

VIGILÂNCIA

POR LENTES

OPACAS:

mapeamento da transparência

e responsabilização de projetos

de reconhecimento facial no Brasil

cesec



LAPIN

Ficha técnica

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

LABORATÓRIO DE POLÍTICAS PÚBLICAS
E INTERNET - LAPIN

Equipe CESeC

COORDENAÇÃO

Julita Lemgruber
Sílvia Ramos
Pablo Nunes
Mariana Siracusa

Equipe Panóptico

opanoptico.com.br

contatopanoptico@cesecseguranca.com.br

Bluesky e Instagram: @opanopticobr

COORDENADOR

Pablo Nunes

COORDENADORA DE PESQUISA

Thallita G. L. Lima

PESQUISADORAS

Yasmin Rodrigues
Thaís Gonçalves Cruz

VOLUNTÁRIOS DE PESQUISA

Rodrigo Raimundo
Gabriel Leite

COORDENADOR DE COMUNICAÇÃO

Caio Brasil

ASSISTENTE DE COMUNICAÇÃO

Ana Carolina Aguiar

COORDENADOR DE DESIGN

Renato Cafuzo

DESIGNER ASSISTENTE

Fabiano Ferreira

Sobre este relatório

EDIÇÃO E REVISÃO DE TEXTO

Marília Gonçalves

COMPOSIÇÃO DE CAPA

Renato Cafuzo

DIAGRAMAÇÃO

Tomaz Alencar

Como citar o documento

Lima, Thallita. et al. Vigilância por lentes opacas: mapeamento da transparência e responsabilização nos projetos de reconhecimento facial no Brasil. Rio de Janeiro: CESeC, 2024.

Equipe Lapin

lapin.org.br

contato@lapin.org.br

contato@lapin.org.br /lapinbr

DIRETORA-PRESIDENTE

Cynthia Picolo

CONSELHO CONSULTIVO

Alexandra Krastins Lopes
Thiago Moraes

MEMBROS-FUNDADORES E ASSOCIADOS

José Renato Laranjeira
Otávio Mayrink

ASSISTENTE EXECUTIVA

Luaní Marcelli

COORDENADOR DE PROJETOS

Felipe Rocha da Silva

COORDENADORA DE ADVOCACY

Mariana Monteiro Freitas

COORDENADOR GT - VIGILÂNCIA

Pedro Diogo Carvalho Monteiro

COORDENADOR GT - COMUNICAÇÃO

Yuri Lima

PESQUISADORES

Ana Carolina Sousa Dias
Camila Cristina da Silva
Fernanda Mateus Rosa da Silva
Katiele Ferreira
Luiza Morales
Maria Luiza Duarte Sá
Pedro Peres
Raquel Rachid

WEBDESIGNER

Miranda Almeida

Dados Internacionais de Catalogação na Publicação (CIP)

Vigilância por lentes opacas
[livro eletrônico]: mapeamento da
transparência e responsabilização
nos projetos de reconhecimento
facial no Brasil / Thallita Lima. [et
al.] – Rio de Janeiro : CESeC, 2024.
4.500 kb.

Outros autores: Thaís Cruz, Pedro
Diogo, Felipe da Silva, Cynthia
Picolo, Pablo Nunes
Formato: PDF
ISBN: 978-85-5969-050-7

1. Vigilância - Segurança pública.
2. Reconhecimento facial.
3. Transparência na segurança
pública. I. Lima, Thallita. II. Título.

CDD-353.3

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

Índices para catálogo sistemático:

1. Vigilância : Segurança pública 353.3

Apresentação

—
Cynthia Picolo

Pablo Nunes
—

Desde 2019, o Brasil tem testemunhado um aumento significativo no uso de dispositivos digitais de vigilância pelo Estado, especialmente câmeras de reconhecimento facial. Após duas eleições, o que se pode afirmar é que, embora essas câmeras tenham se tornado parte involuntária do cotidiano de milhões de brasileiros, seu funcionamento, os responsáveis por sua operação e os custos envolvidos em sua aquisição permanecem grandes interrogações. Essa falta de transparência não é apenas uma falha administrativa, mas uma ameaça direta aos direitos dos cidadãos, abrindo espaço para abusos de poder e erosão da confiança pública.

Este relatório lança um olhar crítico sobre os mecanismos de transparência pública no uso de câmeras de reconhecimento facial na segurança pública em todas as cinco regiões do Brasil. Fruto da colaboração entre o Centro de Estudos de Segurança e Cidadania (CESeC) e o Laboratório de Políticas Públicas e Internet (Lapin), a pesquisa apresentada aqui mensura o grau de transparência ativa e passiva em 50 casos de uso de reconhecimento facial, propondo uma análise aprofundada de seu atual estado de opacidade. Os resultados são alarmantes: a maioria desses projetos opera sem atender aos padrões mínimos de transparência, o que deveria ser uma exigência básica em qualquer democracia.

O CESeC tem monitorado o uso de reconhecimento facial na segurança pública brasileira desde o início da utilização em larga escala no Brasil, revelando que 90% das pessoas presas com o uso dessa tecnologia em 2019 eram negras, acusadas de crimes sem uso de violência. O ***relatório da Rede de Observatórios da Segurança*** também indicou que, naquele ano, ao menos quatro estados haviam registrado prisões com o uso de reconhecimento facial. A partir desse primeiro levantamento, foi criado o projeto ***Panóptico***, que vem acompanhando e estudando em profundidade os casos de uso dessa tecnologia no Brasil, com publicações específicas sobre os

estados do **Rio de Janeiro**, de **Goiás**, da **Bahia** e do **Ceará**. O projeto mantém um site atualizado mensalmente com os casos de uso de reconhecimento facial no país, onde estão disponíveis a metodologia de monitoramento e o banco de dados utilizados para a escolha da amostra analisada neste relatório.

O Lapin, por sua vez, foi uma das primeiras organizações brasileiras a realizar um **estudo avaliando diferentes políticas públicas que utilizam reconhecimento facial**, incluindo casos de uso pelos órgãos de segurança pública. O estudo revelou que, dos cinco requisitos básicos analisados para o uso de algoritmos de reconhecimento facial — existência de regulação específica, adoção de boas práticas, publicação do número de erros e da acurácia, existência de mecanismos para proteger os direitos do titular e informações sobre as formas de aquisição da tecnologia —, os casos de uso para segurança pública não cumpriam ao menos dois. Isso demonstra uma grave falha na implementação dessas tecnologias, que deveria estar orientada pela transparência e pela proteção dos direitos dos cidadãos.

Desde a publicação do relatório do Lapin em 2021, pouco mudou na esfera da transparência, mas muito se avançou na adoção dessa tecnologia no Brasil. Dados atualizados em julho de 2024 revelam que há ao menos 264 casos de uso de reconhecimento facial para fins de segurança no Brasil, abrangendo todas as cinco regiões e quase a totalidade das Unidades Federativas. Em um contexto em que ainda se patina na regulação da Inteligência Artificial, a transparência, que deveria ser um dever do Estado, continua a ser negada à população. Esse cenário não só impede o controle social sobre essas tecnologias, como também perpetua práticas discriminatórias e violações de direitos.

Estamos lidando com uma tecnologia que tem se provado arriscada, facilitando a vigilância massiva da população por meio de lentes enviesadas por raça e gênero. Além disso, essa tecnologia ameaça a proteção de dados pessoais dos cidadãos e não garante o acesso a informações básicas sobre seu uso. As tecnologias de reconhecimento facial deveriam ser banidas de espaços públicos, pois representam um retrocesso nos direitos dos cidadãos, perpetuam a discriminação contra a população negra e continuam a alimentar o encarceramento em massa. No entanto, em vez de avançarmos na garantia de direitos, estamos caminhando na direção oposta, relegando a população ao desconhecimento do avanço sobre seus direitos.

Com este relatório, CEsC e Lapin procuram não apenas mapear as falhas de transparência, mas também contribuir para o debate sobre a necessidade de se banir o uso de reconhecimento facial em espaços públicos. Ao identificar elementos que tornam ainda mais preocupante o uso dessa tecnologia, esperamos fomentar uma reflexão crítica e responsável que leve à proteção dos direitos fundamentais das pessoas e à implementação de políticas públicas verdadeiramente justas, eficazes e transparentes.



Vigilância por lentes opacas:

mapeamento da transparência
e responsabilização nos projetos
de reconhecimento facial no Brasil

—
Thallita Lima

Thaís Cruz

Pedro Diogo

Felipe da Silva
—

Nos últimos anos, a implementação de tecnologias de reconhecimento facial (TRF) para fins de segurança pública e persecução penal tem sido apresentada no discurso público como uma promessa e uma oportunidade para otimizar a gestão da segurança em diversas partes do mundo. No entanto, estudos e casos concretos mostram que, na prática, a disseminação do uso de TRF leva a uma vigilância massiva, indiscriminada e desproporcional dos cidadãos. Além disso, já são amplamente conhecidos limites, falhas e erros envolvidos na adoção dessas ferramentas, incluindo padrões discriminatórios que afetam desigualmente determinados grupos sociais em função de marcadores de classe, cor e gênero (Buolamwini; Gebru, 2018; Nunes; Lima; Cruz, 2023; Benjamin, 2020). Assim, a produção sistemática de falsos positivos — os “erros do sistema” — tem gerado diversas formas de constrangimento e violência, em geral, contra pessoas que

já estão socialmente vulneráveis. O uso de TRF, portanto, tem contribuído para a criminalização de populações que historicamente já são alvo da violência.

No Brasil, também se observa um aumento significativo nos investimentos voltados para a implementação de TRF para fins de segurança pública e persecução penal. O Panóptico, projeto realizado pelo Centro de Estudos de Segurança e Cidadania (CESeC) desde 2020, constatou que todos os estados do país já adotaram, estão adotando ou planejam adotar o reconhecimento facial em atividades policiais. Atualmente, segundo esse monitoramento, existem 264 projetos ativos, e aproximadamente 75,4 milhões de brasileiros (37% da população) estão potencialmente sob vigilância por câmeras de reconhecimento facial na segurança pública.¹ É da necessidade de produzir meios de monitoramento e avaliação deste processo que o CESeC e o Laboratório de Políticas Públicas e Internet (Lapin) se unem na realização da pesquisa que apresentamos aqui.

O uso de reconhecimento facial no Brasil teve início na década de 2010, impulsionado por grandes eventos como as Olimpíadas. No entanto, a adoção dessa tecnologia ganhou destaque em 2019, principalmente devido à Portaria n.º 793, de 24 de outubro de 2019, que estabelece a utilização de recursos do Fundo Nacional de Segurança Pública para estimular a instalação de sistemas de videomonitoramento com reconhecimento facial, inteligência artificial ou outras tecnologias similares.² De acordo com a Portaria, tais sistemas são considerados parte integrante das estratégias de redução e controle da violência e criminalidade. Essas e outras medidas subsequentes, contudo, não foram acompanhadas da devida transparência nem de padrões regulamentares que assegurem o escrutínio sobre o uso das TRF, principalmente por parte da sociedade civil, dificultando a certificação do discurso de que a tecnologia é eficaz para atingir a essa finalidade específica.

Os órgãos de segurança pública e os responsáveis pela supervisão da implementação das TRF no Brasil falham na prestação de contas à população, alegando um limbo regulatório. Assim, o tratamento de dados coletados para fins de segurança pública por meio das TRF é realizado sem salvaguardas mínimas, desconsiderando os riscos associados à tecnologia e a despeito da emenda à Constituição da República que incluiu o direito à proteção de dados como direito fundamental autônomo³, dos princípios da administração pública⁴ e da regulação infraconstitu-

1. Atualização de 08 de agosto de 2024.

2. BRASIL. Ministério da Justiça e Segurança Pública. Portaria N.º 793, de 24 de outubro de 2019. **Diário Oficial da União**: seção 1, Brasília-DF, edição 208, p. 55, 24 de out. 2019. Disponível [neste link](#). Acesso em: 09 set. 2024.

3. BRASIL. Constituição de 1988. Constituição da República Federativa do Brasil, art. 5º, inc. LXXIX. Brasília, DF: Câmara dos Deputados, [2018]. Disponível [neste link](#). Acesso em: 19 set. 2024.

4. BRASIL. Constituição de 1988. Constituição da República Federativa do Brasil, art. 37º. Brasília, DF: Câmara dos Deputados, [2018]. Disponível [neste link](#). Acesso em: 19 set. 2024.

cional.⁵ Na prática, observa-se a expansão e dispersão de projetos em todo o território nacional sem a devida regulamentação, padronização tecnológica e adoção de mecanismos de publicidade, transparência e avaliação do uso dessas tecnologias como política pública.

Dessa forma, a implementação dos projetos avança aceleradamente sem que haja garantias de proteção dos direitos fundamentais, tornando os espaços públicos verdadeiros laboratórios de experimentação de tecnologias. Neste sentido, o caso da Bahia é emblemático. O relatório “***O sertão vai virar mar: expansão do reconhecimento facial na Bahia***” (2023) mostrou que o uso das TRF no estado se expandiu para mais de 70 municípios mesmo sem apresentar indicadores claros de efetividade na redução da criminalidade. Segundo dados da Secretaria de Segurança Pública da Bahia, no período entre 2018 e 2022, os índices de criminalidade e os indicadores de violência permaneceram praticamente inalterados ou até aumentaram em algumas regiões do estado.

A descentralização dos projetos de segurança pública, com a aquisição por diversos municípios, levanta preocupações sobre um possível processo de desresponsabilização no uso dessa tecnologia, por meio de sua pulverização sem diretrizes e normativas básicas de uso. No Brasil, cada entidade decide sobre qual tecnologia utilizar, o tipo de *software*, as empresas fornecedoras, os bancos de dados a serem empregados, os requisitos de análise de vídeo e as localidades onde serão implementadas, entre outros aspectos. Esse cenário é agravado pelas lacunas de informação, como, por exemplo, a respeito do orçamento dos projetos, dos gastos operacionais, do uso prático e da produção de relatórios de impacto que avaliem a eficiência da política pública.

No relatório “***Das Planícies ao Planalto: como Goiás influenciou a expansão do reconhecimento facial na segurança pública brasileira***” (2023), o Panóptico observou como o incentivo à “modernização da segurança” não foi acompanhado de mecanismos de responsabilização, prestação de contas e transparência. No caso de Goiás, questões básicas como quem gere os dados, como são armazenados, onde as câmeras estão instaladas e se estão em funcionamento não foram respondidas pelas prefeituras e pelos órgãos responsáveis pelas iniciativas. Um exemplo da opacidade na qual essa política tem operado é que dos 37 municípios goianos que realizaram pregões para aquisição de infraestrutura para o reconhecimento facial (câmeras, *software*, computadores etc.), em 12 não há contratos disponíveis nos Portais de Transparência e os responsáveis não respondem às solicitações de informação enviadas.

De forma geral, não há informações detalhadas e de fácil acesso sobre o uso do reconhecimento facial no Brasil, como ele está sendo operacionalizado e qual é a verba

⁵ Como, por exemplo, a Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709/2018 – LGPD) e a Lei de Acesso à Informação Lei (Lei n.º 12.257/2011 – LAI).



pública investida nesta tecnologia. Na linguagem de Administração Pública, não se percebe a transparência ativa nem a passiva.⁶ Os mecanismos de acesso à informação são fundamentais para os cidadãos, as instituições públicas e as entidades da sociedade civil organizada, por permitirem o monitoramento e a avaliação das políticas públicas, assegurando transparência e prestação de contas. Esse é um aspecto crucial para o fortalecimento da democracia e para a confiança pública de que as instituições estão utilizando seus recursos em conformidade com os direitos fundamentais e respeito aos princípios constitucionais da Administração Pública como legalidade, impessoalidade, moralidade, publicidade e eficiência.⁷

Nesse cenário, realizamos o mapeamento e a avaliação dos projetos de reconhecimento facial em uso no Brasil, com foco na transparência, no acesso à informação e na prestação de contas. Com base nessa pesquisa, elaboramos um índice de transparência para o uso do reconhecimento facial no Brasil que pode ser replicado e ampliado como ferramenta de contínuo monitoramento e análise crítica das práticas adotadas no país. Neste relatório, apresentamos essa pesquisa e o caminho que nos levou à construção dessa ferramenta fundamental para garantir o direito do cidadão à informação.

O texto está dividido em quatro partes. Primeiramente, detalhamos a metodologia de coleta das informações e produção do índice. Em seguida, realizamos uma análise panorâmica dos projetos de reconhecimento facial dentro da amostra dos 50 casos avaliados. Destaca-se, de forma geral, a carência de informações sobre fornecedores, operadores, custos e políticas de proteção de dados. Mais de 70% dos projetos não informam o modo de aquisição e cerca de 80% não possuem relatórios de impacto.

6. A transparência ativa dá-se pela divulgação voluntária das informações, enquanto a transparência passiva ocorre por meio de pedido de informação via Lei de Acesso à Informação n.º 12.257/2011 – LAI.

7. BRASIL. Constituição de 1988. Constituição da República Federativa do Brasil, art. 37º. Brasília, DF: Câmara dos Deputados, [2018]. Disponível [neste link](#). Acesso em: 19 set. 2024.

Se algo fica evidente neste cenário, não são os dados, mas a opacidade em que se realizam esses projetos.

Na terceira parte, aprofundamos nos indicadores de transparência ativa e passiva das iniciativas. Seguimos destacando as dificuldades de acesso à informação, tanto em termos de transparência ativa quanto passiva. A transparência ativa é limitada pela falta de relatórios de impacto e dados essenciais. Na transparência passiva, obstáculos como barreiras burocráticas e limitações técnicas nos sistemas de solicitação dificultam o acesso dos cidadãos, ilustrando a necessidade de melhorias na comunicação e na acessibilidade das informações públicas.

Por fim, apresentamos o índice desenvolvido com base na análise dos projetos. A produção desses dados contribuirá para um debate informado sobre a implementação de TRF como política pública de segurança. A proposta não é ranquear os projetos analisados, mas produzir indicadores de transparência para uma reflexão sobre como a expansão dessa política pública não tem levado em conta princípios básicos da Administração Pública.

Dado que o Estado insiste em adotar essas tecnologias, o presente relatório contribui para uma discussão mais ampla e crítica sobre seu uso na segurança pública. Examinando a implementação das TRF, ajudamos a identificar as deficiências e as irracionalidades da aplicação da política pública.





Metodologia

O objetivo final desta pesquisa foi construir um índice de **transparência**. Este termo comumente se refere à abertura para a comunicação de informações e processos ao público e à clareza dessa comunicação, que deve garantir ciência e escrutínio social não somente sobre as iniciativas em si, mas também sobre a forma como os dados dos titulares são tratados. O conceito de transparência é crucial para construir confiança entre o governo e a sociedade, particularmente em um contexto no qual a vigilância tem sido cada vez mais normalizada. Cabe ressaltar que, apesar de ter ganhado destaque no debate da adoção de TRF, principalmente por suas implicações éticas, legais e sociais, esse não é um conceito monolítico. O termo se insere em um campo de disputa no qual diferentes atores — órgãos públicos, cidadãos ou sociedade civil organizada — lutam para definir o que significa ser transparente (Ananny; Crawford, 2018).

A transparência não é, portanto, simplesmente um estado final preciso em que tudo é claro e aparente, mas um sistema de observação e conhecimento que promete uma forma de prestação de contas, responsabilização e controle da política pública. Tendo como entendimento que a transparência pode ser usada tanto para promover a responsabilização quanto para mascarar a opacidade, dependendo de como e de quais informações são apresentadas (Ananny; Crawford, 2018; Meijer; Hart; Worthy, 2018), esta pesquisa adota uma perspectiva de transparência que envolve não apenas o nível de acesso e divulgação das informações sobre os projetos de reconhecimento facial, mas a qualidade da informação que é disponibilizada.

Assim, para chegar a um índice de transparência, passamos por cinco etapas: (1) revisão de literatura; (2) coleta de informações via LAI, documentos oficiais e artigos de imprensa; (3) construção da base de dados; (4) análise quantitativa e qualitativa

dos dados coletados; (5) e construção do índice. Selecionamos 50 projetos das Secretarias de Segurança Pública, das Guardas Municipais, dentre outros órgãos de segurança pública nas cinco regiões brasileiras: 18 projetos pertencem à esfera estadual e 32, à esfera municipal. De todos os projetos selecionados para a amostra havia indícios de operação, seja por meio de fontes midiáticas ou de publicação no Diário Oficial da União ou no Portal da Transparência.

Inicialmente, realizamos uma revisão da literatura sobre o conceito de transparência na intersecção com o debate de uso de tecnologias de reconhecimento facial como política pública e levantamos iniciativas nacionais e internacionais que analisam transparência de políticas públicas, como Transparência Brasil, Open Knowledge Brasil, Associação Brasileira de Jornalismo Investigativo (Abraji), entre outras. Essa etapa teve como objetivos compreender o atual estado do debate na área e conhecer outras experiências e metodologias para identificar lacunas que este relatório pretende abordar. Além disso, estabelecer um marco teórico para a análise dos dados coletados e a confecção de pontos de atenção que são constituintes da matriz de análise dos projetos aqui abordados.

Em seguida, criamos uma base de dados com a amostra de projetos a ser analisada, a partir do **monitoramento de projetos ativos** de reconhecimento facial no Brasil, do Panóptico. Do total de 264 projetos ativos, extraímos uma amostra de 50 casos, com o objetivo de capturar a diversidade tanto regional quanto de operadores responsáveis pelas iniciativas. A seleção foi realizada de forma a assegurar que todas as regiões do país (Centro-Oeste, Nordeste, Norte, Sudeste e Sul) tivessem dez casos cada. Foram incluídos projetos conduzidos por diferentes tipos de operadores, como a Guarda Civil Metropolitana, operadores municipais e estaduais. Essa abordagem permitiu uma variedade de contextos, práticas e níveis de transparência em diferentes esferas e localidades do país.

A base de dados desta pesquisa é composta pelas categorias de informações básicas dos projetos como: (i) esfera — municipal ou estadual; (ii) ano de ativação; (iii) status; (iv) local de utilização; (v) operador; (vi) custo do projeto; (vii) modo de aquisição; (ix) local de utilização; (x) informações sobre o grau de acesso à informação nos canais do licitante e do operador do projeto; (xi) informações sobre resultados de uso (pessoas presas, número de pessoas desaparecidas encontradas, informações sobre falsos positivos e relatório de impacto); (xii) dados sobre política de proteção de dados; (xiii) grau de retorno por LAI; e (xiv) qualidade das respostas.⁸

Essas categorias foram escolhidas com o objetivo de fornecer uma perspectiva ampla e detalhada do nível de transparência da operação dos projetos de TRF. Ao somar informações sobre a estrutura administrativa, financeira e operacional dos projetos

8. Todas as categorias estão melhor detalhadas no Anexo I.

aos indicadores de acesso à informação, eficácia e impacto, a pesquisa busca avaliar não apenas a transparência formal dos dados disponibilizados, mas também a forma como esses projetos são implementados e monitorados. A consideração de políticas de proteção de dados e o grau de retorno por LAI reforçam o compromisso com a privacidade e a responsabilidade pública, assegurando que os direitos dos cidadãos sejam protegidos e que os órgãos envolvidos mantenham algum padrão de prestação de contas. Todos os dados produzidos nesta etapa estão abertos e disponíveis em uma **planilha** online.

A partir dessa base de dados, elaboramos uma matriz de níveis de transparência ativa e passiva de cada projeto. Neste relatório, entendemos a **transparência ativa** como a divulgação proativa de informações pelos órgãos públicos, disponibilizando dados e documentos de interesse público sem a necessidade de solicitações formais. Exemplos incluem a acessibilidade digital dos dados, sua publicação no Portal da Transparência, em sites oficiais dos órgãos e em reportagens de veículos de grande circulação. Por **transparência passiva**, entendemos a disponibilização de informações mediante solicitação via Lei de Acesso à Informação (LAI). Isso inclui não somente respostas a pedidos de informação, mas também o atendimento das solicitações no prazo legal e a qualidade das respostas fornecidas.

A análise dos dados coletados, tanto nas categorias de transparência passiva como de transparência ativa, foi realizada por meio de métodos qualitativos e quantitativos. A análise qualitativa se baseou na interpretação do conteúdo de documentos, respostas de pedidos via LAI e relatórios para identificar práticas de transparência e prestação de contas. Já a análise quantitativa buscou desenvolver indicadores de transparência e responsabilização com base nos dados coletados.

Finalmente, foi elaborado um índice de níveis de transparência de projetos ativos de reconhecimento facial e realizada uma análise sobre disponibilidade, acessibilidade e nível de informação sobre cada projeto. Esse índice foi calculado com base na transparência ativa e passiva dos projetos de reconhecimento facial analisados neste relatório e leva em conta duas dimensões: qualidade e completude de dados disponíveis e facilidade de acesso à informação. Ele utiliza os critérios e a escala a seguir:

1. TRANSPARÊNCIA ATIVA

Essa dimensão avalia o quão proativo um órgão da Administração Pública é na divulgação de informações sobre os projetos de reconhecimento facial. Ela é dividida nas seguintes categorias:

a) Disponibilidade de informações e documentos oficiais (0 – 4 pontos):

Aqui avaliamos as informações básicas publicizadas e se os documentos oficiais relacionados ao projeto, como editais, contratos e termos de referência estão disponíveis

publicamente. Os componentes desse cálculo são as categorias do banco de dados apresentadas a seguir, em que cada componente é avaliado de acordo com a disponibilidade da informação e de sua acessibilidade:

- **custo do projeto:** verifica se os custos estão claramente especificados e disponíveis (0 – 0,5);
- **operador e nível de informação em seus canais sobre o projeto:** identifica se o operador do projeto está claramente indicado (0 – 0,5);
- **modo de aquisição:** avalia se o modo como o projeto foi adquirido (licitação, doação etc.) é conhecido (0 – 0,5);
- **local de utilização:** determina se o local onde o projeto está implementado é especificado (0 – 0,5);
- **documentos oficiais:** verifica se os documentos relevantes, como termos de referência, contratos e editais, estão acessíveis (0 – 0,5);
- **órgão licitante e nível de informação em seus canais sobre o projeto:** avalia a clareza sobre qual órgão realizou a licitação (0 – 0,5);
- **software e empresa detentora:** verifica se os dados sobre o *software* utilizado e a empresa responsável são conhecidos (0 – 0,5);
- **empresa contratada:** identifica se a empresa contratada para implementação do projeto é divulgada (0 – 0,5).

A disponibilização desses dados e documentos é fundamental para garantir a transparência das ações governamentais e permitir o escrutínio público. Além disso, também foi avaliado o grau de informação nos canais oficiais do órgão licitante e do operador das TRF.

b) Publicação de relatórios de impacto (0 – 3 pontos):

Verificamos se há relatórios de impacto e se esses são acessíveis e disponíveis ao público. Para o cálculo são atribuídos:

- **Três pontos** se os relatórios de impacto estão completos e publicamente disponíveis;
- **Dois pontos** se o órgão produz o relatório, se ele está completo e pode ser acessado via requerimento de informação;
- **Um ponto** se o órgão produz o relatório, mas esse não é disponibilizado ao público; e
- **Nenhum ponto** se não há produção de relatório.

Os relatórios de impacto são importantes para avaliar os efeitos do projeto, tanto positivos quanto negativos, e garantir que as decisões sejam baseadas em evidências.

c) Políticas de proteção de dados (0 – 3 pontos):

Examinamos a existência e a divulgação de políticas de proteção de dados e segurança da informação. O cálculo foi feito atribuindo:

- **Três pontos** se uma política de proteção de dados e segurança da informação estiver publicada e acessível;
- **Dois pontos** se há uma política de proteção de dados e segurança da informação, mas não está acessível;
- **Um ponto** se há apenas política de segurança da informação;
- **Um ponto** se há apenas política de proteção de dados;
- **Nenhum ponto** se não há política de proteção de dados ou de segurança da informação.

A transparência em relação a essas políticas é crucial, especialmente em projetos que lidam com o processamento de dados pessoais sensíveis, como o reconhecimento facial, para assegurar que os direitos fundamentais, como privacidade e proteção de dados dos cidadãos, estão sendo respeitados e também se está sendo assegurada a prerrogativa de finalidade e proporcionalidade no processamento desses dados de acordo com a Lei Geral de Proteção de Dados (LGPD).

2. TRANSPARÊNCIA PASSIVA

Essa dimensão do nosso índice mede capacidade, eficácia e clareza do órgão em responder às solicitações de informação via LAI, e inclui as seguintes categorias:

a) Resposta a solicitações via LAI (0 – 3 pontos):

Avaliamos se os órgãos respondem às solicitações de acesso à informação dentro do prazo legal. A capacidade de responder eficazmente às solicitações de informação via LAI é um indicador chave do compromisso do órgão com a transparência e a prestação de contas. O cálculo foi realizado levando em contas os seguintes critérios:

- **Três pontos** se todas as solicitações foram respondidas dentro do prazo;
- **Um ponto e meio** se as solicitações foram respondidas fora do prazo;
- **Nenhum ponto** se a solicitação não foi respondida.

b) Grau do retorno de pedidos via LAI (0 – 3 pontos):

Mensuramos a completude e clareza das respostas recebidas pelas solicitações via LAI, avaliando se as perguntas foram respondidas parcialmente ou não foram res-

pondidas. O cálculo foi feito seguindo os seguintes critérios:

- **Três pontos** para respostas completas e claras das solicitações;
- **Um ponto e meio** para respostas parciais das solicitações (ausência de dados, falta de resposta de alguma pergunta e respostas redundantes);
- **Nenhum ponto** se a solicitação não foi respondida.

Respostas completas e claras indicam um alto nível de compromisso com a transparência e a satisfação das necessidades informacionais dos cidadãos.

c) Acessibilidade das informações (0 – 4 pontos):

Analisamos a facilidade de acesso às informações pelos cidadãos, incluindo a usabilidade dos sistemas eletrônicos de informações (e-SIC). A acessibilidade é fundamental para garantir que os cidadãos possam exercer plenamente seu direito de acesso à informação.

- **Quatro pontos** se as informações estavam disponibilizadas e se seu acesso era fácil;
- **Três pontos** se havia um nível de acessibilidade intermediário;
- **Um ponto** se a informação está disponível, mas difícil de ser acessada;
- **Nenhum ponto** para ausência de informação e, portanto, de acessibilidade.

No índice, cada critério pode receber até a pontuação máxima indicada, totalizando dez pontos para transparência ativa e dez pontos para transparência passiva. O Índice de Transparência é calculado como a média dessas duas pontuações.

$$\text{Índice de Transparência} = \frac{(\text{Transparência ativa} + \text{Transparência passiva})}{2}$$

Essa abordagem permite uma avaliação equilibrada que considera tanto a proatividade dos órgãos em divulgar informações quanto a sua capacidade de atender às demandas dos cidadãos, proporcionando uma visão abrangente da transparência dos projetos de reconhecimento facial no Brasil.

Panorama geral

dos projetos de reconhecimento facial

Todos os projetos que fazem parte da amostra de análise dessa pesquisa foram iniciados entre os anos de 2019 e 2024, sendo a maioria (23 projetos) entre 2021 e 2023. Este, contudo, não é um recorte intencional. Trata-se, na verdade, de um reflexo do avanço geral do uso de reconhecimento facial no Brasil.⁹

Apesar de haver indícios de operação em todos os casos, como delimitamos na metodologia, foram encontradas ambiguidades em relação ao status de dez projetos com base em respostas de pedidos via LAI. Um dos casos mais emblemáticos é o da Polícia Civil do Amapá (PC-AP) que, de acordo **com seu próprio site**, indicou o uso de *software* de reconhecimento facial para a captura de foragidos da Justiça, como vemos na figura a seguir.¹⁰ Porém, em resposta ao nosso pedido via LAI, foi informado que a PC-AP “não trabalha com *software* de reconhecimento facial”.

⁹. Ver mais no banco de dados do monitoramento, que está aberto e disponível [neste link](#). Acesso em: 13 ago. 2024.

¹⁰. Todas as respostas que obtivemos encontram-se no anexo III deste documento.

Quarta, 06 de outubro de 2021 - 09:54h - 2425

POLÍCIA CIVIL UTILIZA SOFTWARE DE RECONHECIMENTO FACIAL PARA IDENTIFICAR SUSPEITO DE FURTO

Por: Assessoria de Comunicação PC-AP

Postar

Compartilhar 0



Captura de tela de site (...). Fonte: Polícia Civil do Amapá, 2021.

Resposta

X

Categoria da resposta	Manifestação atendida
Tipo de resposta	Resposta conclusiva
Resposta	Senhor usuário, informamos que a Polícia Civil do Amapá não trabalha com software de reconhecimento facial.
Observação	
Data e hora	29/05/2024 09:44
Anexos	

Protocolo 0004.335011918042024 | Resposta via LAI, 2024.

Em Goiás, foi identificado um problema de inconsistência em um projeto estadual. De acordo com o veículo de informação local, haveria uma parceria entre o Governo Estadual e a Prefeitura Municipal de Catalão, ***na qual operariam 350 câmeras fixas com capacidade de reconhecimento facial e leitura de placas***. Em resposta ao pedido via LAI, no entanto, a Ouvidoria respondeu que não havia sistemas de reconhecimento facial em execução por parte do Estado. Ainda em Goiás, outro projeto segue a mesma tendência. A Prefeitura Municipal de Mineiros informou que não há sistema de reconhecimento facial sendo utilizado no município. Contudo, há um ***contrato de prestação de serviços*** cujo objeto é a contratação de uma empresa especializada para implantar o sistema de videomonitoramento em vias urbanas.

Embora o contrato não mencione especificamente o termo “reconhecimento facial”, a categoria “videomonitoramento” é frequentemente utilizada para abranger diversos tipos de sistemas com diferentes capacidades de captura de imagem e análise de dados, tais como as TRF (Nunes; Lima; Rodrigues, 2023).¹¹

Já em Fortaleza, estado do Ceará, o projeto foi identificado por meio de uma reportagem da mídia local, sendo uma ação do Governo estadual a implementação de ***câmeras em mais de 180 pontos de ônibus para reconhecimento facial de criminosos***. Em resposta, a Secretaria de Segurança Pública e Defesa Social afirmou que o Programa Segurança no Ponto não faz uso de reconhecimento facial. No projeto estadual do Amazonas, há informações de que foram ***entregues à Polícia Militar, em setembro de 2021, viaturas com câmeras de reconhecimento facial***. De forma contrária, a Secretaria de Segurança Pública do estado (SSP-AM) informou que “atualmente não é empregado em nenhum dos serviços contratados por esta pasta alguma tecnologia de reconhecimento facial”. No entanto, mencionou que existe um projeto em implementação, mas que se trata de cooperação técnica celebrada recentemente com a Associação Comercial do Amazonas. Ainda assim, não forneceu mais esclarecimentos sobre o projeto atual.

O mesmo ocorreu com a Prefeitura de Maricá, no estado do Rio de Janeiro. Em 2022, foi publicado no ***Diário Oficial de Maricá o Processo Administrativo n.º 4774/2021***, que determinava a aquisição do *software* de reconhecimento facial. Em resposta por LAI, a prefeitura, contudo, informa não possuir sistema de reconhecimento facial. Não foi diferente com as prefeituras de Florianópolis (SC), de Balneário Camboriú (SC), de Ribeirão Pires (SP) e com a Polícia Militar de Santa Catarina. Todas apresentaram ambiguidades semelhantes, que também acabam reforçando a opacidade sobre os projetos de reconhecimento facial. Com uma resposta negativa e conclusiva, os órgãos não fornecem mais informações. Não fica claro, portanto, se a tecnologia foi utilizada e os projetos já foram finalizados e, se for este o caso, quais seriam os resultados e as justificativas para sua finalização.

Dos projetos em que a resposta foi positiva em relação ao estado ativo de uso de TRF, muitos não apresentam informações suficientes para a identificação de como a tecnologia está sendo usada, por quem, quem fornece, como está sendo adquirida e quais são as garantias de proteção de dados e segurança da informação existentes. Ao mesmo tempo, os portais de transparência e as páginas dos operadores dos projetos evidenciam a ausência de informações sobre as iniciativas, incluindo as mais básicas como órgão licitante, operador do projeto e informações contratuais.

11. Esse cenário foi abordado em outro estudo. De acordo com Nunes, Lima e Rodrigues (2023), entre os 51 municípios identificados em Goiás, 44 mencionaram explicitamente o uso de tecnologia de reconhecimento facial em seus termos de referência ou projetos. Os sete municípios restantes propuseram a implementação de sistemas de videomonitoramento, sem especificar o uso de reconhecimento facial. Contudo, os projetos eram de uso de tecnologia de reconhecimento facial.

Entre os projetos de reconhecimento facial analisados — desconsiderando os dez que relataram não utilizar a tecnologia e, portanto, não forneceram mais informações —, 55% não identificaram a empresa fornecedora. Em relação aos operadores da tecnologia, 32,5% não foram identificados, e em 55% dos casos não há informações sobre qual foi o órgão licitante. A situação se torna ainda mais crítica ao examinar dados mais específicos: cerca de 72,5% dos projetos não fornecem informações sobre o modo de aquisição da tecnologia, e 47,5% não revelam o custo total do projeto.

As informações recebidas e/ou coletadas foram organizadas e analisadas conforme os seguintes aspectos: (i) modelos, empresas e sistemas; (ii) custos, modo de aquisição e modelo contratual; (iii) políticas de segurança da informação e proteção de dados; e (iv) informações sobre resultados de uso. Foram identificados 11 modelos de *software* de reconhecimento facial utilizados, incluindo: Axxon Next SW-ANV-FRCT-RTL, Hiki-Center Professional, SecurOS, SAFR, Holosens Huawei, VMS Digifort versão Enterprise 7.3.0.1, além dos analíticos da Digifort e da Dahua. No total, foram mapeadas 22 empresas fornecedoras, o que indica que algumas empresas distribuem *softwares* desenvolvidos por outras. Por exemplo, a Brisanet e a Tecno-it Serviços e Comunicação LTDA fornecem o *software* da Hikvision. Importante mencionar que foram contadas as empresas parceiras e que fazem parte dos consórcios estabelecidos.

Além disso, dois projetos são desenvolvidos por órgãos públicos: um pelo Instituto Curitiba de Informática e outro pela Secretaria de Justiça e Segurança Pública do Amapá. A lista completa das empresas identificadas é apresentada a seguir.

TABELA 1 – LISTA DE EMPRESAS FORNECEDORAS DE RECONHECIMENTO FACIAL
Brisanet
Consórcio Smart City – CLD – Construtora, Laços Detentores e Eletrônica LTDA, Flama Serviços LTDA, Camerite Sistemas S.A. e PK9 Tecnologia e Serviços LTDA
Consuma Comercial LTDA
Dahua Technology
Digifort
Helper Tecnologia
Ideal Comércio e Serviços LTDA
L8 Group
MOPEN MANUTENÇÃO E OPERAÇÃO DE EQUIPAMENTOS ELETRO-ELETRÔNICOS LTDA
Oi S/A e Avantia
Protenet
Quasar Tecnologia e Yan Tecnologia
Radium Tecnologia
SISGRAPH LTDA
Tecno-it – Serviços e Comunicação LTDA
TELEQUIPE SERVIÇOS E ALUGUÉIS DE MÁQUINAS, EQUIPAMENTOS E SOFTWARE LTDA
Teltex Tecnologia

A somatória total dos projetos que apresentam dados sobre o custo de operação é de R\$ 969.375.507,62. O projeto com valor mais alto é o da Bahia, que equivale a 68,7% desse total. Porém, não só os números chamam atenção. Em resposta ao nosso pedido via LAI, Goiânia respondeu que a “solução de reconhecimento facial foi doada pela empresa [...]. Portanto, não houve custo à Prefeitura”. No entanto, junto aos demais documentos enviados estava o contrato celebrado entre o município de Goiânia e a empresa Tecno-it Serviços e Comunicação LTDA no valor de R\$17.945.600,00, que seria usado para a infraestrutura adicional necessária para o videomonitoramento. Ou seja, ainda que a tecnologia seja doada, isso não significa que não haverá custos para o órgão licitante.

Vale aqui mencionar que a escolha entre licitação pública¹² e pregão eletrônico¹³ pode influenciar significativamente a burocratização de um projeto. A licitação pública, com seu rigor procedimental, pode oferecer maior segurança jurídica e permitir um controle mais detalhado sobre a qualificação dos fornecedores, embora a sua maior complexidade e o tempo necessário para execução possam ser vistos como desvantagens em contextos que demandam rapidez. Já o pregão eletrônico, com sua eficiência e acessibilidade, pode aumentar a participação e competitividade, mas deve ser utilizado com cautela em projetos que exijam altos níveis de especialização e precisão técnica.

A ausência de clareza sobre qual modalidade de contratação foi utilizada e quais critérios orientaram essa escolha levanta preocupações sobre a conformidade do processo com as melhores práticas de gestão pública e sobre a adequada alocação dos recursos públicos. Portanto, é essencial que essas informações sejam amplamente divulgadas, garantindo que o controle social possa ser exercido de maneira efetiva, assegurando que a transparência e a responsabilidade pública sejam mantidas em todos os estágios do processo de aquisição. É fundamental que o órgão licitante informe claramente o modo de aquisição, porque isso não apenas revela como os recursos públicos estão sendo alocados, mas também garante que os processos sigam critérios legais e éticos, minimizando riscos de corrupção e favorecimento indevido.

12. A licitação pública e o pregão eletrônico são ambos instrumentos legais para a contratação de serviços e aquisição de bens da Administração Pública, apesar disso, apresentam diferenças significativas que afetam diretamente a transparência e a *accountability* do processo. A licitação pública, tradicionalmente, é um procedimento mais formal e burocrático, estruturado em etapas como apresentação de propostas, habilitação técnica, julgamento e adjudicação. Esse modelo visa garantir a escolha da proposta mais vantajosa para a Administração Pública, tanto em termos de preço quanto de qualidade técnica, e é frequentemente utilizado em projetos de maior complexidade, nos quais a avaliação técnica desempenha um papel crucial.

13. O pregão eletrônico é realizado em ambiente virtual, o que permite maior agilidade e alcance. A principal vantagem do pregão é sua capacidade de democratizar o processo de concorrência, ampliando o número de participantes e reduzindo os custos operacionais tanto para os órgãos públicos quanto para os fornecedores. No entanto, essa simplificação e rapidez podem, em alguns casos, resultar em menos rigor na avaliação técnica das propostas, especialmente em projetos complexos como os de TRF, nos quais a qualidade do serviço contratado, as políticas de segurança de dados e de privacidade são tão importantes quanto o custo.

Em relação à política de segurança da informação e proteção de dados, 75% dos responsáveis pelos projetos não informaram se a possuem. A Prefeitura Municipal de Porto Alegre, estado do Rio Grande do Sul, indicou que, no momento, não há banco de dados e, portanto, não realiza tratamento de dados. Sete prefeituras responderam que seguem algum tipo de protocolo de segurança: Goiânia (GO), São Paulo (SP), Bahia (BA), Recife (PE), Belo Horizonte (MG), Cachoeiro de Itapemirim (ES) e Curitiba (PR). A Prefeitura de Curitiba hospeda os dados em uma rede isolada, sem acesso à internet, com seu perímetro protegido por firewall.¹⁴ A Prefeitura de São Paulo utiliza segurança e redundância *cloud* provida pela Microsoft, e seu banco de dados é criptografado com controle de acesso auditável e acessível somente para a rede interna. Já a de Belo Horizonte mencionou que segue as diretrizes da LGPD, mas não forneceu detalhes adicionais. A gestão municipal de Cachoeiro de Itapemirim também afirmou ter ferramentas específicas para proteger a privacidade dos dados, mas não especificou quais ferramentas são utilizadas.

A Secretaria de Segurança Pública da Bahia informou que os dados são armazenados em uma área privada e estão hospedados no *data center* de seu Centro de Operações e Inteligência. Esse ambiente é isolado da rede externa por um *firewall*, com acesso restrito, exigindo autenticação e assinatura de um Termo de Confidencialidade. Além disso, o acesso à plataforma é restrito a servidores autorizados e registrado por meio de logs.¹⁵

Por outro lado, a Prefeitura de Goiânia mencionou apenas que são adotados protocolos de acesso à sala de monitoramento, permitindo entrada somente para aqueles que trabalham no Centro de Controle Integrado da Prefeitura, onde há controles de autenticação e gerenciamento de risco. Já a Ouvidoria da Secretaria de Defesa Social de Pernambuco informou que são realizados três protocolos:

- i) Implementação do princípio do menor privilégio**, atribuindo aos usuários apenas os privilégios necessários para o desempenho de suas funções, com o objetivo de mitigar riscos de acessos não autorizados;
- ii) Promoção da conscientização dos usuários** quanto a proteção e sigilo no tratamento dos dados do banco de dados; e

14. Um *firewall* é um sistema de segurança que monitora e controla o tráfego de rede, protegendo contra acessos não autorizados e ataques. Ele funciona como uma barreira entre uma rede interna segura e redes externas, decidindo o que permitir ou bloquear com base em regras predefinidas. *Firewalls* podem ser baseados em *hardware*, *software* ou ambos.

15. Logs são registros que capturam uma série de eventos e atividades que ocorrem em sistemas, aplicativos e outros componentes tecnológicos. Cada entrada em um log geralmente inclui informações detalhadas como a data e a hora do evento, a natureza do evento (por exemplo, um *login* bem-sucedido ou uma tentativa de acesso falha), o usuário ou o processo envolvido e qualquer mensagem de erro ou resultado associado. Os logs são essenciais para monitorar a segurança, diagnosticar problemas e realizar auditorias, permitindo que administradores identifiquem comportamentos anômalos, resolvam falhas e mantenham a integridade do sistema.

iii) Utilização de dados anonimizados no processo de reconhecimento facial.

(Secretaria de Defesa Social Pernambuco via LAI, 2024)

Chama a atenção que 72,5% das entidades não informaram se elaboram relatórios de impacto à proteção de dados pessoais. Apenas dois órgãos confirmaram a produção desses relatórios: São Paulo (SP) e Curitiba (PR). A Prefeitura de São Paulo declarou que o documento faz parte do edital e será atualizado ao longo do processo de implantação. Por sua vez, a Prefeitura de Curitiba informou que apresenta relatórios mensais previstos nos termos de referência. Muito embora haja a produção desses relatórios por parte desses dois projetos, é importante salientar que se tratam de documentos internos. Ou seja, não estão acessíveis ao público. Dos que responderam à pergunta feita via LAI, sete projetos não produzem relatórios de impacto: Goiânia, Bahia, Paraíba, Recife, Aracaju, Cachoeiro de Itapemirim e Porto Alegre.

	Cachoeiro (ES)	Goiânia (GO)	Porto Alegre (RS)	Curitiba (PR)	São Paulo (SP)	BA	PE	PA	SE
Relatório de impacto	X	X	X	□	□	X	X	X	X
Proteção de dados	■	■	X	■	■	■	■	■	■
Segurança da Informação	■	■	X	■	■	■	■	■	■

X não possui □ reservado ■ possui

Das informações requisitadas sobre os resultados do uso das TRF, 87,5% não responderam sobre o número de pessoas desaparecidas que foram encontradas com o auxílio da tecnologia. Dos órgãos que informaram, quatro disseram não ter esse dado (Prefeitura de Goiânia, Secretaria Municipal de Segurança e Prevenção de Belo Horizonte, Polícia Militar da Paraíba e Prefeitura de Porto Alegre), porque a TRF não é utilizada para esse fim, por não possuírem banco de dados sobre desaparecidos ou porque o sistema ainda estava em fase inicial. Apenas a Prefeitura de São Paulo afirmou ter esse dado, indicando que “até a presente data foram localizadas cinco pessoas desaparecidas, conforme dados oficiais da GCM e SMDHC”.

Em relação ao número de pessoas detidas com o uso do reconhecimento facial, 80% dos órgãos não forneceram essa informação. Entre os que responderam, dois apresentaram os dados e cinco informaram que ainda não têm esses registros. Dois projetos indicaram o número de pessoas presas com base em outros canais. Entre os estados que forneceram os dados, a Bahia se destaca com o maior número de detenções por reconhecimento facial, totalizando 1.750 pessoas presas nos últimos seis anos. Mais da metade dessas detenções está relacionada a crimes de menor gravidade, como furtos e inadimplência de pensão alimentícia.

Questões mais específicas e pertinentes para avaliar os impactos do uso de TRF são ainda mais opacas. Nenhum órgão confirmou ou reconheceu a existência de erros. Sete órgãos relataram que não há erros, citando que a taxa de assertividade da tecnologia estaria calibrada para mais de 90%, ou alegaram que o sistema ainda estaria na fase inicial e, portanto, não havia dados disponíveis. Cerca de 82,5% dos órgãos simplesmente não responderam à solicitação. Entre os estados que não reconhecem erros, destacam-se Bahia, Sergipe e Rio de Janeiro, onde há registros públicos de falhas no uso da tecnologia. Na Bahia, ***o sistema de reconhecimento facial da Secretaria de Segurança Pública já identificou erroneamente pelo menos três pessoas***. No Rio de Janeiro, ***quatro pessoas foram injustamente presas em 2024*** devido a erros da TRF. Em Sergipe, ***um jovem negro foi detido durante uma partida de futebol após ser incorretamente identificado como suspeito pelo sistema*** — o governador suspendeu o uso da tecnologia no estado após a repercussão do caso.¹⁶

Ademais, nas solicitações de informação também questionamos se há registro do número de falsos positivos e erros de identificação no uso de TRF. Oito órgãos informaram que esses dados não são contabilizados, reiterando a justificativa de que não há erros porque, segundo eles, estes não existem. Aproximadamente 80% dos órgãos não forneceram qualquer informação sobre o assunto. Somente uma iniciativa fez apontamentos mais concretos sobre taxas de erros e falsos positivos. O caso foi do Governo de Pernambuco, que, mesmo não divulgando informações exatas sobre esses números, forneceu alguns detalhes sobre seu protocolo de abordagem. Foi informado que o Governo registrou 26 apontamentos de similaridade com base no reconhecimento facial, deixando vaga a quantidade de falsos positivos entre eles.

Explicado o funcionamento da utilização da ferramenta de reconhecimento facial, podemos afirmar a inexistência de ocorrência que se enquadrou no conceito de falso positivo, tendo em vista que **NENHUMA** pessoa foi conduzida para a Delegacia de Polícia sem que tivesse mandado de prisão ativo expedido contra sua pessoa. Ao longo de todo o período carnavalesco, por exemplo, o *software* de reconhecimento apontou similaridade de 26 pessoas com faces de pessoas constantes no banco de dados de pessoas com mandados de prisão em aberto. Desses 26 apontamentos realizados, houve vários com percentual de reconhecimento diversos que desencadearam a adoção do protocolo acima detalhado. Importante que se diga que muitos não chegaram a ter a identidade checada, seja porque o analista de inteligência adotou alguma das ações previstas no protocolo ou porque o alvo não foi encontrado no meio da multidão.¹⁷

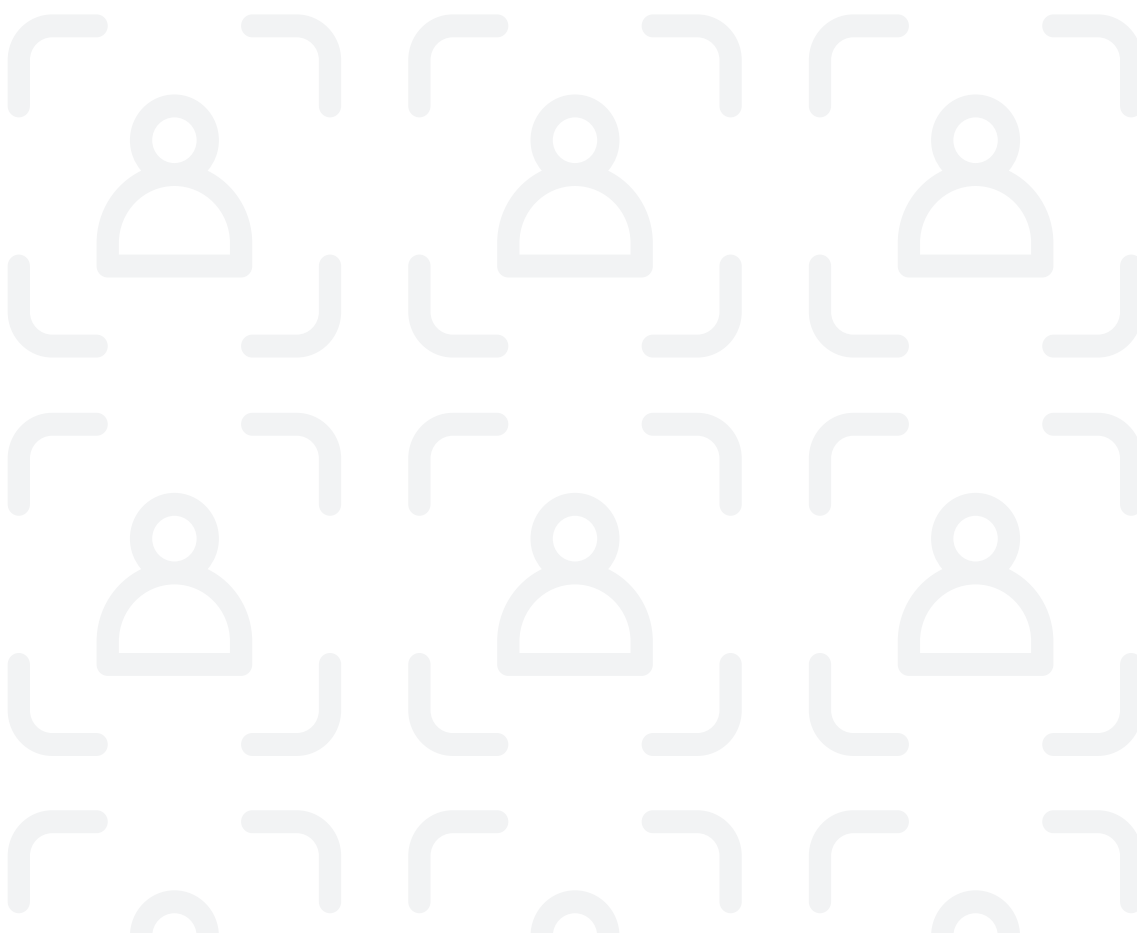
16. Ver mais em: SOUSA, Raquel. et al. Esportes, Dados e Direitos: O uso de Reconhecimento Facial nos Estádios Brasileiros. CESeC: São Paulo, 2024. Disponível [neste link](#). Acesso em: 13 set. 2024.


17. Resposta ao pedido de acesso à informação ao Governo de Pernambuco de número 202440154/2024.

Ao ser igualmente questionado, o Governo do Pará respondeu que as informações sobre o número de prisões, o número de pessoas desaparecidas localizadas e o número de falsos positivos têm caráter “sigiloso”, sem justificar o motivo de tal sigilo. A Lei de Acesso à Informação, em seu artigo 4, inciso III, define a informação de caráter sigiloso como “(...) aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado”. Essa justificativa, no entanto, não parece caber no caso em questão.

Essa falta de dados revela um cenário preocupante em relação ao uso do reconhecimento facial no policiamento, sobretudo porque há uma ambiguidade em relação à existência ou não desses dados. Deve-se levar em consideração que nenhuma tecnologia possui uma taxa de assertividade de 100%, logo os erros inevitavelmente acontecem. Ocorre que os erros ocasionados pelo reconhecimento facial se materializam em prisões injustas, constrangimentos inadequados, abordagens policiais violentas e violação dos direitos humanos.

A transparência e a visibilidade do número de pessoas detidas com o uso de TRF servem para mensurar a eficiência da tecnologia e, conseqüentemente, da política pública de segurança. Se esses indicadores são constantemente negligenciados, a população não tem como saber se as políticas realizadas em seu estado ou município estão de fato funcionando, ou seja, se o dinheiro público está sendo bem aplicado. A falta de quantificação e o não reconhecimento dos erros da tecnologia podem ser interpretados como uma forma de falta de transparência deliberada.





Acesso, barreiras e dificuldades

nos percursos da transparência ativa e passiva

Após o mapeamento dos projetos e a identificação de suas principais características, passamos a uma análise qualitativa da transparência ativa e passiva nessas iniciativas. Essa análise foi feita com base no acesso a sites governamentais das prefeituras, secretarias, polícias e Portais de Transparência dos entes federativos — estados e municípios —, bem como no uso da Lei de Acesso à Informação por meio de questionários sobre os pontos já discriminados. A seguir apresentamos os resultados dessa análise.

1. A TRANSPARÊNCIA (NÃO TÃO) ATIVA:

A transparência ativa se caracteriza pelo dever de órgãos públicos publicizarem informações, de forma proativa e espontânea, por meio de seus portais e outros canais (Araújo; Marques, 2019). Ao estabelecer uma política pública, a Administração deve, então, conferir ampla publicidade a seus atos, modos de aquisição, dispêndio do erário, resultados, dentre outras informações. No entanto, o que sobressai nesta análise em relação à transparência ativa é a dificuldade de encontrar informações que deveriam ser facilmente acessíveis.

O mecanismo mais evidente dessa modalidade ativa são os Portais de Transparência, utilizados por entidades federativas e órgãos públicos para divulgação ampla e acessível de informações de interesse público. Por este meio, as informações são disponibilizadas pelo Estado sem prévia ação da pessoa interessada. Assim, qualquer pessoa pode pesquisar sobre um contrato público, o vencimento de um servidor, o andamento de uma licitação, entre outras informações que, caso não estejam classificadas como sigilosas, estarão disponíveis nesses sítios eletrônicos. Não encontramos grandes dificuldades no acesso às informações pelos Portais de Transparência. Nas entidades pesquisadas durante a coleta de dados deste relatório, há um padrão: um ícone “Transparência” nos menus dos sites, permitindo à pessoa interessada fazer a busca pelo dado que lhe interessa.

Entretanto, se a ferramenta funciona bem, isso não significa que os mecanismos de transparência ativa estão sendo efetivos. Há uma acentuada falta de informações nos portais sobre os sistemas de reconhecimento facial utilizados. Muitas vezes, a fonte primária sobre a existência de sistemas de reconhecimento facial são os meios de comunicação jornalísticos.

Compreendendo o reconhecimento facial como uma linha da política de segurança pública, o que se espera é a divulgação voluntária pela Administração Pública de informações quanto a seu uso e, sobretudo, os seus resultados. Mas, conforme vimos, as prefeituras e os governos estaduais não tendem a divulgar voluntariamente informações como o número das prisões realizadas com base nas TRF. Por outro lado, o Governo do Estado da Bahia, por meio da sua Secretaria de Segurança Pública, divulga no seu portal de notícias as prisões realizadas com a ferramenta, em tom propagandista.



Outra ferramenta relevante para a transparência ativa é o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), previsto na LGPD e fundamental para a identificação de potenciais riscos aos titulares em relação ao tratamento de seus dados, útil para o escrutínio social e as autoridades reguladoras. Não existe uma legislação específica para regulamentar o tratamento de dados pessoais em investigações criminais e segurança pública, de forma que a confecção desse instrumento é voluntária. Entretanto, tendo em vista a sensibilidade do campo, o RIPD seria um instrumento de importante valor para o incremento de um modelo de gestão pública mais transparente. Conforme relatado anteriormente, apenas São Paulo (SP) e Curitiba (PR) apontaram a realização do RIPD, o que expõe a não efetivação da transparência.

A necessidade de tantos pedidos de respostas via LAI é a maior expressão dos gargalos de transparência ativa. A falta de informações disponíveis de forma voluntária pela Administração Pública obriga pessoas interessadas na realização de pedidos específicos de acesso à informação. Nesse sentido, podemos dizer que quanto mais dificuldades e barreiras existem na transparência ativa, mais a Administração terá de resolver essas situações respondendo a pedidos por meio dos mecanismos de transparência passiva.

LEI DE ACESSO À INFORMAÇÃO

E A AREIA MOVEDIÇA DA BUROCRACIA INFORMACIONAL

Se a transparência ativa se caracteriza pela espontaneidade e proatividade dos atores estatais, sua versão passiva se caracteriza pela ação do cidadão em buscar informações sobre a atividade pública. Nesse sentido, este relatório também buscou verificar gargalos e barreiras à transparência passiva em iniciativas que envolvem o uso de sistemas de identificação biométrica.

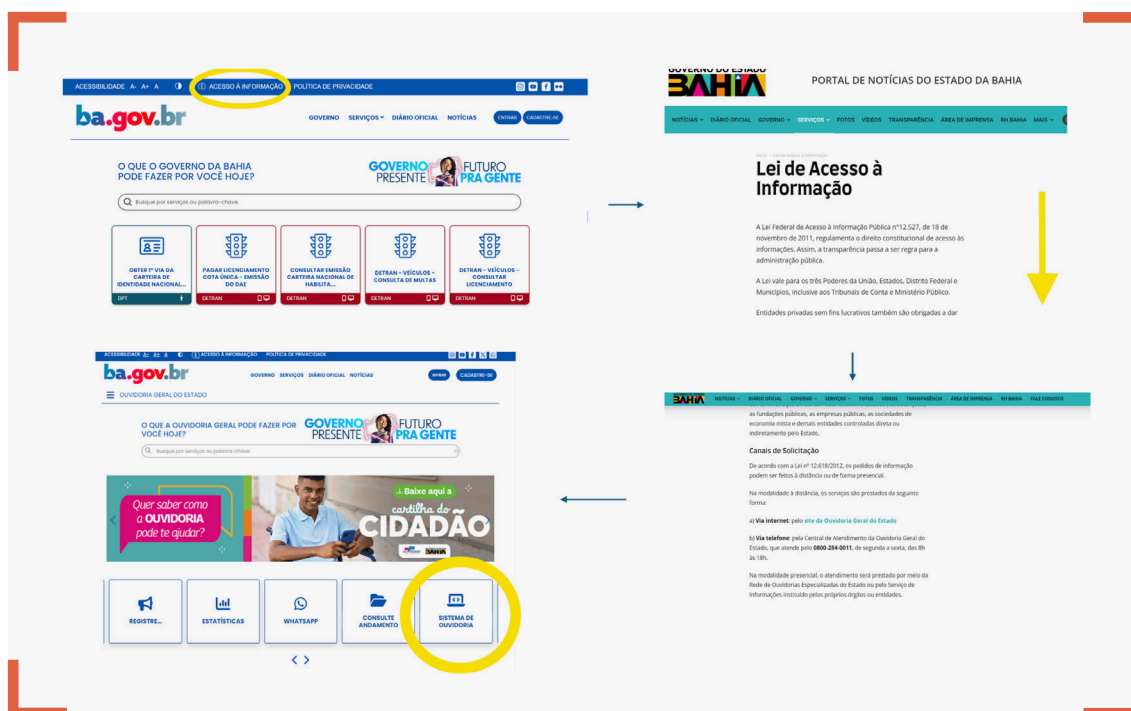
Um primeiro ponto são as plataformas utilizadas para a realização de pedidos de acesso à informação em plataformas digitais como o e-SIC, o FalaBR, entre outras que são utilizadas pela Administração Pública. As variadas plataformas têm exigências diferentes, que impactam qualitativamente no engajamento das pessoas com os sistemas de acesso à informação. Entre as exigências, destaca-se o fato do nível de informação exigido para a realização do cadastro junto às plataformas.

Tomemos como exemplo o Governo Estadual do Amapá, que usa o e-SIC e, para cadastro, exige os seguintes dados: nome, tipo de pessoa (física ou jurídica), o Cadastro de Pessoa Física (CPF) e o endereço eletrônico (e-mail). Só com o fornecimento desses dados pessoais é possível aceder ao site e fazer o pedido de acesso à informação, padrão que se repete em similares plataformas. O direito à informação da Administração Pública somente é efetivado, portanto, após o cadastro com dados pessoais.

Outra plataforma é o Fala.Br, utilizado por diferentes entes federativos e que tem o

objetivo de integrar serviços de ouvidoria e acesso à informação. Ela pode ser usada de duas formas: (i) a partir de login por cadastro de pessoa física e senha, que funcionará para o serviço específico que o cidadão está buscando; ou (ii) por meio de seu login no serviço governamental SouGov, que permite aceder amplamente diferentes serviços de acesso à informação.

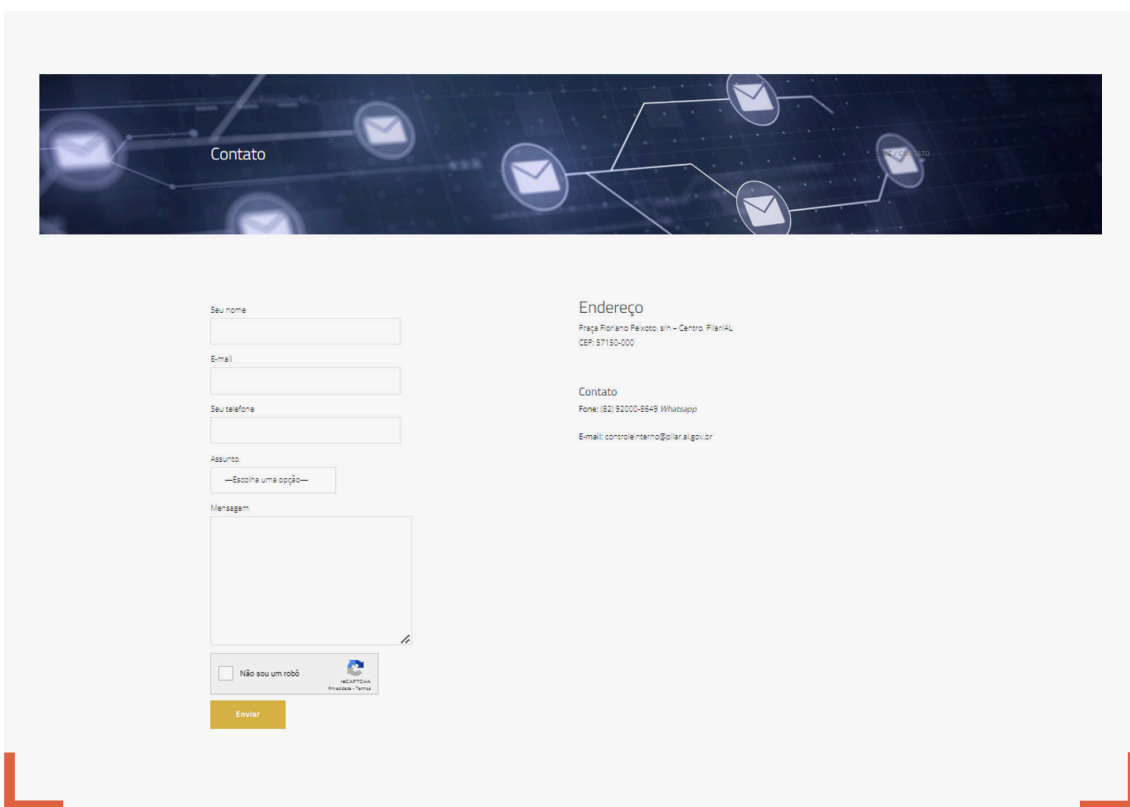
Também avaliamos a facilidade de chegar ao endereço eletrônico no qual se faz o pedido. No caso do Governo da Bahia, por exemplo, a pessoa interessada deve aceder ao endereço geral do Governo do Estado e seguir diferentes passos até finalmente chegar na plataforma TAG utilizada pela Ouvidoria, como mostram as imagens a seguir.



Imagens retiradas do Portal do Governo do Estado da Bahia

O longo caminho até o sistema amplia a possibilidade de desvios durante a sucessão de cliques. Compreendemos esse decurso de tempo como uma barreira ao acesso integral à informação, devido ao desgaste que promove, algo que a versão eletrônica dos canais de atendimento deveria evitar.

Ainda em relação às plataformas, destaca-se o caso do site da Prefeitura de Pilar (AL). Ao acessar o ícone do e-SIC no endereço, a pessoa interessada é encaminhada para uma página de contato com a Prefeitura. Essa página foge bastante dos padrões existentes na Administração Pública, inclusive não fornecendo um protocolo específico para o pedido de informação. Nesse caso específico, o pedido não foi respondido, o que contribui para a compreensão dessa infraestrutura de solicitação como deficitária na transparência passiva.

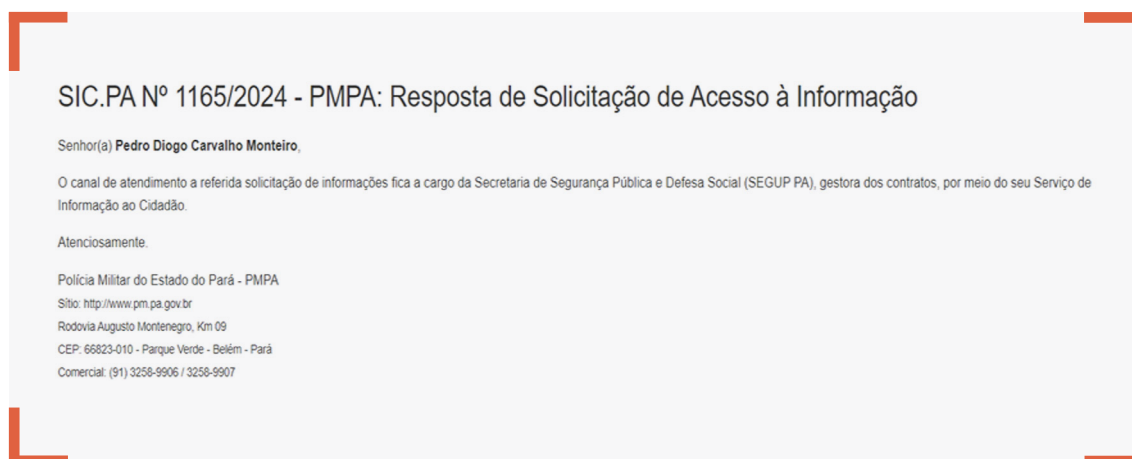


Imagens retiradas do Portal da Prefeitura Municipal de Pilar.

Outro exemplo que dificultou a realização de pedidos via LAI foi o limite de caracteres das plataformas usadas para esse fim. Percebemos que isso faz que elementos do pedido sejam reduzidos ou leva a pessoa a fragmentá-lo. Esse foi o caso da Prefeitura de São José de Campos (SP), no qual foi necessário realizar três pedidos — de número 8678, 86788 e 86784 — para complementar o padrão de questionário utilizado na pesquisa. O mesmo ocorreu com a Prefeitura de Vitória (ES), caso em que precisamos fazer dois pedidos — de números 2024.036.850 e 2024.036.853 —, e com

a Polícia Militar da Paraíba, em que também fizemos dois pedidos — de números 00099.001928/2024-0 e 00099.001927/2024-6.

Também se configura como barreira à transparência passiva a necessidade de fazer pedido adicional para um diferente órgão para conseguir as respostas. A exemplo, isso ocorreu nos pedidos de acesso à informação feitos ao Governo do Pará: foi necessária a realização de dois pedidos de acesso à informação, levando a um dispêndio de tempo maior para chegar a informações relevantes.



Tela do e-SIC do Governo do Estado do Pará

Notáveis também são os casos em que não há qualquer retorno das autoridades aos pedidos de acesso à informação, a exemplo do que ocorreu com a Prefeitura de Rosário do Catete,¹⁸ no estado do Sergipe, que até o momento da finalização desta pesquisa não havia respondido ao nosso pedido. O mesmo ocorreu com as prefeituras de Petrolina, de Paulista e com os Governos Estaduais de Roraima e Rondônia.

Alguns pedidos também foram prorrogados além do prazo máximo indicado na LAI, que é de 20 dias para resposta. A Prefeitura Municipal de Goiânia e a Prefeitura de Curitiba, por exemplo, levaram cerca de dois meses para responder. O tempo de resposta é um fator importante a ser considerado, especialmente em anos eleitorais. Se enviássemos o pedido em junho, talvez não recebêssemos respostas.

Todos esses eventos expõem situações em que, apesar de a Lei de Acesso à Informação abrir caminhos para mais transparência e para a efetivação do princípio da publicidade, existem diferentes gargalos no modo como a burocracia informacional está sendo operada. Nesse sentido, ficam evidentes os modos como a transparência

passiva pode ser sabotada, não somente por causa da recusa na informação, mas também por essas dificuldades e barreiras. Esses mecanismos precisam ser mais diretos e de fácil manuseio, de forma que qualquer pessoa interessada possa ter acesso a elementos informativos essenciais das políticas públicas implementadas.

O que nossa pesquisa revela é que tanto nos processos de transparência ativa quanto de transparência passiva, existem impedimentos à efetivação do direito à informação como corolário da democracia no Brasil. Esse problema ganha contornos mais delicados quando estamos tratando de política de segurança pública, uma pauta que envolve a possibilidade de restrição da liberdade, além de outros desdobramentos sensíveis, e exige, portanto, maior acurácia. Esses contornos se agravam quando adicionamos nessa equação o uso de uma tecnologia como o reconhecimento facial, que está em franca expansão no território nacional e tem sido criticada por falta de eficiência, discriminação algorítmica com base em raça e gênero e violação de direitos a privacidade e proteção de dados. Nesse sentido, abordar o nível de transparência conferido pelas autoridades às escolhas feitas no âmbito dessa política pública se torna extremamente necessário.

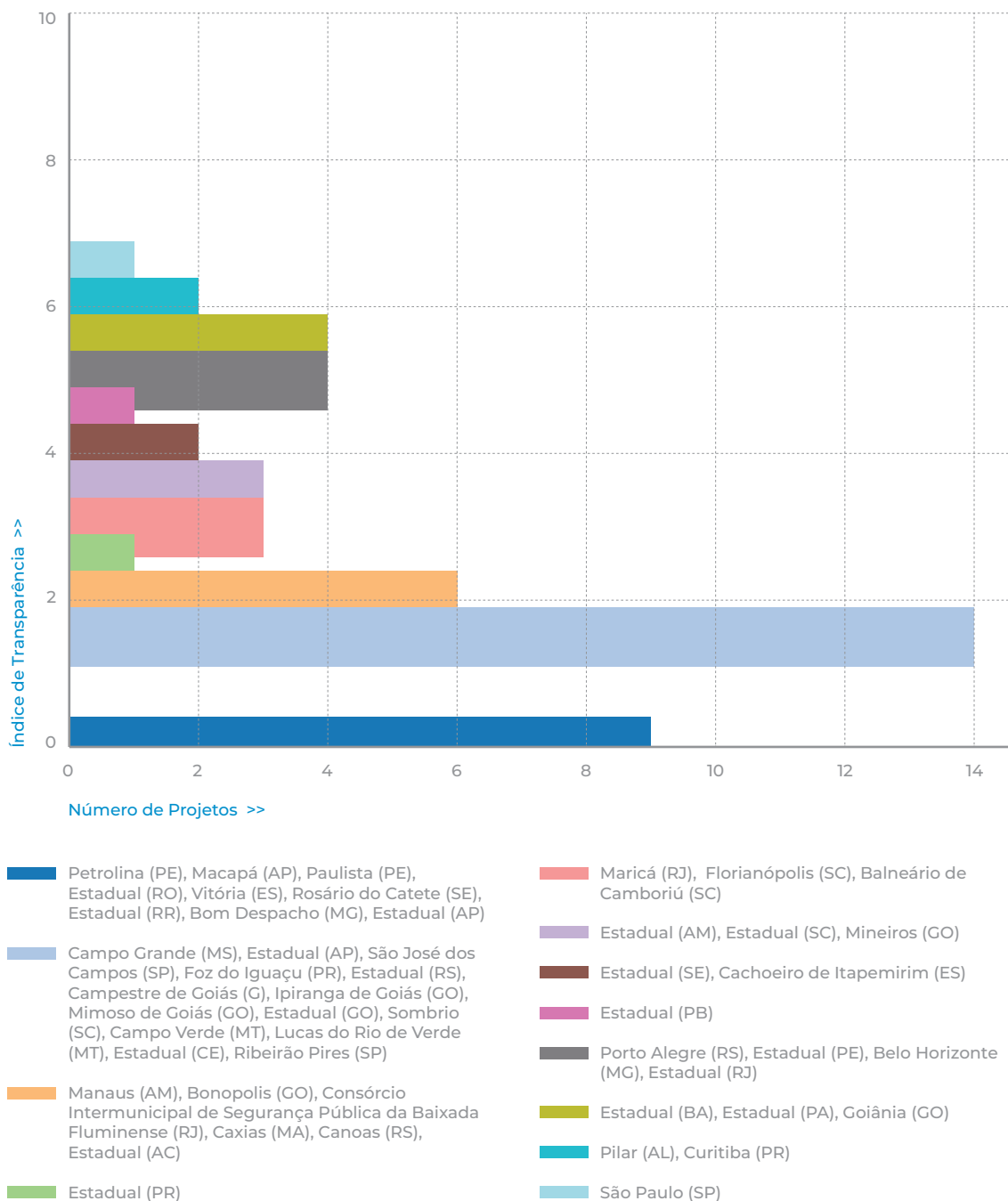




O nível de transparência dos projetos

Com base na análise que apresentamos neste relatório, desenvolvemos um índice de transparência que permite uma visualização panorâmica dos níveis de transparência ativa e passiva da amostra dos projetos de reconhecimento facial selecionados para esta pesquisa. Esse índice não tem como objetivo criar um ranqueamento dos projetos, nem oferecer uma análise comparativa geral, tendo em vista que se trata de uma amostra limitada. A proposta é demonstrar como a implantação e a operacionalização dessas tecnologias como política pública têm acontecido com níveis baixos de transparência, de prestação de contas e de participação pública, além de violar uma série de direitos.

ÍNDICE DE TRANSPARÊNCIA DOS PROJETOS



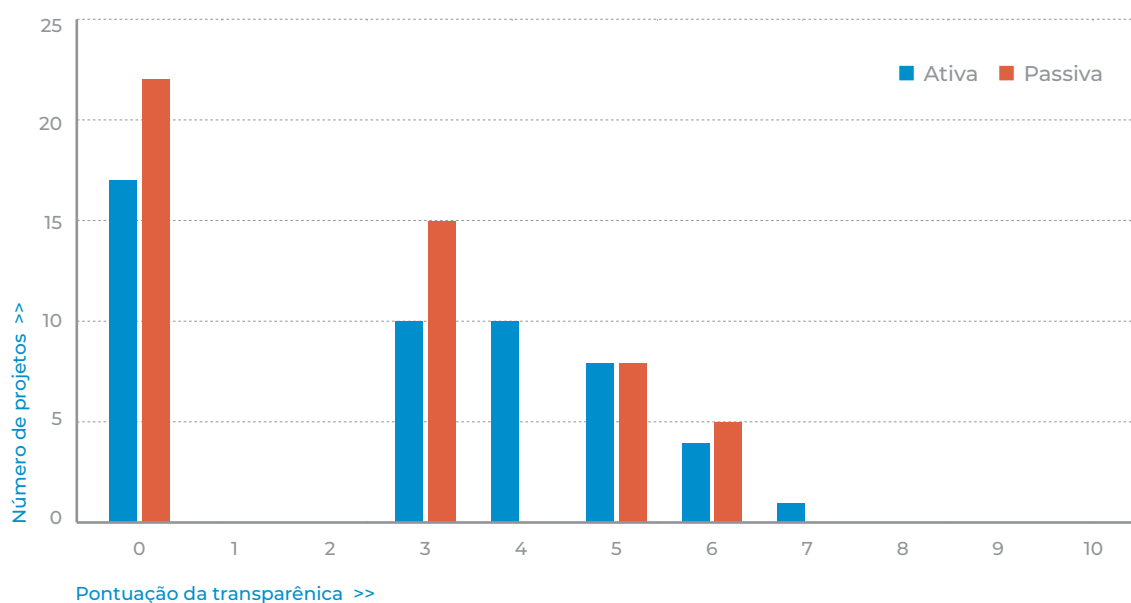
Fonte: CESeC e Lapin, 2024.

O gráfico acima destaca a elevada quantidade de projetos muito pouco transparentes. Mais de 70% deles têm um índice de transparência inferior a quatro, sendo que aproximadamente 18% apresentam índice igual a zero. Apenas o projeto municipal de São Paulo obteve a nota máxima (sete pontos) em termos de transparência ativa devido à quantidade e à qualidade das informações fornecidas. Ressalta-se que, mesmo assim, ainda não há informações claras sobre o uso operacional de TRF. Em contraste, 34% dos projetos não pontuaram em transparência ativa, o que significa que em 17 iniciativas não há qualquer informação disponível. Boa parte da amostra concentrou-se entre três e cinco pontos. A soma desses projetos equivale a 56% do total.

No que diz respeito à transparência passiva, o cenário fica ainda mais preocupante. Dos 50 projetos analisados, 22 não obtiveram nenhuma pontuação. Ou seja, em 44% da amostra não obtivemos um retorno considerável e/ou não recebemos resposta alguma ao pedido de informação. Todos os projetos ficaram abaixo de sete pontos, sendo seis a maior nota registrada. Essa pontuação foi obtida por cinco projetos: três municipais — um de São Paulo (SP), um de Pilar (AL) e um de Curitiba (PR) — e dois estaduais do Pará. Isso significa que, embora tenhamos recebido algumas respostas de acordo com a Lei de Acesso à Informação, nem todas apresentaram a qualidade e a completude necessárias. É importante ressaltar que a ausência de um dado — neste caso, a falta de resposta — também é uma informação significativa.

No gráfico a seguir, observa-se que a maior parte dos projetos têm nota inferior a três pontos tanto na transparência passiva quanto na ativa. Se compararmos as duas formas de transparência, notamos que há um maior número de projetos que zeraram na transparência passiva.

ÍNDICE DE TRANSPARÊNCIA DOS PROJETOS

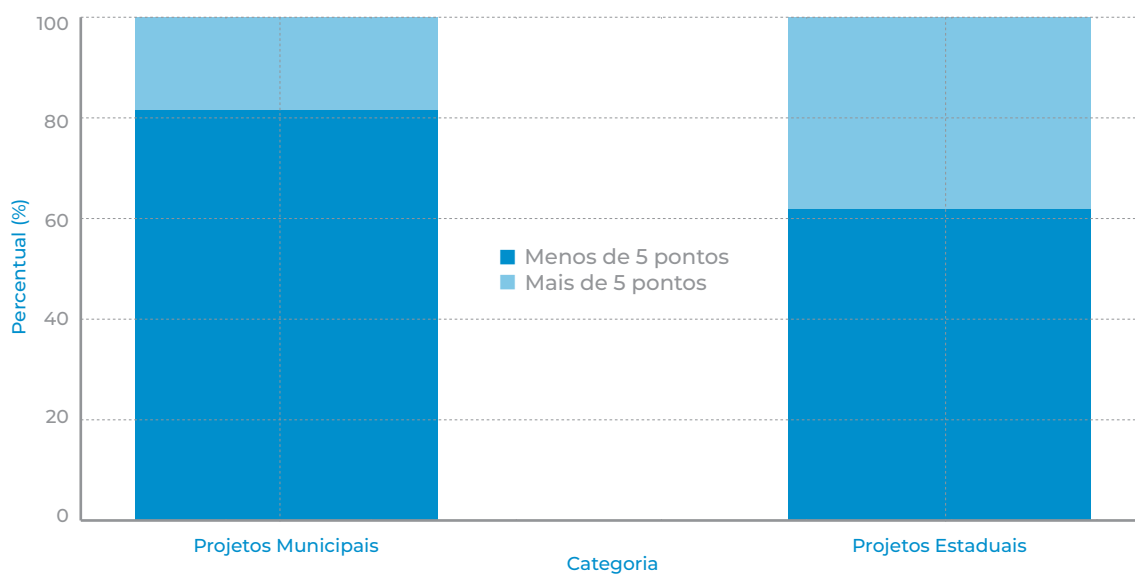


Fonte: CESeC e Lapin, 2024.

Os dados nos convidam a refletir sobre a diferença entre os projetos municipais e estaduais de TRF. Mas, antes de analisá-los, é preciso indicar, como sinalizado no panorama geral, que a amostra é composta por 18 projetos estaduais e 32 municipais. Logo, as estatísticas aqui apresentadas levam em consideração o total de cada esfera. Dos projetos municipais, 81,25% registraram menos de cinco pontos na transparência ativa. Em relação à transparência passiva, 78,13% pontuaram abaixo de seis. Já dos projetos estaduais, 61,11% pontuaram menos de cinco em transparência ativa, e apenas dois projetos atingiram seis pontos na transparência passiva. Esses números podem indicar um padrão de menor transparência nos projetos municipais, especialmente na dimensão de transparência ativa, onde uma maior proporção de

projetos estaduais atinge pontuações mais altas. A disparidade nas pontuações sugere diferenças significativas nas práticas de divulgação e na resposta às demandas por informações entre as duas esferas de governo. Essa tendência pode refletir diferenças estruturais e institucionais na gestão dos dados, recursos disponíveis, ou até mesmo nos níveis de controle e fiscalização aplicados em cada contexto.

COMPARAÇÃO DA TRANSPARÊNCIA ATIVA EM PROJETOS DE RECONHECIMENTO FACIAL



Fonte: CESeC e Lapin, 2024.

Este é um cenário preocupante, porque observamos nos últimos anos um processo de municipalização dos projetos de TRF e, conseqüentemente, das políticas de segurança pública.¹⁹ É preciso mencionar o quanto esse movimento já é controverso por si só, já que, de acordo com o artigo 144 da Constituição Federal do Brasil, a segurança pública não é responsabilidade ou dever dos municípios. Assim, os municípios que estão implementando tecnologias de reconhecimento facial se encontram em uma espécie de limbo jurídico que pode favorecer uma dinâmica desregulada de aquisição e operacionalização de TRF. A ausência de responsabilidade formal pela segurança pública nos municípios implica que eles não são devidamente cobrados ou responsabilizados pela gestão e transparência dessas tecnologias.

Os dados analisados evidenciam a complexidade e os desafios associados à transparência nos projetos de reconhecimento facial no Brasil. Embora algumas iniciativas

¹⁹ Sobre esse tópico, a implementação de reconhecimento facial em Goiás é um exemplo. Ver mais em: NUNES, Pablo; LIMA, Thallita G. L.; RODRIGUES, Yasmin. **Das planícies ao planalto: como Goiás influenciou a expansão do reconhecimento facial na segurança pública brasileira**. Rio de Janeiro: CESeC, 2023. Disponível [neste link](#). Acesso em: 13 set. 2024.

tenham apresentado um grau mediano em termos de transparência ativa, a realidade é que a grande maioria dos projetos apresenta níveis insuficientes de clareza e prestação de contas. A baixa pontuação em transparência, especialmente a passiva, considerando que quase metade dos projetos não ofereceu respostas satisfatórias, reflete uma desconexão entre a implementação dessas tecnologias e a disponibilidade das informações ao público. As variações nas pontuações entre os projetos municipais e estaduais indicam que a transparência é influenciada por uma série de fatores contextuais e operacionais, resultando em uma disparidade significativa na qualidade da informação disponível.

Esse cenário levanta questões importantes sobre a confiabilidade e a responsabilidade na condução desses projetos, sugerindo que, apesar dos alegados “avanços” em direção à modernização da política pública, a transparência ainda é uma área em que há muito a ser aprimorado para garantir que os cidadãos tenham acesso completo e preciso às informações que impactam diretamente suas vidas e seus direitos.

Tabela 2. Índice de Transparência de acordo com a amostra

Projeto	Operador	Ano de início	Custo do Projeto	Transparência Ativa	Transparência Passiva	Índice de Transparência
São Paulo, SP	Não identificado	2023	R\$ 9.800.000,00	7	6	6,5
Pilar, AL	Guarda Municipal	2019	R\$ 203.000,00	6	6	6
Curitiba, PR	Guarda Municipal	2021	R\$ 3.132.931,56	6	6	6
Bahia (estadual)	Polícia Militar	2019	R\$ 665.437.861,33	6	5	5,5
Pará (estadual)	Polícia Militar e Polícia Civil	2021	R\$ 20.193,00	5	6	5,5
Goiânia, GO	Guarda Civil Metropolitana	2022	R\$ 17.945.600,00	6	5	5,5
Pará (estadual)	Centro Integrado de Operações	2024	R\$ 20.193,00	5	6	5,5
Porto Alegre, RS	Guarda Municipal	2023	R\$ 2.340.400,00	5	5	5
Pernambuco (estadual)	Secretaria de Segurança Pública e correlatos	2023	R\$ 1.619.999,00	5	5	5
Belo Horizonte, MG	Secretaria Municipal de Segurança e Prevenção	2023	R\$ 3.467,50	5	5	5
Rio de Janeiro (estadual)	Polícia Militar	2023	R\$ 18.000.000,00	5	5	5
Paraíba (estadual)	Polícia Militar	2023	R\$ 100.000.000,00	4	5	4,5
Aracaju, SE (estadual)	Secretaria de Segurança Pública de Sergipe	2022	R\$ 1.225.995,45	5	3	4
Cachoeiro de Itapemirim, ES	Guarda Civil Municipal	2023	R\$ 12.390,00	3	5	4
Amazonas (estadual)	Polícia Militar	2021	R\$ 3.754.851,75	4	3	3,5
Santa Catarina (estadual)	Polícia Militar	2021	Sem informação	4	3	3,5

Tabela 2. Índice de Transparência de acordo com a amostra						
Projeto	Operador	Ano de início	Custo do Projeto	Transparência Ativa	Transparência Passiva	Índice de Transparência
Mineiros, GO	Não identificado	2022	Sem informação	4	3	3,5
Maricá, RJ	Guarda Municipal	2022	R\$ 11.396.700,00	3	3	3
Florianópolis, SC	Não identificado	2023	Sem informação	3	3	3
Balneário de Camboriú, SC	Não identificado	2023	Sem informação	3	3	3
Paraná (estadual)	Polícia Militar	2022	R\$ 383.980,50	5	0	2,5
Manaus, AM	Secretaria de Segurança Pública e correlatos	2021	R\$ 2.994.820,00	4	0	2
Bonópolis, GO	Não identificado	2022	R\$ 254.834,29	4	0	2
Baixada Fluminense, RJ	Consórcio Intermunicipal de Segurança Pública na Baixada Fluminense (CISPBAF)	2022	R\$ 76.938.186,00	4	0	2
Caxias, MA	Guarda Municipal	2023	Sem informação	4	0	2
Canoas, RS	Guarda Municipal	2023	R\$ 11.298.999,98	4	0	2
Acre (estadual)	Polícia Militar	2023	Sem informação	4	0	2
Campo Grande, MS	Guarda Civil Metropolitana	2020	Sem informação	0	3	1,5
Amapá (estadual)	Centro de Comando e Controle de Operações	2021	R\$ 5.000.000,00	0	3	1,5
São José dos Campos, SP	Guarda Civil e demais forças de segurança	2021	Sem informação	3	0	1,5
Foz do Iguaçu, PR	Centro de Controle e Operações (CCO)	2021	Sem informação	3	0	1,5
Rio Grande do Sul (estadual)	Polícia Civil e Brigada Militar e Departamento de Comando e Controle Integrado (DDCI da Secretaria Estadual de Segurança Pública)	2021	R\$ 10.900.000,00	3	0	1,5
Campestre de Goiás, GO	Não identificado	2022	R\$ 261.479,12	3	0	1,5
Ipiranga de Goiás, GO	Não identificado	2022	R\$ 255.581,57	3	0	1,5
Mimoso de Goiás, GO	Não identificado	2022	R\$ 259.523,32	3	0	1,5
Goiás (estadual)	Polícia Militar e demais forças de segurança	2023	R\$ 467.100,00	0	3	1,5
Sombrio, SC	Não identificado	2023	Sem informação	0	3	1,5
Campo Verde, MT	Não identificado	2023	Sem informação	0	3	1,5

Tabela 2. Índice de Transparência de acordo com a amostra

Projeto	Operador	Ano de início	Custo do Projeto	Transparência Ativa	Transparência Passiva	Índice de Transparência
Lucas do Rio de Verde, MT	Não identificado	2023	R\$ 1.553.312,00	0	3	1,5
Fortaleza, CE (estadual)	Polícia Militar	2024	Sem informação	0	3	1,5
Ribeirão Pires, SP	Guarda Civil Municipal	2024	Sem informação	0	3	1,5
Petrolina, PE	Guarda Municipal	2020	Sem informação	0	0	0
Macapá, AP	Polícia Civil	2021	Sem informação	0	0	0
Paulista, PE	Secretaria de Segurança Pública e correlatos	2021	Sem informação	0	0	0
Estadual, RO	Polícia Militar	2021	Sem informação	0	0	0
Vitória, ES	Guarda Civil Municipal	2022	R\$ 15.000.000,00	0	0	0
Rosário do Catete, SE	Não identificado	2023	R\$ 153.690,00	0	0	0
Roraima (estadual)	Polícia Militar e demais forças de segurança	2023	Sem informação	0	0	0
Bom Despacho, MG	Não identificado	2023	R\$ 9.000.000,00	0	0	0
Amapá (AP)	Polícia Militar	2024	Sem informação	0	0	0

Fonte: CESeC e Lapin, 2024.





Conclusão

Na última década, o Brasil viveu a multiplicação e pulverização do uso das tecnologias de reconhecimento facial tanto em projetos públicos, como os de segurança pública, como privados, como os que observamos no âmbito do lazer e dos esportes. Apesar desse aumento expressivo, a maior parte da população desconhece que tem seus dados coletados e mais ainda a forma como eles são tratados e utilizados. A despeito desse direito ser garantido legalmente, os cidadãos estão sujeitos a abordagens policiais inadequadas, a terem seus dados vendidos para o desenvolvimento de *softwares* de IA e inúmeras outras possibilidades de uso de dados que nem conseguimos mensurar. É nesse cenário que decidimos realizar uma pesquisa sobre transparência.

Com isso, podemos observar como a crescente implementação das TRF no Brasil é marcada por uma alarmante falta de transparência e prestação de contas, revelando um cenário de opacidade que compromete os direitos fundamentais dos cidadãos, assim como fere os princípios que regem a formatação de políticas públicas, como publicidade e eficiência. A ausência de regulamentação específica, aliada à dispersão das responsabilidades, e a ausência de mecanismos de prestação de contas entre diferentes esferas da Administração Pública expõem os labirintos burocráticos da política pública de segurança que produz riscos desnecessários e flexibiliza os direitos das pessoas. O cenário atual brasileiro de expansão de iniciativas de uso de TRF reforça a necessidade de uma reflexão crítica e responsável sobre o uso dessas tecnologias.

A análise dos dados coletados para esta pesquisa demonstra que a maioria dos projetos de TRF para segurança pública no Brasil opera sem atender aos padrões mínimos de transparência ativa e passiva. Isso significa que a população não conhece informações essenciais sobre o funcionamento dessas tecnologias, os custos envolvidos, os fornecedores contratados ou mesmo a real eficácia dessas ferramentas na alegada redução da criminalidade. A falta de transparência e a dificuldade de acesso a informações reforçam um contexto em que a vigilância massiva é implementada sem o devido controle social, abrindo espaço para abusos, usos desproporcionais das ferramentas e possíveis práticas discriminatórias.

Considerando a ausência de evidências sobre a eficácia dessas tecnologias no aumento da segurança e na redução da criminalidade, a falta de monitoramento e avaliação adequados do seu uso, os graves e repetidos casos de discriminação atrelados, como a produção de falsos positivos, fica evidente que a continuidade do uso de TRF como política pública de segurança não se justifica. A segurança pública deve ser orientada por políticas baseadas em evidências, com transparência e respeito aos direitos fundamentais, garantindo que quaisquer medidas adotadas sejam eficazes, proporcionais e sujeitas a mecanismos robustos de controle, prestação de contas e responsabilização.

Diante dessas constatações, o banimento do uso de tecnologias de reconhecimento facial no Brasil, especialmente em atividades de segurança pública, é uma medida urgente e necessária. Sem garantias de transparência, controle social efetivo e respeito aos direitos fundamentais, a continuidade dessas práticas não só perpetua desigualdades e discriminações, como também enfraquece a confiança da população nas instituições públicas. O banimento das TRF é um passo crucial para a defesa dos direitos e liberdades fundamentais, assegurando, assim, que as políticas de segurança pública estejam verdadeiramente comprometidas com a segurança de todos.

Referências

ALSUR. Reconhecimento facial em Latam. Tendências na implementação de uma tecnologia perversa. **Alsur**, 2021. Disponível [neste link](#). Acesso em: 20 set. 2024.

ANANNY, Mike; CRAWFORD, Kate. Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. **new media & society**, v. 20, n. 3, p. 973-989, 2018.

BENJAMIN, Ruha. **Race after technology**: Abolitionist tools for the new Jim code. Boston: Polity, 2020.

BISCHOFF, Paul. Facial recognition technology (FRT): 100 countries analyzed. **Comparitech**, 28 de junho de 2021. Disponível [neste link](#). Acesso em: 20 set. 2024.

BRASIL. Ministério da Justiça e Segurança Pública. Portaria N ° 793, de 24 de outubro de 2019. **Diário Oficial da União**: seção 1, Brasília-DF, edição 208, p. 55, 24 de out. 2019. Disponível [neste link](#). Acesso em: 09 set. 2024.

BRASIL. Constituição de 1988. **Constituição da República Federativa do Brasil**, art. 5º, inc. LXXIX. Brasília, DF: Câmara dos Deputados, [2018]. Disponível [neste link](#). Acesso em: 19 set. 2024.

BRASIL. Constituição de 1988. **Constituição da República Federativa do Brasil**, art. 37º. Brasília, DF: Câmara dos Deputados, [2018]. Disponível [neste link](#). Acesso em: 19 set. 2024.

BROWNE, Simone. Digital epidermalization: Race, identity and biometrics. **Critical Sociology**, v. 36, n. 1, p. 131-150, 2010.

BUOLAMWINI, Joy; GERBRU, Timnit. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. In: **Proceedings of the 1st Conference on Fairness, Accountability and Transparency**, edited by Sorelle A. Friedler and Christo Wilson, New York, n. 81, p.77-91, 2018. Disponível [neste link](#). Acesso em: 20 set. 2024.

FERGUSON, Andrew Guthrie. **The rise of big data policing**: Surveillance, race, and the future of law enforcement. New York: NYU Press, 2017.

MEIJER, Albert; 'T HART, Paul; WORTHY, Ben. Assessing government transparency: An interpretive framework. **Administration & Society**, v. 50, n. 4, p. 501-526, 2018.

NUNES, Pablo; LIMA, Thallita G. L.; RODRIGUES, Yasmin. **Das planícies ao planalto**: como Goiás influenciou a expansão do reconhecimento facial na segurança pública brasileira. Rio de Janeiro: CESeC, 2023. Disponível [neste link](#). Acesso em: 20 set. 2024.

NUNES, Pablo; LIMA, Thallita G. L.; CRUZ, Thaís G. **O sertão vai virar mar**: expansão do reconhecimento facial na Bahia. Rio de Janeiro: CESeC. 2023. Disponível [neste link](#). Acesso em: 20 set. 2024.

SOUSA, Raquel. et al. **Esportes, Dados e Direitos**: O uso de Reconhecimento Facial nos Estádios Brasileiros. CESeC: São Paulo, 2024. Disponível [neste link](#). Acesso em: 13 set. 2024.

Anexo I

Sumário de categorias do banco de dados:

REGIÃO: Indica a região geográfica do Brasil (e.g., Centro-Oeste).

UF: Unidade Federativa onde o município está localizado.

MUNICÍPIO: Nome do município onde o projeto está sendo implementado.

ESFERA: Esfera de governo responsável pelo projeto (municipal, estadual ou federal).

ANO DE ATIVAÇÃO: Ano em que o projeto foi ativado.

STATUS: Status atual do projeto (e.g., em uso).

OPERADOR: Entidade responsável pela operação do sistema de reconhecimento facial.

LOCAL DE UTILIZAÇÃO: Local onde o sistema está sendo utilizado (e.g., Via pública).

CUSTO DO PROJETO: Custo total do projeto.

MODO DE AQUISIÇÃO: Método pelo qual o equipamento foi adquirido (e.g., Doação/Contrato).

EDITAL E TERMO DE REFERÊNCIA: Disponibilidade de edital e termos de referência.

OBJETO DO CONTRATO: Descrição do objeto do contrato.

ÓRGÃO RESPONSÁVEL PELO CONTRATO:

Órgão responsável pela contratação.

EMPRESA CONTRATADA: Empresa ou entidade contratada para implementar o projeto.

RELATÓRIO DE IMPACTO: Indicação da existência de um relatório de impacto.

POLÍTICA DE PROTEÇÃO DE DADOS: Existência de políticas de proteção de dados e segurança da informação.

IMPRENSA: Referências de artigos da imprensa relacionados ao projeto.

DOCUMENTOS OFICIAIS: Links para documentos oficiais do projeto.

LAI SOLICITAÇÃO/PROTOCOLO: Protocolo da solicitação de acesso à informação.

LAI RESPOSTA: Resposta recebida pela solicitação de acesso à informação.

GRAU DO RETORNO DE LAI: Grau de retorno obtido por meio das solicitações feitas via LAI (e.g., Respondida, Não respondida).

GRAU DE DIFICULDADE DE ACESSO À INFORMAÇÃO: Grau de dificuldade encontrado para acessar as informações.

OBSERVAÇÕES DAS PESQUISADORAS: Observações feitas pelas pesquisadoras durante a coleta de dados.

STATUS (PÓS-LAI): Status do projeto após as respostas das solicitações LAI.

Anexo II

Perguntas enviadas por LAI

Anexo III

Respostas dos pedidos por LAI

