados de Prisão.

ESTADO	COMPARTILHAMENTO DE IMAGENS	COMPARAÇÃO COM LISTAS DE PROCURADOS/DESAPARECIDOS
Rio de Janeiro	Imagens faciais capturadas não são compartilhadas com outros órgãos públicos ou entidades privadas.	Sim, comparadas com o banco de dados de pessoas com mandados de prisão do RJ, integrado pelo Portal de Segurança.
Rio Grande do Sul	Imagens não são compartilhadas com outros órgãos ou entidades privadas.	Sim, comparadas apenas com listas de pessoas desaparecidas. Critérios: registros policiais. Informações mantidas sob sigilo.
Roraima	Podem ser compartilhadas com forças de segurança, autoridades policiais, agências de inteligência e outros órgãos governamentais.	Sim, comparadas com listas de procurados e desaparecidos baseadas em registros criminais e fontes oficiais.
São Paulo	Não há sistema implementado, mas durante os testes não houve compartilhamento de imagens.	Não há sistema implementado, mas durante os testes as imagens foram relacionadas a desaparecidos e procurados, com anonimização por HASH.
Tocantins	Sim, imagens são compartilhadas com o Ministério da Justiça, Receita Federal e Ministério da Gestão e Inovação.	Sim, o sistema ABIS compara imagens com listas de desaparecidos, criminosos e suspeitos, seguindo a LGPD.

Fonte: DPU/DNDH e CESeC

9. Nos espaços onde foram instalados os equipamentos de reconhecimento facial, são colocados avisos sobre a captura de imagens faciais e processamento biométrico? Quais são os meios utilizados para informar?

O uso de avisos para informar o público sobre a captura de imagens faciais e o processamento biométrico varia amplamente entre os estados brasileiros. Em Alagoas e no Pará, há sinalização nos locais monitorados, e o Pará destaca o uso de placas e avisos sonoros e luminosos em câmeras e totens de segurança. Já em Roraima, foi afirmado que haverá avisos nos locais de instalação. Por outro lado, estados como Bahia, Pernambuco, Rio de Janeiro e Rio Grande do Sul não utilizam qualquer tipo de aviso, alegando que "o uso da tecnologia é exclusivamente para apoiar as forças policiais". No Espírito Santo e em São Paulo, onde a tecnologia ainda está em fase de testes ou planejamento, não há avisos instalados até o momento, mas o Espírito Santo prevê ações alinhadas à LGPD após a definição do Grupo de Trabalho.

Alguns estados não detalharam suas práticas. Tocantins, por exemplo, não menciona a existência de avisos, enquanto no Paraná, durante os testes, não havia sinalização nos locais monitorados. Mato Grosso também se encontra em fase de análise e testes, sem informações adicionais sobre avisos ao público. Esse panorama revela uma falta de uniformidade nas práticas de transparência e comunicação sobre o uso de tecnologias de reconhecimento facial, refletindo diferentes abordagens e níveis de preocupação com a informação ao público.

10. Foram adotadas medidas para corrigir distorções relacionadas ao viés discriminatório da tecnologia algorítmica? Caso positivo, quais?

11. Existe a necessidade da utilização de dados pessoais para treinar a ferramenta? Quais são os bancos de dados utilizados? Em caso positivo, as pessoas são informadas que seus dados pessoais estão sendo usados para alimentar a ferramenta?

TABELA 8. MEDIDAS PARA CORRIGIR VIÉS E COLETA DE DADOS PESSOAIS

ESTADO	MEDIDAS PARA CORRIGIR VIÉS DISCRIMINATÓRIO	NECESSIDADE DE DADOS PESSOAIS E BANCOS UTILIZADOS	RESPOSTA DETALHADA SOBRE USO DE DADOS PESSOAIS
Alagoas	Questão técnica direcionada à empresa; não especificou medidas concretas.	Treinamento com servidores e banco próprio da SSP; não especifica se dados são pessoais ou anonimizados.	O treinamento será feito com servidores da SSP e empresa contratada; uso de banco próprio da SSP; sem clareza sobre anonimização ou consentimento.
Bahia	Configuração para alertas acima de 90% de similaridade; protocolos operacionais para agentes.	Utilização de dados do Banco Nacional de Mandados de Prisão; não há notificação aos indivíduos.	Uso de dados do Banco Nacional de Mandados de Prisão para apoiar forças policiais sem notificação aos indivíduos.
Espírito Santo	Testes no projeto piloto para identificar e corrigir vieses, avaliando cenários diversos.	Dados processados para segurança pública em servidores controlados pela SESP, conforme LGPD.	Em fase de planejamento; dados processados exclusivamente para segurança pública em servidores controlados pela SESP conforme a LGPD.
Mato Grosso	Em fase de análise/testes; nenhuma medida específica mencionada.	Em fase de análise/testes; nenhuma informação adicional.	Em fase de análise/testes; nenhuma informação adicional fornecida.
Pará	Triangulação de posições faciais; não há auditorias específicas informadas.	Não há treinamento; utiliza imagens cadastradas no sistema para fins investigativos.	Não há treinamento; utiliza faces cadastradas no sistema para fins investigativos; sem especificação de bases ou notificações.
Paraná	Testes com dados diversos; auditorias internas e ajustes contínuos.	Período de testes utilizou dados de bancos abertos como LFW, VG Face2; muitos sem consentimento explícito.	Testes utilizaram dados de bancos como LFW, VGGFace2, MegaForce; muitos sem consentimento explícito.
Pernambuco	Treinamento com grupos étnicos proporcionais.	A empresa contratada informou que não utiliza dados pessoais; nenhum banco especificado.	A empresa contratada informou que não utiliza dados pessoais; nenhuma especificação de bases utilizadas.
Rio de Janeiro	Protocolos diferenciados para abordagens; distorções discriminatórias não aplicadas à segurança pública.	Não realiza treinamento de ferramentas; utiliza dados de mandados de prisão expedidos.	Não realiza treinamento; utiliza dados de mandados de prisão expedidos.
Rio Grande do Sul	Nenhuma menção de medidas para corrigir vieses.	Produto contratado para busca de desaparecidos; nenhuma menção de treinamento.	Ferramenta contratada para busca de desaparecidos; sem informação sobre treinamento.
Roraima	Afirmou genericamente melhorias nos dados de treinamento e transparência.	Utiliza bancos públicos e privados; consentimento das pessoas é tratado de forma geral, sem explicação prática.	Necessidade de dados pessoais para treinamento; utiliza bancos públicos (LFW, MegaFace) e privados; sem explicação clara sobre consentimento.

ESTADO	MEDIDAS PARA CORRIGIR VIÉS DISCRIMINATÓRIO	NECESSIDADE DE DADOS PESSOAIS E BANCOS UTILIZADOS	RESPOSTA DETALHADA SOBRE USO DE DADOS PESSOAIS
São Paulo	Estudos em fase inicial; compromisso com transparência e ações corretivas.	Testes utilizam CPF para validação; baseiam-se em mandados de prisão e dados fornecidos por declarantes.	Testes em andamento; validação utiliza CPF, mandados de prisão e registros policiais; dados de desaparecidos baseados no declarante.
Tocantins	Não especificou medidas; treinamento conduzido pela empresa fornecedora do sistema.	Treinamento realizado pela empresa fornecedora do sistema ABIS; sem detalhes adicionais.	Treinamento feito pela empresa fornecedora do sistema ABIS; nenhuma especificação adicional.

Fonte: DPU/DNDH e CESeC

12. Existe a necessidade da utilização de dados sensíveis ou sigilosos para treinar a ferramenta? Se sim, qual a base legal e quais camadas adicionais de segurança são aplicadas para proteger esses dados?

As respostas sobre a utilização de dados sensíveis no treinamento de ferramentas de reconhecimento facial variam significativamente entre os estados. Alagoas, Pará e Pernambuco afirmaram que não utilizam dados sensíveis nesse contexto. Outros estados, como o Espírito Santo, ainda em fase de planejamento, informaram que não há necessidade de dados sensíveis ou sigilosos para o treinamento da tecnologia. Por sua vez, o Rio de Janeiro destacou que não realiza treinamentos e desenvolvimentos de ferramentas de inteligência artificial, enquanto o Rio Grande do Sul relatou que, para o uso atual da ferramenta, nunca houve necessidade de treinamento com dados sensíveis.

Por outro lado, estados como Paraná e Roraima reconheceram a necessidade de utilizar dados sensíveis para aprimorar algoritmos de reconhecimento facial. O Paraná destacou o uso de imagens faciais, consideradas dados biométricos pela LGPD, como essenciais para o desenvolvimento dos sistemas, enquanto Roraima apontou que utiliza dados sensíveis em contextos de segurança pública, fundamentando-se em regulamentações como a LGPD no Brasil e o GDPR na Europa. Ambos os estados relataram medidas rigorosas de proteção, como criptografia, controle de acesso e auditorias. Em São Paulo, onde ainda não há sistema implementado, mas testes estão sendo conduzidos, mencionou-se a segregação de ambientes de dados sensíveis e a criptografia como parte das práticas de segurança. Por fim, Tocantins informou que o treinamento das ferramentas foi conduzido pela empresa fornecedora do sistema, sem envolvimento direto do estado.

13. Quando o produto é ou foi disponibilizado para utilização pelo estado, há alguma exigência governamental prévia para a proteção de dados e para a abordagem ética em direitos humanos? E, para a iniciativa privada envolvida na licitação, há alguma exigência de cunho ético para aquisição do sistema?

TABELA 9. ABORDAGEM ÉTICA EM DIREITOS HUMANOS

ESTADO	RESPOSTA SOBRE CONFORMIDADE LEGAL E ÉTICA
Alagoas	Todas as exigências legais quanto ao serviço serão cumpridas e fiscalizadas junto à empresa contratada.
Bahia	Dados capturados utilizados exclusivamente para apoiar a SSP, com base no Banco Nacional de Mandados de Prisão.
Espírito Santo	Projeto piloto usa infraestrutura do Estado; fornecedores deverão cumprir exigências de proteção de dados e ética. Termos de confidencialidade para usuários finais.
Mato Grosso	Tecnologia em fase de análise e testes.
Pará	Dados do contrato e participação da iniciativa privada estão no Termo de Referência.
Paraná	O uso do reconhecimento facial no Brasil está em evolução; equilíbrio entre inovação tecnológica e proteção de direitos fundamentais é necessário.
Pernambuco	O processo de utilização da ferramenta segue preceitos legais e éticos.
Rio de Janeiro	O Software FindFace deve cumprir princípios da LGPD, garantindo proteção de dados e ética.
Rio Grande do Sul	Cumpre a LGPD e monitora a iniciativa privada por fiscais e gestores para assegurar conformidade com contrato, LGPD e LAI.
Roraima	Exigência estatal de proteção de dados e abordagem ética; conformidade com LGPD e GDPR mencionada genericamente.
São Paulo	Testes seguem padrão de ética e respeito aos direitos humanos preconizados pelas instituições da Pasta.
Tocantins	Contrato e Termo de Referência exigem conformidade com LGPD; proteção de dados garantida por Termo de Sigilo e normas vigentes.

Fonte: DPU/DNDH e CESeC

14. Quais são os procedimentos operacionais para abordagem das pessoas identificadas pelo sistema?

TABELA 10. PROCEDIMENTOS OPERACIONAIS

ESTADO	RESPOSTA SOBRE CONFORMIDADE LEGAL E ÉTICA
Alagoas	Protocolos padrão da PMAL e PCAL: proporcionalidade, uso progressivo da força, ética e apoio de serviços de saúde para desaparecidos.
Bahia	Alertas para perfis com similaridade acima de 90%. Confirmada a correspondência, a equipe policial é acionada seguindo protocolo interno rigoroso.
Espírito Santo	Em fase de planejamento. Caso contratada, seguirá protocolos das instituições de segurança pública para identificar desaparecidos e foragidos.
Mato Grosso	Tecnologia em análise e testes; nenhuma resposta detalhada.
Pará	Viatura é enviada para verificar identidade e veracidade do alerta.
Paraná	Alertas do sistema seguidos de verificação manual, planejamento estratégico, abordagem respeitosa e confirmação de identidade.
Pernambuco	Suspeita identificada pelo sistema, análise de similaridade facial, vigilância e pesquisa adicional, e acionamento de polícia ostensiva. Procedimentos detalhados nos artigos 289 e 290 do CPP.
Rio de Janeiro	Procedimentos descritos no Procedimento Operacional Padrão nº 316, processo SEI-350487/000092/2024; sem acesso público.

ESTADO	RESPOSTA SOBRE CONFORMIDADE LEGAL E ÉTICA
Rio Grande do Sul	Correspondência confirmada pelo sistema, status verificado no Sistema de Consultas Integradas, detalhes informados à Brigada Militar e protocolo gerado no SINESP CAD.
Roraima	Protocolos gerais mencionados, sem detalhes específicos.
São Paulo	Sem sistema implementado; testes seguem procedimentos operacionais padrão estabelecidos pelas instituições.
Tocantins	Reconhecimento facial usado como triagem; confirmação por especialista e laudo de comparação facial necessários para indiciamento ou prisão.

Fonte: DPU/DNDH e CESeC

15. Considerando a relevância da publicidade da informação em relação aos danos para garantia de direitos às pessoas abordadas e presas, a Secretaria tem produzido relatórios públicos de impacto sobre os casos de erro na abordagem identificada pela tecnologia de reconhecimento facial? Se sim, com qual frequência? Com publicação em que plataforma?

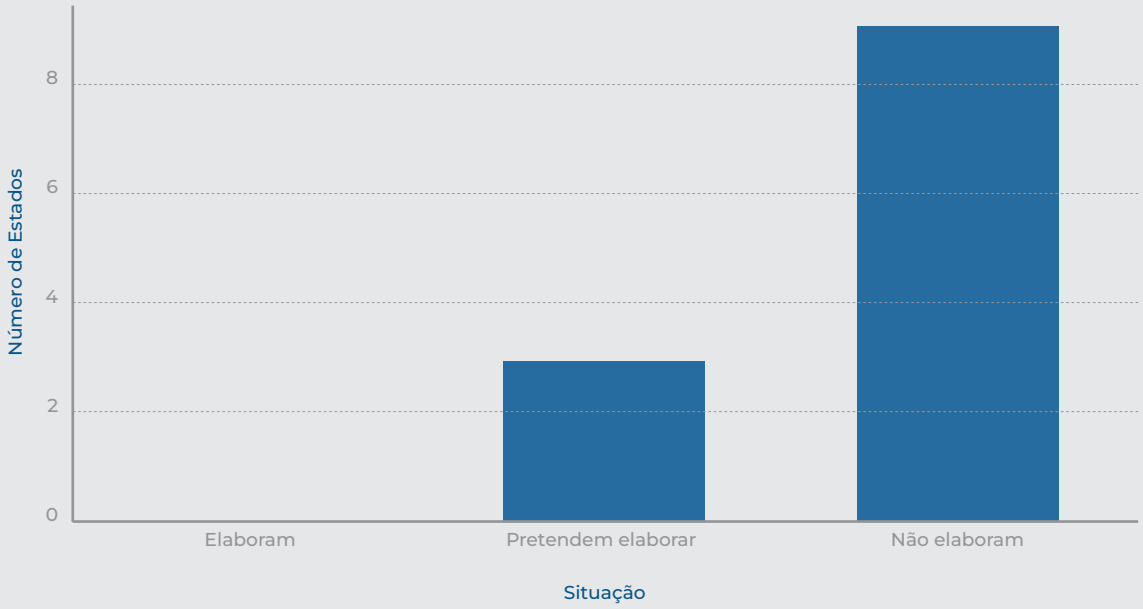
TABELA 11. RESPOSTA SOBRE A PRODUÇÃO DE RELATÓRIOS E PRODUÇÃO DE DADOS SOBRE ERROS

ESTADO	RESPOSTA SOBRE RELATÓRIOS DE ERROS
Alagoas	Sistema não implementado; relatórios ainda não são confeccionados.
Bahia	Não há registro de erros; sistema alerta similaridade acima de 90%, com análises adicionais antes de abordagem.
Espírito Santo	Tecnologia em planejamento; relatórios não aplicáveis nesta fase. Futuramente, a tecnologia será tratada como indicativo preliminar.
Mato Grosso	Tecnologia em análise e testes; nenhuma informação adicional.
Pará	Não produz relatórios deste tipo.
Paraná	Durante os testes, relatórios não foram produzidos.
Pernambuco	Não produz relatórios públicos; casos de incompatibilidade entre dados e imagens não são considerados erros.
Rio de Janeiro	Não produz relatórios públicos devido à LGPD; relatórios podem ser fornecidos à ANPD mediante requisição.
Rio Grande do Sul	Não produz relatórios deste tipo.
Roraima	Reconhece a importância de relatórios, mas não informa se os produz ou pretende fazê-lo.
São Paulo	Sem sistema implementado; estudos em curso coletam informações para futuros relatórios técnicos, sem confirmação de publicidade.
Tocantins	Reconhece a importância de relatórios, mas não indica se os produz ou se pretende produzi-los.

Fonte: DPU/DNDH e CESeC

Importante pontuar que **nenhum** dos estados que responderam a este quesito informou produzir relatórios de impacto sobre casos de erro relacionados ao uso da tecnologia. Alguns estados que ainda não implementaram o reconhecimento facial declararam a intenção de produzir tais relatórios no futuro, mas sem fornecer detalhes concretos ou cronogramas para sua efetivação.

ELABORAÇÃO DE RELATÓRIOS PÚBLICOS SOBRE ERROS DE RECONHECIMENTO FACIAL



Fonte: DPU/DNDH e CESeC

16. Houve prisões mediadas pelo uso da tecnologia? Quantas? Há menção no Auto de Prisão em Flagrante? Se não, que forma de registro tem sido utilizada para identificar as prisões feitas com base na identificação por reconhecimento facial?

TABELA 12. PRISÕES COM O USO DA TECNOLOGIA

ESTADO	PRISÕES E USO DA TECNOLOGIA
Alagoas	Sistema não implementado; não possui informações sobre prisões.
Bahia	2.054 prisões realizadas através dos alertas do Reconhecimento Facial recepcionados nos CICOMs. Demais perguntas não respondidas.
Espírito Santo	Tecnologia em planejamento; destinada à prisão de foragidos com mandados em aberto, não à prisão em flagrante. Resposta não aplicável nesta fase.
Mato Grosso	Tecnologia em análise e testes; nenhuma informação adicional.
Pará	1.870 alertas emitidos, 147 abordagens para checagem, 11 conduções à delegacia. Demais perguntas não respondidas.
Paraná	Durante os testes, cerca de 40 pessoas com mandados de prisão foram detidas, mas os BOs não mencionam o uso da tecnologia.
Pernambuco	3 prisões baseadas em reconhecimento facial, todas por mandados existentes; controle pelo Centro Integrado de Inteligência de Defesa Social.
Rio de Janeiro	325 prisões mediadas pela tecnologia; detalhes mencionados nos BOs da PM, mas competência dos Autos de Prisão é da Polícia Civil.
Rio Grande do Sul	Ferramenta usada apenas para busca de pessoas desaparecidas.
Roraima	Descrição abstrata sobre integração da tecnologia nos processos de prisão; sem informações concretas sobre prisões efetuadas.
São Paulo	Sem sistema implementado; 3 prisões realizadas em cenários de testes fechados.
Tocantins	Não houve prisões.

Fonte: DPU/DNDH e CESeC

17. Qual órgão/instituição, do setor público ou privado, é responsável pela gestão do banco e dos dados utilizados para fins de reconhecimento facial?

18. Quais outros órgãos ou instituições do setor público ou pessoa jurídica de direito privado estão envolvidos nas atividades relacionadas ao uso do sistema de reconhecimento facial, em especial, em relação ao uso de dados pessoais?

TABELA 13. ÓRGÃO RESPONSÁVEL PELO BANCO DE DADOS E INSTITUIÇÕES ENVOLVIDAS NO COMPARTILHAMENTO

ESTADO	ÓRGÃO RESPONSÁVEL PELO BANCO DE DADOS	ÓRGÃOS E INSTITUIÇÕES ENVOLVIDOS
Alagoas	SSP/AL	SSP/AL, com serviço operacional realizado pela empresa contratada.
Bahia	SSP-BA (Banco Nacional de Mandados de Prisão), COI, alimentado pela Superintendência de Inteligência.	SSP-BA, Polícia Militar do Estado da Bahia, Polícia Civil do Estado da Bahia.
Espírito Santo	SESP (Secretaria da Segurança Pública e Defesa Social do ES).	Durante o projeto piloto, dados permanecem em servidores da SESP. Se contratada, todos os órgãos de segurança pública e justiça criminal poderão acessar mediante termo de confidencialidade.
Mato Grosso	Secretaria de Segurança Pública em conjunto com a Polícia Judiciária Civil.	Apenas instituições de segurança pública com acesso para análises relacionais e associativas dos dados.
Pará	Centro Integrado de Operações da Secretaria de Estado de Segurança Pública e Defesa Social do Pará.	Não compartilha dados de reconhecimento facial com outros órgãos.
Paraná	Repositório temporário com imagens gerido pela PMPR durante os testes.	Testes realizados exclusivamente pela PMPR, geridos pela DDTQ.
Pernambuco	Centro Integrado de Inteligência de Defesa Social.	Centro Integrado de Inteligência de Defesa Social gerencia e controla os dados pessoais.
Rio de Janeiro	TJRJ, Detran e Polícia Civil do Rio de Janeiro.	Nenhum outro órgão ou instituição pública ou privada está envolvido.
Rio Grande do Sul	PROCERGS (Companhia de Processamento de Dados do Estado do Rio Grande do Sul).	SSP/RS (e vinculadas), PROCERGS e Empresa DGT (contratada).
Roraima	Gestão abstrata mencionada, sem especificar os órgãos envolvidos.	Afirma abstratamente que outros órgãos podem estar envolvidos, sem especificar.
São Paulo	GTI/SSP responsável pelos estudos em andamento sobre identificações biométricas.	Testes utilizam dados do CNJ, SAP e PCSP.
Tocantins	Instituto de Identificação.	Órgãos policiais/judiciais, Ministério da Justiça, Receita Federal e Ministério da Gestão e Inovação.

Fonte: DPU/DNDH e CESeC

19. Caso haja a participação de pessoa jurídica de direito privado em qualquer etapa da gestão do reconhecimento facial, houve por parte da SSP a notificação à Autoridade Nacional de Proteção de Dados, conforme rege o artigo 4°, inciso III, §4° da Lei Geral de Proteção de Dados Pessoais?

TABELA 14. PARTICIPAÇÃO DE PESSOA JURÍDICA DE DIREITO PRIVADO E NOTIFICAÇÃO À ANPD

ESTADO	RESPOSTA
Alagoas	Assim que o sistema iniciar operação e gestão dos dados, será realizada a devida comunicação.
Bahia	Informou que não se aplica.
Espírito Santo	Tecnologia em planejamento; todos os dados permanecem em servidores controlados pela SESP. Não se aplica no momento.
Mato Grosso	Tecnologia em análise e testes; nenhuma informação adicional.
Pará	Informou que não houve participação de pessoa jurídica em qualquer etapa da gestão.
Paraná	Testes realizados como Prova de Conceito (PoC); não houve notificação à ANPD, pois foram testes.
Pernambuco	Gestão exclusiva do Centro Integrado de Inteligência de Defesa Social (PE).
Rio de Janeiro	Não houve participação de pessoa jurídica de direito privado em qualquer etapa da gestão.
Rio Grande do Sul	Não há participação de pessoa jurídica de direito privado. A empresa DGT fornece tecnologia, mas não possui acesso aos dados.
Roraima	Explicou abstratamente o artigo 4º, inciso III, §4º da LGPD, sem responder diretamente à pergunta.
São Paulo	Sem sistema implementado; testes realizados sem participação de pessoa jurídica de direito privado na gestão dos estudos.
Tocantins	Gestão do reconhecimento facial exclusiva do Instituto de Identificação do Estado.

Fonte: DPU/DNDH e CESeC

20. Demais informações que considerar relevantes sobre a matéria.

As respostas dos estados em relação às informações adicionais sobre a matéria refletem, em grande parte, a ausência de dados relevantes ou complementares. Alagoas reiterou que o sistema de reconhecimento facial ainda está em fase de desenvolvimento e não está operacional, enquanto Bahia, Rio de Janeiro e Tocantins informaram que não há informações adicionais a serem fornecidas. Pará sequer respondeu à questão, evidenciando a falta de transparência em relação ao tema.

Pernambuco limitou-se a informar disponibilidade para esclarecer dúvidas futuras, sem oferecer detalhes adicionais. Já o Rio Grande do Sul destacou a utilização da plataforma exclusivamente para a localização de pessoas desaparecidas, mas sem fornecer mais detalhes sobre a operação. Por outro lado, Roraima apresentou considerações genéricas sobre o uso do sistema e a gestão de dados pessoais, sem informações concretas e específicas. Essas respostas revelam uma clara lacuna na disponibilização de dados aprofundados ou no detalhamento do funcionamento e do impacto dos sistemas de reconhecimento facial.

cesec

DPU
DEFENSORIA PÚBLICA DA UNIÃO