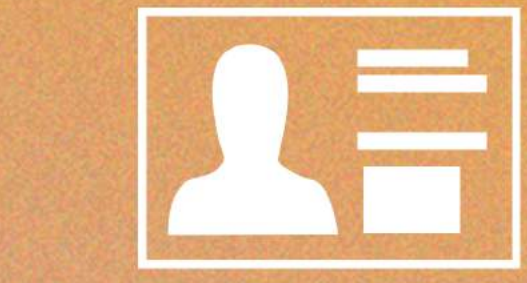
R E S U M O

VIGILÂNCIA AUTOMATIZADA:

uso de reconhecimento facial pela Administração Pública



LAPIN

LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET

Realização:
Laboratório de Políticas Públicas e Internet - LAPIN

Autoria:
Carolina Reis
Eduarda Costa Almeida
Fernando Fellows Dourado
Felipe Rocha da Silva

Revisão:
Amanda Espiñeira
José Renato Laranjeira de Pereira
Thiago Moraes

Diagramação/Ilustrações:
Pietra Polo

Sugestão de citação:
REIS, Carolina; ALMEIDA, Eduarda; DA SILVA; Felipe; DOURADO, Fernando. Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela administração pública no Brasil: versão resumida. Brasília: Laboratório de Políticas Públicas e Internet, 2021.

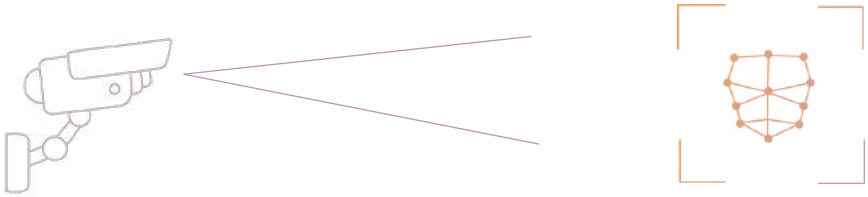
A pesquisa conduzida neste relatório foi concluída em maio de 2021.

lapin.org.br **@lapin.br** **/lapinbr** **/lapinbr**

Nas cinco regiões do Brasil, tecnologias de vigilância estão sendo utilizadas pelo setor público de diversas maneiras, com destaque para as **câmeras de videomonitoramento e a tecnologia de reconhecimento facial** (RF).

O uso de sistemas de RF aumentou exponencialmente nos últimos anos. Pesquisas demonstram que eles já são implantados pelo menos desde 2011 no país.[1] A partir de então, os casos de uso se proliferaram e projetos legislativos que propõem regulamentações sobre o tema avançam nas câmaras legislativas das regiões do Brasil. É sobre esse fenômeno que vamos tratar brevemente neste resumo do *Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela Administração Pública no Brasil*.

A tecnologia de reconhecimento facial funciona da seguinte forma:



Uma câmera coleta a imagem de um rosto que passa por ela.

O sistema identifica métricas específicas do rosto daquela pessoa, como a distância entre os olhos, largura do queixo e o comprimento da boca.

Com essas informações, um software calcula uma espécie de fórmula que consiste na **assinatura facial**, como uma digital do dedo, que é a chave para identificação dessa pessoa.[2] Essa assinatura é comparada com outras já armazenadas em um banco de dados de imagens ou de assinaturas de indivíduos que se pretende identificar. Assim, quando as assinaturas faciais são compatíveis, é possível identificar um sujeito de forma automatizada.

---

[1] INSTITUTO IGARAPÉ. Reconhecimento Facial no Brasil, 2019. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em 12 mar 2021.

[2] ELECTRONIC FRONTIER FOUNDATION (EFF). Face Recognition. 2017. Disponível em: https://www.eff.org/pages/face-recognition. Acesso em: 5. mai. 2020.

A assinatura facial é a combinação de características físicas únicas da pessoa, por isso ela é classificada como um dado biométrico.[3]

E por que isso é importante?

Diferentemente de outras informações, como senhas e números de telefone, a alteração das características faciais de um indivíduo é bastante difícil. O funcionamento dessa tecnologia é arriscado justamente em razão da natureza dos dados tratados.

Outro risco diz respeito à possibilidade de erro do sistema. Identificar uma pessoa como sendo outra ou simplesmente não identificá-la pode levar a situações de discriminação ou restrição de direitos. O que isso significa na prática?
Aqui vai um exemplo:

Um homem já foi preso por engano após ser identificado erroneamente pelo sistema de RF, mesmo sendo inocente.[4]

EM OUTROS CONTEXTOS, O PROBLEMA SE REPETE!

Uma estudante de Brasília deixou de ser reconhecida pelo sistema de RF e teve seu benefício de passe livre bloqueado depois que passou a usar seu cabelo cacheado e não foi identificada pela tecnologia.[5] Essas tecnologias têm despertado diversos questionamentos sobre seus impactos nos espaços públicos e na vida cotidiana das pessoas sob o argumento de colocarem em risco direitos humanos e liberdades civis ao permitir a violação de direitos fundamentais, como a privacidade, a liberdade e a proteção de dados pessoais.

---

[3] THALES. Biometrics: authentication & identification (definition, trends, use cases, laws and latest news) - 2020 review. 2020. Disponível em: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics. Acesso em: 5 mai. 2020.

[4] ALMEIDA, Emily. Homem é preso por engano em Copacabana. 2019. Disponível em: https://bandnewsfmrio.com.br/editorias-detalhes/homem-e-preso-por-engano-em-copacabana. Acesso em: 13 mar 2021.

[5] TEIXEIRA, Isadora. Biometria facial nos ônibus não reconhece mudança visual de alunos. 2018. Disponível em: https://www.metropoles.com/distrito-federal/transporte-df/biometria-facial-nos-onibus-nao-reconhece-mudanca-visual-de-alunos. Acesso em: 8 abr. 2021.

PRINCIPAIS IMPACTOS NEGATIVOS DO USO DAS TECNOLOGIAS DE RECONHECIMENTO FACIAL

Vigilância em Massa

A vigilância por dados biométricos em larga escala ocorre de forma irrestrita, sem definição prévia de um alvo específico e muitas vezes ininterruptamente.

Violação de Direitos Fundamentais

O uso de tecnologias de RF afronta a privacidade, a liberdade de ir e vir, e a presunção de inocência, já que permite o monitoramento e identificação das pessoas quando ocupam espaços públicos como se fossem suspeitas.

Racismo

Em razão de diferenças significativas quanto à acurácia de sistemas de reconhecimento facial na avaliação de rostos de pessoas não brancas, importa destacar que soluções em tecnologias de RF refletem o racismo na sociedade.[6]

Transfobia

Os sistemas de RF reiteradamente negam visibilização a identidades divergentes, conflitando com a auto-identificação de gênero,[7] acirrando violências e reforçando o cerceamento de direitos às pessoas transsexuais e não-binárias.

Violação dos direitos de crianças e adolescentes

Por serem sujeitos de direito em desenvolvimento, crianças e adolescentes têm capacidade de discernimento ainda em formação, o que as deixa mais vulneráveis ao mau uso do seus dados pessoais por terceiros.

---

[6] BUOLAMWINI, Joy; GEBRU; Timmit. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Conference on Fairness, Accountability, and Transparency, Proceedings of Machine Learning Research 81, 1–15, 2018.

[7] CODING RIGHTS. Reconhecimento Facial no Setor Público e Identidades Trans. Disponível em: https://codingrights.org/docs/rec-facial-id-trans.pdf. Acesso em: 28 fev. 2021.

A Lei Geral de Proteção de Dados (LGPD) figura como um importante instrumento na mitigação das potenciais violações de direitos decorrentes do uso da tecnologia do reconhecimento facial. Vigente desde 2020, a lei estabeleceu alguns princípios e um arcabouço legislativo sobre a proteção para o devido tratamento de dados pessoais em observância ao direito de privacidade e de autodeterminação informativa para aplicação ampla em diversos setores, inclusive para os tratados neste relatório.

Tendo em vista o contexto de proteção de dados, o uso dessas tecnologias de vigilância pela Administração Pública, principalmente a de RF, deve ser estudado de perto para que os cidadãos possam entender os riscos envolvidos. A tecnologia de RF para fins de vigilância biométrica já está sendo combatida por diversos atores da academia e da sociedade civil por seu viés discriminatório, como a pesquisadora Joy Buolamwini, o Big Brother Watch, e a Access Now. Para além desses riscos, este relatório buscou entender melhor outros parâmetros de funcionamento da tecnologia aqui no Brasil.

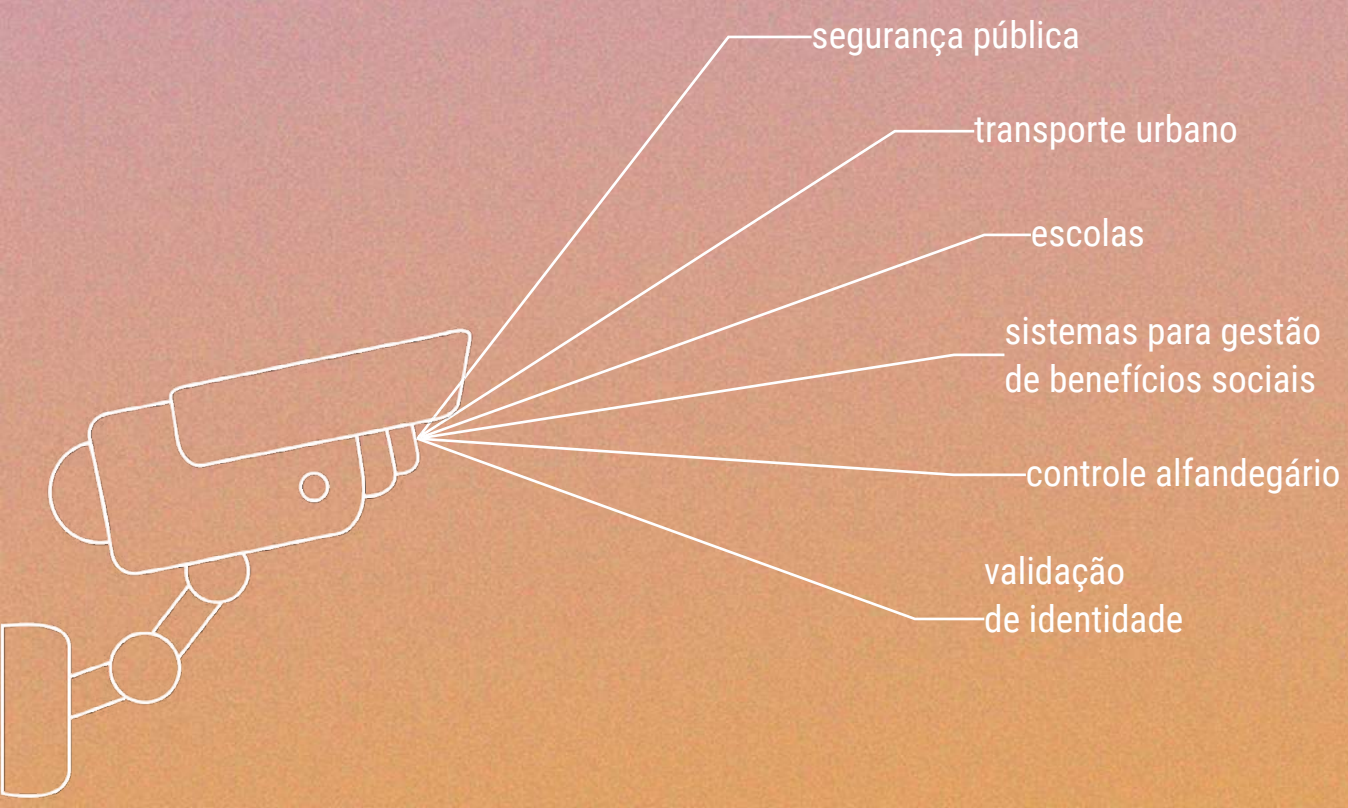
Nessa perspectiva, elegemos cinco eixos de análise sobre as tecnologias de vigilância

1. (In)existência de regulação do uso da tecnologia de reconhecimento facial
2. Origem e meios de aquisição e uso da tecnologia pelo setor público
3. Conhecimento técnico das autoridades públicas sobre funcionamento e riscos envolvidos
4. Análise de risco e impacto das tecnologias de vigilância
5. Formas de prestação de contas pelo uso das tecnologias

Para o desenvolvimento deste relatório, diante das peculiaridades das tecnologias de vigilância, foi necessária a realização de **25 pedidos de informação via Lei de Acesso à Informação (LAI) e 14 entrevistas com diferentes atores**. Dentre eles, estão representantes de entidades da sociedade civil, autoridades públicas e empresas que fornecem tecnologias de vigilância.

Por isso, agradecemos a disponibilidade e generosidade de todos pelas informações concedidas, que foram fundamentais para mapeamento das principais questões que envolvem o uso dessas tecnologias no Brasil.

Após período de coleta de dados, identificamos alguns casos de uso dessas ferramentas pelo poder público voltadas a seis finalidades:



Essas aplicações foram mapeadas nas cinco regiões do Brasil, nas esferas municipal, estadual e federal.

CASOS EMBLEMÁTICOS

Na segurança pública, além do uso de câmeras de videomonitoramento, a tecnologia de RF tem sido utilizada principalmente para identificar pessoas procuradas pela polícia. O caso da Secretaria de Segurança Pública da Bahia nos chama atenção pela recorrência no uso da tecnologia. Até janeiro de 2021, mais de 201 foragidos foram identificados pela SSP/BA[6]. O caso da Secretaria de Segurança do Município de Mogi das Cruzes também é interessante, já que ela recebeu doação da empresa Dahua e a Secretaria tem objetivo de tornar Mogi a "cidade-irmã de YongKang, na China", nos termos da resposta de LAI da Secretaria.

Já para mobilidade urbana, a aplicação de tecnologia de RF tem a finalidade de identificar se a pessoa que está utilizando um benefício, como o passe livre, é aquela que realmente possui o direito à assistência. Esses casos são comuns no Município de São Paulo e no Distrito Federal. Esta hipótese é similar ao controle de presença escolar e acesso a benefícios sociais, em que se objetiva confirmar a identidade do estudante ou do beneficiário, como nas Secretarias Estaduais de Alagoas, Goiás e Tocantins.

Por fim, a Receita Federal está utilizando a tecnologia de reconhecimento facial para fins de controle alfandegário em diferentes aeroportos espalhados por todo o Brasil. Ainda, a tecnologia também está sendo ofertada pela empresa pública Serviço Federal de Processamento de Dados (SERPRO) para validação da identidade dos cidadãos brasileiros junto a órgãos públicos e empresas privadas a partir dos dados biométricos da face disponibilizados na foto da CNH.

[6] Disponível em: http://www.ssp.ba.gov.br/2021/01/8976/Reconhecimento-Facial-alcanca-primeiro-foragido-em-2021.html

O relatório identificou um denominador comum no uso da tecnologia de RF: a falta de transparência e de mecanismos garantidores de proteção de dados e segurança na implementação das tecnologias no Brasil.

Sobre os cinco eixos de análise, apresentamos algumas considerações.

A inexistência de legislação específica aponta para uma margem de discricionariedade no uso dessas tecnologias por parte dos gestores e a falta de rastro legal no tratamento de dados, especialmente no âmbito da segurança pública. A ausência de legislação específica impacta também no padrão de negociação e entrada das tecnologias de RF no país.

Houve, na última década, a disseminação generalizada de práticas agressivas e pouco transparentes na negociação e no estabelecimento de termos de uso. A carência de capacitação local na escolha, instalação, manuseio e herança técnica para lidar com os indissociáveis riscos de violação de direitos fundamentais destas tecnologias também é outro elemento escalonador do risco. O resultado disso é o aprofundamento de uma mentalidade de tecno solucionismo que acaba por ignorar os impactos à esfera privada de indivíduos e a profunda capacidade discriminatória que envolve o uso de tecnologias de videomonitoramento, com destaque ao RF.

Além disso, o que pode ser inferido das experiências investigadas é que a avaliação de riscos não é um elemento priorizado pela Administração Pública quando do emprego dessas tecnologias. Em adição a isso, as discussões legislativas identificadas não demonstram cuidados adequados com a privacidade e a proteção de dados pessoais de indivíduos. O resultado é a experiência brasileira pautada no uso indiscriminado de tais tecnologias aliadas à escassez de informações sobre os riscos envolvidos, indo na contramão das práticas internacionais.

De forma similar à falta de análise de risco e impacto, não há hoje prestação de contas e de dados estatísticos consolidados sobre as atividades de tratamento de dados pessoais pela Administração Pública. Além disso, é fundamental o estudo da eficácia e satisfatoriedade do uso destas tecnologias para os fins almejados, já que uma das maiores justificativas era a suposta ampliação da eficiência estatal, bem como das taxas de falsos positivos e negativos desses sistemas, de modo a aferir seus impactos.

Por isso, o conjunto das experiências do uso de tecnologia de vigilância e de RF pelo setor público apontam para uma falta de transparência no uso da tecnologia e de preparo estrutural da Administração. Nesse sentido, compilaram-se as principais conclusões desenvolvidas neste relatório em uma tabela destacando a presença ou falta de uma regulamentação específica sobre reconhecimento facial, além da existência de mecanismos para o exercício dos direitos do titular, e de registros de erros de acurácia do sistema de RF. Por fim, destacou-se a forma de negociação para uso da tecnologia de RF.

Casos	Regulação específica	Boas práticas	Erro de acurácia	Direitos do titular	Formas de negociação
SSP/BA	X	X[7]	X	X	Licitação
SSP/CE	X	X	X	X	Licitação
PCESP	X	X	X	X	X
PMERJ	X	X	X	X	Teste grátis
Mogi das Cruzes	X	X	X	X	Doação
SEMOB	X	X	X	X	Contratação direta pelas concessionárias
Pilar	X	X	X	X[8]	Licitação
SERPRO	X[9]	X[10]	X	X	Produção própria

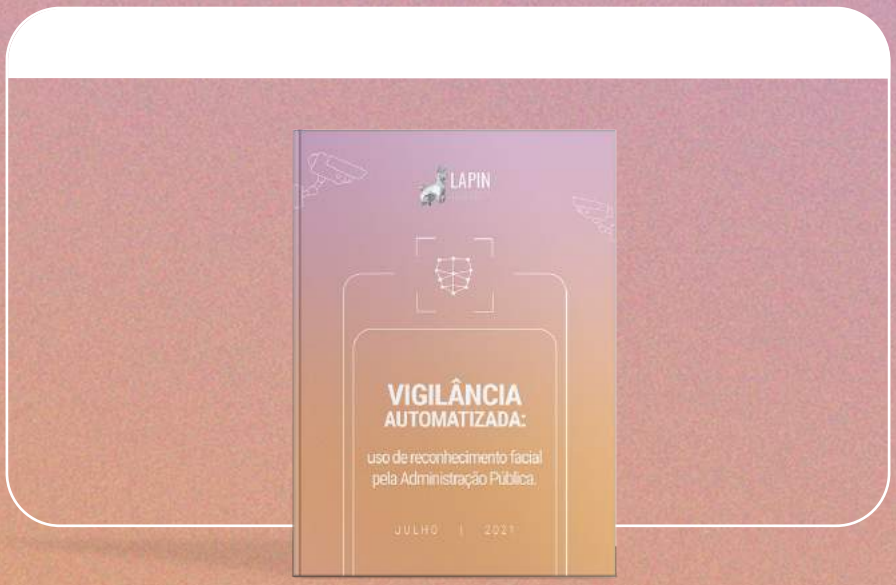
X: Sim | X: Não | X: Existência questionável | X: Sem informação

[7] A SSP/BA informou que possui política de boas práticas para uso da tecnologia. Porém, o documento não está disponível publicamente, o que impossibilita uma análise de se as recomendações são adequadas a proteger direitos dos titulares de dados.

[8] A resposta do Município foi positiva, mas nos parece que a informação prestada pelo Município confunde o conceito de direito dos titulares com consentimento, de forma que dá a entender que quando existe um "consentimento" os direitos dos titulares são exercidos.

[9] A regulamentação ocorreu por meio de portarias, instrumento normativo editado pelo próprio órgão, sem escrutínio público. Vide Portaria RFB n. 1384/2016, Portaria RFB n. 2189/2017, Portaria DENATRAN n. 215/2018 e Portaria DENATRAN n. 72/2017.

[10] Apesar do SERPRO informar que possui política de boas práticas, este documento não foi está público para consulta da população.



Convidamos os leitores para conferirem nosso relatório completo sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela Administração Pública no Brasil. Além de explorarmos com maior profundidade cada aspecto e impacto do uso da RF e câmeras de vigilância, trazemos um retrato de seu uso em cada área pública e informações detalhadas de diversas experiências no Brasil.

LAPIN

LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET

JULHO | 2021