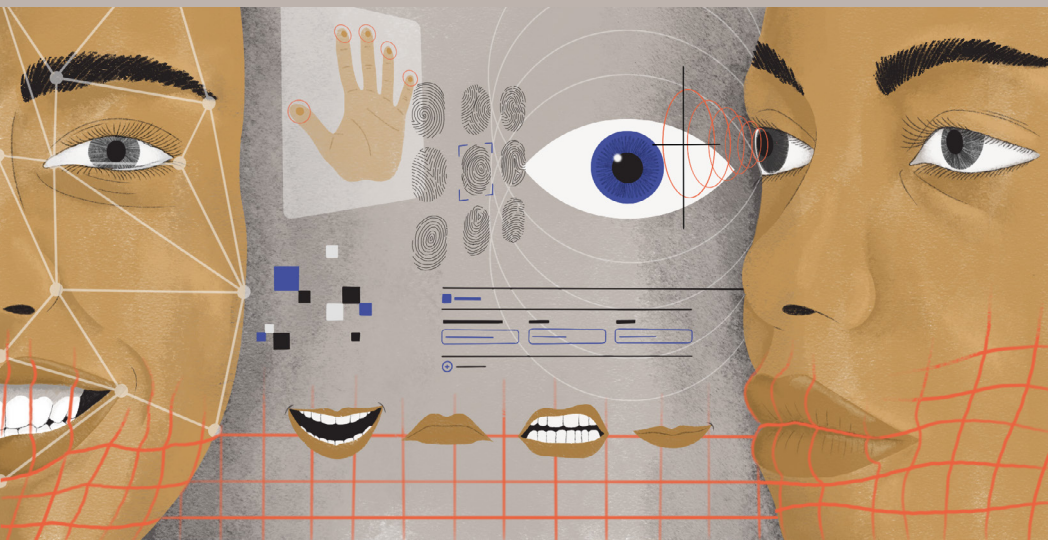


OS PRINCÍPIOS

# 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



## 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 denunciantes, 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 erroneamente<sup>1</sup> 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.

---

<sup>1</sup> “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.

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.

## **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,<sup>2</sup> 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.

## **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;

---

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

- 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.<sup>3</sup>

## **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

---

3 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”.

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;
  - 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;<sup>4</sup>

---

4 Conforme definido na nota de rodapé do Princípio 2.

- 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
- 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 incorreta<sup>5</sup> 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;

---

5 Conforme definido na nota de rodapé do Princípio 2.

- 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.

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.

## **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.

## Notas sobre esta edição em português

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.<sup>1</sup> 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.<sup>2</sup> 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.<sup>3</sup> 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.<sup>4</sup>

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 (INCLLO). A Conectas, organização membro da INCLLO 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 notas reiterando a defesa, feita neste relatório pelas organizações membros da INCLIO, 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.

---

## CONNECTAS 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 Miotto

**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.

## 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 Bussières McNicoll (CCLA), Karim Medhat Ennarah (EIPR), Sehba Meenai (HRLN), Rempport 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.

Leia o relatório na íntegra em [inclo.net/frt](https://inclo.net/frt)