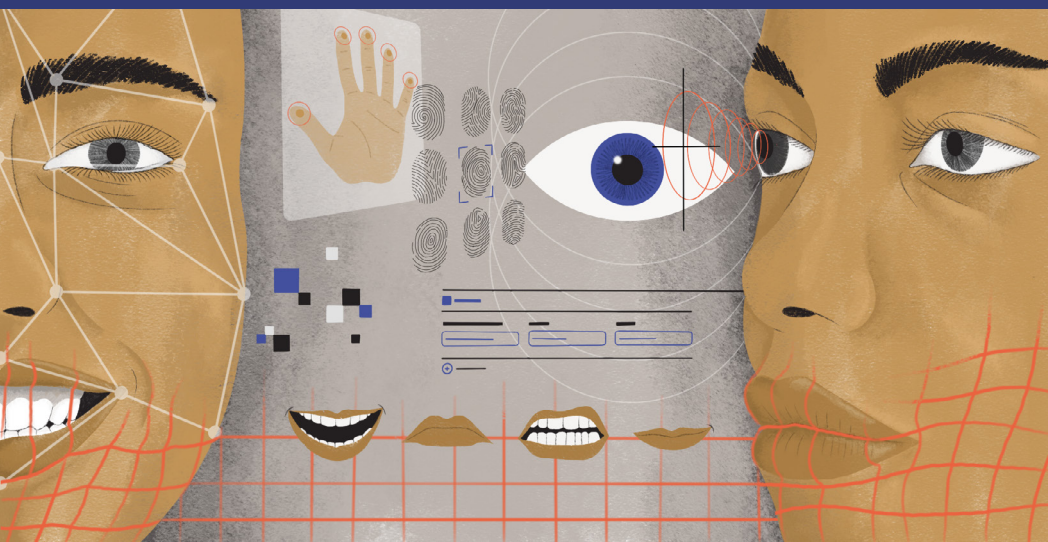




De Olho nos Vigilantes: Combatendo a Propagação do Reconhecimento Facial na Segurança Pública

Princípios para reduzir os danos aos direitos humanos causados por tecnologia de reconhecimento facial



INCLO

Prefácio

Pesquisas e notícias recentes na imprensa brasileira revelam o acelerado processo de aquisição, incorporação e uso de tecnologia de reconhecimento facial na segurança pública no Brasil, sem qualquer regulação. Devido ao uso de dados pessoais e sensíveis, erros de sistema, racismo algorítmico e grande potencial para violar direitos fundamentais dessas ferramentas, tal cenário se mostra alarmante.

Os exemplos e consequências para os direitos humanos são muitos. Em 2024, uma mulher negra foi abordada três vezes pela polícia durante uma festa popular, em Aracaju (SE), após ser reconhecida por tecnologia de reconhecimento facial. Em uma dessas abordagens, ela chegou a urinar nas próprias calças de nervosismo e constrangimento, tendo sido levada pela polícia, apesar de sua inocência.¹ Um soldado do Exército Brasileiro também foi erroneamente identificado como foragido por um desses sistemas. O problema, que teria ocorrido pelo não cumprimento de protocolos, evidencia a ausência de capacitação e reforça o uso problemático pelas polícias.² Já em 2025, um homem negro de 80 anos foi erroneamente reconhecido pelas câmeras de uma Unidade Básica de Saúde (UBS) em São Paulo (SP), confundido com um homem branco acusado pelo crime de estupro; ele foi liberado pela polícia após 10 horas.³ Em uma unidade pública de saúde, uma mulher grávida foi identificada pelo uso de tecnologia de reconhecimento facial. A condução agressiva, segundo relatos da imprensa, levou à antecipação de seu parto.⁴

É a partir do quadro de evidente violação de direitos, pelo reconhecido viés discriminatório dessa tecnologia, a qual, com base em erros de sistema, criminaliza injustamente grupos já vulnerabilizados, que Conectas Direitos Humanos e Instituto da Hora se somam no esforço de tradução e na publicação do relatório “De olho nos Vigilantes: Combatendo a Propagação do Reconhecimento Facial na Segurança Pública” em português (*Eyes on the Watchers: Challenging the Rise of Police Facial Recognition*, no original em inglês) produzido pela International Network of Civil Liberties Organizations (INCLO). A Conectas, organização membro da INCLO desde abril de 2025, considerou fundamental unir-se ao Instituto da Hora nesse trabalho de tradução, pois, além dos motivos elencados acima, o presente relatório traz

1 <https://noticias.uol.com.br/cotidiano/ultimas-noticias/2024/04/28/reconhecimento-facial-erros-falta-de-transparencia.htm>

2 <https://g1.globo.com/rj/rio-de-janeiro/g20/noticia/2024/11/19/soldado-do-exercito-e-presno-no-aterro-flamengo.ghtml>

3 <https://noticias.uol.com.br/cotidiano/ultimas-noticias/2025/04/13/reconhecimento-facial-de-sp-confunde-idoso-com-estuprador-foragido.htm>

4 <https://apublica.org/2025/04/smart-sampa-gravida-e-presa-em-posto-de-saude-e-acaba-tendo-parto-prematuro/>

importantes reflexões para a discussão legislativa em curso no Brasil a respeito do tema. Consideramos que este relatório pode ser fundamental para o debate público.

Terminamos essas palavras iniciais reiterando a defesa, feita neste relatório pelas organizações membros da INCLO, de que a **tecnologia de reconhecimento facial não deve ser utilizada como instrumento na área da segurança pública**. Consideramos que os riscos e potenciais danos relacionados à implementação desses sistemas na área superam quaisquer possíveis benefícios.

CONECTAS DIREITOS HUMANOS



Diretora-executiva: Camila Asano

Diretor de litigância e incidência:
Gabriel Sampaio

Diretora de fortalecimento do movimento de direitos humanos:
Júlia Neiva

Diretor jurídico e financeiro:
Marcos Fuchs

Coordenadora administrativa-financeira:
Fernanda Mito

Coordenadora de enfrentamento à violência institucional: Carolina Diniz

Coordenador de defesa dos direitos socioambientais: João Godoy

Coordenadora de comunicação e engajamento: Morgana Damásio

Conselho deliberativo: Andre Degenszajn, Bruna Benevides, Malak Poppovic, Marcelo Furtado, Natalia Viana, Oscar Vilhena, Renata Reis, Sueli Carneiro, Theo Dias (presidente)

Conselho fiscal: Denise Dora, Heloísa Motoki e Luigi Puntel

Associados e associadas: Anamaria Schindler, Andre Degenszajn, Bruna Benevides, Denise Dora, Douglas Belchior, Flavia Regina de Souza, Hélio Menezes, Heloisa Motoki, Luigi Puntel, Malak Poppovic, Margarida Genevois, Marcelo Furtado, Natalia Viana, Oscar Vilhena, Renata Reis, Sueli Carneiro, Theo Dias.

INSTITUTO DA HORA



Diretora Executiva e Fundadora:
Nina da Hora

Gerente de Projetos: Maria Luiza

Coordenadora de Pesquisa: Letícia Hora
Gestão Administrativa: Elis Lages

Produção: Tradução por Naiade Rufino. Revisão por Julia Neiva, Carla Vreche, Susana Barbery, Marina Rongo, Camila Sabino, Nina da Hora, Maria Luiza, Letícia Hora e Elis Lages.

Índice

Agradecimentos	5
Introdução.....	6
O que é TRF?.....	9
Tipos de TRF	18
TRF na segurança pública: direitos, riscos e danos.....	21
Avaliando o impacto do uso policial de tecnologias de reconhecimento facial sobre os direitos humanos	33
Princípios da INCLO sobre o uso de TRF na aplicação da lei	54
Como usar estes princípios	69
Considerações finais.....	71

Agradecimentos

Este projeto foi desenvolvido, redigido e editado por Olga Cronin (INCLO/ICCL), Víctor Práxedes Saavedra Rionda (INCLO), Elizabeth Farries (University College Dublin Centre for Digital Policy), Kirill Koroteev (INCLO/Agora) e Timilehin Ojo (INCLO/CCLA).

Estes princípios foram elaborados após a reunião anual da International Network of Civil Liberties Organizations (INCLO) de 2023, quando a carência generalizada de conhecimento técnico e jurídico acerca do uso da tecnologia de reconhecimento facial (TRF) na segurança pública foi reconhecida como uma preocupação urgente nas jurisdições de todos os nossos membros e membras. Ao longo de 2023 e 2024, especialistas em direitos humanos das áreas de Direito, Tecnologia, Sociologia e Comunicação, dos 15 países da INCLO, à época, reuniram-se para desenvolver o presente rol de princípios.

Este é um esforço colaborativo das mais de 15 organizações que integravam a INCLO nesse período. Por toda a contribuição para o desenvolvimento, estudo de caso, redação, edição e pesquisa, a INCLO expressa os seus mais sinceros agradecimentos a: Lucila Santos, Myriam Selhi (INCLO), Vanessa Lopez (Dejusticia), Sherylle Dass (LRC), Devon Turner (LRC), Manuel Tufró (CELS), Ben Wizner (ACLU), Kieran Pender (HRLC), David Mejia-Canales (HRLC), Martin Mavenjina (KHRC), Gil Gan-Mor (ACRI), Anaïs Bussièrès McNicoll (CCLA), Karim Medhat Ennarrah (EIPR), Sehba Meenai (HRLN), Remport Ádám (TASZ), Nadine Sherani (KontraS), Emmanuelle Andrews (Liberty), Nathan Freed Wessler (ACLU), Jun Pang (Liberty), Daniel Konikoff (CCLA) e Daniel Ospina Celis (Dejusticia).

A INCLO agradece ainda a Taryn McKay pelo design, a Sam Kelly pela edição e a Alina Najlis pelas ilustrações.

Introdução

Este projeto da International Network of Civil Liberties Organizations se concentra no emprego da tecnologia de reconhecimento facial pelas forças de segurança.

Nosso projeto foi construído a partir do relatório da INCLO de 2021, chamado *In Focus: Facial Recognition Stories and Rights Harms From Around the World* (*Em Foco: Histórias de Reconhecimento Facial e Danos aos Direitos ao Redor do Mundo*, tradução literal)¹. Esse relatório é um compilado de histórias que demonstram os efeitos prejudiciais e emergentes da TRF, a qual pode ser utilizada para mapear, analisar e tentar estabelecer a identidade de um rosto em uma fotografia ou vídeo, dando à pessoa que está utilizando o sistema a capacidade de rastrear ou vigiar outro alguém em tempo real ou em caráter retrospectivo, sem seu conhecimento ou consentimento². Ele descreveu ainda como a TRF, uma tecnologia robusta, porém falha, afeta direitos e o cotidiano de pessoas em 13 países das Américas, África, Europa, Ásia e na Austrália. O relatório examinou os riscos impostos por essa tecnologia ao permitir uma vigilância que pode rastrear indivíduos durante protestos, eventos religiosos, visitas médicas e atividades cotidianas, bem como analisou como a TRF pode gerar a identificação incorreta de pessoas – especialmente não brancas – por crimes que elas não cometeram. Nosso relatório fez uma forte defesa em favor de um debate aberto, público e democrático sobre o uso de tais sistemas.

Três anos depois, o emprego dessa tecnologia transformadora está cada vez mais normalizado e universal. Estima-se que o patamar atual de US\$ 5 bilhões do setor de TRF chegue à marca de US\$ 50 bilhões até 2030³. Em todo mundo, um número

1 *In Focus: Facial Recognition Tech Stories And Rights Harms From Around The World*, International Network of Civil Liberties Organizations, 2021, <https://inclo.net/publications/in-focus-facial-recognition-tech-stories-and-rights-harms-from-around-the-world/>.

2 Akbari, A, “Facial Recognition Technologies 101: Technical Insights” em *The Cambridge Handbook of Facial Recognition in the Modern State*, Cambridge University Press, 2024, pp. 29–43, <https://www.cambridge.org/core/books/cambridge-handbook-of-facial-recognition-in-the-modern-state/facial-recognition-technologies-101/8B3039F97B11F43B78E52BBEB73E8479>.

3 Matulionyte R & Zalnieriute M, “Facial Recognition Technology in Context: Technical and Legal Challenges” em *The Cambridge Handbook of Facial Recognition in the Modern State*, Cambridge University Press, 2024, <https://www.cambridge.org/core/books/cambridge-handbook-of-facial-recognition-in-the-modern-state/facial-recognition-technology-in-context/A4F5E2C52EF9CFD27E8F04D0DD60074D.org/core/books/cambridge-handbook-of-facial-recognition-in-the-modern-state/facial-recognition-technology-in-context/A4F5E2C52EF9CFD27E8F04D0DD60074D>.

cada vez maior de agentes das esferas estatal e privada⁴ está se movimentando para introduzir⁵ ou expandir⁶ seu uso. E, uma vez que leis que versam sobre o uso da TRF vêm sendo aprovadas com proteções inadequadas aos direitos fundamentais⁷, tribunais são cada vez mais responsáveis por entender e julgar os riscos.⁸ É nesse contexto que nós voltamos a abordar esse assunto com urgência.

Aqui, repetimos nosso apelo por uma completa reavaliação e reconsideração do emprego da tecnologia de reconhecimento facial na aplicação da lei. Esse apelo é acentuado por seu possível uso indevido, pela crescente interconexão dos sistemas de vigilância estatais e seu impacto contínuo sobre liberdades individuais. Dada a crescente implementação dessas tecnologias nos países das organizações-membras da INCLO, retomamos o assunto, desenvolvendo um rol de princípios fundamentados em nossa explicação já documentada sobre a tecnologia, suas aplicações, danos e riscos, juntamente com padrões de direitos humanos e uma análise jurídica.

Nossos princípios se concentram no uso da TRF pelas forças de segurança para fins de identificação; eles fornecem uma base para a compreensão dos riscos dessa tecnologia e servem como uma ferramenta de avaliação e *advocacy*. Acreditamos que eles sejam valiosos para a sociedade civil, as pessoas que formulam políticas públicas e leis, o público, a mídia, os tribunais e forças de segurança pública.

Uma vez que, hoje, os riscos da TRF no contexto das práticas policiais não contam com salvaguardas previstas em lei e a tecnologia não pode ser implementada com

4 Lyons, J, *NFL to begin using face scanning tech across all of its stadiums*, The Register, 2 de agosto de 2024, https://www.theregister.com/2024/08/06/nfl_face_scanning_tech/. Veja também Baker, T, *Home Office eyeing expansion of “Orwellian” facial recognition*, Sky News, 30 de agosto de 2023, <https://news.sky.com/story/facial-recognition-technology-labelled-orwellian-as-government-eyes-wider-use-by-police-and-security-agencies-12950942>.

5 Desmarais, A, *Ireland’s new police facial recognition bill has “fundamental defects,” experts say*, Euronews, 1º de março de 2024, <https://www.euronews.com/next/2024/03/01/irish-police-facial-recognition-bill-has-fundamental-defects-experts-say#:~:text=The%20Irish%20Parliament%20passed%20the,to%20this%20law%20in%20December>.

6 Sabbagh, D, “Starmer’s live facial recognition plan would usher in national ID, campaigners say”, *The Guardian*, 2 de agosto de 2024, <https://www.theguardian.com/technology/article/2024/aug/02/starmer-live-facial-recognition-plan-would-usher-in-national-id-campaigners-warn>.

7 Volpicelli, G, *EU set to allow draconian use of facial recognition tech, say lawmakers*, Politico, 16 de janeiro de 2024, <https://www.politico.eu/article/eu-ai-facial-recognition-tech-act-late-tweaks-attack-civil-rights-key-lawmaker-hahn-warns/>.

8 *Glukhin v Russia*, App. No(s),11519/20, <https://hudoc.echr.coe.int/eng?i=001-225655>; veja também *New Jersey Appellate Division One of First Courts in Country to Rule on Constitutional Rights Related to FRTs*, ACLU, junho de 2023, <https://www.aclu-nj.org/en/press-releases/new-jersey-appellate-division-one-first-courts-country-rule-constitutional-rights>.

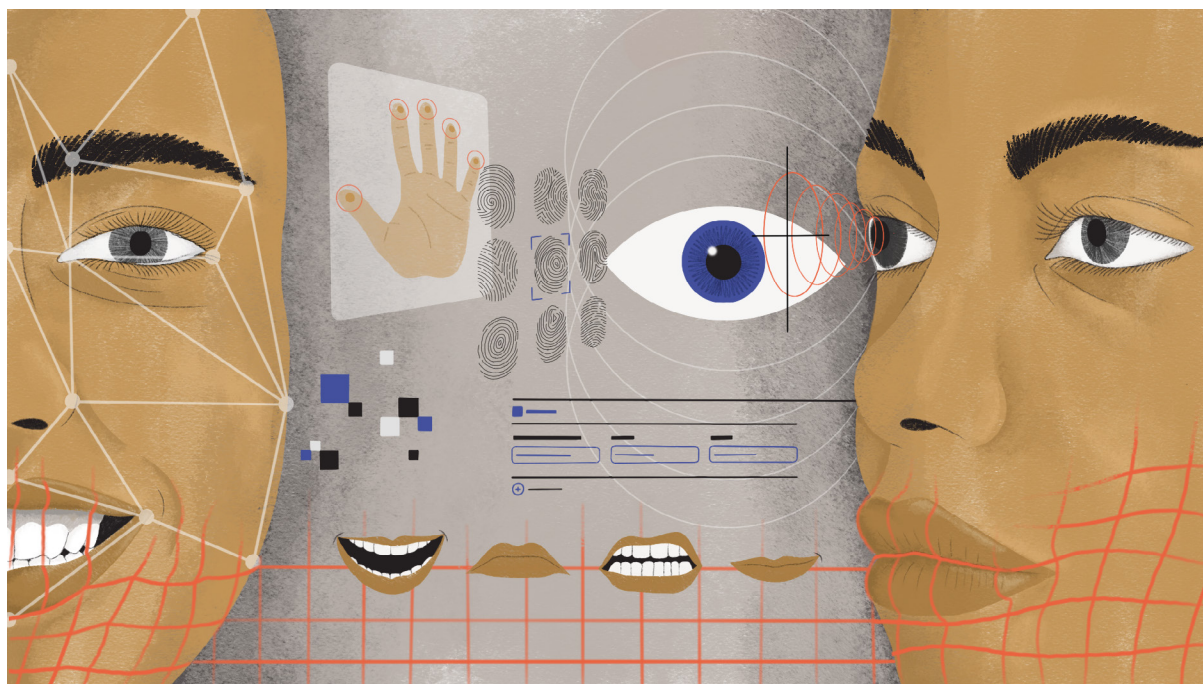
segurança, o uso policial da TRF deve ser banido. Nossos princípios não promovem o uso da TRF na segurança pública, mas mapeiam padrões mínimos existentes de responsabilização e mitigação de danos. Eles servem como uma ferramenta para formar um consenso sobre os problemas significativos apresentados por essa tecnologia e a necessidade de restrições e proibições significativas.

Defendemos a adoção de normas ainda mais rígidas e consoantes às circunstâncias específicas de cada jurisdição, com o objetivo de garantir a proteção dos direitos humanos e a integridade das práticas de execução da lei.

Sobre a INCLO

A INCLO é uma rede de 17 organizações nacionais independentes de direitos humanos e civis que trabalham para a promoção de direitos e liberdades fundamentais. Nós apoiamos e reforçamos o trabalho das organizações-membras em seus respectivos países e promovemos colaborações bilaterais e multilaterais dentro da rede. A INCLO é composta por entidades de direitos humanos com múltiplos temas e públicos, que têm foco nacional e são independentes de seus governos. Elas defendem os direitos de todas as pessoas em seu território nacional, combinando práticas de litígio, incidência legislativa e de base e educação pública.

As 17 organizações que integram a INCLO são: American Civil Liberties Union (ACLU); Al-Haq, na Palestina; Association for Civil Rights, em Israel (ACRI); Canadian Civil Liberties Association (CCLA); Centro de Estudios Legales y Sociales (CELS), na Argentina; Conectas, no Brasil; Dejusticia, na Colômbia; Egyptian Initiative for Personal Rights (EIPR); Human Rights Law Network (HRLN), na Índia; Human Rights Law Centre (HRLC), na Austrália; Hungarian Civil Liberties Union (HCLU); International Human Rights Group Agora (Agora), na Rússia; Irish Council for Civil Liberties (ICCL); Kenya Human Rights Commission (KHRC); KontraS, na Indonésia; Legal Resources Centre (LRC), na África do Sul; e Liberty, no Reino Unido.



Ilustrações de Alina Najlis - © 2024 INCLO

O que é TRF?

A TRF é uma ferramenta que aplica técnicas de inteligência artificial⁹ e biométrica¹⁰ e que é utilizada pelas forças de segurança para tentar identificar ou caracterizar uma pessoa com base em seus traços faciais.¹¹ Nossos princípios se referem aos sistemas que empregam essa tecnologia como conjuntos organizados e estruturados de softwares, hardwares, procedimentos, conjuntos de dados (*dataset*, no original em inglês) e recursos humanos inter-relacionados, implantados – ou seja, configurados e implementados – como uma unidade. Em outras palavras, embora o componente principal do software envolva a detecção

9 Para os fins deste projeto, nos referimos à definição de “sistema de inteligência artificial” nos termos do Artigo 3º (1) da Lei de Inteligência Artificial da União Europeia: “Sistemas de IA”, significa um sistema baseado em máquinas concebido para funcionar com níveis de autonomia variáveis, e que pode apresentar capacidade de adaptação após a implantação e que, para objetivos explícitos ou implícitos, e com base nos dados de entrada que recebe, infere a forma de gerar resultados, tais como previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais”, em conjunto com o Considerando 12 da Lei, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202401689.

10 “Biometria” refere-se à medição de características físicas ou de comportamento pessoal. Sob a premissa de que tais características são únicas e, portanto, passíveis de serem utilizadas para identificar uma pessoa, a biometria refere-se, no campo da Ciência da Computação, à área relacionada à autenticação da identidade por meio da execução automática dessas medições e cálculos. Alguns exemplos de partes do corpo usadas para esse propósito são o rosto, as impressões digitais, o DNA ou a íris.

11 Para obter mais informações sobre a história e o desenvolvimento do reconhecimento facial, veja Raviv, S, *The Secret History of Facial Recognition*, Wired, 21 de janeiro de 2020, <https://www.wired.com/story/secret-history-facial-recognition/>.

de uma imagem facial e a tentativa de identificá-la, ele funciona dentro de uma estrutura e em conjunto com outros hardwares e softwares operados por humanos que interpretam os resultados produzidos.

Para que a TRF é utilizada?

Listaremos a seguir alguns dos principais usos do reconhecimento facial¹²:



VERIFICAÇÃO

O objetivo da verificação baseada em TRF é confirmar a identidade de uma pessoa por meio da comparação de uma única imagem capturada em um momento com uma única imagem armazenada. Por esse motivo, essa verificação também pode ser chamada de “correspondência um a um” (*one-to-one matching*, no original em

¹² Veja Buolamwini, J et al., *Facial Recognition Technologies: A Primer*, maio de 2020, <https://people.cs.umass.edu/~elm/papers/FRTprimer.pdf>.

inglês) ou “comparação um a um” (*one-to-one comparison*, no original em inglês). Exemplos disso incluem uma pessoa que tenta desbloquear o próprio smartphone com o seu rosto ou quando a fotografia de alguém tirada em um posto de controle de um aeroporto é comparada com a de seu passaporte.

IDENTIFICAÇÃO

O objetivo da identificação baseada em TRF é determinar a identidade de uma pessoa desconhecida, cujo rosto está capturado em uma foto ou vídeo, por meio da comparação da imagem dela com um banco de dados de referência de imagens de pessoas conhecidas. Tal processo também pode ser designado como “identificação de um para muitos” (*one-to-many identification*, no original em inglês). Esse é o uso tradicional dos sistemas de vigilância baseados em tecnologia de reconhecimento facial, os quais constituem o objeto destes princípios. Alguns exemplos incluem a tentativa da polícia em identificar alguém mediante a comparação entre a imagem de uma pessoa extraída de um circuito fechado de televisão (CFTV) pausado ou das mídias sociais e banco de dados de carteiras de motorista, registros eleitorais ou passaportes, ou mediante a comparação da imagem capturada no CFTV, em tempo real ou ao vivo, com uma lista de vigilância de indivíduos conhecidos.

CLASSIFICAÇÃO, MEDIÇÃO E DETECÇÃO DE CARACTERÍSTICAS FACIAIS

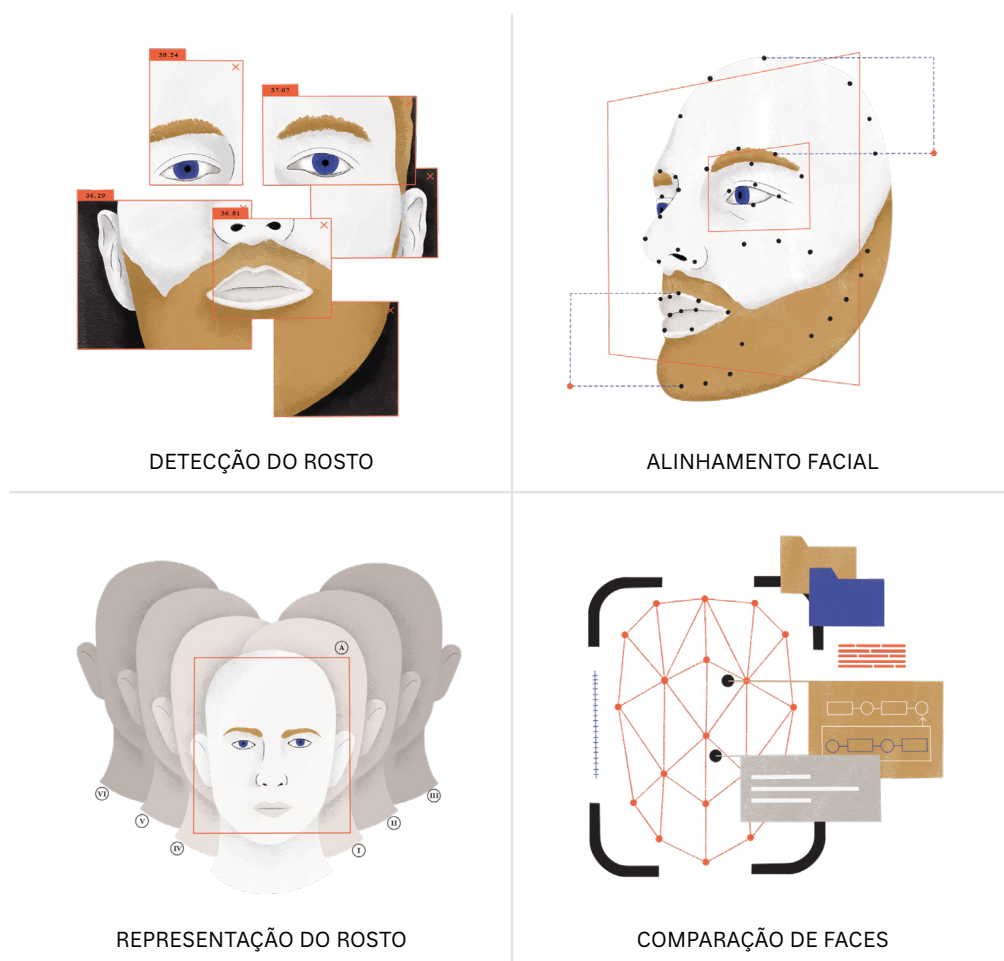
O objetivo da classificação das características faciais é obter informações sobre os traços que, posteriormente, são utilizados em uma tentativa de medição (para, por exemplo, estimar a idade) ou de categorização (para, por exemplo, identificar o gênero). Ela também pode envolver a verificação da presença ou ausência de certos elementos (detectando, por exemplo, se alguém está com óculos). Um exemplo desse uso é a categorização de um grande número de pessoas em agrupamentos menores para fins de marketing¹³, uma prática que levanta sérias preocupações sobre perfilamento, privacidade e proteção de dados pessoais.

RECONHECIMENTO DE EMOÇÕES FACIAIS

O objetivo do reconhecimento de emoções faciais é tentar inferir os sentimentos ou as emoções de alguém com base em suas expressões faciais. Por exemplo,

13 Kuligowski, K, *Facial Recognition Advertising: The New Way to Target Ads to Customers*, Business News Daily, 20 de outubro de 2023, <https://www.businessnewsdaily.com/15213-walgreens-facial-recognition.html>.

a gigante varejista estadunidense *Walmart* já fez uso de reconhecimento facial para tentar identificar a insatisfação de clientes.¹⁴ A precisão e o embasamento científico¹⁵ desse uso “pseudocientífico”¹⁶, extremamente controverso, são altamente contestados.¹⁷



14 Peterson, H, *Walmart is developing a robot that identifies unhappy shoppers*, Business Insider, 19 de julho de 2017, <https://www.businessinsider.com/walmart-is-developing-a-robot-that-identifies-unhappy-shoppers-2017-7>.

15 Stanley, J, *Experts Say “Emotion Recognition” Lacks Scientific Foundation*, American Civil Liberties Union, 18 de julho de 2019, <https://www.aclu.org/news/privacy-technology/experts-say-emotion-recognition-lacks-scientific> e Romero, A, *AI Emotion Recognition is a Pseudoscientific Multi-billion Dollar Industry*, The Algorithmic Bridge, 12 de julho de 2022, <https://www.thealgorithmicbridge.com/p/ai-emotion-recognition-is-a-pseudoscientific>.

16 Hern, A, “Information commissioner warns firms over ‘emotional analysis’ technologies”, The Guardian, 25 outubro 2022, <https://www.theguardian.com/technology/2022/oct/25/information-commissioner-warns-firms-over-emotional-analysis-technologies>.

17 Barrett, LF, Adolphs, R, Marsella, S, Martinez, AM & Pollak, SD (2019), “Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements”, *Psychological Science in the Public Interest*, 20(1), 1–68. <https://doi.org/10.1177/1529100619832930>.

Notas técnicas complementares a estes princípios

De modo geral, o emprego da TRF compreende as etapas abaixo. Entretanto, deve-se observar que essa é uma versão simplificada de um processo bastante complexo e de uma sequência de ações que englobam diversos fatores:¹⁸

ETAPAS DO RECONHECIMENTO FACIAL

1. **DETECÇÃO DO ROSTO:** Localização de um ou mais rostos em uma imagem ou vídeo e, se houver, retorno das coordenadas das caixas que delimitam cada um deles.
2. **ALINHAMENTO FACIAL:** Modificação dos dados do rosto (como dimensionamento ou corte), com base nos seus elementos geométricos, adaptando a uma forma canônica a fim de permitir a sua comparação com um banco de dados ou lista de vigilância de imagens faciais.
3. **REPRESENTAÇÃO DO ROSTO:** Transformação dos pixels da imagem em dados úteis à comparação computacional. Podem consistir em um conjunto de modelos ou, dependendo da técnica, de características ou formatos.
4. **COMPARAÇÃO DE FACES:** Comparação de dados obtidos na etapa anterior com o banco de referência para avaliar, com uma pontuação de probabilidade, a verificação, a identificação ou a categorização do rosto.

Imagem de consulta

A imagem facial não identificada de um indivíduo específico que a polícia deseja identificar geralmente é designada como “imagem de consulta”. Essas imagens podem variar amplamente em termos de ângulo, formato, qualidade e pixelização. Tal variabilidade pode resultar em uma série de problemas.

18 Sáez Trigueros, D, Meng, L & Hartnett, M, *Face Recognition: From Traditional to Deep Learning Methods*, 2018, <https://arxiv.org/pdf/1811.00116>.

O ponto principal pautado aqui é que, na verdade, as imagens faciais são extraídas de diversas fontes distintas e envolvem, no mínimo, pessoas em poses diferentes, imagens capturadas em condições de iluminação muito díspares e rostos obscurecidos em graus variados devido à posição da câmera, às roupas ou ao uso de óculos de sol etc.

FATORES QUE PODEM AFETAR AS IMAGENS DE CONSULTA:

1. **POSE:** A posição do rosto na imagem de consulta afeta a tentativa do processo de comparação.
2. **ILUMINAÇÃO:** iluminação do ambiente pode afetar os padrões de textura detectados em um rosto, incluindo a possibilidade de destacar ou minimizar certos traços ou alterar o formato do rosto.
3. **EXPRESSÃO:** Além de afetar, principalmente, o reconhecimento de emoções faciais, a configuração do grande grupo muscular de nossos rostos também pode afetar as etapas de identificação e verificação.
4. **OCULTAÇÃO:** O uso de acessórios ou outras formas de cobrir parte do rosto, como roupas, máscaras ou mãos, pode resultar na indisponibilidade de parte das informações faciais para fins de reconhecimento facial. Isso também pode afetar as informações que podem ser capturadas, alterando, por exemplo, a simetria do rosto.
5. **ROSTOS IMPRECISAMENTE LOCALIZADOS:** Enquanto os fatores acima se referem ao ambiente em que uma pessoa se encontra, este aponta para as falhas dos sistemas durante a detecção facial ou a delimitação das características faciais em uma foto ou vídeo, o que dificulta determinar onde um rosto ou traço começa ou termina.

Conjunto de dados de treinamento

Além das imagens de consulta e de banco de dados (*databases*, no original em inglês), há um terceiro conjunto que precisa ser ponderado por estes princípios: o conjunto de dados, que consiste na coleção de imagens inseridas no sistema durante a fase de treinamento, antes da implementação e uso do sistema na segurança pública. Essa fase de treinamento tem o objetivo de ensinar o sistema a reconhecer padrões (neste caso, traços faciais) com base em milhares de imagens de rostos. Essa etapa também se propõe a aumentar a robustez do sistema para suplantar as condições desafiadoras, mencionadas acima, que podem afetar a sua confiabilidade, tais como imagens com rostos parcialmente cobertos ou obscurecidos.

É fundamental compreender o processo de treinamento, bem como os conjuntos de dados nele envolvidos, para conseguir assimilar a origem de alguns danos associados aos sistemas de TRF. A própria natureza dos conjuntos de dados de treinamento pode ser a fonte do viés refletido pelas TRF¹⁹ devido às seguintes causas:

VIESES DOS CONJUNTOS DE DADOS

- *Viés de captura:* Relacionado à origem das fotos. Influenciado tanto pelo dispositivo utilizado quanto pelas preferências de quem coleta, e está relacionado a fatores que afetam a confiabilidade, mencionados anteriormente, como a iluminação ou a posição do rosto.
- *Viés de categoria ou rotulagem:* Relacionado à ambiguidade e imprecisão na semântica visual, resultando tanto do fato de imagens semelhantes serem colocadas em categorias diferentes quanto, por outro lado, de imagens distintas serem agrupadas na mesma categoria.
- *Viés negativo:* Relacionado à parte da informação visual deixada de lado do conjunto de dados devido ao foco em características específicas.

19 Tommasi, T, Patricia, N, Caputo, B & Tuytelaars, T (2015). *A Deeper Look at Dataset Bias*. ArXiv, abs/1505.01257.: <https://arxiv.org/ftp/arxiv/papers/1505/1505.01257.pdf>.

FUNCIONAMENTO NA VIDA REAL²⁰

Os sistemas de reconhecimento facial operam em cenários da vida real e não refletem as condições de um ambiente controlado. Falhas nos conjuntos de dados, nos bancos de referência/listas de vigilância e nas imagens de consulta resultam em uma precisão limitada, podendo gerar graves violações de direitos fundamentais. **Os índices de precisão apresentados pelos fornecedores desses sistemas e por quem defende a TRF costumam estar embasados em condições** impecáveis de um ambiente controlado, que envolvem a comparação de imagens nítidas e de alta qualidade com iluminação perfeita, nas quais rostos foram capturados de forma ideal – como em fotos para pedidos de visto e fichas criminais – e comparados com outras imagens nítidas, de alta qualidade e controladas. Entretanto, esses apoiadores e apoiadoras não mencionam as seguintes deficiências:

- Formação técnica limitada das forças de segurança pública na qualidade de usuários finais:

Assim como ocorre com outras tecnologias digitais – e mais ainda com as ferramentas baseadas em inteligência artificial –, é fundamental compreender minuciosamente como um sistema funciona, incluindo suas falhas e limitações, para mitigar riscos e danos. Ao considerar sua implantação, o treinamento e os procedimentos constituem os elementos centrais do sistema.

- Métricas e indicadores de desempenho distorcidos:

Como ferramentas contestadas, esses sistemas serão acompanhados por métricas e números na tentativa de legitimar seu uso, seja por forças policiais ou fornecedores dos sistemas. Tais números e métricas devem ser fortemente questionados e confrontados pelo público, pela mídia e sociedade civil, levando em consideração ao menos duas questões: 1) algumas métricas e dados podem ser resultado de testes realizados em cenários ideais ou de ambiente controlado, e não em contextos da vida real; e, 2) algumas métricas e números podem se referir a um caso específico de uso de TRF, o que pode não ser relevante ou representativo para o caso de

20 Veja Akbari, A, “Facial Recognition Technologies 101. Technical insights” em *The Cambridge Handbook of Facial Recognition in the Modern State*, março de 2024, https://www.cambridge.org/core/services/aop-cambridge-core/content/view/8B3039F97B11F43B78E52BBEB73E8479/9781009321198c3_29-43.pdf/facial_recognition_technologies_101.pdf.

uso proposto que está sendo considerado por uma força policial ou por um Estado ao legislar sobre o uso da TRF.

Em nome da democracia e da transparência, pessoas com cidadania ou residência em um país devem saber quais instrumentos são utilizados para monitorá-las. Para ferramentas tecnológicas extremamente controversas, como a TRF, deve haver escrutínio público sobre como são medidas as suas taxas de acurácia e as condições em que ela é testada.

- Multiplicidade de atores gera uma cadeia de falhas cumulativas:

Diferentes atores participam do desenvolvimento e na implantação de sistemas de reconhecimento facial, o que pode afetar o seu desempenho final. Alguns deles, como acadêmicos que desenvolvem um algoritmo, podem não estar cientes do uso que será feito da tecnologia.

Há ainda aqueles que podem não ter o interesse público como prioridade. A título de exemplo, corretoras de dados (cujo negócio consiste em coletar dados pessoais para vendê-los a, ou seu uso por, terceiros) podem fornecer conjuntos de dados de treinamento, um fornecedor de tecnologia pode implementar um algoritmo em uma ferramenta comercial ou um contratante oferecer uma “solução integral” (que inclui partes adquiridas de terceiros).

Por fim, pessoas formuladoras de políticas que podem desempenhar um papel no design de um sistema, controladoras de dados responsáveis pelos bancos de dados de imagens utilizadas e as responsáveis pela segurança pública, usuárias finais dos sistemas, também constituem exemplos de pessoas humanas envolvidas no desenvolvimento e na implantação de sistemas de reconhecimento facial. Elas podem carecer de capacitação técnica para compreender as implicações do que estão tentando regular.

Ter uma compreensão profunda acerca da diversidade de atores envolvidos no desenvolvimento e na implantação dos sistemas de reconhecimento facial, desde a sua criação até seu uso, é de grande importância para compreender por que o uso dessa tecnologia pela polícia é tão problemático para a proteção dos direitos fundamentais. Esse conhecimento também é valioso para entender melhor onde e por qual motivo surgem questões relacionadas à transparência e à precisão.



Tipos de TRF

Para fins destes princípios, usamos as seguintes definições:

1. Reconhecimento facial em tempo real ou ao vivo:
 - a. O reconhecimento facial em tempo real ou ao vivo envolve a comparação de uma transmissão de vídeo ao vivo de rostos captada por uma câmera com uma lista de vigilância predeterminada. O objetivo é encontrar uma possível correspondência que gere um alerta para a polícia ou para a pessoa usuária. Tais sistemas envolvem a captura de dados biométricos faciais por meio de uma transmissão de vídeo em tempo real, a comparação com uma lista de vigilância e uma possível identificação, sendo que tudo isso ocorre instantaneamente, ou de forma quase instantânea ou sem um atraso significativo. Exemplos:
 - i. O uso da TRF em tempo real pela Polícia Metropolitana de Londres, no Reino Unido.²¹

21 Metropolitan Police Service live facial recognition policy document, <https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/policy-documents/lfr-policy-document2.pdf>.

- ii. O uso da TRF em tempo real pela rede varejista estadunidense Rite Aid.²²
- iii. O uso da TRF em tempo real pelas autoridades em Moscou, Rússia.²³

2. Identificação biométrica facial remota retrospectiva:

- a. O reconhecimento facial retrospectivo envolve a comparação de imagens de rostos desconhecidos com um banco de dados de referência, que contém imagens de pessoas conhecidas, a fim de tentar estabelecer sua identificação. Para cada busca, o sistema retorna uma lista de possíveis correspondências, as quais são acompanhadas da pontuação de similaridade. Não há garantia de que a pessoa cuja identidade está sendo procurada estará no banco de dados de referência ou que, se a “verdadeira correspondência” estiver nele, ela receberá a pontuação de similaridade mais alta na lista. Também não há garantia de que a pessoa que conduz a busca na TRF selecione corretamente a correspondência verdadeira, mesmo que ela esteja na lista de resultados. Exemplos:
 - i. Uso da TRF para rastrear um manifestante em Moscou.²⁴
 - ii. Uso da TRF que suscitou a identificação incorreta e prisões indevidas de Robert Williams,²⁵ Michael Oliver,²⁶ Nijer Parks,²⁷

22 Bhuiyan R, “Rite Aid facial recognition misidentified Black, Latino and Asian people as ‘likely’ shoplifters”, *The Guardian*, 20 de dezembro de 2023, <https://www.theguardian.com/technology/2023/dec/20/rite-aid-shoplifting-facial-recognition-ftc-settlement>.

23 Vincent, J, *Moscow rolls out live facial recognition system with an app to alert police*, The Verge, 30 de janeiro de 2020, <https://www.theverge.com/2020/1/30/21115119/moscow-live-facial-recognition-roll-out-ntechlab-deployment>.

24 *Glukhin v Russia*, App. No(s), 11519/20, <https://hudoc.echr.coe.int/eng?i=001-225655>

25 Williams, R, *I Did Nothing Wrong. I Was Arrested Anyway*, American Civil Liberties Union, 15 de julho de 2021, <https://www.aclu.org/news/privacy-technology/i-did-nothing-wrong-i-was-arrested-anyway>.

26 Stokes, E, *Wrongful arrest exposes racial bias in facial recognition technology*, CBS News, novembro de 2020, <https://www.cbsnews.com/news/detroit-facial-recognition-surveillance-camera-racial-bias-crime/>.

27 Bryan, K et al., “Government Users of Facial Recognition Software Sued by Plaintiff Alleging Wrongful Imprisonment Over Case of Mistaken Identity”, *The National Law Review*, janeiro de 2021, <https://natlawreview.com/article/government-users-facial-recognition-software-sued-plaintiff-alleging-wrongful>.

Randal Reid,²⁸ Alonzo Sawyer,²⁹ Porcha Woodruff³⁰ e Harvey Eugene Murphy Jr³¹, nos Estados Unidos.

iii. Uso da TRF na Argentina, quando Guillermo Ibarrola foi incorretamente identificado e erroneamente preso, detido e acusado de praticar assalto à mão armada em uma cidade onde ele nunca esteve, a 600km de sua cidade natal, Buenos Aires.³²

3. Sistema de identificação biométrica facial iniciado por pessoa operadora:

- a. O reconhecimento facial iniciado por pessoa operadora é um uso quase em tempo real da TRF, no qual uma autoridade policial utiliza um dispositivo móvel para tirar foto de alguém e realiza uma busca imediata em um banco de dados de referência de imagens. De forma semelhante à TRF retrospectiva, cada uma dessas buscas retornará uma lista de possíveis correspondências acompanhadas por uma pontuação de similaridade. Exemplos:
 - i. Uso do sistema de reconhecimento facial Blue Wolf contra palestinos pelas autoridades israelenses.³³
 - ii. Uso da TRF iniciada por pessoa operadora pela polícia de Gales do Sul.³⁴

28 Hill, K & Mac, R, “Thousands of Dollars for Something I Didn’t Do”, *The New York Times*, 31 de março de 2023, <https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html>.

29 Johnson, K, *Face Recognition Software Led to His Arrest. It Was Dead Wrong*, *Wired*, 28 de fevereiro de 2023, <https://www.wired.com/story/face-recognition-software-led-to-his-arrest-it-was-dead-wrong/>.

30 Hill, K, “Eight months pregnant and arrested after false facial recognition match”, *The New York Times*, 6 de agosto de 2023, <https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html>.

31 Robledo, A, “Texas man says facial recognition led to his false arrest, imprisonment, rape in jail”, *USA Today*, 24 de janeiro de 2024, <https://eu.usatoday.com/story/news/nation/2024/01/24/sunglass-hut-robbery-facial-recognition-arrest/72343044007/>.

32 Naundorf, K, *The Twisted Eye in the Sky Over Buenos Aires*, *Wired*, 13 de setembro de 2023, <https://www.wired.com/story/buenos-aires-facial-recognition-scandal/>.

33 Robins-Early, N, “How Israel uses facial-recognition systems in Gaza and beyond”, *The Guardian*, 19 de abril de 2024, <https://www.theguardian.com/technology/2024/apr/19/idf-facial-recognition-surveillance-palestinians>.

34 Facial Recognition Technology, South Wales Police, <https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/>.



TRF na segurança pública: direitos, riscos e danos

Impacto real e provável aos direitos humanos

Decidir se uma força de segurança pública deve utilizar um sistema de TRF com base em sua alegada “precisão” denota, consciente ou inconscientemente, uma má interpretação sobre a complexidade contextual dessa tecnologia biométrica e de suas prováveis e profundas implicações aos direitos humanos fundamentais.

Mesmo se todos os sistemas de TRF destinados à segurança pública fossem precisos 100% do tempo, os riscos aos direitos humanos fundamentais se multiplicariam significativamente. Os sistemas de TRF podem privar as pessoas de seu anonimato, reduzindo-as a placas veiculares ambulantes³⁵ e, ainda mais, reforçar a dinâmica de poder inerente às interações polícia-população em direção à polícia.

35 Orientações 05/2022 sobre a utilização da tecnologia de reconhecimento facial no domínio da aplicação da Lei, European Data Protection Board, documento aprovado em 26 de abril de 2023, p.15, https://www.edpb.europa.eu/system/files/2024-05/edpb_guidelines_202304_frtlawenforcement_v2_pt.pdf.

A fim de assegurar que essa poderosa tecnologia de vigilância não seja usada de modo indevido, abusivo ou banalizado, deve-se levar em consideração toda a vida útil de um sistema de TRF, sua conexão com outros sistemas de vigilância, o uso, armazenamento e destruição de identificadores biométricos faciais e as salvaguardas técnicas e organizacionais em vigor (ou não) para eles, quando se contempla os prováveis riscos aos direitos humanos associados à TRF.

Em defesa da democracia e do direito a um julgamento justo, é essencial que saibamos quais ferramentas podem levar alguém a ser alvo de prisão ou à imputação de um crime. Assim, também é preciso considerar os mecanismos de transparência e supervisão de cada componente da tecnologia e etapa no uso da TRF pelas polícias, a independência e a eficácia – ou a ausência delas – desses mecanismos, e a questão de como responsabilizar os sistemas de TRF – em constante mudança – utilizados pelas forças de segurança, assim como as pessoas envolvidoras, fabricantes e usuárias desses sistemas.

Mesmo se todos os sistemas de TRF destinados à segurança pública fossem precisos 100% do tempo, os riscos aos direitos humanos fundamentais se multiplicariam significativamente. Os sistemas de TRF apresentam o risco de privar as pessoas de seu anonimato, reduzindo-as a placas veiculares ambulantes e, ainda mais, reforçando a dinâmica de poder inerente às interações polícia-população em direção à polícia.

Direitos fundamentais em risco com o uso policial da TRF

Os direitos a seguir são comprometidos pelo uso policial da TRF. O nível do impacto sobre eles depende, como em cada forma de uso individual de um sistema de TRF pelas forças de segurança (seja ela retrospectiva, em tempo real ou iniciada por pessoa operadora), de diversos fatores. Tais elementos abrangem a arquitetura do sistema contra quem a tecnologia é utilizada – incluindo seus subsistemas e algoritmos centrais, o conjunto de dados empregado no treinamento de algoritmos e a finalidade da utilização da TRF – e as consequências de seu uso.

Nenhum dos direitos fundamentais listados abaixo é absoluto. Reconhece-se que os países podem interferir neles na busca de objetivos legítimos de interesse público, desde que tais interferências sejam proporcionais, limitadas ao estritamente necessário em uma sociedade democrática e utilizem os métodos menos intrusivos possíveis. É necessário encontrar um equilíbrio entre garantir que o Estado disponha de ferramentas eficazes e legítimas para cumprir suas funções e a proteção dos direitos e liberdades fundamentais. Importa assinalar igualmente que, quando consideramos o uso da TRF pelas forças de segurança, diferentes jurisdições respeitam e defendem esses direitos de maneira e em graus distintos, o que dá ainda mais contexto às implicações aos direitos humanos relativas ao uso da TRF.

I DIREITO À DIGNIDADE

Conforme expresso na Declaração Universal dos Direitos Humanos, todos os seres humanos nascem livres e iguais em dignidade e direitos.³⁶ E em virtude de serem humanas, todas as pessoas merecem respeito.

Os dados biométricos faciais de uma pessoa estão interligados à sua identidade em caráter permanente e irrevogável. O tratamento deles, em todas as circunstâncias, constitui em si mesmo uma interferência grave em diversos direitos, incluindo à privacidade, independentemente do resultado da tentativa de identificação (incorreta ou correta).³⁷ Essa ação invasiva é uma das razões pelas quais os dados recebem proteção legal adicional em certos países³⁸.

Essa interferência grave está relacionada ao direito à dignidade, de ser valorizado, respeitado e tratado de maneira ética, e não como uma mercadoria.³⁹ Caso uma

36 Artigo 1, Declaração Universal dos Direitos Humanos, https://brasil.un.org/sites/default/files/2025-03/ONU_DireitosHumanos_DUDH_UNICRio_20250310.pdf.

37 *Orientações 05/2022 sobre a utilização da tecnologia de reconhecimento facial no domínio da aplicação da Lei*, European Data Protection Board, documento aprovado em 26 de abril de 2023, p.5, https://www.edpb.europa.eu/system/files/2024-05/edpb_guidelines_202304_frtlawenforcement_v2_pt.pdf.

38 O artigo 4º (14) do Regulamento Geral de Proteção de Dados da União Europeia define “dados biométricos” como dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos. De acordo com o Artigo 9º do Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, é proibido o tratamento de dados biométricos, salvo em determinadas circunstâncias. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>. Veja também Biometric Information Privacy Act, Illinois State Legislature, 2008, <https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57>.

39 *Orientações 05/2022 sobre a utilização da tecnologia de reconhecimento facial no domínio da aplicação da Lei*, European Data Protection Board, documento aprovado em 26 de abril de 2023, p.15, https://www.edpb.europa.eu/system/files/2024-05/edpb_guidelines_202304_frtlawenforcement_v2_pt.pdf.

pessoa sinta que está sob vigilância – constante ou não – como consequência do uso de TRF, pode acabar mudando seu comportamento para evitar determinados locais, situações sociais ou eventos culturais nos quais a TRF esteja sendo empregada, podendo impactar gravemente na sua capacidade de viver uma vida digna.⁴⁰

Como adverte o Comitê Europeu para a Proteção de Dados, “a dignidade humana requer que os indivíduos não sejam tratados como meros objetos. A TRF calcula características existenciais e altamente pessoais – os traços faciais – em um formato de leitura automática, com o objetivo de os utilizar como matrícula ou cartão de identificação humano, objetificando, assim, o rosto da pessoa”.

II DIREITO À PRIVACIDADE

O direito à privacidade é uma expressão da dignidade humana e está relacionado à proteção da autonomia e da identidade pessoal.⁴¹ Ele inclui uma expectativa razoável de privacidade em público e é reconhecido como um direito de “porta de entrada”, pois possibilita a realização de outros direitos.

Se um sistema de TRF na segurança pública permite que pessoas sejam identificadas em espaços públicos e/ou que seus movimentos, interesses e associações sejam monitorados, em tempo real ou de forma retrospectiva, elas correm o risco de perder não apenas seu direito à privacidade, mas também outros direitos conexos que se baseiam nele. Isso inclui o direito à manifestação, de livre associação e expressão quanto à sua sexualidade, crença e/ou afiliação política.

A forma como a TRF afeta o direito à privacidade pode ser ainda mais exacerbada quando o sistema é utilizado à distância, em tempo real ou de forma retrospectiva, sem o consentimento, a participação ativa ou o conhecimento da pessoa. Esse é um ponto crucial quando consideramos o emprego da TRF na segurança pública, já que algumas aplicações podem configurar vigilância em massa, de forma secreta e/ou contínua. Além disso, o fato de que as listas de vigilância e os bancos de dados de referência da TRF – bem como o escaneamento de inúmeras pessoas em tempo real ou retrospectivamente –, inevitavelmente,

40 *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, European Union Agency for Fundamental Rights, 2020, p.20, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf.

41 *A/HRC/55/46: Legal safeguards for personal data protection and privacy in the digital age*, Office of the High Commissioner of Human Rights, 18 de janeiro de 2024, <https://www.ohchr.org/en/documents/thematic-reports/ahrc5546-legal-safeguards-personal-data-protection-and-privacy-digital>.

envolvem o tratamento de dados faciais de pessoas que não têm qualquer relação com determinados crimes, mas que ainda assim permanecem em uma espécie de “reconhecimento virtual”,⁴² destaca como essa tecnologia interfere seriamente no direito à privacidade.

III DIREITOS À LIBERDADE DE EXPRESSÃO, DE REUNIÃO PACÍFICA E DE ASSOCIAÇÃO

Os direitos à liberdade de opinião e de expressão são condições indispensáveis para o pleno desenvolvimento da pessoa humana. Eles proporcionam a troca e o desenvolvimento de opiniões na sociedade e, em conjunto, constituem a pedra fundamental de toda sociedade livre e democrática.⁴³ O direito humano fundamental de reunião pacífica e associação fomenta e protege a capacidade dos indivíduos de se expressarem individual e coletivamente.⁴⁴

Se uma força policial faz uso da TRF – em tempo real, iniciada por pessoa operadora ou de forma retrospectiva – para monitorar e/ou tentar identificar indivíduos que estejam se reunindo livremente, participando de um protesto em espaço público ou congregando em local de culto, essa tecnologia pode, potencialmente, revelar suas tendências políticas e/ou crenças religiosas. Em um protesto, ainda que a polícia esteja tentando encontrar uma pessoa específica que tenha sido incluída em uma lista de vigilância por meio de um mecanismo legal, alguns usos da TRF podem fazer com que a totalidade de participantes da manifestação – a maioria da qual não seria do interesse da polícia – tenham seus dados biométricos tratados e, possivelmente, armazenados, em tempo real ou de forma retrospectiva, sem conhecimento, participação ativa ou seu consentimento.

O simples reconhecimento de que forças de segurança estão utilizando a TRF de tal forma afeta gravemente a expectativa razoável das pessoas de permanecerem anônimas em espaços públicos. E isso pode resultar em um efeito inibidor sobre a capacidade ou decisão delas de se reunir, manifestar opiniões, trocar informações livremente e adotar comportamentos necessários e vitais para uma

42 Garvie, C, Bedoya, A & Frankle, J, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Georgetown Law Center on Privacy and Technology, outubro 2016, <https://www.perpetuallineup.org/risk-framework>.

43 UN Human Rights Committee, General comment No.34, CCPR/C/GC/34, para.2., <https://documents.un.org/doc/undoc/gen/g11/453/31/pdf/g1145331.pdf>.

44 UN Human Rights Committee, General comment No.37, CCPR/C/GC/37, para.1, <https://documents.un.org/doc/undoc/gen/g20/232/15/pdf/g2023215.pdf>.

democracia saudável, assim, prejudicando a participação política.⁴⁵ Especialistas alertam que, nas sociedades democráticas, os efeitos inibidores de longo prazo da TRF ainda não foram totalmente avaliados pelos tribunais ou autoridades de segurança.⁴⁶

IV DIREITO DE PROTEÇÃO DE DADOS PESSOAIS

Todas as pessoas têm direito à proteção de seus dados pessoais. E o uso de tecnologias intrusivas pela polícia, como a TRF, pode representar riscos significativos a esse direito, uma vez que tal tecnologia abarca o tratamento de dados pessoais sensíveis e pode induzir a resultados discriminatórios e enviesados; além de, também, levantar questões no âmbito do consentimento.

O fato de uma pessoa estar ciente de que foi fotografada ou gravada por câmeras de vigilância em um espaço público não significa que ela tenha concordado em disponibilizar os próprios dados biométricos publicamente e/ou consentido que eles sejam extraídos de uma imagem, tratados de modo a criar um modelo biométrico e armazenados ou utilizados para fins de identificação pela polícia, em tempo real ou em algum momento futuro.

Diferentes países apresentam salvaguardas legais diversificadas e, em alguns casos, inexistentes, para a extração, uso, retenção e/ou destruição de dados biométricos.

A depender da forma como a TRF é usada, sua interferência no direito à proteção de dados pessoais pode ser consideravelmente agravada caso uma pessoa seja submetida a qualquer forma de “perfilamento” ou processamento automatizado. Tal tratamento pode consistir no uso dos dados biométricos faciais para avaliar alguns de seus aspectos pessoais e/ou para analisar ou prever, de forma equivocada, elementos relativos ao seu desempenho profissional, situação econômica, saúde, preferências pessoais, seus interesses, confiabilidade, comportamento, localização ou deslocamentos.

V DIREITO À IGUALDADE E A NÃO DISCRIMINAÇÃO

45 Murray, D et al., “The Chilling Effect of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe”, *Journal of Human Rights Practice*, Volume 16, Issue 1, fevereiro de 2024, pp. 397–412, <https://doi.org/10.1093/jhuman/huad020>.

46 Murray, D, “Police Use of Retrospective Facial Recognition Technology: A Step Change in Surveillance Capability Necessitating an Evolution of the Human Rights Law Framework”, *Modern Law Review*, dezembro 2023, <https://doi.org/10.1111/1468-2230.12862>.

Todas as pessoas são iguais perante a lei e têm o direito, sem qualquer forma de discriminação, à mesma proteção legal.⁴⁷

Quando utilizados para tentar identificar uma pessoa, os diversos usos de sistemas de TRF na segurança pública, que são compostos por distintos algoritmos e treinados em diferentes conjuntos de dados e em condições variadas, podem resultar em diferentes taxas de erros. Todavia, ainda que essas taxas variem de acordo com múltiplos fatores que podem impactar o desempenho de um sistema de TRF, tais erros não afetam todas as pessoas igualmente. Estudos sobre a TRF demonstraram nitidamente a existência de vieses raciais e de gênero,⁴⁸ o que significa que mulheres e pessoas não brancas têm maior probabilidade de serem identificadas erroneamente e, conseqüentemente, estão potencialmente mais sujeitas a acusações injustas por parte da polícia, em comparação com homens de pele clara.

Além disso, algumas autoridades tendem a aplicar a TRF com mais frequência em comunidades marginalizadas, as quais já são excessivamente vigiadas, policiadas e encarceradas.⁴⁹ Ou seja, a TRF pode ser utilizada como uma ferramenta para criar ou aprofundar desigualdades estruturais e discriminação. Tais vieses

47 Artigo 7, Declaração Universal dos Direitos Humanos, https://brasil.un.org/sites/default/files/2025-03/ONU_DireitosHumanos_DUDH_UNICRio_20250310.pdf.

48 Buolamwini, J & Gebru, T, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, 2018, <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>. Veja também Buolamwini, J, *Response: Racial and Gender bias in Amazon Rekognition – Commercial AI System for Analyzing Faces*, Medium, 25 de janeiro de 2019, <https://medium.com/@Joy.Buolamwini/response-racial-and-gender-bias-in-amazon-rekognition-commercial-ai-system-for-analyzing-faces-a289222eeced>. Veja também Deborah Raji, I & Buolamwini, J, "Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products", *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society*, <https://dl.acm.org/doi/10.1145/3306618.3314244>. Veja também Cook, C, Howard, J, Sirotin, Y, Tipton, J & Vemury, A, "Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems", *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 2019, <https://ieeexplore.ieee.org/document/8636231>. Veja também NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software, 19 de dezembro de 2019. O Instituto Nacional de Normas e Tecnologia dos Estados Unidos (NIST, em sua sigla em inglês) escreveu: "Com que nível de precisão os softwares de reconhecimento facial identificam pessoas de sexo, idade e origem racial variados? De acordo com um novo estudo do Instituto Nacional de Normas e Tecnologia (NIST), a resposta depende do algoritmo que está no centro do sistema, da aplicação que o utiliza e dos dados que lhe são fornecidos – mas a maioria dos algoritmos de reconhecimento facial apresenta diferenciais demográficos. Um diferencial significa que a capacidade de um algoritmo de apresentar a correspondência de duas imagens da mesma pessoa varia de um grupo demográfico para outro". <https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software>.

49 Amnesty International, *Israel/OPT: Israeli authorities are using facial recognition technology to entrench apartheid*, 2 de maio de 2023, <https://www.amnesty.org/en/latest/news/2023/05/israel-opt-israeli-authorities-are-using-facial-recognition-technology-to-entrench-apartheid/>.

são fortemente agravados pelo fato de que muitas autoridades de segurança pública sequer reconhecem a existência deles – quanto mais tomam medidas para compreender a razão pela qual eles existem – ou fazem questionamentos rigorosos sobre a tecnologia comprada e implementada, especialmente em relação ao perfil demográfico das pessoas contra as quais ela é aplicada. Equívocos em torno dos chamados índices de “precisão”⁵⁰ exacerbam ainda mais esses problemas, ameaçando o direito das pessoas à proteção igualitária contra a discriminação.

VI DIREITOS DAS PESSOAS COM DEFICIÊNCIA

Ex-Relator Especial da ONU sobre os direitos das pessoas com deficiência documentou que alguns algoritmos apresentam vieses inerentes contra pessoas com deficiência, especialmente aquelas com condições como a síndrome de Down, acondroplasia, fissura labial ou palatina, bem como outras que resultam em diferenças faciais.

Ele relatou que esses problemas fizeram com que algumas pessoas com deficiência fossem “consideradas não confiáveis”, pois o seu rosto não estava em conformidade com a norma programada para o sistema de TRF. O relator apelou aos países para que considerem a imposição de uma moratória sobre a venda e uso dessas tecnologias, até que seja realizada uma auditoria completa sobre os seus efeitos, com a participação de organizações representativas de pessoas com deficiência.⁵¹

50 Gerchick, M & Cagle, M, *When it Comes to Facial Recognition, There is No Such Thing as a Magic Number*, American Civil Liberties Union, 7 de fevereiro de 2024, <https://www.aclu.org/news/privacy-technology/when-it-comes-to-facial-recognition-there-is-no-such-thing-as-a-magic-number>.

51 *Report of the Special Rapporteur on the rights of persons with disabilities on Artificial Intelligence and the rights of persons with disabilities*, dezembro de 2021, <https://www.ohchr.org/en/calls-for-input/2021/report-special-rapporteur-rights-persons-disabilities-artificial-intelligence>.

VII DIREITO À PRESUNÇÃO DE INOCÊNCIA

Um elemento fundamental dos julgamentos justos e do Estado de Direito é o fato de todos os seres humanos serem considerados inocentes até que se prove o contrário.⁵²

A utilização da TRF por uma autoridade de segurança pública requer que ela rode um modelo biométrico em um banco de dados de referência de modelos biométricos, se a TRF for utilizada em caráter retrospectivo, ou que rode modelos biométricos obtidos a partir de um vídeo ao vivo e os compare com uma “lista de vigilância” de modelos biométricos, se a tecnologia for utilizada em tempo real. Por sua natureza, esses processos requerem, efetivamente, a geração de múltiplas falsas correspondências. E em última instância, isso significa que, por causa desses sistemas, pessoas inocentes sempre acabarão em listas usadas pelas autoridades que cumprem a função da aplicação da lei quando elas tentarem encontrar e/ou identificar um indivíduo suspeito ou de interesse.

Quando os dados biométricos faciais de uma pessoa são incluídos em um banco de dados de referência – em alguns casos, simplesmente por serem titulares de uma carteira de motorista ou passaporte,⁵³ – ou em uma lista de vigilância, com base em um conjunto de critérios geralmente desconhecidos ou totalmente ocultos⁵⁴, estabelecidos por uma autoridade, isso implica que ela estará sujeita a buscas por parte da polícia com o intuito de encontrar ou identificar alguém de interesse. Na verdade, todas as pessoas relacionadas em um banco de dados ou lista de vigilância são tratadas como potenciais suspeitas de crimes ou de interesse, interferindo no seu direito à presunção de inocência. Como resultado, muitos indivíduos que não têm nada a ver com um determinado crime específico sob investigação, com relação ao qual é efetuada uma busca na TRF, podem enfrentar consequências severas indevidamente, como acontece no caso de identificações incorretas.

52 Artigo 11, Declaração Universal dos Direitos Humanos, https://brasil.un.org/sites/default/files/2025-03/ONU_DireitosHumanos_DUDH_UNICRio_20250310.pdf.

53 Boffey, D, “Police to be able to run face recognition searches on 50m driving licence holders”, *The Guardian*, 20 de dezembro de 2023, <https://www.theguardian.com/technology/2023/dec/20/police-to-be-able-to-run-face-recognition-searches-on-50m-driving-licence-holders>.

54 *Big Brother Watch: complaint against private sector facial recognition*, AWO Agency, <https://www.awo.agency/blog/big-brother-watch-complaint-against-private-sector-facial-recognition/>. Veja também <https://www.awo.agency/files/2022-07-25-Facewatch-Coop-ICO-Complaint.pdf>.

E está cada vez mais evidente que os problemas atrelados à identificação incorreta são acentuadamente agravados pela forma como a imagem de uma pessoa é posteriormente utilizada em um reconhecimento fotográfico.⁵⁵

Se o modelo biométrico de uma pessoa for mantido em um banco de dados de referência específica ou em uma lista de vigilância comumente utilizada ou acessada por uma autoridade de aplicação da lei, pode-se dizer que ela está presa em um alinhamento virtual perpétuo, mesmo quando não tem nenhuma ligação com um crime específico.⁵⁶

VIII DIREITO A UM RECURSO EFETIVO

Todas as pessoas têm direito a um recurso efetivo contra atos que violem seus direitos fundamentais.⁵⁷

Independentemente de uma força de segurança pública fazer uso da TRF em tempo real, iniciada por uma pessoa operadora, em caráter retrospectivo para monitorar ou tentar identificar uma pessoa, mesmo quando o faz por vias legais, o sistema pode errar e, de fato, erra. Isso ocorre porque a tecnologia não foi projetada para fornecer à polícia uma única identificação positiva ou “correspondência”. Na melhor das hipóteses, ela fornece uma lista de suposições de quem essa pessoa poderia ser, isto é, de possíveis pessoas candidatas com pontuações de similaridade.

Um valor limiar é fixado para determinar quando o software indicará que ocorreu uma provável correspondência. E, caso esse valor seja definido em um nível muito baixo ou muito alto, ele pode criar uma alta taxa de falsos positivos ou de falsos negativos, respectivamente. Não existe uma configuração de limiar que elimine todos os erros. Além disso, o tamanho da lista de pessoas candidatas gerada dependerá da configuração definida pela pessoa usuária.

De qualquer forma, não há garantia de que a “correspondência verdadeira” será apresentada na lista, pois a pessoa que está sendo procurada pode não estar no banco de dados de referência. Tampouco há garantia de que, se ela estiver, de

55 Hill, K, “Facial Recognition Led to Wrongful Arrests. So Detroit Is Making Changes”, *New York Times*, 29 de junho de 2024, <https://www.nytimes.com/2024/06/29/technology/detroit-facial-recognition-false-arrests.html#:~:text=The%20person%20running%20the%20search,provided%20the%20store's%20surveillance%20video>.

56 Garvie, C, Bedoya, A & Frankle, J, *The Perpetual Line-Up, Unregulated Police Face Recognition in America*, Georgetown Law Center on Privacy and Technology, outubro 2016, <https://www.perpetuallineup.org/>.

57 Artigo 8, Declaração Universal dos Direitos Humanos, https://brasil.un.org/sites/default/files/2025-03/ONU_DireitosHumanos_DUDH_UNICRio_20250310.pdf.

fato, no banco, estará no topo da lista de candidatas. Também não há garantia de que a escolha a ser feita por profissional da segurança pública será a da “correspondência verdadeira” da lista, se é que ela existe.

Os estágios iniciais de uma operação da TRF em tempo real são inteiramente baseados em um tratamento automatizado, por meio do qual o sistema compara imagens capturadas em um feed ao vivo com imagens de uma lista de vigilância e, em seguida, cria alertas para possíveis ações a serem tomadas. De maneira análoga aos sistemas de TRF retrospectiva, o fato de ditas “correspondências” serem ou não encontradas depende da “configuração de similaridade” selecionada. Estudos mostram que, quanto menor o limiar definido, mais correspondências serão encontradas; contudo, provavelmente, menos precisas elas serão. Por outro lado, um limiar mais alto produz menos correspondências com um grau mais alto de confiança em sua exatidão.⁵⁸

Esses problemas inevitáveis à TRF fazem com que pessoas inocentes, que por acaso se pareçam com outras, sejam arrastadas para uma rede policial de indivíduos suspeitos sem justa causa. Quando tais são injustamente submetidos à ação policial com base no uso dessa tecnologia e não são informados de que a ação estava condicionada a esse uso⁵⁹ – sem serem informados de que foi motivada por essa tecnologia, nem tendo meios legais para descobrir exatamente como ela foi utilizada contra eles,⁶⁰ – levantam-se sérias preocupações sobre o direito a um recurso efetivo. Dado que essa é uma tecnologia relativamente nova na segurança pública, tal questão tem se tornando mais evidente à medida que mais casos de identificação incorreta e prisões indevidas têm vindo à tona.⁶¹

A identificação incorreta de uma pessoa como parte acusada de um crime pode trazer um impacto prejudicial à sua vida, seja ela baseada em uma ação tomada

58 Fussey, P & Murray, D, *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, Human Rights Centre, University of Essex, julho de 2019, p.107, <https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf>.

59 MacMillan, D et al., “Police seldom disclose use of facial recognition despite false arrests”, *Washington Post*, 6 de outubro de 2024, <https://www.washingtonpost.com/business/2024/10/06/police-facial-recognition-secret-false-arrest/>.

60 Williams, R, “I Was Wrongfully Arrested Because of Facial Recognition Technology. It Shouldn't Happen to Anyone Else”, *Time*, 29 de junho de 2024, <https://time.com/6991818/wrongfully-arrested-facial-recognition-technology-essay/>.

61 Sanford, A, *Artificial Intelligence Is Putting Innocent People at Risk of Being Incarcerated*, Innocence Project, 14 de fevereiro de 2024, <https://innocenceproject.org/artificial-intelligence-is-putting-innocent-people-at-risk-of-being-incarcerated/>.

imediatamente após o erro de identificação, como em um episódio em tempo real⁶², ou depois de algum tempo, como em um caso retrospectivo.⁶³

Contudo, é de suma importância apontar que as preocupações no âmbito do direito a um recurso efetivo não dizem respeito apenas a erros de identificação. Quando a tecnologia “acerta” e identifica corretamente uma pessoa não significa, necessariamente, que o uso do sistema é legítimo, proporcional, necessário e compatível com os direitos humanos.⁶⁴ A utilização de TRFs que identificam “corretamente” indivíduos ainda pode causar graves violações de direitos humanos⁶⁵ e, quando combinadas com outras tecnologias de vigilância e sistemas de armamento, podem resultar, até mesmo, em crimes de guerra.⁶⁶

IX DIREITO A UM JULGAMENTO JUSTO E AO DEVIDO PROCESSO LEGAL

O impacto real do emprego da TRF na aplicação da lei – seja quando ela falha⁶⁷ ou funciona⁶⁸ – pode ser devastador. No momento em que esse relatório foi redigido, e somente nos Estados Unidos da América (EUA), há sete casos conhecidos de autoridades que prenderam e encarceraram indevidamente pessoas com base no uso de TRF suscetível a erros⁶⁹ – seis delas são negras. Não se sabe, porém, quantos indivíduos presos e encarcerados injustamente nesse país podem ter

62 Clayton, J, “I was misidentified as shoplifter by facial recognition tech”, BBC, 26 de maio de 2024, <https://www.bbc.com/news/technology-69055945>.

63 Bhuiyan, J, “Facial recognition used after Sunglass Hut robbery led to man's wrongful jailing, says suit”, *The Guardian*, 23 de janeiro de 2024, <https://www.theguardian.com/technology/2024/jan/22/sunglass-hut-facial-recognition-wrongful-arrest-lawsuit>.

64 *Glukhin v Russia*, App. No(s), 11519/20, <https://hudoc.echr.coe.int/eng?i=001-225655>.

65 Gan-Mor, G & Pinchuk, A, *In Focus: Facial Recognition Tech Stories and Rights Harms from Around the World: Surveillance in the West Bank/Occupied Palestinian Territories*, International Network of Civil Liberties Organizations, janeiro 2021, p.11, <https://www.inclo.net/pdf/in-focus-facial-recognition-tech-stories.pdf>. Veja também *Israel and Occupied Palestinian Territories: Automated Apartheid: How facial recognition fragments, segregates and controls Palestinians in the OPT*, Amnesty International, maio de 2023, <https://www.amnesty.org/en/documents/mde15/6701/2023/en/>. Veja também Frenkel, S, “Israel Deploys Expansive Facial Recognition Program in Gaza”, *New York Times*, 27 de março de 2024, https://www.nytimes.com/2024/03/27/technology/israel-facial-recognition-gaza.html?ugrp=c&unlocked_article_code=1f00.5Dlt.O0vTOELrgEOM&smid=url-share.

66 Fatafta, M, e Leufer, D, *Artificial Genocidal Intelligence: how Israel is automating human rights abuses and war crimes*, Access Now, 9 de maio de 2024, <https://www.accessnow.org/publication/artificial-genocidal-intelligence-israel-gaza/>.

67 Williams, R, *I Did Nothing Wrong. I Was Arrested Anyway*, American Civil Liberties Union, 15 de julho de 2021, <https://www.aclu.org/news/privacy-technology/i-did-nothing-wrong-i-was-arrested-anyway>.

68 *Glukhin v Russia*, App. No(s), 11519/20, <https://hudoc.echr.coe.int/eng?i=001-225655>.

69 *ACLU calls on Detroit Police Department to end use of faulty facial recognition technology following yet another wrongful arrest*, American Civil Liberties Union, 7 de agosto de 2023, <https://www.aclumich.org/en/press-releases/aclu-calls-detroit-police-department-end-use-faulty-facial-recognition-technology>.

aceitado acordos judiciais.⁷⁰ Se as autoridades não publicizam o uso da TRF para as pessoas detidas, interrogadas, presas, acusadas ou processadas após uma busca nesses sistemas, isso constitui uma clara violação do direito ao devido processo legal e, em casos de processo criminal, a um julgamento justo.⁷¹

A opacidade em torno do uso de sistemas de TRF e de como eles operam pode ofuscar a capacidade de pessoas julgadas de entender completamente como o caso foi construído e, em algumas situações, negar-lhes os meios para contestar em juízo a precisão e a confiabilidade dessas tecnologias. Tal questão é ainda mais preocupante quando a parte acusada pertence a um grupo demográfico que sofre de forma desproporcional devido aos problemas de viés na TRF e pode precisar de maior conhecimento técnico para contestar os resultados do sistema. Tudo isso resulta em um desequilíbrio entre o acesso à informação e o poder na dinâmica da interação entre a polícia e civis, o que é incompatível com o devido processo legal.

Avaliando o impacto do uso policial de tecnologias de reconhecimento facial sobre os direitos humanos

O uso da TRF pela polícia está em conformidade com os padrões internacionais de direitos humanos?

Muitos de nossos direitos estão consagrados no Pacto Internacional sobre Direitos Civis e Políticos (PIDCP), na Convenção Europeia dos Direitos Humanos (CEDH), na Carta dos Direitos Fundamentais da União Europeia (Carta da UE) e na Convenção Americana sobre Direitos Humanos (CIDH).⁷²

70 Press, E, “Does A.I. Lead Police to Ignore Contradictory Evidence?”, *The New Yorker*, 13 de novembro de 2023, <https://www.newyorker.com/magazine/2023/11/20/does-a-i-lead-police-to-ignore-contradictory-evidence>.

71 MacMillan, D et al., “Police seldom disclose use of facial recognition despite false arrests”, *Washington Post*, 6 de outubro de 2024, <https://www.washingtonpost.com/business/2024/10/06/police-facial-recognition-secret-false-arrest/>.

72 Consulte os Artigos 8º–11º da CEDH, os Artigos 12º, 17º, 18º, 19º, 21º e 22º do PIDCP e os Artigos 11º, 12º, 13º, 15º e 16º da CIDH.



Tais direitos não são absolutos. Todavia, de acordo com a legislação internacional de direitos humanos, de modo geral, eles apenas poderão ser restringidos ou limitados se isso:

- Estiver previsto ou prescrito em lei e não seja arbitrário;
- Defender um objetivo legítimo;
- For estritamente necessário em uma sociedade democrática para atingir o objetivo em questão; e
- For proporcional ao objetivo legítimo.

→ PREVISÃO EM LEI E NÃO ARBITRARIEDADE

O significado de “lei” nesse contexto implica certos requisitos mínimos de inteligibilidade, precisão, acessibilidade e previsibilidade. Isso serve para permitir que indivíduos prevejam as consequências de seus atos e controlem seu comportamento e conduta de forma adequada, mas também para protegê-los contra interferências arbitrárias de Estados quando eles exercem seu poder. Assim, uma lei que preveja o uso da TRF – e, portanto, o tratamento de dados biométricos faciais – que não seja publicizado não pode ser considerada um dispositivo legal, pois a mera aprovação legislativa sem atender aos requisitos básicos de inteligibilidade e acessibilidade, em primeiro lugar, não pode ser considerada “lícito”. Qualquer interferência em um direito deve ter base

jurídica e apresentar qualidade suficiente para garantir a proteção contra interferências arbitrárias.

- **Exemplo:** No caso da Europa, em relação ao uso da TRF na segurança pública, o Comitê Europeu para a Proteção de Dados declarou o seguinte:

“Os termos da base jurídica devem ser suficientemente claros para dar aos cidadãos uma indicação adequada das condições e das circunstâncias em que as autoridades têm poderes para recorrer a quaisquer medidas de recolha de dados e de vigilância secreta. Uma mera transposição para o direito nacional da cláusula geral do artigo 10º da Diretiva de Proteção de Dados na Aplicação da Lei⁷³ careceria de rigor e previsibilidade.”⁷⁴

- **Exemplo:** No Reino Unido, onde a polícia faz uso da TRF ao vivo e de forma retrospectiva, não há base jurídica explícita ou específica para isso. Em contrapartida, a segurança pública se baseia em uma série de outras leis e poderes advindos do Direito Consuetudinário.⁷⁵
- **Exemplo:** Uma pesquisa feita com 38 iniciativas de TRF, em nove países latino-americanos, constatou que apenas 14 delas indicavam a existência de regulamentos relativos ao seu uso. Mesmo assim, a maioria deles não regia o uso da TRF de forma estrita e, ao invés disso, concedia autorizações de uso de forma ampla (“para supervisionar o cumprimento das disposições sobre evasão no transporte público”, para “funções

73 Artigo 10º, da Diretiva de Proteção de Dados na Aplicação da Lei: Tratamento de categorias especiais de dados pessoais “O tratamento de dados pessoais que revelem a origem racial ou étnica, opiniões políticas, crenças religiosas ou convicções filosóficas, a filiação sindical, o tratamento de dados genéticos, dados biométricos destinados a identificar uma pessoa singular de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou à orientação sexual só é autorizado se for estritamente necessário, se estiver sujeito a garantias adequadas dos direitos e liberdades do titular dos dados, e se: (a) for autorizado pelo direito da União ou de um Estado-Membro; (b) Se destinar a proteger os interesses vitais do titular dos dados ou de outra pessoa singular; ou (c) Estiver relacionado com dados manifestamente tornados públicos pelo titular dos dados.

74 *Orientações 05/2022 sobre a utilização da tecnologia de reconhecimento facial no domínio da aplicação da Lei*, European Data Protection Board, p. 5, https://www.edpb.europa.eu/system/files/2024-05/edpb_guidelines_202304_frtlawenforcement_v2_pt.pdf.

75 Lei de Proteção de Dados de 2018 (*Data Protection Act 2018*), Lei sobre Regulamentação dos Poderes de Investigação de 2000 (*Regulation of Investigatory Powers Act 2000*), Lei da Proteção de Liberdades Cívicas de 2012 (*Protection of Freedoms Act 2012*), Lei dos Direitos humanos de 1998 (*Human Rights Act 1998*), Lei da Igualdade de 2010 (*Equality Act 2010*), Lei de Provas Policiais e Criminais de 1984 (*Police and Criminal Evidence Act 1984*).

do processo de verificação de imigração, controle de estrangeiros e migratório” etc.).⁷⁶

→ DEFESA DE UM OBJETIVO LEGÍTIMO

Os direitos à privacidade, à liberdade de expressão e associação vêm com cláusulas de limitação. Por exemplo, nos termos da Convenção Europeia dos Direitos Humanos, uma interferência no direito à privacidade somente pode ser considerada legítima se for “necessária para a segurança nacional, para a segurança pública, para o bem-estar econômico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou para a proteção dos direitos e das liberdades de terceiros”.⁷⁷ Mas, se não houver evidência de que a conduta de uma pessoa tenha qualquer ligação com um objetivo legítimo, então, há pouca ou nenhuma justificativa para uma interferência em seus direitos.

- **Exemplo:** O artigo 6º da Diretiva da UE sobre Proteção de Dados na Aplicação da Lei (LED) obriga as pessoas controladoras de dados a distinguir entre diferentes categorias de titulares de dados (ou seja, pessoas). Nesse ínterim, o Comitê Europeu para a Proteção de Dados declarou:

“No que diz respeito aos titulares de dados em relação aos quais não haja indícios que levem a acreditar que o seu comportamento possa ter um nexos, ainda que indireto ou longínquo, com o objetivo legítimo de acordo com a diretiva, muito provavelmente não há justificativa para uma ingerência. Se não for aplicável ou possível qualquer distinção em conformidade com o artigo 6º da Diretiva de Proteção de Dados na Aplicação da Lei, a exceção à regra desse artigo tem de ser rigorosamente analisada no contexto da avaliação da necessidade e da proporcionalidade da ingerência.”⁷⁸

76 Venturini, J e Garay, V (Nogueira, P trans.) *Facial recognition in Latin America Trends in the implementation of a perverse technology*, AISur, 2021, https://www.alsur.lat/sites/default/files/2021-10/ALSUR_Reconocimiento_%20facial%20en%20Latam_EN_Final.pdf.

77 Artigo 8º (2), Convenção Europeia dos Direitos Humanos.

78 *Orientações 05/2022 sobre a utilização da tecnologia de reconhecimento facial no domínio da aplicação da Lei*, European Data Protection Board, p. 23, https://www.edpb.europa.eu/system/files/2024-05/edpb_guidelines_202304_frtlawenforcement_v2_pt.pdf.

O artigo ainda complementou que a distinção entre diferentes categorias de titulares de dados é “um requisito essencial no que diz respeito ao tratamento de dados pessoais que envolva reconhecimento facial” devido à probabilidade de falsos positivos e falsos negativos.

→ NECESSIDADE EM UMA SOCIEDADE DEMOCRÁTICA PARA ATINGIR O OBJETIVO EM QUESTÃO

A parte final do teste de três etapas envolve identificar a gama de direitos impactados pela interferência, a fim de determinar a necessidade - ou não - da medida, e avaliar se a interferência compromete de forma adequada ou inadequada outros direitos concorrentes. Como parte dessa avaliação, a medida proposta deve ser respaldada por evidências que descrevam o problema que se pretende resolver, como ela será efetivamente eficaz para enfrentar esse problema, uma análise sobre se tal é ou não a medida menos intrusiva possível para lidar com a questão e uma explicação do motivo pelo qual medidas já existentes não são suficientes para resolvê-la. Sempre que considerarmos uma medida, ferramenta ou lei relativa à vigilância, especialmente uma tão poderosa, em escala, intrusiva e invasiva como a TRF, em todas as suas formas de uso, devemos avaliar se ela é ou não eficaz. Isso porque a eficácia de uma ferramenta ou método de vigilância está diretamente relacionado à sua necessidade e proporcionalidade. Ademais, caso a medida proposta envolva o tratamento de dados sensíveis, como dados biométricos faciais, um critério mais rigoroso deve ser aplicado à avaliação de sua efetividade.

- **Exemplo:** Em *Glukhin vs. Russia*, o Tribunal Europeu de Direitos Humanos decidiu que o uso de TRF para identificar e prender um manifestante pacífico violou os direitos de privacidade e liberdade de expressão dele. O Tribunal proferiu que os dispositivos legais nacionais aplicáveis não atendiam ao requisito de “qualidade de lei” e que o tratamento dos dados pessoais de Glukhin não poderia ser considerado “necessário em uma sociedade democrática”. Especificamente, observou que: “A legislação nacional não contém nenhuma limitação sobre a natureza das situações que podem dar origem ao uso da tecnologia de reconhecimento facial, os objetivos pretendidos, as categorias de pessoas que podem ser visadas ou o tratamento de dados pessoais sensíveis. Ainda, o governo não fez referência a nenhuma salvaguarda processual para o uso da tecnologia de reconhecimento facial na Rússia, como procedimentos de autorização, procedimentos a serem seguidos para examinar, utilizar e armazenar os

dados pessoais obtidos, mecanismos de controle de supervisão ou os recursos disponíveis”.⁷⁹

- **Exemplo:** Em *S. and Marper vs. the United Kingdom*,⁸⁰ o Tribunal Europeu de Direitos Humanos decidiu que a retenção indefinida de dados biométricos (nesse caso, impressões digitais e amostras de DNA) de pessoas acusadas, mas não condenadas, não era necessária em uma sociedade democrática. Ao proferir que o Reino Unido falhou em manter um equilíbrio justo entre os interesses públicos e privados concorrentes, declarou que: “O Tribunal considera que a natureza genérica e indiscriminada dos poderes de retenção das impressões digitais, amostras celulares e perfis de DNA de pessoas suspeitas, mas não condenadas por delitos, conforme aplicável no caso das presentes partes requerentes, suscitou na falha em manter um equilíbrio justo entre os interesses públicos e privados em jogo. O Estado requerido ultrapassou qualquer margem de apreciação aceitável nesse aspecto. Consequentemente, a retenção em pauta constitui uma ingerência desproporcional no direito das partes requerentes ao respeito à vida privada e não pode ser considerada necessária em uma sociedade democrática.”

→ PROPORCIONALIDADE

Se o teste de necessidade tiver um resultado insuficiente, não há necessidade de um teste de proporcionalidade. No entanto, se o primeiro apresentar um resultado positivo, uma avaliação da proporcionalidade deverá ser aplicada. Este princípio apoia-se na ideia de que uma medida não deve exceder o necessário para atingir o objetivo. Dessa forma, as vantagens da medida devem prevalecer às suas desvantagens. Um teste que examina a proporcionalidade, caso a caso, deve avaliar a importância do objetivo e se a medida atende a ele, avaliar o escopo, a extensão e a intensidade da interferência, bem como examinar quais salvaguardas estão em vigor com relação à medida, a fim de reduzir os riscos aos direitos associados.

- **Exemplo:** Segundo a declaração da Autoridade Europeia para a Proteção de Dados: “No cerne da noção de proporcionalidade jaz o conceito de um exercício de equilíbrio: a ponderação da intensidade da interferência frente

⁷⁹ *Glukhin vs. Russia*, App. No(s), [11519/20](https://hudoc.echr.coe.int/eng?i=001-225655), <https://hudoc.echr.coe.int/eng?i=001-225655>.

⁸⁰ *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 e 30566/04, § 102, ECHR 2008-V.

à importância (“legitimidade”, usando a terminologia do *Common Law*) do objetivo alcançado em um dado contexto.

“Um teste bem-feito, para ser completo e preciso, precisa da identificação expressa e da estruturação em um quadro coerente dos diferentes elementos dos quais a ponderação depende.”⁸¹

A TRF é confiável? É discriminatória?

Há diversas etapas envolvidas no uso da TRF, seja ela em tempo real, retrospectiva ou iniciada por uma pessoa operadora. Em cada uma delas, há riscos de erro e de identificação incorreta, bem como de vigilância discriminatória, desproporcional e desnecessária. Logo, todas as fases devem ser cuidadosamente analisadas quando houver uma avaliação de como a TRF afeta direitos fundamentais⁸². E, dado que a tecnologia tem exibido nitidamente vieses raciais e de gênero,⁸³ tais preconceitos devem ser sempre pautados durante a análise de cada etapa. As respostas às perguntas apresentadas a seguir também podem influenciar nos

81 EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 2019, https://edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf.

82 EFF, Electronic Privacy Information Center (EPIC) e the National Association of Criminal Defense Lawyers (NACDL), amicus brief in *State of New Jersey v. Francisco Arteaga*, <https://www.eff.org/document/state-new-jersey-v-francisco-arteaga>.

83 Buolamwini, J, e Gebu, T, “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification”, *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, 2018, <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>.

Veja também Deborah Raji, I, e Buolamwini, J, “Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products”, *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society*, <https://dl.acm.org/doi/10.1145/3306618.3314244>.

Veja também Cook, C, Howard, J, Sirotni, Y, Tipton, J, e Vemury, A, “Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems”. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 2019 <https://ieeexplore.ieee.org/document/8636231>. Veja também *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, 19 de dezembro de 2019. O Instituto Nacional de Normas e Tecnologia dos Estados Unidos (NIST), em sua sigla em inglês) escreveu: “Com que nível de precisão os softwares de reconhecimento facial identificam pessoas de sexo, idade e origem racial variados? De acordo com um novo estudo do Instituto Nacional de Normas e Tecnologia (NIST), a resposta depende do algoritmo que está no centro do sistema, da aplicação que faz uso do algoritmo e dos dados que

lhe são fornecidos – mas a maioria dos algoritmos de reconhecimento facial apresenta diferenciais demográficos. Um diferencial significa que a capacidade de um algoritmo de apresentar a correspondência de duas imagens da mesma pessoa varia de um grupo demográfico para outro”. <https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software>. Veja também Findley, B, “Why Racial Bias is Prevalent in Facial Recognition Technology”, *Harvard Journal of Law and Technology*, novembro 2020, <https://jolt.law.harvard.edu/digest/why-racial-bias-is-prevalent-in-facial-recognition-technology>.

testes mencionados acima, a fim de saber se o uso da TRF está previsto em lei e não é arbitrário: ela tem um objetivo legítimo? É estritamente necessária em uma sociedade democrática? Ela é proporcional ao objetivo legítimo? A INCLO agradece a pesquisa, as avaliações de auditoria, as leis-modelo e as estruturas éticas criadas por Radiya-Dixit,⁸⁴ Davis, Perry e Santow.⁸⁵ Estendemos nossos agradecimentos também a Lynch, Campbell, Purshouse e Betkier⁸⁶ pelo apoio para identificar e moldar as perguntas.

IMAGEM DE CONSULTA

Envolve agente policial que, por meio de um dispositivo móvel, CFTV ou outra fonte, obtém a imagem de uma pessoa a fim de compará-la com um banco de dados de imagens de pessoas conhecidas, utilizando tecnologia de reconhecimento facial. As questões a serem consideradas em relação a esta etapa incluem:

- De onde vem a imagem de consulta?
- Por que essa imagem foi escolhida?
- Quem obteve essa imagem?
- Há quanto tempo a imagem de consulta existe?
- Ela foi obtida por meio de circuito fechado de televisão, de uma câmera corporal, de um telefone celular ou de uma conta de mídia social?
- Ela foi obtida, armazenada e compartilhada de forma lícita/legal?
- Qual é a qualidade da imagem? Qual é sua resolução? A iluminação é boa?
- A pessoa está olhando diretamente para a câmera na imagem?
- Há algo obstruindo o rosto da pessoa?
- Quem teve acesso à imagem antes de ela ser usada em uma busca na TRF?

84 Radiya-Dixit, E, *A Sociotechnical Audit: Assessing Police Use of Facial Recognition*, Cambridge: Minderoo Centre for Technology and Democracy, 1º de outubro de 2022, <https://doi.org/10.17863/CAM.89953>.

85 Davis, N, Perry, L & Santow, E, *Facial Recognition Technology: Towards a model law*, Human Technology Institute, The University of Technology, setembro 2022 <https://www.uts.edu.au/sites/default/files/2022-09/Facial%20recognition%20model%20law%20report.pdf>.

86 Lynch, N, Campbell, L, Purshouse, J & Betkier, M, *Facial Recognition Technology in New Zealand: Towards a Legal and Ethical Framework*, Law Foundation of New Zealand, 30 de novembro de 2020, <https://doi.org/10.25455/wgtn.17204078.v1>.

- Existe uma base jurídica para o tratamento da imagem de modo a extrair os traços faciais da pessoa e criar dados biométricos?
- Existe um mecanismo de supervisão robusto e efetivo que serve de salvaguarda aos direitos fundamentais da pessoa cuja imagem está servindo de prova?

SELEÇÃO DE BANCO DE DADOS DE REFERÊNCIA

De modo análogo às imagens de consulta, a seleção do banco de dados de referência desempenha um papel significativo não apenas para a confiabilidade de uma busca na TRF retrospectiva, mas também em quão discriminatório um sistema pode ser em termos de quem é submetido à busca. A natureza da tecnologia e o uso de bancos de dados de referência, inevitavelmente, colocam pessoas inocentes em risco de serem identificadas erroneamente e também trazem risco de vigilância. Por exemplo, em Buenos Aires, Argentina, o sistema de TRF em tempo real da cidade – criado para procurar pessoas-alvos de buscas – foi considerado inconstitucional por diversos motivos e, principalmente, porque cerca de 15 mil indivíduos que não eram fugitivos foram incluídos no banco de dados sem aprovação judicial. Isso resultou em buscas na TRF envolvendo a pessoa governante do país, figuras políticas, ativistas de direitos humanos e jornalistas – e não apenas pessoas foragidas.⁸⁷ As questões a serem consideradas incluem:

- Como o banco de dados de imagens foi compilado?
- Existem critérios inteligíveis, objetivos e limitados com relação a quem incluir no banco de dados?⁸⁸
- Foi realizada uma avaliação de riscos aos direitos fundamentais em relação às pessoas cujas imagens constam no banco de dados?
- Qual é a origem das imagens?

87 Naundorf, K, *The Twisted Eye in the Sky Over Buenos Aires*, Wired, setembro 2023, <https://www.wired.com/story/buenos-aires-facial-recognition-scandal/>.

88 Radiya-Dixit, E, *A Sociotechnical Audit: Assessing Police Use of Facial Recognition*, Cambridge: Minderoo Centre for Technology and Democracy, 1º de outubro de 2022, <https://www.mctd.ac.uk/wp-content/uploads/2022/10/MCTD-FacialRecognition-Report-WEB-1.pdf>. Veja também *Guidelines on facial recognition*, Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data, Convention 108, Council of Europe, julho 2021, <https://rm.coe.int/guidelines-facial-recognition-web-a5-2750-3427-6868-1/1680a31751>.

- Quais medidas técnicas e de segurança estão em vigor para proteger o banco de dados e impedir o acesso indevido?
- Se o banco de dados de imagens tiver a sua origem em um sistema de justiça penal, qual é a base jurídica para o uso dessas imagens?
- Se o banco de dados de imagens tiver a sua origem em um sistema de justiça penal, as imagens são de pessoas que foram presas, acusadas e/ou condenadas?
- Se o banco de dados de imagens tiver a sua origem em um sistema de justiça penal, há um período de retenção previsto em lei para o armazenamento dessas imagens?
- Se o banco de imagens tiver a sua origem em um sistema de justiça penal, há risco de que um número desproporcional de pessoas de uma comunidade específica esteja nele porque já existe uma super-representação de integrantes dela nas prisões do Estado? (Se esse for o caso, essas pessoas correrão um risco maior de serem identificadas equivocadamente em uma busca na TRF).
- A força policial tem um código de conduta e/ou orientação por escrito referentes à retenção e exclusão de fotografias de pessoas presas e/ou condenadas tiradas por policiais?
- Qual é a base jurídica para a criação ou o acesso a esse banco de dados?
- O banco de dados foi criado e as imagens armazenadas e tratadas licitamente?
- Há quanto tempo existem as imagens no banco de dados? Elas estão atualizadas?
- As imagens foram obtidas por meio de circuito fechado de televisão, câmeras corporais, telefones celulares ou em contas de redes sociais?
- Qual é a qualidade das imagens? Qual é a sua resolução? A iluminação é boa?
- O banco é composto por imagens de pessoas olhando diretamente para a câmera?
- Há algo obstruindo o rosto dessas pessoas cujas imagens estão no banco de dados?

- Quais são as salvaguardas em vigor para proteger a segurança do banco de dados?
- Quem tem acesso ao banco de dados?
- Existe uma política de *login* para documentar quem acessa o banco de dados, quando e como?⁸⁹
- Existe base jurídica para o processamento das imagens no banco de dados de forma a extrair as características faciais das pessoas nele contidas? E uma base legal que autorize a busca na TRF em relação a uma imagem de referência?
- A pessoa na imagem de consulta não está no banco de dados? (Se esse for o caso, todas as correspondências estimadas retornadas pelo sistema estarão incorretas).
- Quando a imagem de uma pessoa deixa de ser necessária para o propósito inicial de sua inclusão no banco de dados, a imagem é excluída de maneira tempestiva e efetiva?
- Existe um mecanismo de supervisão robusto e efetivo que serve de salvaguarda aos direitos fundamentais das pessoas cujas imagens estão no banco de dados?

LISTAS DE VIGILÂNCIA

Listas de vigilância são bancos de dados de referência utilizadas na aplicação em tempo real da TRF, a qual envolve a comparação entre um feed de vídeo ao vivo de rostos e uma lista de vigilância predeterminada com o objetivo de encontrar uma possível correspondência que gere um alerta para a polícia ou para a pessoa usuária do sistema agir instantaneamente, quase instantaneamente ou sem atraso significativo. As questões que precisam ser consideradas com relação a quem incluir ou não em uma lista de vigilância são as mesmas que precisam ser avaliadas quando se opta ou compila imagens de consulta e bancos de dados de referência. Para cada uso em tempo real da TRF, perguntas adicionais precisam ser feitas:

89 Davis, N, Perry, L & Santow, E, *Facial Recognition Technology: Towards a model law*, Human Technology Institute, The University of Technology, setembro 2022, <https://www.uts.edu.au/sites/default/files/2022-09/Facial%20recognition%20model%20law%20report.pdf>.

- Qual é a base legal para incluir a imagem de uma pessoa em uma lista de vigilância em cada uso específico de TRF em tempo real?
- De onde a autoridade de aplicação da lei obterá as imagens para incluir em uma lista de vigilância?
- Essas imagens deverão ter qualidade ou tempo determinado?
- Por quanto tempo uma imagem pode ficar em uma lista de vigilância?
- Como uma pessoa pode ser removida de uma lista de vigilância?
- Quais critérios específicos devem ser atendidos antes que a imagem de uma pessoa seja incluída em uma lista de vigilância ou antes que qualquer lista de vigilância seja criada?⁹⁰
- Quais protocolos devem ser seguidos antes que a imagem de uma pessoa seja adicionada?
- Quem pode solicitar e conceder permissão para que a imagem de uma pessoa seja adicionada a uma lista de vigilância em cada implementação?
- Como a autoridade de aplicação da lei avaliará e demonstrará que a criação de uma lista de vigilância, ou a inclusão de uma pessoa na lista, é necessária e proporcional?
- Como uma pessoa saberá se está em uma lista de vigilância?
- Que recurso estará disponível para essa pessoa caso ela seja indevidamente incluída em uma lista de vigilância?
- Que recurso estará disponível para essa pessoa caso ela seja indevidamente identificada e submetida a uma ação devido a um erro na criação da lista de vigilância?
- Os detalhes específicos de como e quando uma pessoa é incluída em uma lista de vigilância serão disponibilizados ao público para cada implementação da TRF em tempo real?

90 Radiya-Dixit, E, *A Sociotechnical Audit: Assessing Police Use of Facial Recognition*, Cambridge: Minderoo Centre for Technology and Democracy, 1º de outubro de 2022, <https://www.mctd.ac.uk/wp-content/uploads/2022/10/MCTD-FacialRecognition-Report-WEB-1.pdf>.

POTENCIAL EDIÇÃO/ADULTERAÇÃO DE FOTOGRAFIAS

Há casos documentados de autoridades policiais que editam imagens de consulta antes de as utilizar em uma busca na TRF retrospectiva, colocando em considerável risco a confiabilidade do resultado e, portanto, comprometendo os direitos de indivíduos posteriormente detidos com base nos resultados dessa busca. Uma pesquisa feita nos Estados Unidos mostra que a Divisão de Identificação Facial do Departamento de Polícia de Nova York, que tem permissão para editar imagens de consulta, utiliza ferramentas para praticar ações, tais como: remover expressão facial, inserir olhos de uma pessoa diferente na imagem e/ou usar uma ferramenta para criar uma bochecha ou queixo, caso o indivíduo não esteja completamente visível.⁹¹ Uma situação alarmante foi a de policiais que, após rodarem uma imagem pixelada de CFTV de uma pessoa suspeita de furto em uma loja e sem que fossem identificadas correspondências, decidiram que seria uma boa ideia fazer uma busca utilizando a imagem do ator hollywoodiano Woody Harrelson, porque acharam a pessoa suspeita parecida com ele. Posteriormente, prenderam um homem, “que acreditavam ser uma correspondência – não com Harrelson, mas com o indivíduo suspeito cuja foto não havia produzido resultado possível”.⁹² Em outras partes dos EUA, a polícia foi flagrada executando buscas na TRF utilizando retratos falados, ou seja, imagens desenhadas à mão ou geradas por computador baseadas em descrições feitas por testemunhas oculares.⁹³ As perguntas a serem consideradas incluem:

- Com que fundamento essa edição pode ser justificada?
- Considerando as preocupações significativas relativas a direitos, as forças policiais devem ter permissão para alterar imagens de consulta dessa maneira?
- Deveria haver, no mínimo, uma base jurídica para tal edição?

BUSCA ALGORÍTMICA

Essa etapa envolve o subsistema que compara uma foto de consulta com um banco de dados de imagens – no caso de TRF retrospectiva ou iniciada por pessoa operadora – ou imagens de rostos obtidas de filmagens em vídeos ao vivo com imagens faciais de uma lista de vigilância. Considerando que os algoritmos da

91 Garvie, C, *Garbage In, Garbage Out*, Georgetown Law Center on Privacy and Technology, 2019, <https://www.flawedfacedata.com/>.

92 Ibid.

93 Ibid.

TRF são criados e desenvolvidos por empresas privadas (as quais geralmente não estão abertas a auditorias independentes e/ou avaliações de risco), que eles são comprovadamente enviesados contra qualquer pessoa que não seja um homem branco de meia-idade⁹⁴ e são treinados com o uso de diferentes conjuntos de dados e, provavelmente, produzem resultados distintos dependendo de algoritmos específicos, as questões a seguir devem ser consideradas:

- Que medidas a polícia tomou para auditar de forma independente a veracidade das alegações do fornecedor sobre o sistema de TRF e seu respectivo algoritmo?⁹⁵
- Direitos de propriedade impediram que a polícia obtivesse informações sobre como o algoritmo funciona e os riscos que ele apresenta?⁹⁶
- Existe um mecanismo legal para obrigar fornecedores a publicar e/ou divulgar determinadas informações sobre seus algoritmos?
- Antes de qualquer uso de TRF, a polícia faz avaliações regulares do impacto sobre os direitos fundamentais e demonstra que tal uso pela segurança pública não tem um efeito prejudicial sobre os direitos do público e/ou que não tem o potencial de produzir efeitos discriminatórios?
- Os resultados dessas avaliações são publicados?
- Quais medidas a polícia tomou para mitigar os riscos impostos às pessoas desproporcionalmente afetadas pela TRF?
- A polícia avalia e divulga a demografia do banco de dados de treinamento subjacente ao algoritmo, de modo a garantir que ele seja representativo da população onde a tecnologia será aplicada?⁹⁷

94 81% of “suspects” flagged by Met’s police facial recognition technology innocent, independent report says, Sky News, 4 de julho de 2019, <https://news.sky.com/story/met-polices-facial-recognition-tech-has-81-error-rate-independent-report-says-11755941>. Veja também Fussey, P & Murray, D, *Independent Report on the London Metropolitan Police Service’s Trial of Live Facial Recognition Technology*, Human Rights Centre, University of Essex, julho 2019, <https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf>. Veja também Buolamwini, J & Gebru, T, “Gender Shades: Intersectional Accuracy Disparities em Commercial Gender Classification”, *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, 2018, <https://proceedings.mlr.press/v81/buolamwini18a.html>.

95 Radiya-Dixit, E, *A Sociotechnical Audit: Assessing Police Use of Facial Recognition*, Cambridge: Minderoo Centre for Technology and Democracy, 1º de outubro de 2022, <https://www.mctd.ac.uk/wp-content/uploads/2022/10/MCTD-FacialRecognition-Report-WEB-1.pdf>.

96 Lynch, N; Campbell, L; Purshouse, J; Betkier, M, *Facial Recognition Technology in New Zealand: Towards a Legal and Ethical Framework*, Law Foundation of New Zealand, 30 de novembro de 2020, <https://doi.org/10.25455/wgtn.17204078.v1>.

97 Ibid.

- A polícia publica os dados demográficos das pessoas que são submetidas a buscas na TRF?⁹⁸
- A polícia publica os dados demográficos de prisões, abordagens policiais e revistas, além de outros desdobramentos resultantes do uso da TRF?⁹⁹
- A polícia tem mecanismos de responsabilização em vigor para lidar com identificações incorretas quando elas ocorrem, incluindo um para notificar pessoas afetadas e oferecer reparação?
- Que mudanças a polícia faz em seus protocolos, bancos de dados e sistemas quando toma conhecimento de que uma identificação incorreta ocasionou abordagem policial e revista, prisão, detenção ou acusação de uma pessoa?
- A polícia tem mecanismos de responsabilização em vigor para tomadas de decisões automatizadas injustas e infundadas quando elas ocorrem por conta da TRF, incluindo um mecanismo para notificar as pessoas afetadas e oferecer reparação?

A “salvaguarda” de HITL é realmente uma salvaguarda?

Forças de segurança pública que desejam aliviar as preocupações relativas à identificação incorreta pela TRF e às violações de direitos humanos costumam dizer que não há nada com que se preocupar, pois haverá uma proteção “humana no circuito” (*human-in-the-loop*, no original em inglês) frente a qualquer decisão automatizada e que sempre haverá alguém revisando a lista de pessoas candidatas antes de qualquer outra medida ser tomada, independentemente de o uso ser em tempo real ou retrospectivo. Entretanto, nem sempre um ser humano – seja agente policial ou testemunha ocular – corrigirá uma “correspondência” incorreta da TRF. Michael Oliver, que tem o rosto tatuado, foi preso e detido indevidamente por quase três dias em Detroit, nos Estados Unidos, depois que uma busca na TRF o exibiu como suspeito e uma testemunha ocular o escolheu em um alinhamento de fotografias, mesmo a foto da pessoa suspeita não tendo nenhuma tatuagem no rosto.¹⁰⁰ Com relação às revisões humanas, as questões a seguir devem ser consideradas:

98 Ibid.

99 Ibid.

100 “Faulty Facial Recognition Led to His Arrest – Now He’s Suing”, *Vice*, setembro 2020, <https://www.vice.com/en/article/bv8k8a/faulty-facial-recognition-led-to-his-arrestnow-hes-suing>.

- Qual é a função da pessoa responsável pela revisão no uso da TRF retrospectiva?
- Qual é o papel de uma pessoa responsável pela revisão no uso da TRF ao vivo?
- Que pesquisa foi executada pela segurança pública para demonstrar a precisão das pessoas responsáveis pela revisão?¹⁰¹
- A que treinamento específico as pessoas responsáveis pela revisão foram submetidas em relação às diferentes formas de uso?
- Quais informações adicionais as pessoas responsáveis pela revisão têm sobre um caso ou indivíduos antes ou quando estão revisando uma pessoa candidata?
- A pessoa responsável pela revisão é independente do processo de investigação do suposto delito no centro da pesquisa da TRF?
- Quais medidas são tomadas e/ou que salvaguardas estão em vigor para lidar com os preconceitos das próprias pessoas responsáveis pela revisão?¹⁰²
- A polícia tem mecanismos de responsabilização em vigor para lidar com identificações incorretas após uma revisão humana, incluindo algo para notificar as pessoas afetadas, e oferecer reparação?
- Que mudanças a polícia implementa em seus protocolos com relação à pessoa responsável pela revisão após uma identificação incorreta levar uma pessoa a ser presa, detida ou acusada?
- Os protocolos de “revisão humana” levam em consideração e refletem os diferentes riscos aos direitos que podem se originar do uso em tempo real e retrospectivo da TRF?
- Uma testemunha ocular é informada sobre o uso da TRF pela polícia?

101 Radiya-Dixit, E, *A Sociotechnical Audit: Assessing Police Use of Facial Recognition*, Cambridge: Minderoo Centre for Technology and Democracy, 1º de outubro 2022, <https://www.mctd.ac.uk/wp-content/uploads/2022/10/MCTD-FacialRecognition-Report-WEB-1.pdf>.

102 Tais como o viés de confirmação, que se refere à confirmação das crenças pessoais da pessoa revisora, e o viés de automação, que implica uma tendência a confiar na legitimidade das informações por terem sido produzidas pela tecnologia.

Policiais recebem capacitação adequada em TRF para mitigar os riscos?

Colocar uma ferramenta poderosa como a TRF nas mãos de agentes policiais que não receberam capacitação para utilizá-la e compreendê-la, combinado com a ausência de qualquer tipo de supervisão e avaliação independente desse uso, só poderia servir para consolidar e expandir ainda mais os problemas derivados do uso da TRF na segurança pública. Foi relatado que, embora o *Federal Bureau of Investigation* (FBI) tenha feito dezenas de milhares de buscas na TRF nos últimos anos, apenas 5% de seu quadro, em que 200 agentes fazem uso da TRF, participaram de curso próprio sobre como usar essa tecnologia.¹⁰³ Ainda não se sabe ao certo qual treinamento é dado em outros países onde ela é empregada pela polícia. No âmbito da supervisão, no Reino Unido, existe a figura da pessoa Oficial de Câmeras de Vigilância. Já nos Estados Unidos, foram feitos pedidos para o estabelecimento de um órgão regulador para supervisionar a gestão e a regulamentação de tecnologias complexas, como a TRF, de forma similar a como a indústria farmacêutica é regulamentada,¹⁰⁴ e/ou para a criação de um órgão independente encarregado de certificar as tecnologias de policiamento antes delas serem implementadas.¹⁰⁵ As questões a serem consideradas incluem:

- O que implicaria um curso de capacitação eficiente, com foco em direitos humanos, sobre a utilização da TRF na segurança pública?
- Policiais devem receber um certificado ou credenciamento antes de obterem autorização para utilizar a TRF?
- Essa capacitação seria suficiente para atenuar as problemáticas referentes aos direitos humanos?
- Os detalhes dessa capacitação devem ser publicizados?
- Como seria um órgão/mecanismo de supervisão eficiente?
- Que poderes esse órgão deveria ter para torná-lo eficiente e responsável?

103 Johnson, K, *FBI Agents Are Using Face Recognition Without Proper Training*, Wired, setembro 2023, <https://www.wired.com/story/fbi-agents-face-recognition-without-proper-training/>.

104 Learned-Miller, E, Ordóñez, V, Morgenstern, J, e Buolamwini, J, *Facial Recognition Technologies in the Wild: A Call for A Federal Office*, 29 de maio de 2020, https://assets.website-files.com/5e027ca188c99e3515b404b7/5ed1145952bc185203f3d009_FRTsFederalOfficeMay2020.pdf.

105 Friedman, B, Heydari, F, Isaacs, M & Kinsey, K, "Policing Police Tech: A Soft Law Solution", *Berkeley Technology Law Journal*, Vol. 37, 2022, Disponível em SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4095484.

- A existência de um órgão ou mecanismo de supervisão seria suficiente para reduzir as preocupações?
- Existe o perigo de que os pedidos por capacitação e mecanismos de supervisão acabem legitimando o uso da TRF na segurança pública e funcionem apenas como uma burocracia?

As comunidades afetadas de forma desproporcional são consultadas da maneira adequada?

Uma questão importante a respeito do uso da TRF na segurança pública é que as comunidades afetadas de maneira desproporcional por essa tecnologia propensa a erros não são consultadas de forma transparente. Elas não sabem como essa ferramenta funciona e como ela afeta o sistema de justiça criminal, a vida e os direitos fundamentais das pessoas. As questões a serem consideradas incluem:

- A consulta pública e o envolvimento das comunidades desproporcionalmente afetadas pelo uso da TRF deveriam ser compulsórios?
- Como essa consulta poderia ser eficiente?
- A consulta compulsória deveria incluir a apresentação de informações detalhadas ao público sobre a tecnologia específica empregada pela polícia, a forma como ela é utilizada, como os diferentes subsistemas e algoritmos funcionam, detalhes das bases de dados em que ela foi treinada e a produção de uma avaliação de impacto sobre a proteção de dados pessoais e outra sobre direitos fundamentais?
- A consulta deveria incluir detalhes de como as imagens de consulta são escolhidas e como os bancos de dados de referência e as listas de vigilância são criados?
- A consulta deveria ser feita toda vez que a polícia alterar suas políticas ou o uso de tecnologias específicas?

As pessoas são informadas de que estão sendo submetidas à TRF?

Outro problema significativo de transparência é que as pessoas simplesmente não sabem que a TRF está sendo usada no ambiente. Por exemplo, no Reino Unido, quando há uso de TRF ao vivo, a polícia deve alertar o público sobre isso. Todavia, a divulgação geralmente acontece nas mídias sociais, maneira insuficiente de alertar sobre tal uso, considerando que muitas pessoas não as acessam e aquelas que o fazem podem não ter visto tal publicação. A polícia no Reino Unido também deve sinalizar a área física onde há uso da TRF em tempo real, para que o público possa evitar a região, caso não deseje que seus dados biométricos sejam tratados.

No entanto, as sinalizações costumam ser instaladas muito perto da área, de modo que, muitas vezes, acaba ficando muito em cima ou muito complicado evitá-la. As questões a serem consideradas incluem:

- A legislação de proteção de dados na União Europeia estabelece que os indivíduos têm o direito de saber sobre o tratamento de seus dados pessoais. Por exemplo, no caso de circuito fechado de televisão, pessoas controladoras de dados devem dispor de sinalizações indicando o uso de CFTV, e tais placas devem incluir, no mínimo, as seguintes informações:
 - A identidade e as informações de contato da pessoa controladora de dados;
 - Os dados de contato da pessoa encarregada, caso tenha sido designada;
 - As finalidades para as quais os dados pessoais são tratados;
 - O propósito e a base jurídica do tratamento;
 - Quaisquer terceiros a quem os dados pessoais possam ser divulgados;
 - As medidas de segurança referentes às imagens e gravações de CFTV;
 - O período de retenção de imagens e gravações de CFTV; e
 - A existência de direitos de titulares dos dados e de apresentar uma denúncia à autoridade local de proteção de dados.
- A sinalização poderia resolver de alguma forma a questão da transparência?
- Quão efetiva e amplamente aplicada já é a política de sinalização de CFTV?

As informações técnicas sobre o sistema foram divulgadas às pessoas acusadas com base na TRF?

Um terceiro problema de transparência que apareceu nos Estados Unidos é que, quando a TRF é empregada em investigações que levam à prisão alguém e essa pessoa acusada é levada aos tribunais, a equipe de defesa tem sido impedida de acessar qualquer informação sobre como o sistema operou, sua propensão a erros ou vieses e, até mesmo, o nome do próprio sistema.¹⁰⁶ Em uma vitória significativa da transparência, em junho de 2023, em um dos primeiros casos desse tipo, a Divisão de Apelação do Tribunal Superior de Nova Jersey, ao observar que a tecnologia de reconhecimento facial é “nova e não testada”, decidiu no caso *State of New Jersey vs. Francisco Arteaga*¹⁰⁷ que as seguintes informações, conforme solicitado pela defesa, tinham que ser divulgadas ao réu:

1. O nome e o fabricante do software de reconhecimento facial utilizado para conduzir a busca nesse caso, bem como o(s) algoritmo(s), número(s) de versão e o(s) ano(s) de desenvolvimento;
2. O código-fonte do(s) algoritmo(s) de reconhecimento facial;
3. Uma lista das medições, pontos nodais ou outras marcas de identificação exclusivas usadas pelo sistema na criação de vetores de características faciais, incluindo, caso essas marcas tenham pesos diferentes, as pontuações dadas a cada uma;
4. As taxas de erros do sistema de reconhecimento facial utilizado, incluindo as de falsa aceitação e falsa recusa (também denominadas taxas de falso positivo ou de correspondência e taxas de falso negativo ou de não correspondência), bem como a documentação sobre como as taxas de erros foram calculadas, incluindo se refletem condições operacionais ou de teste;
5. O desempenho do(s) algoritmo(s) utilizado(s) nos Testes de Fornecedores de TRF aplicáveis do Instituto Nacional de Normas e Tecnologia dos Estados Unidos (NIST, na sua sigla em inglês) se disponível;

¹⁰⁶ *New Jersey Appellate Division One of First Courts in Country to Rule on Constitutional Rights Related to Facial Recognition Technologies*, ACLU, junho de 2023, <https://www.aclu-nj.org/en/press-releases/new-jersey-appellate-division-one-first-courts-country-rule-constitutional-rights>.

¹⁰⁷ Superior Court of New Jersey Appellate Division Docket No. A-3078-21 State of New Jersey vs. Francisco Arteaga, decisão de 7 de junho de 2023, <https://law.justia.com/cases/new-jersey/appellate-division-published/2023/a-3078-21.html>.

6. A cópia original da foto “probatória” ou de consulta enviada;
7. Todas as cópias editadas da foto “probatória” ou de consulta inseridas no sistema de reconhecimento facial, observando, se aplicável, qual cópia editada produziu a lista de pessoas candidatas na qual constava a ré e uma lista de edições, filtros ou quaisquer outras modificações feitas nessa foto;
8. Uma cópia da foto do banco de dados correspondente à foto “probatória” ou de consulta, junto com a porcentagem de correspondência, o número de classificação ou a pontuação de confiança atribuída à foto na lista de pessoas candidatas pelo sistema de reconhecimento facial;
9. Uma lista ou descrição do número de classificação ou das pontuações de confiança produzidas pelo sistema, incluindo a escala na qual o sistema se baseia (por exemplo, porcentagem, logarítmica ou outra);
10. Uma cópia da lista completa de pessoas candidatas retornada pelo sistema de reconhecimento facial ou das 20 primeiras da lista se houver mais de 20, em ordem de classificação, e incluindo a porcentagem de correspondência ou a pontuação de confiança atribuída à cada foto pelo sistema de reconhecimento facial;
 - a. Uma lista dos parâmetros utilizados do banco de dados, incluindo:
 - b. Quantas fotos há no banco de dados;
 - c. Como as fotos foram obtidas;
 - d. Por quanto tempo as fotos são armazenadas;
 - e. Com que frequência limpezas são feitas no banco de dados;
 - f. Qual é o processo para uma pessoa ser removida do banco de dados;
 - g. Quem tem acesso ao banco de dados;
 - h. Como o banco de dados é mantido;
 - i. A política de privacidade do banco de dados;
11. O relatório produzido por pessoa analista ou técnica que operou o software de reconhecimento facial, incluindo quaisquer anotações feitas sobre a possível correspondência em relação a quaisquer outros indivíduos na lista de pessoas candidatas; e
12. O nome e as capacitações, certificações ou qualificações, da pessoa analista que executou a busca no sistema de reconhecimento facial.



A lista de itens acima é uma compilação útil de detalhes a serem considerados quando buscamos transparência no uso da tecnologia de reconhecimento facial pelas forças de segurança pública. Pontos semelhantes devem ser divulgados no âmbito do uso em tempo real e, especificamente, os parâmetros de como, por que e quando uma lista de vigilância foi criada e como uma pessoa foi incluída nela.

Princípios da INCLO sobre o uso de TRF na aplicação da lei

Nossos princípios não endossam o uso da TRF pela polícia. Ao invés disso, eles destacam padrões mínimos de responsabilização e mitigação de danos quando eles existem. Nossos princípios servem como uma ferramenta para formar um consenso sobre os graves riscos apresentados por essa tecnologia e a urgente necessidade de restrições rigorosas e proibições expressas.

Estes princípios foram concebidos para abordar:

- O uso direto da TRF na aplicação da lei;
- Qualquer uso da TRF para fins de aplicação da lei feito por uma autoridade de outra jurisdição; e
- Qualquer uso da TRF para fins de aplicação da lei feito por terceiro.

OS PRINCÍPIOS

1. Autoridades de aplicação da lei não devem fazer uso da TRF sem uma base jurídica específica.
2. Avaliações de impacto sobre os direitos fundamentais devem ser compulsórias.
3. Avaliações de impacto sobre os direitos fundamentais devem ser independentes da avaliação do fornecedor.
4. Não deve haver aquisição ou implementação de uma nova TRF sem a garantia de independência futura em relação ao fornecedor.
5. Todas as versões de todas as avaliações devem ser disponibilizadas ao público antes da implementação da tecnologia de reconhecimento facial.
6. Consulta pública deve ser obrigatória.
7. Autoridades devem informar ao público como as imagens analisadas são utilizadas em uma operação de TRF.
8. As especificações técnicas de qualquer sistema de TRF devem ser divulgadas ao público antes da implementação.
9. TRF ao vivo é proibida.
10. Autorização judicial prévia deve ser compulsória.
11. Autoridades devem documentar cada busca na tecnologia de reconhecimento facial retrospectiva ou iniciada por pessoa operadora.
12. Um resultado de TRF por si só não constitui base suficiente para interrogatório, prisão ou detenção.
13. Deve ser compulsória a divulgação dos detalhes de operações de tecnologia de reconhecimento facial feitas contra indivíduos.
14. Qualquer identificação incorreta de uma pessoa pela tecnologia deve ser notificada.

15. A apresentação de relatórios anuais pelas autoridades sobre casos de identificação incorreta deve ser obrigatória.
16. Um órgão independente para a supervisão da TRF deve ser estabelecido antes da implementação dessa tecnologia.
17. Esse órgão deve publicar relatórios anuais.
18. Avaliações de impacto devem ser disponibilizadas ao órgão supervisor antes da implementação do sistema.

Uso da TRF

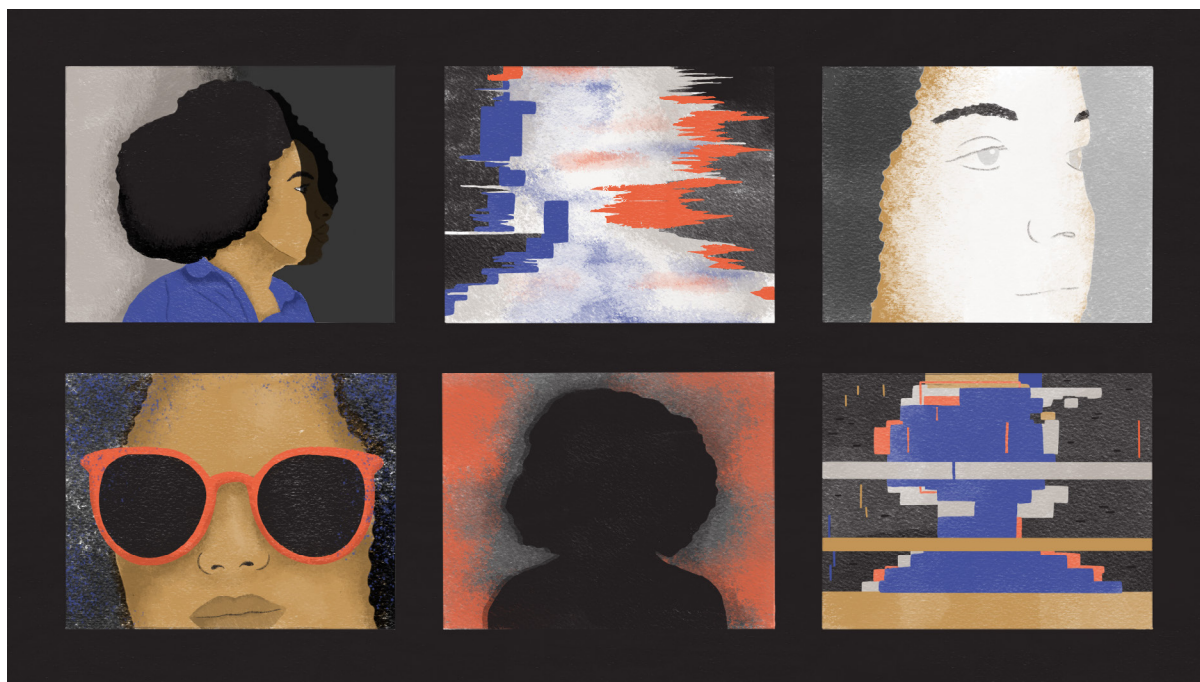
PRINCÍPIO 1: As autoridades de aplicação da lei não devem utilizar TRF ou coletar, armazenar, usar ou divulgar informações pessoais relacionadas a qualquer uso dessa tecnologia, a menos que tais ações sejam autorizadas por lei específica.

Essa lei deve especificar as circunstâncias estritas sob as quais o uso da TRF pode ser autorizado, bem como deve ser redigida de modo a garantir que pessoas com cidadania ou residência no país possam entender e prever as condições e circunstâncias exatas em que ela está ou será implementada.

A lei também deve declarar explicitamente que a TRF nunca deve ser usada para:

- Identificar denunciante, jornalistas ou fontes jornalísticas;
- Identificar pessoas que não tenham vínculo probatório, direto ou indireto, com um crime;
- Categorizar pessoas por uma característica protegida ou pontuação social;
- Tentar inferir as emoções ou intenções de uma pessoa;
- Tentar prever as ações futuras de uma pessoa;
- Identificar manifestantes ou coletar informações sobre pessoas que participam de reuniões pacíficas; ou
- Identificar pessoas dentro ou ao redor de seções eleitorais.

Qualquer uso de tecnologia de reconhecimento facial também deve estar em plena conformidade, no mínimo, com os princípios a seguir:



BASE LEGAL

PRINCÍPIO 2: Qualquer base legal para o uso da TRF por uma autoridade de aplicação da lei deve incluir um dever intransferível, por sua parte, de executar uma série de avaliações de impacto no que tange a todos os direitos fundamentais, antes da implantação de qualquer nova forma de uso da TRF. Tais avaliações devem incluir, entre outros, o exame do impacto sobre os direitos fundamentais e outra da necessidade absoluta e da proporcionalidade do uso da TRF.

A primeira forma de avaliação deve identificar, examinar e abordar os efeitos adversos de uma implementação da tecnologia de reconhecimento facial aos direitos humanos. Essa avaliação deve descrever explicitamente:

- Os parâmetros específicos de uso da TRF, inclusive se ela é retrospectiva ou iniciada por pessoa operadora, quem a utilizará, contra quem ela será usada, onde será usada, por qual motivo e como ela será usada;
- Os direitos afetados, principalmente os direitos à privacidade, à proteção de dados pessoais, à liberdade de expressão e reunião pacífica e à não discriminação;
- A natureza e a extensão dos riscos a esses direitos;
- Como cada um desses riscos será atenuado;

- Uma justificativa comprovada de como e por qual motivo os benefícios da implementação prevalecerão sobre os impactos a direitos; e
- Recurso disponível para alguém identificado erroneamente¹⁰⁸ ou cujos dados biométricos tenham sido tratados, quando não deveriam ter sido.

Qualquer avaliação da necessidade absoluta e da proporcionalidade do uso da TRF deve detalhar a necessidade da sua implementação para um objetivo expresso e legítimo, além de incluir:

- Evidência do problema abordado por meio da implementação da TRF;
- Uma explicação baseada em evidências sobre como a implementação da tecnologia será realmente eficaz para sanar o problema; e
- Uma demonstração de por que medidas existentes e menos intrusivas, que não incluem a TRF, não seriam suficientes para atender ao objetivo legítimo.

Uma autoridade não deve implantar nenhuma nova forma de uso de tecnologia de reconhecimento facial se uma avaliação de impacto determinar que o sistema e a demografia do conjunto de dados de treinamento do algoritmo dele produzem, direta ou indiretamente, resultados enviesados contra qualquer característica protegida – incluindo raça, gênero ou idade – em um ambiente operacional.

Uma autoridade de aplicação da lei não deve implantar nenhuma nova forma de uso da TRF se ela não for estritamente necessária ou proporcional.

Essas avaliações serão feitas anualmente para cada tecnologia de reconhecimento facial implementada. Se um sistema de TRF for reprovado por qualquer uma dessas avaliações, ele será desativado.

IMPOSSIBILIDADE DE EXCLUSÃO DA BASE LEGAL

PRINCÍPIO 3: As obrigações das autoridades de aplicação da lei dispostas no Princípio 2 se aplicam independentemente da existência de mecanismos legais explícitos que exijam que fornecedores de sistemas de TRF publiquem ou divulguem certas informações sobre seus algoritmos e dados de origem.

¹⁰⁸ “Identificação incorreta”, para os fins destes princípios, significa a seleção incorreta de alguém em uma lista de pessoas candidatas por pessoa revisora humana na TRF, busca essa que precede uma ação decorrente da aplicação da lei contra a pessoa candidata – como, entre outras coisas, ser inserida em um banco de dados ou lista de referência, ser interrogada, presa, detida ou processada.

AVALIAÇÃO DO RISCO DE DEPENDÊNCIA DE FORNECEDORES

PRINCÍPIO 4: As autoridades de aplicação da lei não devem adquirir ou implantar qualquer nova TRF sem uma avaliação prévia do risco de dependência de seus fornecedores, incluindo, entre outros:

- Uma avaliação de interoperabilidade e compatibilidade com os sistemas existentes;
- Uma avaliação da propriedade e da portabilidade dos dados, avaliando os custos de sua migração para um sistema de outro fornecedor;
- Uma comparação dos sistemas, componentes e algoritmos proprietários com as alternativas abertas existentes, se houver; e
- Uma estratégia para mudança de fornecedor, se necessário, incluindo os custos previsíveis para tal.

A aquisição de sistemas de tecnologia de reconhecimento facial deve favorecer ofertas de fornecedores que maximizem padrões abertos e interoperabilidade; e minimizem componentes proprietários.

É dever do fornecedor explicar, em linguagem simples, como um sistema de TRF específico funciona, e é igualmente dever das autoridades de aplicação da lei entender completamente como a tecnologia e o sistema operam.

Essa avaliação será feita anualmente para cada sistema implementado. Se o risco de dependência do fornecedor vier a aumentar, serão tomadas medidas para reduzir a dependência de terceiros, incluindo, se necessário, a desativação da tecnologia.

PUBLICAÇÃO DOS RESULTADOS DA AVALIAÇÃO DE RISCO

PRINCÍPIO 5: Todas as versões de todas as avaliações, incluindo as de necessidade absoluta e de proporcionalidade e as de impacto aos direitos humanos,¹⁰⁹ feitas antes da implementação de qualquer TRF, bem como seus resultados, devem ser disponibilizadas ao público antes da implementação da tecnologia, de modo a maximizar o alcance da divulgação, especialmente entre as pessoas com maior probabilidade de serem submetidas ao uso específico da TRF.

109 Essas avaliações devem ser feitas de acordo com definições e padrões internacionais.

CONSULTA PÚBLICA

PRINCÍPIO 6: Antes da implementação de um sistema de TRF por qualquer autoridade de aplicação da lei, deve-se fazer consultas públicas relevantes, incluindo nelas integrantes de comunidades que serão afetadas de maneira desproporcional pelo seu uso. Essas consultas devem incluir o compartilhamento de:

- Detalhes sobre como a tecnologia e o sistema operam de forma esclarecedora e acessível;
- Detalhes sobre os parâmetros do uso esperado pelas autoridades dentro da respectiva jurisdição, incluindo as condições estritas sob as quais o sistema é usado;
- Detalhes das imagens utilizadas como imagens de consulta e de quaisquer dispositivos por meio dos quais elas são capturadas;
- Detalhes das imagens que constam em todos os bancos de dados de referência;
- Dados demográficos das pessoas que se espera que sejam submetidas ao uso do sistema;
- Todas as avaliações de impacto por escrito exigidas por estes princípios; e
- Detalhes das salvaguardas em vigor para evitar o uso arbitrário do sistema.

Uma consulta pública relevante também requer:

- A publicação de todas as contribuições feitas pelo público, especialistas, sociedade civil e demais agentes durante o processo de consulta;
- A concessão de tempo suficiente para que as autoridades reflitam sobre essas contribuições antes de tomar qualquer decisão referente à implementação; e
- O estabelecimento de mecanismos e garantias para assegurar que o processo de consulta possa influenciar, moldar e até mesmo cancelar a implementação.

IMAGEM DE CONSULTA

PRINCÍPIO 7: As autoridades de aplicação da lei devem usar as ferramentas disponíveis para tornar público todos os detalhes de como as imagens de consulta

são usadas em uma operação de TRF, de maneira acessível e inteligível, on-line e off-line. Tais detalhes devem identificar, entre outros:

- Os critérios necessários para que a imagem de uma pessoa se torne uma imagem de consulta;
- As fontes das imagens de consulta;
- O período em que essas imagens de consulta são retidas antes de serem destruídas;
- A base legal para obter, reter e tratar as imagens de consulta; e
- A informações de contato do órgão supervisor (consulte o Princípio 16) designado para proteger os direitos fundamentais das pessoas cujas imagens são usadas em uma busca na TRF.

ESPECIFICAÇÕES TÉCNICAS E POLÍTICAS DIVULGADAS AO PÚBLICO

PRINCÍPIO 8: Antes da implementação de qualquer tecnologia de reconhecimento facial por uma autoridade de aplicação da lei, ela deve disponibilizar ao público, de forma clara e inteligível, as especificações técnicas detalhadas dos sistemas que planeja utilizar. Esses detalhes devem incluir, entre outros:

- Uma descrição detalhada de todos os componentes de hardware e software (nome e fabricante, número da versão do algoritmo e ano de desenvolvimento) a serem utilizados no sistema. Isso inclui servidores, bancos de dados, equipamentos de rede, câmeras e quaisquer softwares ou serviços de terceiros integrados ao sistema;
- Um detalhamento do sistema em seus vários subsistemas e módulos, descrevendo a funcionalidade e a finalidade de cada parte. Devem ser incluídos o algoritmo principal de reconhecimento facial e os sistemas auxiliares, tais como pré-tratamento de imagens, criptografia de dados e interfaces da pessoa usuária;
- Uma representação visual do projeto e da arquitetura do sistema, ilustrando como os dados são coletados, tratados, armazenados e acessados. Devem ser incluídos os pontos de entrada de dados, as etapas de tratamento, os locais de armazenamento e os processos de recuperação de dados;
- As taxas de erros do sistema de TRF usado, incluindo de falsos positivos e de falsos negativos, bem como a documentação sobre como elas foram

calculadas, inclusive se refletem condições operacionais ou de teste (ambiente controlado) que representam a demografia do local onde a TRF será implementada; e

- Uma lista dos parâmetros utilizados do banco de dados de referência, incluindo:
 1. A base legal e o procedimento interno que devem ser seguidos antes de inserir uma pessoa no banco de dados;
 2. As fontes das imagens do banco de dados;
 3. Quantas imagens há no banco de dados;
 4. Como as imagens são obtidas;
 5. Por quanto tempo as imagens armazenadas são mantidas no banco de dados;
 6. Com que frequência limpezas são feitas no banco de dados;
 7. O processo para as imagens serem removidas do banco de dados;
 8. Quem tem acesso ao banco de dados, quando e sob quais circunstâncias;
 9. Como o banco de dados é mantido;
 10. A identidade da pessoa/unidade responsável pela manutenção e supervisão do banco de dados;
 11. A política de privacidade e proteção de dados para o banco de dados;
 12. Como a autoridade de aplicação da lei avaliará e demonstrará que a criação de um banco de dados de referência, ou a inclusão de uma pessoa nesse banco de dados, é necessária e proporcional?
 13. Os critérios para a inclusão de uma pessoa no banco de dados de referência.

USOS PROIBIDOS

PRINCÍPIO 9: Nenhum sistema de TRF será usado em dados de vídeos ou de imagens em movimento em tempo real ou gravados.¹¹⁰

AUTORIZAÇÃO JUDICIAL PRÉVIA

PRINCÍPIO 10: Agentes de aplicação da lei não terão permissão para utilizar a TRF a menos que haja autorização judicial prévia para tal uso, salvo em casos urgentes devidamente justificados, nos quais a aprovação deverá ser dada por uma pessoa superior hierarquicamente e totalmente independente da investigação. Nesses casos excepcionais, a autorização judicial ainda deverá ser solicitada, sem atraso indevido e, no máximo, 48 horas após o uso.

Qualquer agente de aplicação da lei que conduzir uma busca na TRF retrospectiva deve ser independente da investigação do delito e, caso faça uso dessa tecnologia, ter concluído uma capacitação, a qual será atualizada anualmente.

Esse treinamento deve se concentrar em como utilizar o sistema relevante, em como avaliar os impactos de seu uso aos direitos humanos, em como determinar se ele é estritamente necessário e proporcional e em como estar plenamente em conformidade com a lei que sustenta o uso dessa tecnologia.

REGISTRO DO USO

PRINCÍPIO 11: As autoridades de aplicação da lei devem documentar cada busca na TRF retrospectiva ou iniciada por pessoa operadora e entregar essa documentação trimestralmente ao órgão supervisor. O material incluirá os itens a seguir.

- Para o uso da TRF retrospectiva, uma cópia de qualquer pedido por escrito solicitado para uma busca na tecnologia deve incluir:
 - A data e hora da solicitação;

110 Como exemplo de situações cobertas por esse princípio, consulte o Cenário 3, página 43 das diretrizes do Comitê Europeu para a Proteção de Dados (EDPB) [Diretrizes 05/2022 sobre o uso de tecnologia de reconhecimento facial na aplicação da lei](#) e o Artigo 307.5 - 3.2 do [manual sobre o uso de TRF de 2024 do Departamento de Polícia de Detroit \(DPD\)](#), que proíbe o uso de TRF em streaming ao vivo ou vídeos gravados. O manual diz que: “É vedado o uso de Reconhecimento Facial em transmissões ao vivo ou em vídeos gravados. Essa proibição se aplica a todos os vídeos, sejam eles originados a partir do próprio DPD, de pessoas privadas com cidadania ou de qualquer outra fonte”.

- O nome e o cargo de agente de aplicação da lei solicitante e a da delegacia em que tem vínculo;
 - Detalhes de como o pedido foi necessário e proporcional;
 - O motivo do pedido, incluindo, entre outros, qualquer suspeita de crime subjacente;
 - O nome da autoridade judicial a quem o pedido foi solicitado e, em circunstâncias excepcionalmente urgentes, o nome da pessoa responsável de nível hierárquico superior que concedeu a autorização temporária;
 - O resultado da solicitação; e
 - Se a solicitação foi concedida, a composição/conjunto do banco de dados de referência em que a busca foi feita.
- Para uso da TRF retrospectiva e iniciada por pessoa operadora, a documentação deve incluir:
 - O resultado de cada busca, o número de pessoas candidatas retornadas em cada pesquisa e todas as ações da autoridade após cada busca;
 - O nome e o cargo de agente que fez a busca; e
 - Informações agregadas sobre o uso da TRF, incluindo:
 - O número total de pedidos de busca na TRF;
 - O número total de pedidos de busca na TRF que geraram indícios;
 - O número de buscas na TRF seguidas de prisão ou acusações;
 - O número de identificações incorretas da TRF;¹¹¹
 - O número de indivíduos que apareceram como uma provável correspondência no resultado da busca na TRF e que, posteriormente, foram interrogados, presos e/ou acusados;
 - A composição demográfica dos indivíduos nas fotos de consulta por raça e gênero; e

111 Conforme definido na nota de rodapé do Princípio 2.

- Informações sobre o sistema de TRF e o(s) algoritmo(s) utilizado(s), incluindo fornecedor, versão, limite de similaridade e se esse limite foi ajustado para uma busca específica.

Além dos itens acima, todo banco de dados de imagens utilizadas por uma autoridade de aplicação da lei para uma busca na TRF deve ser auditado, no mínimo, uma vez ao ano, a fim de garantir que nele não constem imagens que já não podem ser legalmente mantidas, que não contenha informações incorretas e que não esteja sendo acessado ou utilizado de maneira inadequada ou ilícita.

Essas auditorias também devem ser entregues ao órgão supervisor.

Qualquer informação adicional solicitada pelo órgão supervisor para cumprir suas obrigações legais deve ser fornecida em um prazo razoável.

PROIBIÇÃO DE AÇÃO

PRINCÍPIO 12: Qualquer agente de aplicação da lei não interrogará, prenderá, deterá ou tomará qualquer medida contra um indivíduo com base apenas no uso da TRF. O uso dessa tecnologia não resultará na inclusão de uma pessoa em um alinhamento fotográfico ou presencial. Agentes também não podem tomar medidas com base apenas na combinação de um indício gerado por TRF e de uma testemunha ou um procedimento de identificação confirmatório, como alinhamento fotográfico ou presencial. Um resultado da TRF é apenas um indício investigativo. Ele não constitui uma prova confiável e qualquer resultado deve ser seguido de ações investigativas independentes e confiáveis, antes da adoção de qualquer providência.

OBRIGAÇÃO DE DIVULGAÇÃO

PRINCÍPIO 13: As autoridades de aplicação da lei devem divulgar às pessoas detidas, interrogadas, presas, acusadas ou processadas mediante o uso da tecnologia de reconhecimento facial, bem como a seus representantes legais (se houver), sem restrições, os detalhes da operação da TRF em questão e as especificações técnicas do sistema envolvido na investigação ou no procedimento aplicável. Essas especificações devem incluir todos os detalhes listados no Princípio 8 e:

- O código-fonte de cada algoritmo utilizado;
- Os dados usados para treinamento e ajuste fino do sistema;

- Uma lista de quais medições, pontos nodais ou outras marcas de identificação exclusivas são usadas pelo sistema na criação de vetores de características faciais, incluindo, caso essas marcas tenham pesos diferentes, as pontuações dadas a cada uma;
- Acesso a um ambiente de teste com uma versão executável do software;
- A cópia original da imagem de consulta utilizada;
- Toda e qualquer informação associada à imagem de consulta, incluindo metadados, que estava sob a posse ou foi disponibilizada à pessoa que executou a busca na TRF;
- Detalhes do valor limite do sistema de TRF fixado pelo fabricante (e pela autoridade de aplicação da lei, caso ela altere o valor) para determinar quando o respectivo software indica que ocorreu uma provável correspondência; e
- Especificamente no caso de uso da TRF retrospectiva:
 - Todas e quaisquer cópias editadas da imagem de consulta utilizada, observando, se aplicável, qual delas produziu a lista de pessoas candidatas que incluía a parte acusada, e uma lista de edições, filtros ou quaisquer outras modificações feitas na imagem;
 - Uma cópia da foto do banco de dados correspondente à imagem de consulta, além do número de classificação e das pontuações de similaridade atribuídas à imagem na lista pelo sistema de TRF;
 - Uma lista ou descrição do número de classificação e das pontuações de similaridade produzidas pelo sistema de TRF, incluindo a escala na qual ele se baseia;
 - Uma cópia da lista completa das pessoas candidatas retornada pelo sistema de TRF, em ordem de classificação e incluindo a pontuação de similaridade atribuída à cada imagem por ele;
 - O relatório por escrito produzido pela pessoa que executou a busca na TRF, incluindo a data, o horário da busca e quaisquer anotações feitas sobre a possível correspondência em relação a quaisquer outros indivíduos na lista de pessoas candidatas; e
 - O nome e as capacitações, certificações ou qualificações da pessoa que rodou a imagem de consulta em uma busca na TRF.

RELATÓRIO DE IDENTIFICAÇÕES INCORRETAS

PRINCÍPIO 14: Qualquer identificação incorreta¹¹² de uma pessoa por uma tecnologia de reconhecimento facial deve ser notificada a ela por autoridade. Isso deve acontecer o mais breve possível após a detecção e registro do erro.

APRESENTAÇÃO DO RELATÓRIO ANUAL DE IDENTIFICAÇÕES INCORRETAS

PRINCÍPIO 15: As autoridades de aplicação da lei que usam TRF devem produzir um relatório anual com estatísticas anonimizadas sobre identificações incorretas.

Esses relatórios devem incluir a natureza, a origem, o impacto do erro e todas as medidas tomadas pela autoridade de aplicação da lei em resposta às identificações incorretas relativas ao uso do sistema de TRF, pessoas operadoras que usam o sistema de TRF e os procedimentos e protocolos de uso da TRF. Tais relatórios devem ser disponibilizados ao público e entregues ao órgão supervisor conforme descrito no Princípio 16.

ÓRGÃO SUPERVISOR INDEPENDENTE

PRINCÍPIO 16: Um órgão independente para a supervisão da TRF deve ser estabelecido antes da implementação da tecnologia por uma autoridade de aplicação da lei, a fim de avaliar o uso e sua conformidade, ou não, com os direitos fundamentais, o regulamento aplicável e estes princípios. Esse órgão deve:

- Ser estabelecido e regido por lei;
- Ser separado e independente da pessoa que ocupa o cargo de chefe do Executivo ou do respectivo país;
- Ter os fundos, a competência, a especialização e o quadro de pessoal – equipes jurídica e tecnológica – necessários para cumprir suas responsabilidades;
- Ter acesso livre e imediato às informações necessárias para conduzir seu trabalho;
- Disponibilizar um relatório anual ao público sobre seu trabalho e constatações; e
- Apresentar relatórios anuais ao parlamento do país.

112 Conforme definido na nota de rodapé do Princípio 2.

O órgão supervisor contará com a experiência e os recursos necessários para desenvolver uma metodologia de avaliação do uso da TRF e da conformidade, ou não, com os direitos fundamentais, os regulamentos aplicáveis e estes princípios. Essa metodologia de avaliação deve incluir o conjunto mínimo de requisitos que o sistema deve atender e abaixo do qual ele deverá ser desativado.

O órgão supervisor terá o poder de requerer a desativação do sistema quando não houver cumprimento do conjunto mínimo de requisitos.

RELATÓRIO ANUAL DO ÓRGÃO SUPERVISOR INDEPENDENTE

PRINCÍPIO 17: O órgão supervisor independente dedicado à tecnologia de reconhecimento facial descrito no Princípio 16 publicará relatórios anuais que incluirão todas as avaliações por escrito mencionadas nestes princípios e:

- Uma avaliação detalhada e comentários sobre a base legal determinada para fins de aplicação da lei no que tange ao uso da TRF;
- O número de imagens de consulta individuais utilizadas em buscas na TRF;
- O número de imagens utilizadas em referências e bancos de dados;
- O número de correspondências verdadeiras e falsos positivos por implementação;
- O número de prisões por implementação;
- O número de abordagens policiais e revistas por implementação;
- O número total de pedidos de uso da TRF solicitados;
- O número total de implementações da TRF;
- O número de pedidos solicitados ou buscas feitas a partir de uma autorização judicial;
- O número de pedidos ou implementações feitos com urgência; e
- Os motivos do pedido de busca, incluindo, entre outros, qualquer suspeita de crime subjacente.

AVISO PRÉVIO DAS AVALIAÇÕES DE IMPACTO AO ÓRGÃO DE FISCALIZAÇÃO

PRINCÍPIO 18: Além do Princípio 5, os detalhes e as constatações de cada avaliação de impacto, conforme descrito nos Princípios 2 e 3, devem ser disponibilizados

ao órgão supervisor antes da implementação do sistema para fins de análise das constatações da autoridade de aplicação da lei.

Como usar estes princípios

Conforme demonstrado neste relatório, a implementação generalizada de sistemas de tecnologias de reconhecimento facial na segurança pública tem um impacto negativo sobre a vida e os direitos fundamentais de quem se encontra sob a vigilância dessas tecnologias. Os riscos e danos são expressivos e, na ausência de estruturas legais que prevejam responsabilização e transparência, a busca ou a obtenção de reparação por eles é muito difícil. Pior ainda, nos casos em que as pessoas sequer têm ideia de que a TRF está sendo utilizada contra elas, é praticamente impossível qualquer acesso à reparação.

Diante do uso cada vez mais disseminado da tecnologia de reconhecimento facial pelas forças de segurança pública em todo o mundo, o objetivo deste relatório e dos presentes princípios é ajudar a reduzir esses danos e capacitar a sociedade civil e a população em geral com informações compreensíveis sobre essas tecnologias. Esperamos que essas informações possam ser utilizadas como forma de expressar a oposição à implementação da TRF em seus respectivos países.

Para atingir tais objetivos, acreditamos que os princípios podem ser utilizados das quatro seguintes maneiras:

1. Este documento pode ter a função de ferramenta de advocacy no diálogo e debate sobre a TRF com pessoas formulam leis e políticas públicas. Nossos princípios abrangem o espectro integral da implantação de um sistema de TRF, desde o estabelecimento da base legal que permite seu uso até a implementação prática da TRF na aplicação da lei. Princípios como o 1, 2, 6 e 12 abordam salvaguardas de alto nível essenciais que devem ser incorporadas a qualquer legislação que reja essa tecnologia. Essas disposições legais mínimas são formuladas a partir dos princípios de transparência, participação pública e acesso à reparação que fazem parte do consenso básico de regimes democráticos. Os princípios também fornecem requisitos detalhados, além dos regulamentos básicos, abrangendo diretrizes de desenvolvimento e políticas públicas. Por exemplo, o Princípio 4 descreve o que uma avaliação que visa reduzir a dependência de fornecedor deve incluir. Outro exemplo é o Princípio 13, que explica as informações que devem ser divulgadas às pessoas detidas ou processadas após o uso da TRF.

2. Além da formulação de leis e políticas, esperamos que este documento sirva como uma ferramenta para, durante a interação com as forças de segurança, a definição de protocolos e procedimentos sobre o uso da TRF. Uma das principais preocupações é a interação entre uma TRF, as pessoas que usam ele dentro da segurança pública e os efeitos disso em uma investigação ou processo, com possíveis danos. Por esse motivo, incluímos considerações como o Princípio 11, que expõe a documentação a ser produzida ao usar os sistemas, como registros de uso para facilitar a responsabilização.
3. Os princípios estão enraizados em normas e jurisprudência internacionais de direitos humanos, refletindo a ideia de que naturalmente protegem os direitos fundamentais essenciais às democracias. Por esse motivo, acreditamos que estes princípios podem ser úteis no julgamento de casos contra os danos causados pelos sistemas de TRF nos tribunais. Estes princípios servem como uma ferramenta para contestar o uso dessa tecnologia quando as leis incluem disposições que violam direitos fundamentais ou não apresentam regulamentações específicas para a sua implementação.
4. Por fim, os princípios vêm acompanhados de uma análise e explicação dos danos, riscos e direitos fundamentais afetados devido à implementação da TRF na segurança pública. Listamos, em detalhes, os tipos de perguntas que devem ser feitas às autoridades que a pretendem utilizar. Por fim, esperamos que essas informações ajudem a garantir que qualquer iniciativa de advocacy ou campanha seja fundamentada em um pleno entendimento de todas essas questões. Também desejamos que este documento ajude a sociedade civil a manifestar suas preocupações de forma acessível ao público e que, junto com ela, possa criar e desenvolver campanhas contra o uso da TRF.

Estas são algumas das finalidades que esperamos atender com este relatório e princípios. As questões levantadas aqui não são as únicas que podem ser feitas no debate sobre o uso de sistemas de TRF. De fato, à medida que em que eles se tornarem mais sofisticados, novas considerações surgirão. Entretanto, esperamos que, após a leitura deste documento, as pessoas estejam mais bem informadas sobre os riscos associados à TRF e mais convencidas de que, quando usada pelas forças de segurança pública, não há prova suficiente de seus benefícios às nossas vidas; pelo contrário, muitas indicam uma alta probabilidade de danos.



Considerações finais

As pessoas autoras e colaboradoras deste relatório acreditam que a melhor opção é que a TRF não seja utilizada pela polícia de forma alguma. Conforme explicado exhaustivamente ao longo deste material, os riscos e os prováveis danos relativos ao seu uso superam todos os prováveis benefícios. Os custos substanciais – tanto para a privacidade individual quanto para a confiança da sociedade – tornam injustificável a sua implementação no contexto da segurança pública.