LAPIN
LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET

VIGILÂNCIA AUTOMATIZADA:

uso de reconhecimento facial pela Administração Pública

JULHO | 2021

Sumário Executivo

Tecnologias de vigilância vêm sendo exponencialmente empregadas pela Administração Pública sob o fundamento de melhorar a eficiência estatal. Chama atenção, nesse espaço, a adoção de sistemas de reconhecimento facial (RF) em larga escala em áreas como segurança pública, transporte urbano, escolas, sistemas para gestão de benefícios sociais, controle alfandegário e validação de identificação.

Este relatório é resultado de uma pesquisa empírica na qual foram levantadas informações sobre o uso da tecnologia de RF pelo setor público brasileiro. Inicialmente, notícias e outros relatórios sobre o uso de tais tecnologias foram fundamentais para mapeamento de casos, com base nos quais foram enviados questionários via Lei de Acesso à Informação aos órgãos e entidades da Administração Pública responsáveis por essas aplicações de tecnologias de RF. Além disso, entrevistas com pesquisadores, representantes de autoridades públicas e de empresas foram conduzidas com vistas a obter mais detalhamento sobre como foi realizado o uso desses sistemas. A principal conclusão a que se chega é que o emprego de tecnologias de vigilância não tem sido realizado de forma transparente com a população, o que coloca em risco os direitos e liberdades individuais de cidadãos cujos dados são coletados por esses sistemas.

A despeito das controvérsias envolvendo a confiabilidade de tais tecnologias, seu amplo emprego pelo setor público não é acompanhado, por exemplo, por regulação específica, por mecanismos de prestação de contas aos cidadãos sobre os seus direitos e tampouco pelo emprego de medidas preventivas adequadas de segurança da informação e proteção de dados. Além disso, sua aplicação não tem sido acompanhada de avaliações sobre a proporcionalidade dos impactos que promove em relação aos benefícios que promete para a eficiência da atividade estatal.

Este relatório é dividido da seguinte forma: (I) é feita uma breve introdução sobre o estado atual do uso de sistemas de reconhecimento facial pelo setor público; (II) são apresentadas informações mais detalhadas sobre a metodologia e os objetivos da pesquisa empírica realizada; (III) são desenvolvidos cinco eixos de análise que demonstram a falta de transparência no uso dessas tecnologias; (IV) é elaborado um resumo das informações substanciais expostas ao longo do texto; (V) e, por fim, é apresentada uma tabela sobre as informações de cada caso pesquisado.

Portanto, considerando os riscos inerentes a tais tecnologias, a falta de conhecimento técnico sobre seu funcionamento, a dependência da Administração Pública em relação aos fornecedores e os poucos dados disponíveis quanto a seus riscos e eficiência, é fundamental que especialmente a tecnologia de reconhecimento facial não seja adotada pelo setor público.

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

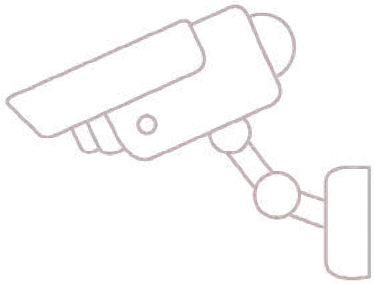
Realização:
Laboratório de Políticas Públicas e Internet - LAPIN

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

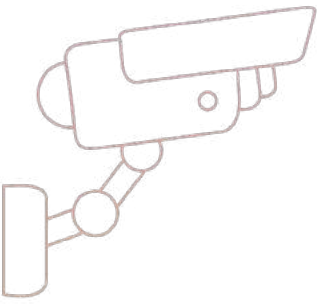
Revisão:
Amanda Espiñeira
José Renato Laranjeira de Pereira
Thiago Moraes

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. Brasília: Laboratório de Políticas Públicas e Internet, 2021.



SUMÁRIO



LAPIN
LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET

1. Introdução

No Brasil, tecnologias de vigilância são utilizadas pelos setores público e privado para diversas finalidades. Dentre as tecnologias de vigilância disponíveis, o uso de tecnologia de reconhecimento facial (RF) aumentou exponencialmente nos últimos anos, além da disseminação das câmeras de videomonitoramento e da ampliação do compartilhamento de dados coletados por ela entre entidades públicas e privadas.

O uso de sistemas de RF não é novidade no Brasil. Registros demonstram que ele já é implantado 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, dos quais trataremos brevemente neste relatório, avançam nas câmaras legislativas de diferentes regiões do Brasil.

A tecnologia de reconhecimento facial funciona a partir do tratamento de informações da face. Em primeiro lugar, coletada a imagem de um rosto, o sistema identifica métricas específicas da pessoa, como a distância entre os olhos, largura do queixo e o comprimento da boca. Com essas informações, o software calcula uma espécie de fórmula que consiste na assinatura facial, que vai ser a chave para identificação dessa pessoa.[2]

Essa assinatura é comparada com outras já armazenadas em um banco de dados com imagens de indivíduos que se pretende encontrar e, quando as assinaturas faciais são compatíveis, é possível identificar um sujeito de forma automatizada. **Pelo fato de os dados coletados para compor a assinatura facial** se relacionarem com características físicas únicas da pessoa, são classificados como **dados biométricos**.[3]

O funcionamento dessa tecnologia é arriscado justamente em razão da natureza dos dados tratados. Diferentemente de outras informações, como senhas e números de telefone, a alteração das características faciais de um indivíduo é expressivamente difícil, já que depende ou da passagem dos anos ou de procedimentos cirúrgicos.

Por isso, se a assinatura facial de um indivíduo está cadastrada na base de dados de um sistema, essa pessoa não teria mais a opção de não ser reconhecida salvo pelo apagamento do dado.[4] Além disso, **não é necessária a ciência da pessoa a ser reconhecida** para que esta tecnologia identifique alguém, diferente da identificação por digital, em que o titular sabe que está sendo submetido a este procedimento.

---

[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.
[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] Evidentemente, fatores adicionais podem interferir nos resultados do sistema de reconhecimento facial, como iluminação, distância ou posicionamento da câmera e posição do rosto, entre outros.

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**. Ou seja, reconhecer alguém erroneamente num contexto de segurança pública, por exemplo, pode levar a abordagens e apreensões indevidas - como ocorreu no Rio de Janeiro, em que uma mulher foi confundida com outra que havia cometido um crime e, por isso, foi direcionada à delegacia.[5]

Ainda, a não-identificação de um indivíduo por um falso negativo da tecnologia de reconhecimento facial em um contexto de assistência social pode acarretar a perda de benefícios, como revelam casos em que erros dos sistemas levaram à abertura de processos administrativos contra indivíduos por acusações infundadas de fraude. Foi isso que aconteceu com uma estudante de jornalismo de Brasília que deixou de ser reconhecida pelo sistema de RF e teve seu benefício bloqueado depois que passou a usar seu cabelo cacheado.[6]

Para o desenvolvimento deste relatório, diante das peculiaridades das tecnologias de vigilância, foi necessário realização de pedidos de informação via Lei de Acesso à Informação e entrevistas com diferentes atores, dentre eles representantes de entidades da sociedade civil, autoridades públicas e empresas que fornecem tecnologias de vigilância. Agradecemos a disponibilidade e generosidade de todos pelas informações concedidas que foram fundamentais para mapeamento das principais questões que envolvem o uso dessas tecnologias em todo Brasil.

a) Casos de uso de tecnologias de vigilância

Neste relatório, apresentamos alguns casos de uso dessas ferramentas pelo poder público voltadas a seis finalidades: **segurança pública, transporte urbano, escolas, sistemas para gestão de benefícios sociais, controle alfandegário e validação de identidade.** Essas aplicações foram mapeadas a nível federal e nas cinco regiões do Brasil, nas esferas municipal e estadual.

Na segurança pública, a tecnologia tem sido utilizada principalmente para identificar pessoas desaparecidas ou procuradas pela polícia. 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. Esta hipótese é similar ao controle de presença escolar, acesso a benefícios sociais e verificação de identidade, em que se objetiva confirmar a identidade do estudante, do beneficiário e do cidadão, respectivamente.

[5] Para mais detalhes, consultar o anexo Segurança Pública, item 9.

[6] 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.

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.

A Lei Geral de Proteção de Dados (LGPD), que está vigente desde 2020, estabeleceu princípios de 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.

Apesar de a LGPD não se aplicar inteiramente ao tratamento de informações pessoais para fins de segurança pública,[7] ela prevê que tais operações deverão observar os princípios de proteção de dados, os direitos do titular e o devido processo legal, bem como determina que haverá uma legislação específica para regulamentar esse tipo de uso.

Como a tecnologia de RF é baseada no tratamento de dados pessoais, essa lei será um importante norte para a análise que realizaremos. Vale ressaltar que, para os casos de uso de RF, a informação pessoal tratada é um dado biométrico, considerado pela LGPD dado sensível, que deve receber maior proteção pelo potencial de uso discriminatório que carrega.[8]

b) Riscos

Além dos riscos inerentes ao tratamento de dados sensíveis, que exigem maior proteção pela LGPD, a tecnologia de reconhecimento facial apresenta outros riscos que devem ser endereçados. A tabela a seguir, baseada na Nota Técnica do LAPIN sobre o Projeto de Lei n. 865/19 de São Paulo,[9] apresenta os principais riscos do uso de tecnologias de monitoramento, principalmente do sistema de RF. Ainda, este relatório mapeou outros riscos diante do uso de tecnologia de reconhecimento facial que devem ser analisados com cuidado pelo setor público.

[7] LGPD, art. 4º.
[8] DONEDA, Danilo. Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados. 2a ed., São Paulo: Thomson Reuters Brasil, 2019. p. 143
[9] Este projeto de lei foi vetado pelo Governador de São Paulo, ele dispunha sobre a instalação de tecnologia de reconhecimento facial (TRF) nas estações do Metrô e da CPTM.

Violação de Direitos Fundamentais

O uso indiscriminado de tecnologias de RF afronta a privacidade, a liberdade de ir e vir, e a inviolabilidade da honra e da imagem das pessoas, já que permite o monitoramento e identificação das pessoas quando ocupam espaços públicos. O uso desse tipo de tecnologia também ameaça o princípio da presunção de inocência, já que trata todo indivíduo como potencial suspeito a ser monitorado e identificado pelo Estado. Trata-se, ainda, de violação ao direito de proteção de dados pessoais, reconhecido como direito fundamental autônomo pelo STF[10] em maio de 2020.

Vigilância em Massa

A vigilância em larga escala ocorre de forma irrestrita, sem definição prévia de um alvo específico e muitas vezes ininterruptamente. Se realizada em locais públicos, traz riscos à privacidade e à proteção de dados de um grande contingente populacional, que terá seus dados coletados e armazenados sem finalidades específicas e sem devida transparência. A situação é ainda mais danosa se os dados coletados forem sensíveis, como são aqueles obtidos por tecnologias de reconhecimento facial.[11]

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 não são neutras e refletem o racismo pré-existente na sociedade.[12] Assim, pensando na sua aplicação em contextos de segurança que remetem ao seletivismo penal e ao aprimoramento de políticas criminais com efeitos nocivamente racializados, trata-se de um risco grave e já observado em diversas situações que representam segurança para algumas pessoas e repressão para outras.[13]

[10] STF. Notícias STF. STF suspende compartilhamento de dados de usuários de telefônicas com IBGE. Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=442902 Acesso em: 02 mar. 2021.
[11] REIS, Carolina. Nota Técnica. Lei 6.712/20. 10 Recomendações para o uso de reconhecimento facial para segurança pública no DF. LAPIN. 2021. Disponível em: https://lapin.org.br/2021/02/22/nota-tecnica-lei-distrital-6712-2020-df/. Acesso em: 01 mar. 2021.
[12] 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.
[13] BEUTIN, Lyndsey. Racialization as a Way of Seeing: The Limits of Counter-Surveillance and Police Reform. 2017. Surveillance & Society 15(1): 5-20.

Transfobia

A imposição de critérios binários na sociedade, ou seja, de classificação entre homem e mulher, promove classificações que reforçam a exclusão e o estigma de pessoas transgênerosexuais e não-binárias. Isso não seria diferente no que diz respeito aos sistemas de reconhecimento facial, os quais reiteradamente negam visibilização a identidades divergentes - conflitando com a auto-identificação de gênero,[14] acirrando violências e reiterando o cerceamento de direitos às pessoas transsexuais e não-binárias.

Violação dos direitos de crianças e adolescentes

A privacidade de crianças e adolescentes é garantida pelo ordenamento jurídico brasileiro tanto no que diz respeito ao direito de imagem quanto ao tratamento de seus dados pessoais em prol do seu melhor interesse, sendo necessário o consentimento específico por seu responsável para tanto.[15] A capacidade de discernimento de crianças e adolescentes não está completamente formada, deixando-as mais vulneráveis ao mau uso de seus dados pessoais por terceiros, como é o caso de uso da tecnologia para verificação da frequência escolar.[16]

[14] 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.

[15] LGPD. Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
§1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

[16] HERMES, P. H.; SUTEL, R. O.; DA SILVA, R. L. A vigilância dos dados pessoais de crianças e adolescentes frente à Lei Geral de Proteção de Dados Pessoais e a doutrina da proteção integral. In: Anais do 5º Congresso Internacional de Direito e Contemporaneidade: Mídias e Direito da Sociedade em Rede. UFSM. 2019. Disponível em: https://www.ufsm.br/app/uploads/sites/563/2019/09/11.5.pdf

Nas próximas páginas, será apresentada uma visão geral da implementação dessas tecnologias pelo setor público por uma perspectiva de proteção de dados pessoais, em que buscamos identificar a aplicação das diretrizes de privacidade e proteção de dados. Este relatório analisou os casos concretos de aplicação de câmeras de videomonitoramento e de tecnologias de RF no Brasil diante de cinco eixos: a regulação dessas tecnologias, a origem e os termos de instalação delas, o conhecimento técnico das autoridades públicas, a análise de risco e impacto delas e formas de prestação de contas pelo uso da tecnologia.

2. Objetivos e metodologia

Este relatório tem o objetivo de analisar as implicações do uso de tecnologias de vigilância pela Administração Pública a nível municipal, estadual e federal em relação a direitos fundamentais e à proteção de dados pessoais. Para tanto, foram analisadas as diferentes finalidades, formas de uso e riscos envolvidos na utilização de duas tecnologias distintas, o videomonitoramento e a tecnologia de reconhecimento facial. Os casos analisados se encontram nas cinco regiões do Brasil: **Nordeste, Sudeste, Centro-Oeste, Norte e Sul.**

Vale mencionar que, em geral, ao descrever elementos específicos de cada caso de uso, a fonte das informações expostas neste relatório são respostas a pedidos de acesso à informação que foram feitas diretamente aos órgãos. Quando não é esse o caso, a referência foi evidenciada, em nota de rodapé.

a) Seleção de casos

A seleção dos casos práticos aqui analisados foi motivada por quatro principais categorias:

1. Presença de riscos iminentes de instauração de sistemas de vigilância massiva (quando a quantidade de pessoas cujos dados estão sendo coletados é expressiva);
2. Potencial impacto negativo do uso para grupos estigmatizados ou populações específicas (como casos que pressupõem a coleta de dados de crianças ou não observam os direitos dos titulares);
3. Uso da tecnologia em contextos em que se tem como consequência a restrição de direitos, liberdades e acesso a benefícios (como casos em que a tecnologia justifica a prisão de um indivíduo);
4. Potencial considerável de violação de direitos fundamentais, especialmente privacidade e proteção de dados pessoais (como situações que podem potencialmente fomentar o exercício do direito à liberdade de expressão diante da instalação de câmeras em locais públicos onde podem ocorrer reuniões de pessoas, por exemplo).

A partir do mapeamento dos casos em análise, foi possível identificar as potenciais violações a direitos e as lacunas regulatórias existentes diante do tratamento de dados pessoais por parte da Administração Pública em cinco principais contextos: segurança pública, escolas e programas sociais, mobilidade urbana, controle aduaneiro e validação de identidade. Assim, fixou-se como escopo deste relatório a investigação dos casos de uso de tecnologias de vigilância no Brasil publicizados pela imprensa e pelos meios de comunicação oficiais na internet até o ano de 2020. Para selecionar as publicações, utilizou-se como parâmetro as seguintes palavras chaves no mecanismo de busca: "reconhecimento facial brasil" e "câmera de vigilância brasil".

Além disso, é relevante frisar que este relatório não tem a pretensão de se tornar uma referência exaustiva em relação aos casos de uso dessas tecnologias. O primeiro passo para a coleta de dados se baseou principalmente em casos noticiados pela mídia, que não necessariamente refletem uma imagem detalhada de todos os usos feitos pela Administração Pública. Além disso, os casos pesquisados não foram suficientes para delimitar conclusões quantitativas sobre a frequência de uso da tecnologia por região ou seus impactos para as atividades da Administração Pública. Porém, priorizou-se aprofundar as aplicações identificadas de modo que este relatório seja compreendido como forma de complementar outras pesquisas de instituições relevantes sobre este tema.[17]

Diante deste recorte, foram analisadas informações de fontes secundárias disponíveis na internet em sites de notícias, além de relatórios elaborados por entidades da sociedade civil e projetos de lei em tramitação no poder legislativo a respeito do uso dessas tecnologias. Além disso, foram solicitados esclarecimentos junto às autoridades estatais sobre a forma de uso das tecnologias em seus respectivos departamentos por meio de pedidos de informação fundamentados na Lei de Acesso à Informação (LAI).[18]

b) Pedidos de acesso à informação

Os requerimentos de informação buscaram compreender as formas de aplicação dos parâmetros de proteção de dados no tratamento de informações pessoais pela Administração Pública. Por isso, as perguntas versaram a respeito da finalidade e duração do tratamento de dados, identificação do controlador e fornecedor da tecnologia, além dos casos da elaboração de relatórios de impacto de proteção de dados, compartilhamento de dados e formas dos titulares exercerem seus direitos previstos em lei. Ainda, foram solicitadas informações sobre questões da eficácia da tecnologia para os objetivos almejados e de segurança da informação dos dados armazenados.

---

[17] Isso inclui as pesquisas realizadas pelo:
1. Instituto Igarapé: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/
2. Associação de Pesquisa Data Privacy Brasil: https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%-C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf.
3. Rede de Observatórios da Segurança: https://www.ucamcesec.com.br/wp-content/uploads/2019/11/Rede-de-Observatorios_primeiro-relatorio_20_11_19.pdf

[18] BRASIL. Lei n. 12.527, de 18 de novembro de 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 31 mar 2021.

c) Entrevistas realizadas

Após esta etapa e a fim de complementar os pedidos de informação, foram realizadas entrevistas com pessoas pesquisadoras, jornalistas, autoridades públicas estaduais e municipais envolvidas no uso das tecnologias e dois fornecedores de sistemas de RF. Os agentes envolvidos nos casos de uso de tecnologias de monitoramento pesquisados foram convidados para entrevista. As entrevistas com as autoridades são, inclusive, uma das principais contribuições deste relatório, já que foram extremamente úteis para melhor compreender a intenção por trás da adoção dessas medidas e acessar as diferentes perspectivas quanto ao tema.

As entrevistas foram feitas sem a divulgação da pessoa participante, e este trabalho indica somente os órgãos ou as empresas dos quais a pessoa entrevistada faz parte. Dessa forma, foi possível obter informações complementares sobre os casos concretos de aplicação das tecnologias de vigilância, a exemplo dos planejamentos de projetos públicos ampliados em que as tecnologias são inseridas, como consórcios e parcerias. Ainda, questionou-se sobre a origem da tecnologia, os resultados de uso e eficiência dos sistemas, além dos instrumentos utilizados para mitigar os riscos aos indivíduos e à sociedade em geral.

Para a etapa das entrevistas, foram contatadas pesquisadoras, órgãos públicos e empresas fornecedoras das tecnologias. Apesar das exaustivas tentativas de contato feitas pelo LAPIN, várias empresas fornecedoras da tecnologia não responderam ao convite de entrevista, como a Huawei, Dahua, NEC, Ponto ID e Facewatch. Por outro lado, as empresas PRODATA e Oi Soluções, bem como as entidades Intervozes, Instituto Igarapé e IDEC, foram solícitas em aceitar nosso pedido de entrevista sobre a forma de uso das tecnologias.

A partir da coleta de informações descrita, o presente relatório traça uma análise qualitativa sobre os impactos dessas tecnologias para a sociedade e para os órgãos públicos que fazem uso do videomonitoramento massificado e do RF no Brasil. Com isso, aponta os métodos de aquisição e uso e os mecanismos de prestação de informação providos pelo Poder Público, de modo a traçar um retrato de como diferentes órgãos têm aplicado as tecnologias.

Nesse sentido, este relatório é dividido de acordo com os seguintes aspectos investigados nos casos de utilização das tecnologias de vigilância:

1. (In)existência de Regulação do uso da tecnologia de reconhecimento facial;
2. Origem e os meios de aquisição e uso da tecnologia;
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.

Em vista desses aspectos centrais, os casos analisados foram organizados de acordo com o contexto de uso das tecnologias de vigilância, os órgãos públicos responsáveis pela implementação e os entes desenvolvedores das tecnologias. No total, foram destacados 20 casos de uso de câmeras de videomonitoramento e de câmeras com RF, listados na tabela abaixo e separados pelas respectivas regiões em que estão localizados os órgãos aplicadores. Maiores detalhes a respeito de cada uso constam no **Anexo** deste relatório.

Entes Federativos	Órgão Responsável	Contexto	Tecnologia	Resposta em Pedido LAI	Entrevista	Desenvolvedor da Tecnologia
Estado da Bahia	Secretaria de Segurança Pública		**RF**	✓	✓	Huawei, Hikvision, Axis
Estado do Ceará	Secretaria de Segurança Pública e Defesa Social		**RF**	✓	✗	SSPDS e UFC
Estado da Paraíba	Secretaria de Segurança Pública e Defesa Social		**RF**	✓	✓	Hikvision
Distrito Federal	Secretaria de Segurança Pública		**CM**	✓	✗	Não informada
Estado de São Paulo	Secretaria de Segurança Pública		**CM**	✓	✓	Microsoft
Estado de São Paulo	Polícia Civil		**RF**	✓	✗	Não informada
Município de Campinas (SP)	Secretaria Municipal de Cooperação nos Assuntos de Segurança Pública		**RF**	✓	✓	Huawei
Município de Mogi das Cruzes (SP)	Secretaria de Segurança		**RF**	✓	✗	Dahua
Estado do Rio de Janeiro	Polícia Militar		**RF**	✓	✓	Oi e Huawei
Estado do Rio de Janeiro	Polícia Civil		**RF**	✓	✗	Não informada
Município de Boa Vista (RR)	Secretaria Municipal de Segurança Urbana e Trânsito		**CM**	✓	✗	Dahua
Estado do Paraná	Secretaria de Estado da Segurança Pública		**RF**	✓	✗	Não informada
Município de Curitiba	Prefeitura Municipal		**RF**	✓	✗	Não informada
Estado de Santa Catarina	Secretaria de Segurança Pública		**RF**	✓	✗	Não informada

Estado do Rio Grande do Sul	Governo do Estado do Rio Grande do Sul		**RF**	✓	✗	Não informada
Município de Porto Alegre	Secretaria Municipal de Segurança de Porto Alegre		**RF**	✓	✗	Não informada
Estado do Alagoas	Secretaria de Estado da Assistência e		**RF**	✓	✗	Ponto ID
Município de Pilar (AL)	Prefeitura Municipal		**RF**	✓	✗	Portabilis Tecnologia LTDA
Município de Recife (PE)	Prefeitura Municipal		**RF**	✓	✗	Ponto ID
Município de Anápolis (GO)	Prefeitura Municipal		**RF**	✗	✗	Ponto ID
Estado do Tocantins	Secretaria de Estado da Educação, Juventude e Esportes		**RF**	✓	✗	Ponto ID
Município de São Paulo (SP)	Secretaria Municipal de Mobilidade e Transportes		**RF**	✓	✗	Não informada
Distrito Federal	Secretaria de Estado de Transporte e Mobilidade		**RF**	✓	✗	PRODATA
União	Receita Federal		**RF**	✓	✗	NEC
União	Serviço Federal de Processamento de Dados		**RF**	✓	✗	SERPRO

 uso de RF para controle de frequência em escolar

 uso de RF para segurança pública

 uso de RF para assistência social

 uso de RF para mobilidade urbana

 uso de RF para controle alfandegário

 uso de RF para verificação de identidade

[**RF**] imagem do rosto para reconhecimento facial

[**CM**] câmera de videomonitoramento comum

3. Eixos de Análise

Como expresso acima, a elaboração deste trabalho teve por intuito criar um retrato sobre o emprego de sistemas de reconhecimento facial pelo poder público sob cinco principais eixos.

O primeiro diz respeito à existência ou não de regulação do uso da tecnologia de reconhecimento facial e qual a posição adotada pelas autoridades no sentido de necessidade de lei ou não. O segundo analisa as diferentes origens dos equipamentos e softwares, bem como suas formas de aquisição pelo Poder Público. O terceiro eixo se refere à existência ou não de conhecimento técnico por parte das autoridades quando da aquisição e utilização. O quarto diz respeito à elaboração de relatórios de impacto à proteção de dados por parte das autoridades adquirentes e executoras dos sistemas.

Por fim, o último eixo se debruça sobre quais as formas de prestação de contas quando do uso da tecnologia de reconhecimento facial pela Administração Pública.

a) (In)existência de Regulação do uso da tecnologia de reconhecimento facial

PRINCIPAIS RESULTADOS

Por se tratar de tecnologia altamente invasiva e com alto potencial de restrição de direitos fundamentais, sua implementação com base em normas gerais, como a Constituição ou a LGPD, não é suficiente.

Apenas um dos entes federativos responsáveis pelos 20 casos analisados possui legislação específica que autoriza o uso de tecnologia de reconhecimento facial, e esta lei possui falhas que podem levar a violações de direitos fundamentais.

É necessário haver legislação específica que autorize o uso da tecnologia em espaços determinados e que contenha disposições relativas a direitos dos titulares de dados, deveres dos agentes de tratamento e medidas de segurança dos dados tratados, bem como previsão dos limites de seu uso.

Apesar do aumento da implementação de tecnologias de reconhecimento facial pela Administração Pública, muitas dessas iniciativas não possuem autorização legislativa que trace parâmetros para seu uso. O uso de tecnologias de RF tem sido visto como vantajoso nos diferentes contextos analisados, como indicaram as respostas recebidas a partir dos pedidos de acesso à informação e das entrevistas realizadas com as autoridades públicas.

Os estados da Bahia e do Rio de Janeiro trouxeram reflexões específicas sobre seu potencial supostamente benéfico para a segurança pública tanto em respostas aos pedidos de acesso à informação enviados, quanto em entrevistas que concederam no escopo da presente pesquisa. Apesar disso, não forneceram dados capazes de comprovar que o número de pessoas foragidas que tenham sido identificadas pelo sistema compense a coleta massiva de dados pessoais de multidões que passam pelos espaços públicos em que as câmeras tenham sido instaladas. Essa falta de detalhamento gera, por si só, dúvidas em relação a qual o custo-benefício por trás do uso desses sistemas.

Contudo, o uso de sistemas de reconhecimento facial pode provocar efeitos adversos à privacidade e ao exercício de direitos em espaços de convívio social. Por exemplo, se há câmeras dotadas com a tecnologia e espalhadas pela cidade, torna-se possível traçar o itinerário de uma pessoa que pode permitir identificar aspectos íntimos de sua vida a partir de uma análise dos locais que frequentou em determinado período. Sabendo disso, este indivíduo pode deixar de realizar atividades que usualmente realizaria se não fosse constantemente vigiado e identificado, ainda que estas atividades não tenham nenhum caráter ilegal. Sua participação em grupos políticos, religiosos ou mesmo relacionados a sua identidade sexual ou de gênero poderia ser afetada pelo medo de poder ser discriminado caso tal informação caísse nas mãos erradas.

Assim, por se tratar de atividade que interfere profunda e diretamente no exercício de diversos direitos fundamentais, o uso de tecnologia de RF deve ser precedido de autorização legislativa específica. Isso porque a Secretaria de Segurança Pública do Estado da Bahia está se valendo da autorização genérica do caput do art. 144 da Constituição Federal em se utilizar de qualquer mecanismo possível para alcançar melhor segurança pública. No entanto, entendeu-se que, em vista dos riscos e impactos negativos da tecnologia explicitados acima, o que inclui a coleta massiva de dados pessoais, é fundamental uma lei específica para endereçar essas peculiaridades.

Apesar do aumento da implementação de tecnologias de reconhecimento facial pela Administração Pública, muitas dessas iniciativas não possuem autorização legislativa que trace parâmetros para seu uso. O uso de tecnologias de RF tem sido visto como vantajoso nos diferentes contextos analisados, como indicaram as respostas recebidas a partir dos pedidos de acesso à informação e das entrevistas realizadas com as autoridades públicas.

Os estados da Bahia e do Rio de Janeiro trouxeram reflexões específicas sobre seu potencial supostamente benéfico para a segurança pública tanto em respostas aos pedidos de acesso à informação enviados, quanto em entrevistas que concederam no escopo da presente pesquisa. Apesar disso, não forneceram dados capazes de comprovar que o número de pessoas foragidas que tenham sido identificadas pelo sistema compense a coleta massiva de dados pessoais de multidões que passam pelos espaços públicos em que as câmeras tenham sido instaladas. Essa falta de detalhamento gera, por si só, dúvidas em relação a qual o custo-benefício por trás do uso desses sistemas.

Contudo, o uso de sistemas de reconhecimento facial pode provocar efeitos adversos à privacidade e ao exercício de direitos em espaços de convívio social. Por exemplo, se há câmeras dotadas com a tecnologia e espalhadas pela cidade, torna-se possível traçar o itinerário de uma pessoa que pode permitir identificar aspectos íntimos de sua vida a partir de uma análise dos locais que frequentou em determinado período. Sabendo disso, este indivíduo pode deixar de realizar atividades que usualmente realizaria se não fosse constantemente vigiado e identificado, ainda que estas atividades não tenham nenhum caráter ilegal. Sua participação em grupos políticos, religiosos ou mesmo relacionados a sua identidade sexual ou de gênero poderia ser afetada pelo medo de poder ser discriminado caso tal informação caísse nas mãos erradas.

Assim, por se tratar de atividade que interfere profunda e diretamente no exercício de diversos direitos fundamentais, o uso de tecnologia de RF deve ser precedido de autorização legislativa específica. Isso porque a Secretaria de Segurança Pública do Estado da Bahia está se valendo da autorização genérica do caput do art. 144 da Constituição Federal[19] em se utilizar de qualquer mecanismo possível para alcançar melhor segurança pública. No entanto, entendeu-se que, em vista dos riscos e impactos negativos da tecnologia explicitados acima, o que inclui a coleta massiva de dados pessoais, é fundamental uma lei específica para endereçar essas peculiaridades.

[19] CF, Art. 144. A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos.

Os processos legislativos têm como pressuposto uma ampliação maior do debate, já que os representantes eleitos refletem, ainda que idealmente, as distintas posições dos cidadãos. Além disso, também permitem maior participação popular, por meio de pesquisas de opinião, audiências públicas ou do acolhimento de contribuições de organizações da sociedade civil e outros setores interessados no tema. Dessa forma, seria viável ampliar a discussão e o entendimento sobre os potenciais riscos da implementação de tecnologia de RF bem como a discussão de alternativas que sejam mais adequadas.

Somente a discricionariedade do gestor para decidir sobre a utilização da tecnologia não é suficiente. Na Administração Pública, a lei é o limite do que é permitido fazer, desde que esta esteja de acordo com legislações anteriores e o próprio ordenamento jurídico. Não havendo autorização legal expressa, capaz de detalhar quais procedimentos de proteção de dados e segurança da informação o órgão utilizador deve adotar e que seja adequada aos princípios e normas precedentes, uma decisão que limita direitos, ainda mais de uma população considerável, como ocorre durante a adoção de reconhecimento facial, pode ser considerada ilegal.[20]

O próprio princípio da discricionariedade decorre da lei e deve ser utilizado dentro de seus limites: havendo duas ou mais possibilidades que se adequem para realizar determinada ação que a lei autoriza, o gestor pode eleger uma delas, considerando também os outros princípios da Administração.[21] Entretanto, num contexto em que não há segurança quanto à legalidade da medida, o gestor deve se abster de implementá-la[22] - como é o caso do uso de tecnologia de RF.

A controvérsia em relação à legalidade do uso da tecnologia se insere na discussão relativa à proteção de dados pessoais enquanto direito fundamental e se relaciona especialmente com a natureza biométrica e sensível dos dados coletados. Assim, se as regras e princípios relacionados ao direito à proteção de dados já se aplicam a dados pessoais comuns, eles são ainda mais inflexíveis quando se trata de dados biométricos.

[20] JUSTEN FILHO, Marçal. Curso de direito administrativo. Revista Dos Tribunais. 2013.
[21] Os princípios da Administração contidos explicitamente na Constituição podem ser encontrados no seu art. 37.
[22] MELLO, Celso Antônio Bandeira de. 2015. Curso de direito administrativo. 32a edição. Editora Malheiros.

Dessa maneira, princípios como o da finalidade e da transparência, que exigem que o titular de dados conheça e concorde com o propósito e as formas do tratamento de dados, se opõem ao caráter sorrateiro da tecnologia de RF. O avanço dos atuais sistemas, ademais, não é capaz de transpor o requisito do princípio da não-discriminação, já que não possuem acurácia suficiente em relação a diferentes gêneros, raças e idades. Por fim, o princípio da necessidade é o mais decisivo: ele determina que os dados coletados e seu tratamento sejam os mínimos necessários para as finalidades que se propõem.

Para os usos da tecnologia de RF analisados neste relatório, se entende que há outras soluções, medidas e possibilidades para se atingir o mesmo propósito de maneira menos invasiva em relação aos dados pessoais. Portanto, se contrário aos princípios mencionados, o uso da tecnologia seria ilegal - inclusive no contexto da segurança pública, já que os princípios da proteção de dados e os direitos do titular também se aplicam a ele.

Decretos ou dispositivos infralegais não preencheriam todos os requisitos da legalidade no caso de tecnologia de RF. A edição dessas normas é resultado da decisão individual de governantes, que não envolvem a sociedade e não permitem uma discussão ampla. Especialmente na hipótese de uso para segurança pública quando inexiste legislação específica que regule o tratamento de dados nesse contexto, decretos ou diplomas infralegais sobre o assunto carecem de lastro legal.

Fora do contexto da segurança pública, a LGPD estabelece, em seu Capítulo IV, as regras para o tratamento de dados pela Administração Pública. Em conjunto com os princípios da proteção de dados pessoais e as regras para o tratamento de dados sensíveis, tal capítulo serve como base para a análise da legalidade e proporcionalidade da implementação de tecnologia de RF. Contudo, por se tratar de tecnologia acentuadamente invasiva, o uso fundamentado apenas na legislação geral existente não é suficiente para justificar todas as interferências em direitos fundamentais que ela pode causar.

Apesar disso, apenas um dos casos analisados por este relatório possui legislação específica autorizando o uso de sistemas de reconhecimento facial para as finalidades particulares.[23]

[23] Este relatório não esgota todos os casos de implementação de tecnologia de RF pela Administração Pública no Brasil. Outros casos existem e alguns deles possuem algum tipo de legislação ou projetos de lei a respeito. Para mais informações sobre outros casos, ver:. Pedro Augusto P. Francisco, Louise Marie Hurel, e Mariana Marques Rielli, "Regulação do reconhecimento facial no setor público: avaliação de experiências internacionais" (Instituto Igarapé, Data Privacy Brasil, junho de 2020), https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf

É o caso do Distrito Federal, que aprovou a Lei Distrital n. 6.712/2020, que "dispõe sobre o uso de tecnologia de reconhecimento facial na segurança pública".[24]

Embora o Distrito Federal, no âmbito da segurança pública, se diferencie ao ser uma das poucas unidades federativas que possuem legislação que regulamenta a implementação da tecnologia, é importante frisar que a lei não se estende a outros campos de aplicação. Dessa forma, o Distrito Federal continua utilizando massivamente a tecnologia de RF no transporte público, por exemplo, sem autorização legislativa para tanto. O uso da tecnologia no transporte público distrital se baseia unicamente numa portaria editada pelo diretor-geral da autarquia responsável pelo transporte urbano do Distrito Federal, o DFTRANS.[25]

Além disso, a lei distrital para o uso da tecnologia na segurança pública é insuficiente e possui pontos preocupantes que devem ser reconsiderados. Por exemplo, a lei é ambígua em relação à possibilidade de vigilância em massa, é omissa sobre medidas de cibersegurança e prestação de contas social, estabelece tempo excessivo para o armazenamento dos dados e não prevê formas para o exercício de direitos pelos titulares de dados.[26]

Outra unidade federativa que ensaiou uma autorização legislativa para o uso da tecnologia de RF na segurança pública foi o Estado de São Paulo. A Assembleia Legislativa aprovou o Projeto de Lei n. 865/19, que dispõe sobre a instalação de tecnologia de reconhecimento facial nas estações do Metrô e da Companhia Paulista de Trens Metropolitanos (CPTM).[27]

---

[24] Lei n. 6.712, de 10 de novembro de 2020, do Distrito Federal. Disponível em: https://www.tjdft.jus.br/institucional/relacoes-institucionais/arquivos/lei-no-6-712-de-10-de-novembro-de-2020.pdf. Acesso em: 3 abr. 2021.
[25] Portaria n. 15, de 30 de abril de 2018, do Distrito Federal. Disponível em: http://www.sinj.df.gov.br/sinj/Norma/39e7cf5acaba49a4a381f9dc2d74e92d/Portaria_15_30_04_2018.html. Acesso em: 3 abr. 2021.
[26] Para mais detalhes, ver: LAPIN. Nota Técnica sobre a Lei Distrital n. 6.712/2020 DF: 10 recomendações para o uso de reconhecimento facial para segurança pública no DF. 2021. Disponível em: https://lapin.org.br/wp-content/uploads/2021/02/NT_LD_67122020_reconhecimento_facial_DF_LAPIN-1.pdf. Acesso em: 3 mar 2021.
[27] Assembleia Legislativa de São Paulo. Projeto de Lei n. 865/2019. Disponível em: https://www.al.sp.gov.br/proProjeto de Lei n° 865, de 2019 (PL 865 / 19)positura/?id=1000278098. Acesso em: 3 abr. 2021.

O trâmite do Projeto foi marcado pela ausência de participação social, e seu texto, de regulamentação limitada, daria margem à vigilância em massa e à violação de direitos fundamentais. Ou seja, trata-se de exemplo de autorização apenas formal, mas insuficiente para contemplar o uso adequado e legal da tecnologia[28]. Apesar disso, as razões para o veto ao Projeto pelo Poder Executivo não tiveram qualquer relação com a deficiência do seu conteúdo, mas meramente em aspectos de constitucionalidade formal.[29]

Portanto, num cenário de pouca regulação para a implementação de tecnologia de RF, não basta apenas editar decretos, diplomas infralegais ou utilizar apenas a legislação geral existente. É necessário editar uma legislação específica, precedida de debate público e abrangente o suficiente para que se possa prever salvaguardas legais de mitigação dos potenciais riscos e interferências das tecnologias.

b) Origem e meios de aquisição e uso da tecnologia

PRINCIPAIS RESULTADOS

Foram identificados padrões de negociação e aquisição da tecnologia de reconhecimento facial que indicam estratégias agressivas para que um reduzido número de empresas seja capaz de controlar esse mercado.

Apesar de identificados casos em que desenvolvimento dos sistemas de reconhecimento facial tenha sido feito no Brasil, a maioria dos aparatos utilizados provêm do exterior, com predominância de países como China, Israel, Estados Unidos e Reino Unido.

As principais formas de uso da tecnologia foi por meio de acordos de cooperação, doação de equipamentos tecnológicos ou pregão eletrônico.

[28] LAPIN. Nota Técnica pelo veto do Projeto de Lei n. 865/19. 2021.
Disponível em: https://lapin.org.br/2021/03/08/nota-tecnica-pelo-veto-do-projeto-de-lei-no-865-19/. Acesso em: 3 abr. 2021.
[29] BUCCO, R. PL do reconhecimento facial no metrô de SP recebe veto total. Tele-Síntese. 2021.
Disponível em: https://www.telesintese.com.br/pl-do-reconhecimento-facial-no-metro-de-sp-recebe-veto-total/.
Acesso em: 3 abr. 2021.

A tecnologia de RF abre um novo mercado no Brasil, de imenso potencial de crescimento, que se expressa na prestação de serviços tanto ao setor público quanto ao setor privado. O sucesso do ingresso no contexto brasileiro depende das estratégias de mercado, gerando maior fatia de mercado para empresas com estratégias mais agressivas de competição. Nesse sentido, identificou-se certos **padrões de negociação** por parte de um punhado de empresas que, a longo prazo, **implicam em termos de renegociação e competição mais restritos.**

Práticas agressivas de entrada no mercado foram observadas por todo o território nacional, sendo a mais comum a procura das empresas de tecnologia de vigilância aos órgãos de segurança. Comumente, esta procura era embasada **sobre um acordo de cooperação[30] ou de doação de equipamentos e softwares por parte das empresas, para testes em eventos específicos ou laboratórios vivos mais amplos**.

A estratégia mais agressiva foi observada nos termos de negociação da Huawei em Campinas; da Oi no Rio de Janeiro; da Hikvision em Salvador e em São Paulo; da STAFF (subsidiária da britânica Facewatch) em Campina Grande; e da Dahua com a Secretaria de Segurança Pública do Município de Mogi das Cruzes. Neste último município, a prefeitura firmou parceria com a empresa Chinesa Dahua para doação de equipamentos, sem custos para a Administração municipal.[31] Esta prática, além de reduzir o custo de instalação futura frente à concorrência, garantindo fatias de mercado, serve como garantia de qualidade para acordos futuros e invariavelmente renova os termos exigidos no acordo.

No entanto, também foram observadas iniciativas de procura e aquisição das tecnologias por meio de consórcios estaduais, como o Consórcio Nordeste, formado em 2019 para promoção de parcerias entre os governos estaduais da região "voltadas à realização de compras conjuntas e à implementação integrada de políticas públicas, como nas áreas de educação e segurança"[32]. Dentre as compras pretendidas pelos governos, incluem-se sistemas de reconhecimento facial.[33]

---

[30] Acordos de cooperação são instrumentos formais em que órgãos públicos podem estabelecer vínculos com empresas que tenham interesses para realização de um propósito comum.
Já a doação de equipamento ocorre quando uma empresa transfere seu produto par a Administração Pública por meio de uma liberalidade. DPC. Diferença entre Instrumentos Celebrados. Disponível em: http://dpc.proad.ufsc.br/diferenca-entre-instrumentos-celebrados/. Acesso em: 3 abr. 2021. USP. Doações e apoio da iniciativa privada. Disponível em: http://www.usp.br/secretaria/wp-content/uploads/Programa-Parceiros-da-USP_2.pdf. Acesso em: 3 abr. 2021.

[31] Para mais detalhes, consultar anexo Segurança Pública, item 8.

[32] IREE. Consórcio Nordeste: entenda o que é a iniciativa. Disponível em: https://iree.org.br/consorcio-nordeste-entenda-o-que-e-a-iniciativa/. Acesso em 28 maio 2021.

[33] MELLO, Patrícia Campos. Nordeste vira palco de guerra fria tecnológica entre EUA e China. 2019. Disponível em: https://gauchazh.clicrbs.com.br/mundo/noticia/2019/09/nordeste-vira-palco-de-guerra-fria-tecnologica-entre-eua-e-china-ck00tdaya01ii01qt7n284xu8.html. Acesso em: 16 abr. 2021.

Outra modalidade utilizada foi a do pregão presencial, a Secretaria de Estado da Assistência e Desenvolvimento Social do Estado de Alagoas e da Prefeitura de Pilar (AL) consagrou a empresa Ponto ID e a Portabilis respectivamente como fornecedoras.[34] Já a contratação da NEC pela Receita Federal para instalação da tecnologia nos aeroportos internacionais como o de Brasília, Guarulhos, Recife, Rio de Janeiro e Salvador para fins de controle aduaneiro ocorreu por meio de **pregão eletrônico**.[35] O pregão é modalidade de licitação para aquisição de bens e serviços comuns feita em sessão pública, por meio de propostas de preços escritas e lances verbais,[36] sendo o processo licitatório mecanismo que garante transparência e prestação de contas para a população.[37]

No que diz respeito à origem das empresas, a imensa maioria das tecnologias de RF implantadas no Brasil são fornecidas por empresas estrangeiras ou por empresas locais que usam componentes de fabricante original do equipamento do exterior. Na maioria dos casos, a proveniência é da China, embora empresas dos EUA, Reino Unido e Israel, para citar alguns, também tenham sido fornecedores importantes para o mercado brasileiro. Em outros, ainda que a empresa seja brasileira, como é o caso da Ponto ID, não conseguiu-se informação suficiente para deduzir que a solução utilizada tivesse sido desenvolvida integralmente no Brasil.[38]

Informações sobre a origem da tecnologia são interessantes porque também refletem a expectativa da autoridade pública sobre os benefícios que pode obter ao ampliar o monitoramento das cidades. Por exemplo, a Secretaria de Segurança do Município de Mogi das Cruzes, em São Paulo, afirmou que sua parceria com a empresa Dahua é motivada pela intenção de tornar Mogi das Cruzes a cidade-irmã de YongKang, na China.[39] Os insumos são invariavelmente importados, conforme destaca o representante da Urbi, concessionária de transporte público do Distrito Federal, em entrevista ao LAPIN, cujo sistema é formado por câmeras oriundas da China, processadores israelenses e sistema operacional coreano.[40]

[34] Para mais detalhes, consultar anexo Escolas e Programas Sociais, item 1.
[35] Para mais detalhes, consultar anexo Aeroportos, item 1.
[36] BRASIL. Decreto n. 3.555, de 8 de agosto de 2000. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/d3555.htm#:~:text=indiretamente%20pela%20Uni%C3%A3o.-,Art.,mat%C3%A9ria%20regulada%20por%20este%20Decreto.. Acesso em: 3 abri. 2021.
[37] Para mais detalhes, consultar anexo Escolas e Programas Sociais, itens 1 e 2, e Órgãos Federais, item 1.
[38] Para mais detalhes, consultar anexo Órgãos Federais, item 2.
[39] Para mais detalhes, consultar anexo Segurança Pública, item 8.
[40] Para mais detalhes, consultar anexo Mobilidade Urbana, item 2.

A maioria dos casos identificados de tecnologia de RF para segurança pública envolve, em algum nível, a presença de empresas chinesas, principalmente Dahua, Hikvision e Huawei. Em alguns casos, o revendedor é uma empresa terceira, que atua mais na montagem ou no mero oferecimento da tecnologia. Um exemplo é o estado da Bahia, onde a filial brasileira da rede espanhola de lojas de departamento El Corte Inglés assinou o contrato para o "Consórcio Safe Bahia 2014". No entanto, o Fabricante de Equipamento Original do hardware de tecnologia de RF (por exemplo, câmeras) e software era a Huawei. Da mesma forma, no caso do Rio de Janeiro, a contratada direta foi a operadora brasileira de telecomunicações Oi, que forneceu a tecnologia de RF desenvolvida pela Huawei.[41]

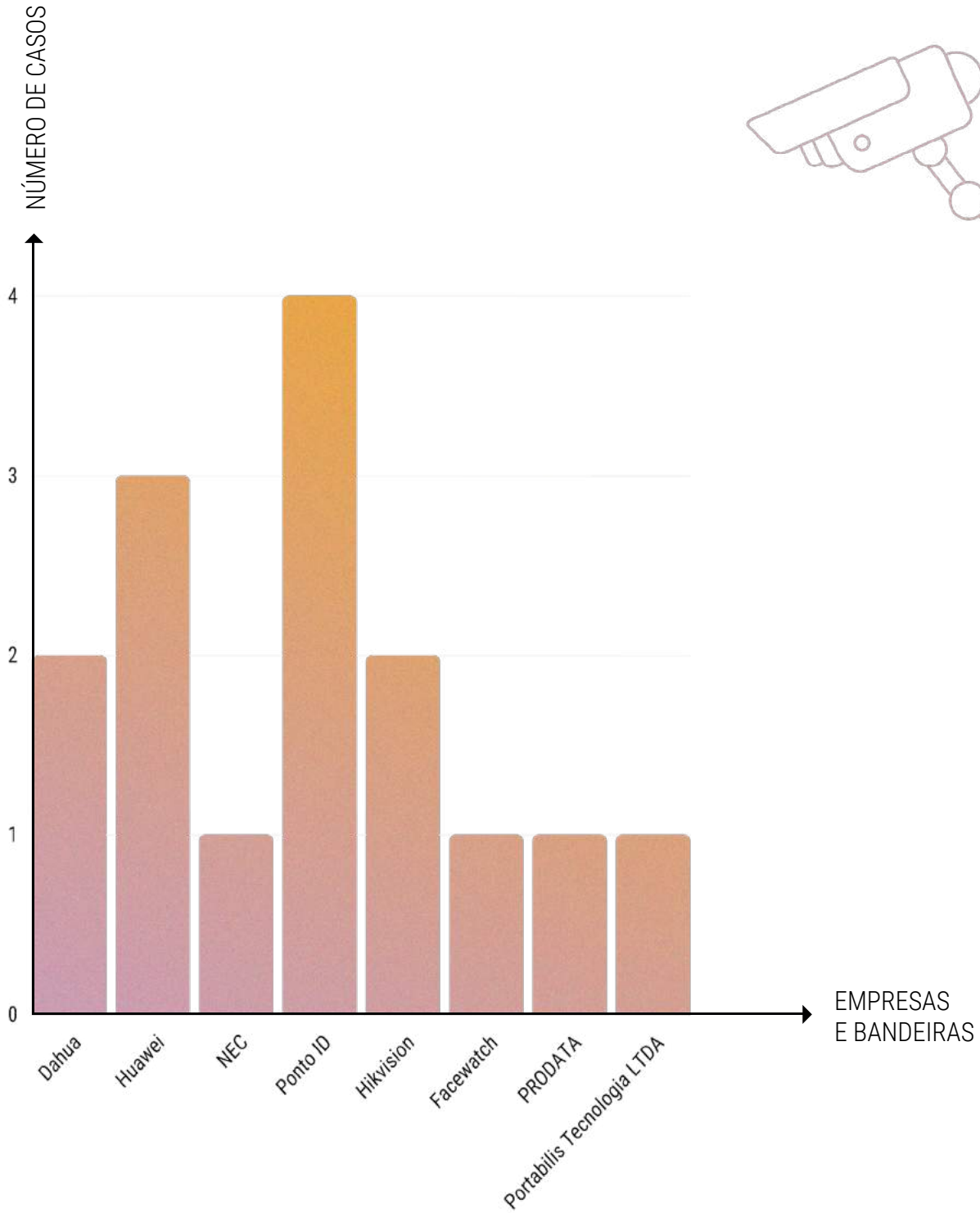
A preferência pelas tecnologias chinesas parece estar relacionada ao seu preço competitivo, como afirmaram alguns representantes de autoridades públicas entrevistadas, como a Secretaria de Segurança Pública da cidade de Campinas e do Estado da Paraíba. Segundo relatório da IPVM, a diferença de preço dos equipamentos de vigilância chineses pode chegar a 10 vezes menos do que alguns de seus concorrentes.[42] O preço mais baixo pode ser justificado por muitos fatores, incluindo as menores taxas de impostos. Por exemplo, a Hikvision é atualmente o único fabricante estrangeiro de videovigilância com operação de montagem na Zona Franca de Manaus.

Além disso, algumas empresas brasileiras que fornecem equipamentos de vigilância têm empresas chinesas como fornecedoras originais do equipamento. Um exemplo é a Intelbras, que é líder nacional em tecnologias de videovigilância. Desde 2018, fechou convênio com a Dahua, no qual esta terá prioridade no fornecimento de equipamentos de CFTV.[43]

[41] Para mais detalhes, consultar anexo Segurança Pública, itens 1 e 9.

[42] While Axis (Sweden) cameras cost on average 372 USD, Hikvision (China) cameras cost around 37 USD. See more on: IPVM. Brazil Assembly Powers Hikvision Local Expansion. 2020. https://ipvm.com/reports/hik-brazil?code=allow

[43] Intelbras social contract also states that Dahua currently owns 10% of the Brazilian company's assets. See more on: Intelbras. Minuta do Prospecto Preliminar da Oferta Pública de Distribuição Primária e Secundária de Ações Ordinárias de Emissão da Intelbras. 2020. http://sistemas.cvm.gov.br/dados/ofeanal/RJ-2020-05588/20201126_Minuta%20do%20Prospecto%20Preliminar.pdf.


NÚMERO DE CASOS
4
3
2
1
0
Dahua
Huawei
NEC
Ponto ID
Hikvision
Facewatch
PRODATA
Portabilis Tecnologia LTDA
EMPRESAS
E BANDEIRAS

c) Conhecimento técnico das autoridades públicas

PRINCIPAIS RESULTADOS

As autoridades públicas demonstraram pouco conhecimento sobre detalhes técnicos de funcionamento das tecnologias e os riscos que delas decorrem, o que pode demonstrar uma falta de treinamento adequado de seus operadores.

Em alguns casos, as empresas fornecedoras da tecnologia possuem amplo acesso aos dados pessoais tratados, mesmo quando incluem dados sensíveis de crianças e adolescentes.

Não foi identificada previsão ou acordo sobre a transferência de conhecimento sobre a tecnologia para o poder público. Isso inclui tanto conhecimento a respeito de como ocorre o tratamento de dados da tecnologia quanto a respeito de como utilizá-la da forma mais eficiente possível.

Aliado à falta de regulamentação e ao processo não competitivo de aquisição de sistemas e tecnologias, **a pesquisa não identificou um esforço sistemático para a formação técnica das autoridades sobre a utilização, os efeitos e os cuidados no uso de tecnologia de RF.**

[43] Intelbras social contract also states that Dahua currently owns 10% of the Brazilian company's assets. See more on: Intelbras. Minuta do Prospecto Preliminar da Oferta Pública de Distribuição Primária e Secundária de Ações Ordinárias de Emissão da Intelbras. 2020. http://sistemas.cvm.gov.br/dados/ofeanal/RJ-2020-05588/20201126_Minuta%20do%20Prospecto%20Preliminar.pdf.

No caso do setor público, essa condição se aprofunda, especialmente por não haver uma previsão de transferência de conhecimento sobre a tecnologia, como destaca a Secretaria de Segurança Pública de Campinas também em entrevista. O projeto inicial previu o desenvolvimento de um sistema local de reconhecimento facial, tal qual a experiência em Campina Grande. No entanto, como não havia previsão de suporte técnico por parte das empresas fornecedoras quando fosse finalizado o período de testes, a estrutura de vigilância foi descontinuada e os agentes públicos não conheciam profundamente os modos de uso do equipamento, bem como seus riscos e formas de endereçá-los.

O desconhecimento denota má gestão de tecnologia, como a ausência de rastreamento de acurácia e falsos positivos, que ocorre quando o sistema identifica uma pessoa de forma equivocada. Isso se agrava quando sua aplicação é em áreas sensíveis, como segurança pública, em que um erro de identificação pode levar uma pessoa inocente a ser detida temporariamente. Ainda, há casos em que gestores acreditavam que as tecnologias eram promissoras, mas elas se transformaram em focos locais e meramente temporários de experimentação tecnológica por parte das empresas fornecedoras, repassando à Administração Pública pouca ou nenhuma herança técnica para se desenvolver a tecnologia no setor público.

A esse respeito, não foram disponibilizados publicamente os índices de acurácia do uso de tecnologia de RF no amplo uso da SSP/BA no Carnaval de Salvador de 2019 e da PMERJ, em cooperação com a Oi, no mesmo período.[44] Isto dificulta escrutínio público sobre a eficácia e a proporcionalidade do uso de tecnologias de vigilância no alcance dos objetivos a que se propõe, como a garantia da segurança pública e a verificação de fraudes em programas sociais.

Outra questão que chama atenção é a permissão de acesso aos dados pessoais conferidos às empresas fornecedoras das tecnologias, sem previsão de exclusão após o fim do contrato. Esse é o caso da Secretaria da Educação, Juventude e Esportes do Estado de Tocantins, que informa que a empresa fornecedora da tecnologia possui amplo acesso aos dados biométricos tratados. Vale dizer que, a esse respeito, apenas o caso do uso de tecnologia de RF pela PMERJ no Rio de Janeiro apresentou cláusula que obrigou a deleção de qualquer informação pessoal utilizada pelas empresas parceiras. [45]

[44] Para mais detalhes, consultar anexo Segurança Pública, itens 1 e 9.
[45] Para mais detalhes, consultar anexo Escolas e Programas Sociais, item 5, e Segurança Pública, item 9.

d) Relatório de Impacto à Proteção de Dados Pessoais

PRINCIPAIS RESULTADOS

- O ampliamento do uso de tecnologias de vigilância pelo setor público brasileiro não tem sido acompanhado de ferramentas adequadas que possibilitem uma análise objetiva dos benefícios obtidos de sua utilização face aos riscos envolvidos.
- As avaliações de risco são instrumentos que podem ser utilizadas pelo poder público para discernir sobre a licitude da atividade de tratamento de dados, compreender os riscos e minimizar os danos.
- Apesar de o setor público já implementar de forma massiva o uso de tecnologias de vigilância sem a realização de uma avaliação prévia dos riscos envolvidos, tanto a prática internacional quanto a legislação nacional indicam para elaboração do Relatório de Impacto à Proteção de Dados anteriormente.

No campo da proteção de dados e da privacidade, a avaliação de risco se dá por meio dos chamados relatórios de impacto à proteção de dados (RIPD), que podem ser definidos como um processo para a avaliação dos impactos sobre a privacidade e sobre a proteção de dados gerados por um projeto, política, programa, serviço, produto ou outra iniciativa que trate dados pessoais.

Recomenda-se que esses instrumentos sejam feitos em consulta com as partes interessadas, de modo a impulsionar a adoção de medidas preventivas necessárias para evitar ou minimizar os impactos negativos do tratamento de dados pessoais.[46] Esses instrumentos representam a superação de uma lógica pautada em medidas meramente reativas a violações à privacidade e à proteção de dados para medidas preventivas aos riscos a esses direitos.[47]

Especialmente em contextos de tratamentos massivos de dados sensíveis, como ocorre com o uso de sistemas de reconhecimento facial, a elaboração deste relatório é altamente recomendada. A necessidade deste estudo resta ainda mais explícito tendo em vista que ele auxiliaria a mapear os riscos e endereçar ações nesse sentido, como é o caso da Secretaria de educação de Alagoas, que permite que a empresa fornecedora da tecnologia tenha acesso aos dados sensíveis dos cidadãos beneficiários de programas sociais para possibilitar a identificação deles. Isto significa um elevado risco para os direitos dos titulares e a realização de relatório de risco seria um instrumento eficiente para endereçamento dessas questões.

Apesar disso, em nenhum dos casos analisados foi identificado que tenha sido elaborada qualquer avaliação de impacto pela Administração Pública de modo a avaliar os riscos à proteção de dados e a outros direitos fundamentais quando do emprego de tecnologias de videomonitoramento e de reconhecimento facial. Não há informações disponibilizadas em meios oficiais referentes aos riscos a que os cidadãos estão submetidos ao serem monitorados pelas tecnologias empregadas pela Administração Pública. Vale ressaltar que muitos dos agentes entrevistados sequer tinham conhecimento sobre o que é um RIPD.

Observa-se, portanto, que o ampliamento do uso de tecnologias de vigilância pelo setor público brasiliero[48] **não é acompanhado das respectivas ferramentas que possibilitam uma análise objetiva dos riscos envolvidos.**

[46] DE HERT, Paul; DARIUSZ, Kloza; WRIGHT, David. Recommendations for a Privacy Impact Assessment Framework for the European Union. Brussels – London, 2012, p.5. Disponível em: https://piafproject.wordpress.com/. Acesso em: 18 de dez. 2020.
[47] DARIUSZ, Kloza. Privacy Impact Assessment as a Means to Achieve the Objectives of Procedural Justice. Jusletter IT. Die Zeitschrift für IT und Recht, 2014, p.2. Disponível em: https://cris.vub.be/en/publications/privacy-impact-assessments-as-a-means-to-achieve-the-objectives-of-procedural-justice(7b7e11e7-641d-4d56-aebf-3e0e7522f7b9).html. Acesso em: 16 de dez. 2020.
[48] INSTITUTO IGARAPÉ. Reconhecimento Facial no Brasil. Instituto Igarapé: 2019. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em: 08 de fev. 2021.

O emprego irrestrito de tecnologias de vigilância impacta negativamente os direitos fundamentais dos indivíduos.[49] Isso porque, além dos impactos diretos sobre a privacidade, o tratamento de dados advindo do uso de tais tecnologias tende a **refletir vieses algoritmos que reforçam discriminações e impactar o direito à proteção de dados da população**.[50] As avaliações de risco, portanto, são instrumentos a serem utilizados pelos agentes de tratamento para discernir sobre a licitude da atividade e compreender os riscos que se impõe.[51]

Dentre os órgãos da Administração Pública para os quais enviou-se questionários sobre a realização de avaliações de risco, **apenas o Serviço Federal de Processamento de Dados (SERPRO), no contexto do serviço DataValid, respondeu ter realizado relatório de impacto à proteção de dados**.[52]

No entanto, a empresa pública informou não divulgar o relatório alegando confidencialidade das informações.[53] Cumpre destacar que, no pedido de acesso à informação feito no escopo desta pesquisa, não foram solicitados os dados pessoais tratados, mas tão somente os resultados do RIPD realizado pela empresa pública.

A relevância da publicização de tais informações se dá pelo fato de o SERPRO, por meio do DataValid, tratar dados pessoais coletados com base em obrigação legal, já que são dados advindos do DENATRAN[54] e da Receita Federal[55] e comercializados com agentes privados. Isso representa uma privatização de dados pessoais fornecidos ao Estado sem que seja dada qualquer possibilidade de o titular se opor

[49] EDRI. Facial Recognition and Fundamental Rights 101. EDRI: 2019. Disponível em: https://edri.org/our-work/facial-recognition-and-fundamental-rights-101/. Acesso em: 08 de fev. 2021.

[50] AMNESTY INTERNATIONAL. Amnesty International Calls for Ban on the Use of Facial Recognition Technology for Mass Surveillance. Amnesty International: 2020. Disponível em: https://www.amnesty.org/en/latest/research/2020/06/amnesty-international-calls-for-ban-on-the-use-of-facial-recognition-technology-for-mass-surveillance/. Acesso em 10 de fev. 2021.

[51] CLARKE, Roger. Privacy Impact Assessment: Its Origins and Development. Computer Law & Security Review, vol. 25 ed. 2ª, 2009, p. 123–135. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0267364909000302?via%3Dihub. Acesso em: 11 de fev. 2021.

[52] Apesar de o SERPRO informar que fizera a avaliação de riscos, a empresa pública não forneceu o conteúdo do relatório. Como justificativa, a empresa informou que o LAPIN não teria legitimidade para requerer o documento. O LAPIN recorreu da resposta dada pelo SERPRO até a última instância, a CGU, e mesmo assim não obteve acesso ao suposto documento. Para mais detalhes, consultar anexo Orgãos Federais, item 2.

[53] Atualmente, o DataValid consta com um aviso de privacidade em seu site, que não substitui o Relatório de Impacto à Proteção de Dados. Disponível em: https://www.loja.serpro.gov.br/datavalid

[54] Portaria DENATRAN n. 215, de 06/08/2018; - Portaria DENATRAN n. 72, de 12/05/2017; e autorização do Denatran ao SERPRO publicada no Diário Oficial da União em 03/08/2017. Discorre do Termo de Autorização emitido pelo Denatran ao Serpro para acesso aos dados de todos os seus sistemas.

[55] Portaria RFB n. 1384/2016, que disciplina a disponibilização de dados não protegidos por sigilo fiscal sob tutela da Receita Federal; e Portaria RFB n. 2189/2017, que autoriza o Serpro a disponibilizar para terceiros dados e informações sob tutela da Receita Federal.

ao tratamento, nos termos do art. 18, §2º, da LGPD.[56] Não divulgar uma avaliação dos riscos realizada dificulta o escrutínio sobre os potenciais riscos, a elaboração de mecanismos para avaliar a acurácia e leva à incompreensão do contexto no qual a tecnologia está sendo utilizada.

Além da resposta dada pelo SERPRO, as demais autoridades informaram, como justificativa para a ausência de avaliações de risco, que (i) as tecnologias foram implementadas antes da Lei Geral de Proteção de Dados e, por esse motivo, não exigiriam a elaboração de RIPD;[57] (ii) a informação sobre a existência do relatório seria sigilosa;[58] e (iii) as imagens são utilizadas para finalidades determinadas.[59] A maioria dos órgãos, no entanto, apenas não informou se os relatórios foram elaborados.[60]

Apesar de amplamente empregadas pela Administração Pública, não há regulamentação sistematizada sobre a obrigatoriedade da realização dos relatórios de impacto quando do uso das tecnologias de vigilância. Há, na verdade, atos normativos do poder executivo que dificultam a coleta de informações sobre tecnologias empregadas que podem gerar riscos à privacidade e à proteção de dados dos cidadãos. Um exemplo é a Portaria CGAI n. 1 de 2016, da Controladoria e Ouvidoria-Geral do Estado do Ceará, que classifica como sigilosos os documentos e informações sobre o uso de equipamentos de vigilância pela Administração Pública estadual.[61]

---

[56] Art. 18 (...) § 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.

[57] A Receita Federal informou, quando questionada sobre a existência de relatórios de impactos, que "(A)a contratação (de tecnologia de RF) antecede a própria Lei Geral de Proteção de Dados (LGPD), não tendo sido feitos, portanto, relatórios previstos nessa lei". Vale ressaltar que o início do uso desses sistemas pela Receita ocorreu em 2016, antes da entrada em vigor da LGPD. Para mais detalhes, consultar anexo Aeroportos, item 1.

[58] A Secretaria de Segurança Pública e Defesa Social do Estado do Ceará informou, quando questionada sobre a existência de relatórios de impacto, que "Os dados obtidos são considerados sigilosos, em conformidade com o que dispõe o art. 5º, inciso XXXIII da Constituição Federal de 1988". Para mais detalhes, consultar anexo Segurança Pública, item 2.

[59] A Secretaria de Segurança Pública do Estado da Bahia informou, quando questionada sobre a existência de relatórios de impacto, que "Não. Conforme já informado, as imagens biométricas são usadas exclusivamente pela SSP para prática de políticas de segurança pública na busca de pessoas com mandado de segurança ou pessoas desaparecidas". Para mais detalhes, consultar anexo Segurança Pública, item 1.

[60] As seguintes autoridades não informaram haver realizado relatório de impacto à proteção de dados pessoais: a Secretaria de Estado da Segurança e Defesa Social da Paraíba, a Secretaria de Segurança Pública do Distrito Federal, a Secretaria de Segurança Pública do Estado de São Paulo, a Polícia Civil do Estado de São Paulo, a Secretaria Municipal de Cooperação nos Assuntos de Segurança Pública do Município de Campinas, a Secretaria de Segurança do Município de Mogi das Cruzes, a Polícia Militar do Estado do Rio de Janeiro, a Secretaria Municipal de Segurança Urbana e Trânsito de Boa Vista, a Secretaria de Estado da Assistência e Desenvolvimento Social do Estado de Alagoas,

[61] CGAI. Portaria CGAI n. 01/2016: Dispõe sobre a uniformização na classificação de informação sigilosa de matéria comum a todos os órgãos e entidades do poder executivo estadual. CGAI: 2016. Disponível em: https://www.cgd.ce.gov.br/wp-content/uploads/sites/33/migracao/2899.pdf. Acesso em 02 de fev. 2021.

Ainda, o risco de implementação dessas tecnologias aumenta quando consideradas as bases de dados que os órgãos públicos utilizam para identificar pessoas pelo uso de tecnologia de RF. Se o banco de dados de imagens faciais for amplo, será possível identificar mais pessoas pela tecnologia, o que aprofunda o risco de vigilância massiva pelo Estado.

Em regra, as secretarias de segurança utilizam a Base Nacional de Mandado de Prisão, base organizada pelo Conselho Nacional de Justiça, e bases regionais geridas pela própria polícia civil estadual de pessoas procuradas e desaparecidas para identificação de pessoas pela tecnologia de RF, a exemplo da Bahia. De modo diverso, a Secretaria de Segurança do Ceará afirmou que o aplicativo utilizado para identificar pessoas por meio de tecnologia de RF realiza uma busca em uma base de identificação civil com quase oito milhões de cadastros. Em outro caso, a Polícia Civil do Rio de Janeiro informou utilizar outras bases de dados para acessar informações das pessoas procuradas, como o Sistema de Consultas da SEPOL (SICWEB), Portal Segurança, Infoseg.[62]

O uso indiscriminado de tais tecnologias pela Administração Pública brasileira, aliado à escassez de informações sobre os riscos envolvidos na atividade de tratamento de dados, vai na contramão das práticas internacionais. O Regulamento Geral de Proteção de Dados da União Europeia, por exemplo, estabelece a obrigatoriedade da elaboração de Relatório de Impacto de Proteção de Dados (RIPD) quando há o tratamento de dados que possa causar elevados riscos aos direitos e liberdades dos indivíduos, especialmente quando monitore de forma sistemática áreas públicas e envolva categorias especiais de dados pessoais em grande escala.[63]

Além disso, o Guia 2/2019 do Conselho Europeu de Proteção de Dados estabelece que, quando do processamento de dados biométricos advindos do uso tecnologias de videomonitoramento, os agentes de tratamento devem avaliar os riscos envolvidos. No que se refere ao uso de tecnologias de vigilância pela Administração Pública para as atividades de segurança, por exemplo, a Diretiva da União Europeia 680/2016 não apenas estabelece a obrigatoriedade da avaliação dos riscos sobre a proteção de dados, como também dispõe sobre o escopo mínimo do relatório.[64]

---

[62] Para mais detalhes, consultar anexo Segurança Pública, itens 1, 2 e 6.

[63] UE. Regulamento 2016/679: relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Parlamento Europeu e Conselho da Europa: 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A32016R0679. Acesso em: 11 de fev. 2021.

[64] CONSELHO EUROPEU DE PROTEÇÃO DE DADOS. Diretiva 2/2019: sobre o tratamento de dados através de dispositivos de video. EDPB: 2019. Disponível em: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf. Acesso em 11 de fev. 2021.

No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD) disciplina os relatórios de impacto de proteção de dados de maneira **menos prescritiva** em relação à regulamentação europeia. A Lei se limita a dispor que a Autoridade Nacional de Proteção de Dados poderá solicitar ao controlador a avaliação de riscos da atividade de tratamento de dados pessoais.[65] A LGPD, no entanto, impõe a **obrigatoriedade** da realização do RIPD quando do **tratamento de dados referente às atividades de segurança pública, atividades de investigação e repressão de infrações penais.**[66]

Apesar da LGPD não definir parâmetros prescritivos sobre o conteúdo dos RIPD e sobre a supervisão dos relatórios por uma autoridade independente, foi apresentado à Câmara dos Deputados um anteprojeto de Lei que propõe uma disciplina mais prescritiva quanto à avaliação dos riscos envolvidos no tratamento de dados para atividades de segurança pública e persecução penal.[67]

Nesse sentido, apesar de o setor público já implementar de forma massiva o uso de tecnologias de vigilância, chama atenção a ausência de avaliação prévia dos riscos envolvidos, o que vai de encontro tanto com a prática internacional quanto com as melhores práticas discutidas nacionalmente.

e) Formas de prestação de contas pelo uso das tecnologias

PRINCIPAIS RESULTADOS

Mesmo que se proceda com a devida avaliação dos riscos no emprego de tecnologias de vigilância, é necessário garantir a devida prestação de contas aos titulares dos dados.

---

[65] LGPD, Arts. 10 § 3º, art. 32 e art. 38.

[66] LGPD. Art. 4, §3º: Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais. § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.

[67] STJ. Comissão entrega à Câmara anteprojeto sobre tratamento de dados pessoais na área criminal. 2020. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/05112020-Comissao-entrega-a-Camara-anteprojeto-sobre-tratamento-de-dados-pessoais-na-area-criminal.aspx. Acesso em 14 de fev. 2021.

Três princípios da disciplina de proteção de dados relacionados ao dever de prestação de contas são fundamentais (art. 6º, LGPD), quais sejam: o livre acesso, a qualidade dos dados e a transparência.

A prestação de contas se materializa sobretudo na efetivação dos direitos dos titulares, bem como na transparência na atuação dos agentes de tratamento.

Não há dados estatísticos sistematizados, consolidados ou publicizados sobre o tratamento de dados realizado por meio de tecnologias de reconhecimento facial pela Administração Pública.

Mesmo que se proceda com a devida avaliação dos riscos no emprego de tecnologias de vigilância pelo poder público, ainda é preciso que as entidades da Administração proporcionem a devida prestação de contas aos titulares dos dados sobre como essas tecnologias têm sido empregadas. Essa prestação de contas se materializa sobretudo na efetivação dos direitos dos titulares, bem como na transparência na atuação dos agentes de tratamento. [68]

68 ALHADEFF J., VAN ALSENOY B., DUMORTIER J.The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions. In: Guagnin D., Hempel L., Ilten C., Kroener I., Neyland D., Postigo H. (eds) Managing Privacy through Accountability. Palgrave Macmillan: London, 2012. Disponível em: https://doi.org/10.1057/9781137032225_4. Acesso em: 08 de fev. 2021.

O princípio do livre acesso, previsto na LGPD, visa garantir aos titulares consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais. A qualidade dos dados garante a exatidão e atualização dos dados para cumprimento da finalidade do tratamento. Por fim, o princípio da transparência assegura aos titulares informações claras, precisas e facilmente acessíveis sobre o tratamento e os respectivos agentes responsáveis. Além desses princípios, também são garantidos aos titulares de dados direitos específicos para a consolidação da proteção de seus dados, previstos nos arts. 17 ao 22 da LGPD.

No entanto, a pesquisa aponta que o uso irrefletido de tecnologia de vigilância pela Administração Pública também se demonstra pela **ausência de prestação de contas sobre a aplicação desses sistemas, o que abrange a elaboração de dados estatísticos consolidados sobre as atividades de tratamento de dados pessoais.**

Das autoridades questionadas por meio do pedido de acesso à informação e de consulta do endereço eletrônico institucional, **poucas fornecem canais para a requisição facilitada de acesso ou de correção aos dados tratados, e, quando o fazem, não são suficientemente acessíveis aos titulares de dados.**

Aliás, é incipiente a própria transparência passiva das autoridades na resposta aos pedidos de acesso à informação. A título de exemplo, mesmo após ter divulgado em seus sites institucionais o uso da tecnologia de reconhecimento facial, a Secretaria de Estado da Segurança Pública de Santa Catarina[69], a Secretaria Municipal de Segurança Pública de Porto Alegre[70] e a Secretaria de Segurança Pública do Estado do Paraná[71] não responderam às perguntas enviadas sobre o pretexto de não utilizarem e não terem utilizado a referida tecnologia.

Dos casos analisados, apenas as entidades que empregam tecnologias de reconhecimento facial no contexto da mobilidade urbana alegam garantir o exercício dos direitos dos titulares. No caso da Secretaria Municipal de Mobilidade e Transportes (SPTrans), há atendimento on-line[72] para os usuários e solicitantes do Bilhete Único.

---

[69] SECOM. SC tem primeiras prisões indicadas por sistema de câmeras de monitoramento. Disponível em: https://www.sc.gov.br/index.php/noticias/temas/seguranca-publica/sc-tem-as-primeiras-prisoes-indicadas-por-sistema-utilizado-em-cameras-de-monitoramento-da-secretaria-de-estado-da-seguranca-publica. Acesso em: 20 de maio de 2021.

[70] MATOS, Lurdinha. Integração garante utilização de Reconhecimento Facial em Porto Alegre. Disponível em: https://ssp.rs.gov.br/integracao-garante-utilizacao-de-reconhecimento-facial-em-porto-alegre. Acesso em: 20 de maio de 2021.

71 BEM PARANÁ. Curitiba inaugura centro de controle e lança a 'Muralha Digital' com mais de 1,7 mil câmeras. Disponível em: https://www.bemparana.com.br/noticia/curitiba-inaugura-centro-de-controle-e-lanca-a-muralha-digital-com-mais-mil-cameras#.YKxrcJNKg1L. Acesso em: 20 de maio de 2020.

[72] Em resposta à requisição de acesso à informação, a SPTrans forneceu o seguinte link para as solicitações de exercício de direitos: http://www.sptrans.com.br/atendimento.

No entanto, apesar de fácil acesso, o atendimento on-line apenas possibilita o exercício dos direitos de acesso, correção e atualização dos dados cadastrais. Não há, por exemplo, fácil disponibilização de informações sobre as entidades públicas e privadas com as quais realiza-se uso compartilhado de dados; ou, então, canal para o exercício do direito de revisão das decisões tomadas com base unicamente em tratamento automatizado de dados pessoais.

No âmbito do transporte público do Distrito Federal, onde desde 2018 é obrigatória a biometria facial em todos os ônibus da frota distrital por força da Portaria n. 15/2018, da Secretaria de Transporte e Mobilidade do Distrito Federal (SEMOB), o canal para o exercício de direitos não se dá por meio da Secretaria, mas sim por meio do Banco de Brasília (BRB) Mobilidade, instituição responsável pelo administração do Bilhete Único. Assim, no Distrito Federal, existe uma aplicação para dispositivos móveis para que os usuários, dentre outras funções, gerenciarem seus dados, o BRB Mobilidade. No entanto, novamente apenas são garantidos os direitos de acesso, correção e atualização dos dados cadastrais. São ausentes, por exemplo, informações sobre o uso compartilhado de dados, além da inexistência de um canal para a solicitação de revisão de decisões tomadas unicamente por tratamento automatizado.

Ao passo que existe alguma garantia aos titulares de dados no contexto da mobilidade urbana, mesmo que incipiente, a realidade é diferente quando se trata da segurança pública e do uso de sistemas de reconhecimento facial para provimento de serviços sociais. Nenhum dos órgãos que empregam a tecnologia nesses setores fornece meios para o exercício de direitos pelos titulares.[73]

Não há, da mesma forma, **dados estatísticos sistematizados, consolidados ou publicizados sobre o tratamento de dados realizado por meio de tecnologias de reconhecimento facial pela Administração Pública.** Os dados são insuficientes para determinar com precisão se o emprego irrestrito das tecnologias de vigilância favorece maior eficiência das atividades do setor público, já que não há uma transparência ativa por parte das autoridades dos relatórios por elas realizados, se é que o são. E daqueles que são divulgados, **a narrativa da eficiência da tecnologia parece não se confirmar estatisticamente.**

Nesse sentido, as informações a que esta pesquisa obteve acesso, e que podem indicar algum grau de eficiência no uso das tecnologias, não foram encontradas por meio de relatórios detalhados disponibilizados de forma ativa nos sites institucionais das autoridades ou fornecidas através dos pedidos de LAI, por exemplo. Pelo contrário, os dados foram acessados por meio de portais de notícias que realizaram pesquisa independente.

[73] Para mais detalhes, consultar anexo Escolas e Programas Sociais, itens 2, 3,4 e 5.

A título de exemplo, no carnaval de Salvador de 2020, das 11,7 milhões de pessoas entre adultos e crianças que estiveram presentes, o uso das mais de 80 câmeras com tecnologia de RF auxiliaram na detecção de 42 foragidos, sendo 13 relacionados ao tráfico de drogas, 14 procurados por roubo, 3 por furto, 2 envolvidos em homicídio e outros.[74]

Já no Rio de Janeiro, a Polícia Militar afirmou que, com o uso de tecnologia de RF no entorno do Estádio do Maracanã, foi possível realizar mais de 63 mandados de prisão durante a Copa América de 2019. **A notícia abordou dois casos de falsos positivos.** No primeiro, a suspeita foi confundida com uma pessoa que cometeu crime que já estava presa. No segundo, um homem foi preso por alguns dias antes que o erro fosse notado.[75]

À primeira vista, parece tratar-se de um caso de sucesso o fato de se ter detido 42 foragidos com o uso da tecnologia no Carnaval de Salvador. No entanto, ao se observar que isso foi feito através da **intromissão na esfera informativa de 11,7 milhões de pessoas, ou seja, mais de 278.000 vezes a quantidade de indivíduos detidos**, percebe-se haver ampla margem para questionar se o benefício obtido com a tecnologia supera de fato os riscos que ela impõe à privacidade de multidões submetidas à vigilância massiva do Estado.

Ainda mais preocupante é o fato de que a tecnologia de RF tem como alvo mais comum no Brasil a população negra, conforme identificado em estudo da Rede de Observatórios de Segurança.[76] Essa evidência levanta um alerta vermelho sobre como essas tecnologias podem ter como alvo grupos específicos de pessoas que são historicamente reconhecidas como alvo de discriminação no Brasil.

[74] GAMA, Aliny. Reconhecimento facial por app captura 42 foragidos no Carnaval de Salvador. UOL, 2020. Disponível em: https://www.uol.com.br/carnaval/2020/noticias/redacao/2020/02/26/reconhecimento-facial-por-app-captura-42-foragidos-no-carnaval-de-salvador.htm?cmpid=copiaecola. Acesso em: 12 de fev. 2021.

[75] Para mais detalhes, consultar anexo Segurança Pública, item 9.

[76] No estudo, 151 casos de uso de FRT foram identificados em 4 estados federais. Em 42 desses casos, havia dados sobre identidade racial. Destes 42, 38 dos indivíduos rastreados eram negros. Veja mais em: Rede de Observatórios da Segurança. Retratos da Violência. 2019. Disponível em: https://www.ucamcesec.com.br/wp-content/uploads/2019/11/Rede-de-Observatorios_primeiro-relatorio_20_11_19.pdf. Acesso em: 24 fev. 2021.

Nesse sentido, o diagnóstico obtido a partir dos casos explorados é que o uso sem avaliações de risco de sistemas de reconhecimento facial pelo setor público se reflete também na ausência de prestação de contas aos titulares, já que estes não têm informações claras, precisas e facilmente acessíveis sobre a realização do tratamento de dados.

Esta prestação de contas poderia se materializar por meio da garantia ao exercício dos direitos dos titulares, possibilitando que estes requeiram as informações diretamente do controlador, ou por meio de dados estatísticos publicados pelas próprias autoridades em seus sites institucionais.

Vale ressaltar que a disponibilização de tais dados é necessária para a própria legitimação do tratamento. Afinal, considerando que o principal argumento para o emprego das tecnologias aqui analisadas seria o suposto ganho de eficiência engendrado pelo emprego do videomonitoramento e do reconhecimento biométrico facial, **é indispensável que essa ideia de tamanha eficiência se comprove por meio de dados que demonstrem os ganhos obtidos a partir da identificação de indivíduos em relação à massiva intromissão na privacidade e proteção de dados de indivíduos.**[77]

4. Conclusão

Este trabalho reuniu exemplos nacionais do uso de câmeras de videomonitoramento e sistemas de reconhecimento facial pelo setor público nas esferas municipal, estadual e federal. Para responder aos questionamentos levantados sobre o impacto do uso destas ferramentas nos espaços públicos e na vida cotidiana, explorou-se cinco eixos de análise das experiências brasileiras. São elas:

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

[77] BABUTA, A.; OSWALD, M.; RINIK, C. Machine learning algorithms and police decision-making: legal, ethical and regulatory challenges. RUSI Whitehall Report: 2018 Disponível em: https://rusi.org/sites/default/files/201809_whr_3-18_machine_learning_algorithms.pdf.pdf. Acesso em 15 de fev. 2021.

As conclusões alcançadas denotam um denominador comum: a falta de transparência e de mecanismos garantidores de proteção de dados e segurança na implementação das tecnologias de vigilância no Brasil.

O uso de tecnologia de RF, por definição, tem como consequência a coleta de dados biométricos, considerados sensíveis pela LGPD e que demandam tratamento diferenciado, com maiores proteções e mecanismos de segurança. A lacuna regulatória para o uso específico destes dados biométricos apresenta riscos em seu uso disseminado e cruzamento com outros tipos de dados.

Apesar disso, os casos explorados indicam uma ampla margem de discricionariedade no uso por parte dos gestores e a falta de rastro legal no tratamento de dados, especialmente no âmbito da segurança pública. Essa ausência de balizas próprias para o uso de sistemas tão invasivos leva a adoções que não garantem mecanismos suficientes ao exercício de direitos de titulares de dados. A necessidade de uma legislação específica, precedida de debate público, abrangente o suficiente para mitigar os potenciais riscos e interferências da tecnologia faz-se, portanto, imperativa para garantir previsibilidade e transparência no uso de tecnologias de RF.

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. A agressividade na forma de venda desses sistemas e a promessa de solução dos problemas na prestação de serviços públicos a partir da mera utilização de tecnologias avançadas se une à falta de reflexão aprofundada sobre os impactos no uso desses sistemas. 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 reconhecimento facial.

Esses fatores poderiam, no entanto, ser mitigados por uma padronização e publicização de análises de risco e impacto, além da edição de legislações específicas. Porém, 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.

Além disso, as discussões legislativas identificadas não demonstram cuidados adequados com a privacidade e a proteção de dados pessoais de indivíduos.

Não há, portanto, uma base suficientemente clara para realizar análises objetivas dos riscos envolvidos. Isto é resultado direto de uma lacuna de regulamentação sistematizada sobre a obrigatoriedade das análises de impacto, fazendo com que a experiência brasileira se paute no uso indiscriminado de tais tecnologias aliado à escassez de informações sobre os riscos envolvidos, indo na contramão das práticas internacionais.

Também se faz necessário que o emprego destas tecnologias pela Administração Pública proporcione a devida prestação de contas aos titulares dos dados. 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, compilou-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. Ainda, destacou-se a forma de negociação para uso da tecnologia de RF.

Por fim, destacou-se a recomendação pelo não uso da tecnologia de reconhecimento facial. Mesmo que se adotem as salvaguardas indicadas neste relatório, considerou-se que a tecnologia de RF ainda apresenta ameaças consideráveis e elevadas ao exercício de direitos fundamentais. Tais precauções, baseadas no conhecimento técnico atualmente existente acerca da tecnologia, apenas mitigam os riscos que esta acarreta.

Casos	Regulação específica	Boas práticas	Erro de acurácia	Direitos do titular	Formas de negociação
SSP/BA	X	X[78]	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[79]	Licitação
SERPRO	X[80]	X[81]	X	X	Produção própria

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

[78] 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.
[79] 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.
[80] 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.
[81] Apesar do SERPRO informar que possui política de boas práticas, este documento não foi está público para consulta da população.

Anexo

SEGURANÇA PÚBLICA

1. Secretaria de Segurança Pública do Estado da Bahia

A Secretaria de Segurança Pública do Estado da Bahia (SSP/BA)[82] utiliza m**ais de 80 câmeras com tecnologia de RF desde 2018 em diferentes regiões**, como Metrô, Arena Fonte Nova, Aeroporto, COI, Elevador Lacerda, Ferry Boat, e Rodoviária. Em resposta ao pedido de informação, a SSP/BA informou que usa a tecnologia para execução de políticas públicas para preservação da ordem pública, contribuindo para a captura de pessoas com Mandado de Prisão ou de pessoas desaparecidas.

O uso de tecnologia de reconhecimento facial (RF) se dá sem qualquer previsão em norma específica, mas, segundo a SSP/BA, o uso já estaria autorizado pelo **art. 144 da Constituição Federal**, que garante uso de ferramentas que tenham como objetivo auxiliar as polícias na manutenção da ordem nos espaços públicos. Sobre os mecanismos de segurança, a SSP/BA informou que observa "as normas Internacionais de Segurança como a ISO 27001, ISO 27002, ISO 27701, bem como o uso das melhores práticas para gerenciamento de serviços de TI estabelecidas pela ITIL".

No caso da SSP/BA, o banco de dados utilizado para identificar as pessoas é o banco de dados do Mandado de Prisão e de Pessoas Desaparecidas e apenas a Secretaria tem acesso aos dados pessoais tratados. A empresa fornecedora da solução de tecnologia de RF foi a Informática El Corte Inglés Brasil Ltda (IECISA) e as empresas fabricantes das câmeras identificadas são Huawei, Hikvision e Axis. Além disso, a fornecedora do software é a Huawei, sendo que o valor do contrato para uso dessa tecnologia resultou em um montante de R$ 9.160.081,71, que se iniciou por conta do Consórcio Bahia-Segura em que foi apresentada solução de videomonitoramento com analíticos, em 2014, para uso na Copa Mundo e Copa das Confederações.

Ainda, a Secretaria informou que ocorre uma constante revisão humana dos algoritmos de RF, na tentativa de evitar decisões equivocadas baseadas em informações inconsistentes. Quando uma pessoa é identificada, as informações são checadas com a Polícia Civil para que se verifique se o mandado de prisão é válido por meio de uma base de dados estadual e da Base Nacional de Mandado de Prisão (BNMP) do Conselho Nacional de Justiça (CNJ).

[82] SSP/BA, pedido de informação via Lei de Acesso à Informação, 12 de nov. de 2020.

Além disso, há protocolos sigilosos sobre a forma de uso de RF,[83] mas não há mecanismos para uma pessoa requerer acesso aos dados coletados pelo sistema, mesmo para o titular de dados.

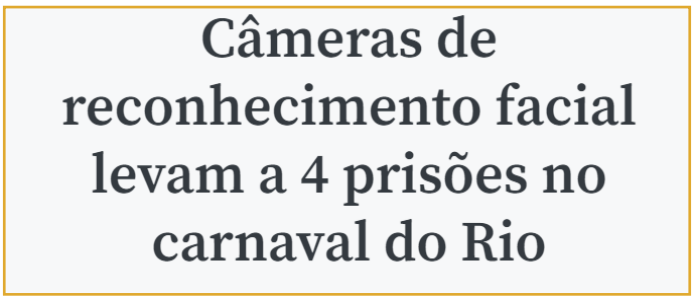
Durante o Carnaval de Salvador de 2019, o Sistema de Reconhecimento Facial da SSP/BA permitiu a identificação de uma única pessoa foragida.[84] Em setembro de 2019, um homem foi abordado de forma violenta após ser erroneamente identificado com outra pessoa que tinha cometido crime.[85] Já em 2020, a SSP/BA divulgou que a tecnologia de RF auxiliou na captura de 42 foragidos da Justiça. Após a identificação pela tecnologia, as pessoas passaram também por um processo de identificação humana.[86] Não foram disponibilizados o número de casos de falsos positivos e erros de acurácia da tecnologia de RF.

Homem é preso por engano em Copacabana

O homem foi detido após identificação no sistema de reconhecimento facial

Inocente é confundida com criminosa por câmera de reconhecimento facial no Rio

Sem documentos, ela foi para a delegacia e só foi liberada após familiares esclarecerem a confusão



Câmeras de reconhecimento facial levam a 4 prisões no carnaval do Rio

[83] SSP/BA, entrevista com agente público, 4 dez. 2020.
[84] SSP. SSP amplia cobertura do Reconhecimento Facial no Carnaval. 2020. Disponível em: http://www.ssp.ba.gov.br/2020/02/7236/SSP-amplia-cobertura-do-Reconhecimento-Facial-no-Carnaval.html. Acesso em: 4 fev. 2021.
[85] REDAÇÃO 4P. Sistema de reconhecimento facial de salvador confunde homem com necessidades especiais com assaltante. 2020. Disponível em: https://midia4p.cartacapital.com.br/sistema-de-reconhecimento-facial-de-salvador-confunde-homem-com-necessidades-especiais-com-assaltante/. Acesso em: 4 fev. 2021.
[86] SSP. Reconhecimento Facial captura 42 foragidos na folia. 2020. Disponível em: http://www.ssp.ba.gov.br/2020/02/7296/Reconhecimento-Facial-captura-42-foragidos-na-folia.html. Acesso em: 4 fev. 2021.

2. Secretaria de Segurança Pública e Defesa Socialdo Estado do Ceará

A Secretaria de Segurança Pública e Defesa Social do Estado do Ceará (SSPDS/CE)[87] utiliza o Sistema Policial Indicativo de Abordagem (**SPIA**) desenvolvido pela Polícia Rodoviária Federal (PRF). Segundo a Secretaria, esse sistema utiliza mais de 3.300 câmeras de monitoramento para subsidiar recursos no combate ao crime, na prevenção de delitos, nos planejamentos estratégicos e nas operações de segurança com um todo. É utilizado no Centro de Comando e Controle (CICC) e na Coordenadoria Integrada de Operações de Segurança (CIOPS), tanto na capital, região metropolitana e interior do Estados do Ceará, tornando-se uma forte aliada na elucidação de crimes em território cearense.

Especificamente sobre a tecnologia de RF, a SSPDS/CE afirmou que ela é um importante instrumento de apoio para a ação das forças policiais, contribuindo tanto para a prevenção de delitos quanto para solucionar os crimes, mas n**ão apresenta justificativas** para essa afirmação. Ademais, a tecnologia de RF é utilizada por meio de um **aplicativo de celular** chamado PCA e desenvolvido pela SSPDS, em parceria com a Universidade Federal do Ceará (UFC).

Quando questionada, a Secretaria afirmou que são sigilosas informações sobre a base de dados utilizada para identificação das pessoas, os riscos e potenciais discriminatórios da tecnologia, e as formas de assegurar direitos dos titulares de dados. Neste caso, a SSPDS/CE afirmou que os cidadãos em geral, mesmo mediante solicitação de informações, não possuem a prerrogativa de acesso aos dados pessoais. Em contradição, em outro pedido de acesso à informação, a SSPDS/CE afirmou que o aplicativo de celular, que permite a identificação da pessoa a partir de tecnologia de RF, realiza uma busca em uma base de identificação civil com quase oito milhões de cadastros.[88]

[87] SSPDS/CE, pedido de informação via Lei de Acesso à Informação, 15 de dez. de 2020.
[88] SSPDS/CE, pedido de informação via Lei de Acesso à Informação, 21 de set. de 2020.

3. Secretaria de Estado da Segurança e Defesa Social da Paraíba

Em 2019, a tecnologia de RF foi utilizada no São João de Campina Grande, uma das maiores festas do Brasil que chega a ser frequentada por mais de 1,5 milhão de pessoas por ano. A empresa Facewatch, fornecedora da tecnologia, instalou 250 câmeras com software de tecnologia de RF por todo espaço do evento possibilitando a abordagens em 250 casos suspeitos e a prisão de 11 pessoas.[89]

Em entrevista sobre o caso de uso,[90] a Secretaria de Estado da Segurança e Defesa Social da Paraíba (SESDS/PB) afirmou que há interesse em continuar utilizando a tecnologia, mas revelou que, com a pandemia da COVID-19, os planos foram postergados. A base de dados utilizada foi a "procurados.pb.gov.br" e, como padrão, a imagem que não era parecida com nenhuma do banco de dados era descartada imediatamente. Já em resposta ao pedido de informação sobre o uso de tecnologia de RF pelo estado como um todo,[91] a SESDS/PB informou que contratou a empresa Brisanet com equipamentos da Hikvision para fornecer a tecnologia de RF para finalidades diversas com base em todos os bancos de dados disponíveis no sistema de segurança pública do Estado.

4. Secretaria de Segurança Pública do Distrito Federal

O Distrito Federal possui um sistema robusto de integração de tecnologias de monitoramento chamado de Centro Integrado de Operações em Brasília (**CIOB**).[92] Sua finalidade é promover a gestão integrada das operações de Segurança Pública, Mobilidade, Fiscalização e Prestação de Serviços Públicos do Distrito Federal.

Esse sistema abrange várias regiões administrativas, sendo aplicado no contexto preventivo e investigativo por parte das forças que compõem o Sistema de Segurança Pública do Distrito Federal, além do acompanhamento em tempo real das Operações Integradas sob a coordenação deste Centro.

---

[89] REDAÇÃO. São João de Campina Grande contou com tecnologia de reconhecimento facial. 2019. Disponível em: https://computerworld.com.br/negocios/sao-joao-de-campina-grande-contou-com-tecnologia-de-reconhecimento-facial/. Acesso em: 5 fev. 2021.

[90] SESDS/PB, entrevista com agente público, 10 nov. 2020.

[91] SESDS/PB, pedido de informação via Lei de Acesso à Informação, 5 nov. 2020.

[92] SSP/DF, pedido de informação via Lei de Acesso à Informação, 18 de jan. de 2021.

Tendo em vista o escopo amplo do CIOB, as imagens coletadas por meio das **câmeras de videomonitoramento são acessíveis por todos os órgãos públicos** que integram o Centro, como a Casa Civil, a Secretaria de Saúde, a Secretaria de Fazenda, a Polícia Militar do Distrito Federal, a Polícia Civil do Distrito Federal, a Companhia Energética de Brasília, o Instituto Brasília Ambiental, entre outros. Ainda, destacou-se que não foram projetados protocolos para implementação do Projeto de Videomonitoramento Urbano ou elaborados relatórios de impacto, conforme informações obtidas via solicitações de informação ao órgão.

Por fim, quando questionada sobre o uso de tecnologia de RF, a SSP/DF afirmou que ainda não utiliza essa ferramenta em suas atividades, mas que **pretende adquirir a tecnologia no futuro**. Essa informação se confunde, no entanto, com notícias que demonstraram casos de uso sistemas de RF pela Polícia Civil do Distrito Federal.[93]

5. Secretaria de Segurança Pública do Estado de São Paulo

O Distrito Federal possui um sistema robusto de integração de tecnologias de monitoramento chamado de Centro Integrado de Operações em Brasília (**CIOB**).[92] Sua finalidade é promover a gestão integrada das operações de Segurança Pública, Mobilidade, Fiscalização e Prestação de Serviços Públicos do Distrito Federal.

Esse sistema abrange várias regiões administrativas, sendo aplicado no contexto preventivo e investigativo por parte das forças que compõem o Sistema de Segurança Pública do Distrito Federal, além do acompanhamento em tempo real das Operações Integradas sob a coordenação deste Centro.

A Secretaria de Segurança Pública do Estado de São Paulo (SSP/SP)[94] utiliza um sistema amplo de videomonitoramento de várias regiões do estado, o **Detecta**. Por meio desse sistema, a Secretaria tem acesso a mais de 1780 câmeras de monitoramento ao vivo das prefeituras de São Paulo, Marília, São Carlos, Santos e outras, além das câmeras de associações de bairros e condomínios que compartilham os vídeos. A SSP informou que não grava essas imagens, mas elas podem ser resgatadas pelo proprietário da câmera.

[93] POLÍCIA CIVIL DO DISTRITO FEDERARL. PCDF reforça plantões, faz campanhas educativas e marca presença na Cidade da Segurança Pública para garantir carnaval seguro aos brasilienses. Disponível em https://www.pcdf.df.gov.br/noticias/9077/pcdf-reforca-plantoes-faz-campanhas-educativas-e-marca-presenca-na-cidade-da-seguranca-publica-para-garantir-carnaval-seguro-aos-brasilienses. Acesso em 31 mai. 2021.

[94] SSP/SP, entrevista com agente público, 18 nov. 2020

Como forma de uso do sistema, a SSP/SP disponibiliza uma **Cartilha pública** que informa sobre o funcionamento do Detecta, como aderir ao sistema e quais as possibilidades de uso.

Ainda a SSP informou que tem acesso a diversas bases de dados de órgãos da Administração Pública, como a da carteira de identidade, a base de boletins de ocorrência, antecedentes criminais e pessoas desaparecidas da Polícia Civil. Do Detran, é possível acessar a base de dados de veículos e da Carteira Nacional de Habilitação, com fotos pessoais e filiação dos cidadãos. Ainda, a SSP/SP acessa a base INFOSEG, que contém fotografias de pessoas de outros estados.[95]

Além do Detecta, a SSP/SP utiliza o DAS, Domain Awareness System, aplicativo desenvolvido pela Microsoft que permite concentração de informações sobre as câmeras de monitoramento, sensores de placas de veículos, alertas de sensores de radiação e de gás tóxico. O DAS foi comprado pela Secretaria em 2013 e permite que o policial visualize até duas câmeras simultâneas ao vivo.[96]

6. Polícia Civil do Estado de São Paulo

Em vista de notícias veiculadas pela imprensa informando que o estado de São Paulo utilizou tecnologia de RF em tempo real no Carnaval de 2020,[97] foi feito pedido de informação à Polícia Civil do Estado de São Paulo (PCESP).[98] Em primeiro momento, ao contrário de todos os pedidos feitos a outros órgãos públicos nesta pesquisa, a polícia afirmou que não fornece informações acerca de procedimentos de Polícia Judiciária, programas e/ou sistemas que são utilizados pela PCESP para pessoas que não façam parte dos quadros da Polícia Civil.

Em um segundo pedido feito pelo LAPIN, a PCESP negou acesso às informações solicitadas afirmando que o pedido de informação via LAI não deve ter como objetivo a obtenção de informações sobre casos concretos.[99]

---

[95] SSP/SP, entrevista com agente público, 18 nov. 2020

[96] SSP/SP, entrevista com agente público, 18 nov. 2020

[97] GOMES, Helton Simões. Pela 1ª vez, SP tem monitoramento facial em tempo real no Carnaval; entenda, 2020. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/02/19/folia-vigiada-sp-tera-reconhecimento-facial-ao-vivo-no-carnaval-entenda.htm. Acesso em: 4 de fev. de 2021.

[98] PCESP, pedido de informação via Lei de Acesso à Informação, 28 de out. de 2020.

[99] PCESP, pedido de informação via Lei de Acesso à Informação, 25 de nov. de 2020.

Em um terceiro pedido de informação, a PCESP afirmou que o sistema de reconhecimento facial foi objeto de testes por parte da polícia durante o Carnaval de 2020, mas não foi objeto de contratação. Foi interposto recurso à PCESP requerendo maiores detalhamentos do caso que foi **indeferido** sem nenhuma fundamentação.[100]

7. Secretaria Municipal de Cooperação nos Assuntos de Segurança Pública do Município de Campinas

Matéria publicada no site oficial do município de Campinas, foi noticiado que "as novas câmeras e os sistemas inteligentes, disponibilizados pela chinesa Huawei e que entrarão em operação no monitoramento da segurança em Campinas, permitirão o reconhecimento facial".[101] Diante dessa informação, foi realizado pedido de informação à Secretaria Municipal de Cooperação nos Assuntos de Segurança Pública.[102] Em resposta, o órgão afirmou que a tecnologia de RF está sendo operacionalizada somente para teste, usando o conceito de **laboratório a céu aberto** que encontra-se no Planejamento Estratégico Campinas Cidade Inteligência.

Este projeto está sendo desenvolvido em parceria com a prefeitura, a empresa **Huawei** e o Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPqD). Especificamente sobre a função da empresa Huawei, em entrevista, a Secretaria de Segurança Pública de Campinas afirmou que a empresa foi a financiadora do uso de tecnologia de RF no laboratório a céu aberto, já que a prefeitura não entendia de forma ampla a operacionalização e o impacto da tecnologia.[103]

Em uma entrevista realizada com um membro do CPqD,[104] identificou-se que o projeto Cidade Segura visa à melhoria da segurança do cidadão por meio do uso da tecnologia, de forma que a tecnologia de RF é apenas mais uma ferramenta para se atingir esse objetivo mais amplo.

---

[100] PCESP, pedido de informação via Lei de Acesso à Informação, 25 de nov. de 2020.
[101] AGEMCAMP. Radares de monitoramento têm reconhecimento facial. 2018. Disponível em: http://www.agemcamp.sp.gov.br/radares-de-monitoramento-tem-reconhecimento-facial/. Acesso em: 4 jan. 2021.
[102] CIMCamp, pedido de informação via Lei de Acesso à Informação, 25 nov. 2020.
[103] SSP/CA, entrevista com agente público, 9 nov. 2020
[104] CPqD, entrevista com pesquisador, 9 nov. 2020

Com isso, foram instaladas 20 câmeras com tecnologia de RF em locais determinados pela equipe de segurança pública do município para testar a acurácia da tecnologia e as formas de abordagem do agente de segurança. A segunda fase desse projeto seria testada em forma de um piloto ainda em 2019, mas, até dia 9 de novembro de 2020, ainda não tinha sido realizada.

Em entrevista, representantes da Secretaria de Campinas afirmaram que o município decidiu por não mais investir na tecnologia de RF visto que o funcionamento adequado apenas era possível em apenas locais específicos e estratégicos. Isso porque a tecnologia não tinha performance satisfatória em locais abertos de grande circulação, de forma que os número de erros de identificação eram significativos.[105]

8. Secretaria Municipal de Cooperação nos Assuntos de Segurança Pública do Município de Campinas

No caso do município de Mogi das Cruzes, a tecnologia de RF foi utilizada em um evento local, a Festa do Divino Espírito Santo, em 2019.[106] Quando solicitadas informações sobre o caso, a prefeitura municipal informou que o emprego de tecnologia de RF se deu por uma "parceria entre a prefeitura e a empresa Chinesa Dahua Technology, sem custos para a Administração municipal. Tal parceria foi motivada pela aproximação entre a cidade e a China, que iniciou em fevereiro de 2019 e, em junho do mesmo ano, começaram as tratativas para **Mogi se tornar cidade-irmã de YongKang, na China**".[107]

[105] SSP/CA, entrevista com agente público, 9 nov. 2020

[106] PORTALNEWS. Segurança tem câmeras de reconhecimento facial. 2019. Disponível em: http://www.portalnews.com.br/_conteudo/2019/05/cidades/103243-seguranca-tera-cameras-com-reconhecimento-facial.html. Acesso em: 4 set. 2020

[107] Prefeitura de Mogi das Cruzes, pedido de informação via Lei de Acesso à Informação, 30 nov. 2020.

9. Polícia Militar do Estado do Rio de Janeiro

O uso de câmeras no carnaval do Rio de Janeiro, em 2019, com a tecnologia de reconhecimento de placa possibilitou a recuperação de um veículo roubado. Ainda, no mesmo evento, o uso de câmeras com a tecnologia de RF deu causa à prisão de quatro pessoas que possuíam mandado de prisão em aberto.[108] Uma **mulher inocente foi confundida** pela tecnologia de RF com uma mulher que cometeu crimes, ela teve de ser conduzida à delegacia e só depois foi liberada. Neste caso, um erro na formação do banco de dados da polícia foi evidenciado, pois a mulher que realmente estava sendo procurada já estava presa desde 2015, mas mesmo assim constava na lista de sujeitos de interesse da polícia.[109] Um **homem também foi preso por engano** após ser identificado erroneamente por tecnologia de RF, além desses casos a PMERJ não informou quantos erros do sistema de reconhecimento facial foram identificados.[110]

Sobre esses casos, a PMERJ[111] informou que a iniciativa se deu através de Termo de Cooperação Técnica, firmado no ano de 2019, com a empresa Oi Móvel, o Detran/RJ e a Polícia Civil do Estado do Rio de Janeiro (PCERJ). O escopo do termo foi o de testar a tecnologia com vistas a, no futuro, ter uma potencial adoção mais ampla pelo órgão.

A atuação da Oi se deu de forma conjunta com a **Huawei**, empresa que fornece a tecnologia de RF. Esclarecendo que a vigência do acordo de cooperação técnica foi testada sob forma de **Prova de Conceito** e se deu em duas etapas. A primeira ocorreu de 1° a 11 de março de 2019, e a segunda de 19 de junho a 19 de outubro de 2019. Por oportuno, cabe destacar que o banco de dados foi cedido pela Secretaria de Polícia Civil, a qual também compunha o Acordo de Cooperação Técnica.

---

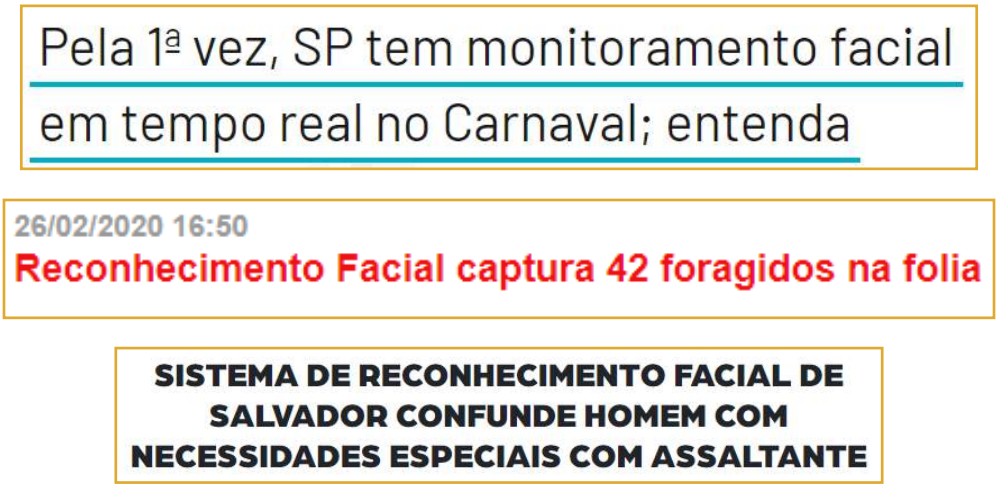
[108] SILVA, Tomaz. Câmeras de reconhecimento facial levam a prisões no carnaval do Rio. 2019. Disponível em: https://www.google.com/url?q=https://agenciabrasil.ebc.com.br/geral/noticia/2019-03/cameras-de-reconhecimento-facial-levam-4-prisoes-no-carnaval-do-rio&sa=D&source=editors&ust=1612476343424000&usg=AOvVaw3YjgowvSATXW-fiX7FkMuW. Acesso em 5 mai. 2020.

[109] CORREIO. Inocente é confundida com criminosa por câmera de reconhecimento facial no Rio. Disponível em: https://www.correio24horas.com.br/noticia/nid/inocente-e-confundida-com-criminosa-por-camera-de-reconhecimento-facial-no-rio/. Acesso em 8 mai. 2020

[110] 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.

[111] PMERJ, pedido de informação via Lei de Acesso à Informação, 2 fev. 2021

Sobre a forma de utilização da tecnologia, a PMERJ evidenciou que "à medida que as pessoas eram visualizadas por uma das câmeras monitoradas pelo sistema, sua face era capturada gerando um código hash que ao ser cruzado com o banco de dados de mandados de prisão, poderia gerar um alerta ou não. Todos os dados de imagens capturados que geraram um banco de imagens foram **deletados ao término da vigência da Cooperação Técnica**, mediante a destruição dos Hard Disks das máquinas utilizadas no monitoramento". No entanto, em entrevista,[112] a PMERJ afirmou que deletou as imagens das pessoas que não são suspeitas, mas armazenou as imagens das pessoas que foram presas.



10. Polícia Civil do Estado do Rio de Janeiro

Já a Polícia Civil do Estado do Rio de Janeiro (PCERJ),[113] quando questionada sobre sua participação no projeto de uso de tecnologia de RF no RJ, afirmou que não foram cedidas informações ou dados pessoais para qualquer órgão. De acordo com respostas da PCERJ ao pedido de informação via LAI, "o procedimento adotado até então foi criar um "barramento" no qual um Policial Civil da Coordenadoria de Comunicações Policiais consultava os dados necessários para o sistema obter êxito na Prova de Conceito." Ainda, o banco de dados da polícia utilizado no uso de tecnologia de RF reunia os dados pessoais de pessoas indiciadas em inquéritos instaurados sob competência da Polícia Civil do Estado do Rio de Janeiro, independente do local de nascimento ou moradia do sujeito.

[112] PMERJ, entrevista com agente público, 9 nov. 2020.
[113] PCERJ, pedido de informação via Lei de Acesso à Informação, 13 nov. 2020.

Em um segundo pedido de informação, a PCERJ[114] afirmou que não acessava o Sistema de Reconhecimento Facial e que este "era operado pelos Policiais Militares e quando havia a identificação de pessoas ou veículos, o sistema gerava um código de identificação, que o operador da PMERJ repassava ao Servidor da Cecopol". Assim, "através do código de identificação informado pelo Policial Militar, o Servidor da Cecopol acessava o sistema denominado GRIFFO, este sistema criado pela DTI/DGTIT, onde se obtinha o nome do suspeito e o nome da mãe dele, com esses dados acessava-se os Sistemas de Consultas da SEPOL (SICWEB), Portal Segurança, Infoseg e o BNMP do CNJ".

11. Secretaria Municipal de Segurança Urbana e Trânsito de Boa Vista

De acordo com informações coletadas do site da empresa Dahua, em 2016, foi instalada uma rede com mais de 100 câmeras em rede na cidade de Boa Vista, capital de Roraima, para auxiliar as atividades de monitoramento policial e de manutenção da segurança pública na cidade. É possível focar e centralizar as imagens das câmeras de rede de modo a permitir detectar, em tempo real, a ocorrência de eventuais crimes. A empresa que fornece a tecnologia das câmeras de videomonitoramento é a Dahua e, além das câmeras, ela desenvolve a solução para armazenamento das imagens.[115] Com base nesses dados, enviamos pedido de informação por meio de LAI à Secretaria Municipal de Segurança Urbana e Trânsito de Boa Vista (SMSUT/BV) a respeito do uso de câmeras com tecnologia de reconhecimento facial. Apesar das informações obtidas online, a prefeitura informou que não faz uso de nenhuma tecnologia de RF.[116]

12. Secretaria de Estado da Segurança Pública do Paraná e Prefeitura Municipal de Curitiba

Em janeiro de 2021, a Prefeitura Municipal de Curitiba (PR) inaugurou o Centro de Controle Operacional (CCO) que integra o projeto "Muralha Digital", desenvolvido em parceria com o Governo do Estado do Paraná com o Instituto das Cidades Inteligentes (ICI).[117]

---

114 PCERJ, pedido de informação via Lei de Acesso à Informação, 18 nov. 2020.
115 DAHUA. Solução de Segurança Dahua para a segurança pública de Boa Vista. 2016. Disponível em: https://www.dahuasecurity.com/br/newsEvents/successStories/6327/43. Acesso em 8 abr. 2021.
116 SMSUT/BV, pedido de informação via Lei de Acesso à Informação, 16 de set. de 2020.
117 SECOM, PREFEITURA MUNICIPAL DE CURITIBA. A cidade que não dorme: Centro de Controle Operacional da Muralha Digital de Curitiba começa a funcionar. 2021. Disponível em: https://www.curitiba.pr.gov.br/noticias/centro-de-controle-operacional-da-muralha-digital-de-curitiba-comeca-a-funcionar/57562. Acesso em 17 mai. 2021.

O CCO, primeira fase do projeto, é uma estrutura municipal que monitora 1.742 câmeras, 191 locais com 804 faixas de radares e 185 botões de pânico em escolas da cidade com o apoio da Polícia Militar e da Guarda Municipal. Das 1.742 câmeras instaladas, 488 estão equipadas com tecnologia de reconhecimento facial.

De acordo com o próprio portal de notícias da Prefeitura de Curitiba, "a segunda fase [do projeto Muralha Digital] deverá ser consolidada entre março e abril [de 2021], com a manutenção e substituição de câmeras existentes, instalação de câmeras em ônibus, terminais e estações-tubo. A terceira fase terá a possibilidade de integração com câmeras particulares". O investimento total do projeto Muralha Digital é estimado em R$ 28 milhões.

Em resposta ao contato do LAPIN com base na Lei de Acesso à Informação, a Secretaria de Segurança Pùblica e Administração Penitenciária do Paraná afirmou desconhecer "qualquer norma que regulamente em específico o uso de tecnologia facial vinculado aos contratos e prestação de serviços", além de categoricamente afirmar que não é prestado nenhum serviço para a Secretaria referente a tecnologia de reconhecimento facial.

De igual maneira, também afirmou não existirem "sistemas ou projetos administrados, desenvolvidos ou em desenvolvimento que tratem do tema reconhecimento facial, bem como, que não há nenhuma licitação ou contrato a respeito" na PMPR.

Não houve resposta para nossos pedidos de informação por parte da Prefeitura Municipal de Curitiba.

13. Secretaria de Segurança Pública do Estado de Santa Catarina

O projeto de videomonitoramento "Bem-Te-Vi", implementado pela Secretaria de Segurança Pública de Santa Catarina, recebeu tecnologia de reconhecimento facial cujos testes se iniciaram em 2019 na cidade de Florianópolis.[118]

[118] SECOM, GOVERNO DO ESTADO DE SANTA CATARINA. SC tem primeiras prisões indicadas por sistema de câmeras de monitoramento. 2019. Disponível em: https://www.sc.gov.br/index.php/noticias/temas/seguranca-publica/sc-tem-as-primeiras-prisoes-indicadas-por-sistema-utilizado-em-cameras-de-monitoramento-da-secretaria-de-estado-da-seguranca-publica. Acesso em 17 mai. 2021.

De acordo com o Comandante da Polícia Militar de Santa Catarina, o coronel Carlos Alberto Araújo Gomes Júnior, a tecnologia de reconhecimento facial seria "um novo sistema que está sendo desenvolvido em conjunto por uma empresa privada com nossa área de inovação e tecnologia".[119]

Apesar dessas informações, obtidas do próprio site do governo do estado, a Secretaria de Segurança Pública do Estado de Santa Catarina, em resposta a pedido de acesso à informação elaborado no bojo desta pesquisa, afirmou que não há norma com aderência ao tema e não há desenvolvimento ou qualquer tecnologia de reconhecimento facial em posse da secretaria.

14. Governo do Estado do Rio Grande do Sul e Secretaria Municipal de Segurança de Porto Alegre

O uso de tecnologia de reconhecimento facial na cidade de Porto Alegre é resultado de uma parceria entre o Governo do Estado, a Prefeitura Municipal, o Ministério Público e o Tribunal de Justiça do Rio Grande do Sul.[120] Através do convênio realizado em 2019, diversos órgãos estaduais e municipais poderiam compartilhar informações a fim de identificar foragidos da justiça e pessoas com mandados de prisão expedidos, além de torcedores com impedimento de ingressar nos estádios e pessoas desaparecidas.

Tratou-se, à época, de um período de testes. Não há informações se o uso posterior da tecnologia pela Secretaria de Segurança Pública do Estado[121] está, de alguma forma, vinculado ao convênio de 2019.

A Secretaria Municipal de Segurança de Porto Alegre afirmou que não desenvolveu ou está empregando a tecnologia de reconhecimento facial em suas atividades. A Secretaria do Estado do Rio Grande do Sul não respondeu os pedidos de acesso à informação.

---

[119] DALCIN. Sistema de videomonitoramento por câmeras completa 20 anos em Santa Catarina. ND Mais. 2020. Disponível em: https://ndmais.com.br/seguranca/sistema-de-videomonitoramento-por-cameras-completa-20-anos-em-santa-catarina/. Acesso em 17 mai. 2021

[120] MATOS. Integração garante utilização de Reconhecimento Facial em Porto Alegre. SECOM SSP. 2019. Disponível em: https://ssp.rs.gov.br/integracao-garante-utilizacao-de-reconhecimento-facial-em-porto-alegre. Acesso em 17 mai. 2021.

[121] O SUL. Secretaria de Segurança do RS apresenta tecnologia de reconhecimento facial à ministra Damares Alves na segunda. 2019. Disponível em: https://www.osul.com.br/secretaria-de-seguranca-do-rs-apresenta-tecnologia-de-reconhecimento-facial-a-ministra-damares-alves-na-segunda/. Acesso em 17 mai. 2021.

1. Secretaria de Estado da Assistência e Desenvolvimento Social do Estado de Alagoas

A Secretaria de Estado da Assistência e Desenvolvimento Social do Estado de Alagoas[122] utiliza tecnologia de RF para **entrega de auxílios sociais aos beneficiários**, como é o caso do Programa de Complementação Alimentar de Gestantes, Nutrizes e Crianças em Situação de Vulnerabilidade Social e Insegurança Alimentar e Nutricional.

Apesar de não haver documentação ou relatório que indique a existência de segurança e minimização de riscos do sistema, a Secretaria afirmou que a tecnologia de RF torna o processo de concessão de benefícios mais eficiente, ágil e seguro do que outras tecnologias, a exemplo da impressão digital.

Além disso, não há qualquer regulamentação que autorize o uso de tecnologia de RF no estado. Ainda assim, a tecnologia já é utilizada em 102 municípios alagoanos para a entrega de benefícios sociais.

A tecnologia foi obtida pelo governo estadual por meio de procedimento licitatório na modalidade pregão, que consagrou a empresa **Ponto ID** como vencedora. O valor do contrato, vigente entre os anos 2018 e 2019, ultrapassou R$ 1,8 milhão.

De acordo com a Secretaria, o acesso aos dados faciais coletados é permitido não só à própria Secretaria, mas também à fornecedora da tecnologia e aos municípios beneficiados. O sistema, ainda segundo a Secretaria, possui taxa de acurácia superior a 99.4%. Por fim, sobre as formas de exercício dos direitos do titular, a Secretaria informou que segue a Lei estadual n. 8.087/2019, que dispõe sobre o acesso à informação no estado, como mecanismos que garantem a identidade do titular.

[122] SEADES/AL, pedido de informação via Lei de Acesso à Informação, 17 de nov. de 2020.

2. Prefeitura do Município de Pilar do Estado de Alagoas

O município de Pilar/AL iniciou a implementação de tecnologia de RF para **aferir a frequência dos alunos** da Escola Municipal Sueli Chagas. A implementação seria resultado de um processo de modernização promovido pelo prefeito local.[123]

Em resposta ao pedido de acesso à informação, a Secretaria Municipal de Educação e Cultura de Pilar afirmou que não existe norma municipal que regulamente o controle de frequência escolar por tecnologia de RF. Além disso, informou que a tecnologia foi adquirida por 144 mil reais em processo licitatório de pregão presencial com empresas nacionais, sendo a empresa Portabilis Tecnologia LTDA a vencedora para fornecimento do software. No que se refere à permissão de acesso aos dados faciais coletados, esta seria concedida não só à Secretaria, mas também à Portabilis, empresa controladora do software.[124]

3. Prefeitura do Município de Recife do Estado de Pernambuco

Apesar da publicação de notícia sobre o uso de tecnologia de RF no âmbito da Escola Municipal Pedro Augusto para aferição de presença dos alunos,[125] a Diretoria Executiva de Tecnologia na Educação da Prefeitura de Recife assegurou que a tecnologia não foi implantada na referida escola em resposta de pedido de informação via LAI.[126] A reportagem do SBT, porém, afirmou que equipamentos equipados com tecnologia de RF, fornecidos pela empresa Ponto ID, foram instalados no pátio da referida escola para registrar a presença dos alunos por meio da leitura digital do rosto. Ainda segundo a reportagem, caso o registro não seja realizado, o estudante seria considerado ausente e uma mensagem seria automaticamente enviada para o celular dos pais ou responsáveis pela criança.

[123] AMA. Prefeitura de Pilar implanta frequência escolar com reconhecimento facial. 2019. Disponível em: https://ama-al.com.br/prefeitura-de-pilar-implanta-frequencia-escolar-com-reconhecimento-facial/. Acesso em: 4 fev. 2021

[124] SEMEC/Pilar, pedido de informação via Lei de Acesso à Informação, 23 de fev. de 2021.

[125] SBT. Frequência Digital Escolar Facial. 2016. Disponível em: https://www.youtube.com/watch?v=qoVNozhnn0I&feature=emb_logo. Acesso em: 4 fev. 2021.

[126] Controladoria Geral do Município, pedido de informação via Lei de Acesso à Informação, 17 dez. 2020.

4. Prefeitura do Município de Anápolis do Estado de Goiás

Em Anápolis/GO, foi instalado sistema de aferição de presença escolar através de tecnologia de RF na Escola Municipal Anapolino de Faria em 2015, como uma solução que traria maior comodidade para os professores e pais dos alunos. A empresa responsável pelo sistema também teria sido a **Ponto ID**.[127] No entanto, quando questionada sobre as formas de uso e eficiência deste projeto por meio das ferramentas da Lei de Acesso à Informação em outubro de 2020, a prefeitura municipal **não respondeu** a esse pedido, tampouco aos contatos posteriores por telefone e e-mail.

5. Secretaria de Estado da Educação, Juventude e Esportes do Estado de Tocantins

Em outubro de 2020, a Gazeta do Cerrado publicou uma reportagem sobre a contratação de um sistema de reconhecimento facial para escolas pela Secretaria de Estado da Educação, Juventude e Esportes do Estado de Tocantins (SEJE/TO) no valor de R$ 19 milhões.[128]

A SEJE/TO afirmou que a regulamentação do uso da tecnologia acontecerá posteriormente à fase de implementação. A tecnologia de RF foi escolhida para ser utilizada pela Secretaria por "oportunizar um melhor acompanhamento e registro da frequência dos estudantes nos ambientes escolares e nos meios de transporte escolares e notificar os responsáveis e órgãos fiscalizadores sobre a ausência do educando nos ambientes educacionais".[129]

A Secretaria informou ainda que a tecnologia de RF é utilizada nos ambientes escolares e prédios públicos para registro de ponto eletrônico. A tecnologia é fornecida pela empresa Ponto ID e a contratação se deu por licitação por pregão eletrônico em 2020.

---

[127] G1. Escola adota reconhecimento facial para controlar frequência de alunos, em Anápolis. Disponível em: http://g1.globo.com/goias/videos/t/todos-os-videos/v/escola-adota-reconhecimento-facial-para-controlar-frequencia-de-alunos-em-anapolis/4193104/. Acesso em 5 mar. 2021.

[128] GAZETA DO CERRADO. Seduc vai contratar novo sistema de gerenciamento escolar por R$ 19 milhões com reconhecimento facial. 2020. Disponível em: https://gazetadocerrado.com.br/seduc-vai-contratar-novo-sistema-de-gerenciamento-escolar-por-r-19-milhoes-com-reconhecimento-facial/. Acesso em: 4 fev. 2021.

[129] SEJE/TO, pedido de informação via Lei de Acesso à Informação, 23 de fev. de 2021.

As entidades envolvidas no processo educacional possuem acesso aos dados biométricos tratados, assim como o Ministério Público e Conselho Tutelar, além da empresa contratada. Por fim, a SEJE/TO destacou não haver necessidade de realização de um relatório de impacto de dados pessoais, porque "os dados dos estudantes já existem na base de dados do sistema vigente, a única alteração será a coleta da Biometria facial e, no dossiê físico e digital do estudante, constam todos os dados" (sic). [130]

MOBILIDADE URBANA

1. Secretaria Municipal de Mobilidade e Transportes de São Paulo

A Secretaria Municipal de Mobilidade e Transportes de São Paulo (SPTrans) utiliza tecnologia de RF para verificação de compatibilidade biométrica facial entre a pessoa que é titular do cartão para o transporte público "Bilhete Único" e aquele que efetivamente utiliza o cartão, na tentativa de evitar fraude no uso do benefício de transporte. Em pedido de acesso à informação, a Secretaria informou que o sistema é exclusivo da SPTrans, de forma que **não há acesso externo** de qualquer natureza, apenas por autorização judicial.

Neste caso, o Decreto Municipal n. 58.639/19 autoriza e regula de forma específica o uso de tecnologia de RF para finalidade de manutenção do benefício do Bilhete Único. Sobre o processo de tratamento de dados pessoais, a SPTrans afirmou que a imagem da pessoa é coletada no ônibus, quando ela apresenta o cartão na catraca, transferida para um datacenter e comparada com a foto capturada no cadastramento do titular.

Quando é detectada alguma incompatibilidade entre a imagem do titular e do usuário do cartão, é realizada uma checagem manual humana. Caso a checagem manual confirme a divergência, o cartão é bloqueado até que a pessoa a justifique. As imagens capturadas **são excluídas depois de 30 dias**.

[130] Idem.

Sobre a existência de uma política de uso e segurança dessas informações, a SPTrans informou que os dados "são mantidos em datacenter com várias camadas de segurança de acesso, utilizando-se cofre de senha" e que existe uma **política própria para os casos de vazamento** de informações. Ainda, o titular é informado sobre o uso de tecnologia de RF quando se cadastra no Bilhete Único e os **direitos da pessoa como titular de dados** podem ser exercidos perante o Posto de Atendimento da SPTrans.

2. Secretaria de Estado de Transporte e Mobilidade do Distrito Federal

A Secretaria de Estado de Transporte e Mobilidade do Distrito Federal (SEMOB), em parceria com as concessionárias de ônibus, usa tecnologia de RF para verificar a compatibilidade entre o titular do cartão de benefício de mobilidade, o Passe Livre, e aquele que utiliza o cartão.[131] A tecnologia foi **adquirida pelas próprias concessionárias por contratação direta** e seu uso é regulamentado pela Portaria n. 15, de 30 de abril de 2018.

A SEMOB afirmou que os dados são utilizados apenas para a finalidade de verificação e são acessados também pelas empresas concessionárias do transporte público, além do Banco de Brasília (BRB), que é a empresa responsável pelo processamento do Sistema de Bilhetagem Único desde de 2019.[132]

No processo de tratamento de dados, o equipamento, instalado na catraca, coleta a imagem facial no momento em que o cartão libera o acesso do usuário. Porém, as demais câmeras de segurança instaladas nos ônibus começam a coleta de imagens desde a entrada do usuário no veículo.

Como padrão, o sistema realiza a primeira comparação de imagens e, se constatada incompatibilidade facial, os arquivos são analisados por técnicos, que produzem laudos. Os Laudos Biométricos são encaminhados ao BRB, onde são abertos processos administrativos em ambiente eletrônico; os laudos permanecem à disposição para os processos administrativos por tempo indeterminado. Caso os titulares queiram ter acesso a seus dados ou exercer outros direitos, é possível fazê-lo por meio da Ouvidoria da SEMOB.

[131] SEMOB, pedido de informação via Lei de Acesso à Informação, 22 set. 2020.
[132] SEMOB. Semob transfere processamento do Sistema de Bilhetagem para o BRB. 2019. Disponível em: http://semob.df.gov.br/semob-transfere-processamento-do-sistema-de-bilhetagem-para-o-brb/. Acesso em: 1 mar. 2021.

Para garantir a segurança dos dados, todo operador que tem acesso aos arquivos biométricos assina um **termo de responsabilidade** para garantir que não fará uso indevido dos dados acessados. Caso contrário, o operador estará sujeito às sanções civis, administrativas e criminais pertinentes.

Ainda de acordo com o mesmo pedido de acesso à informação, as concessionárias afirmaram que os dados cadastrais dos usuários são importados da base de dados de bilhetagem do BRB e mantidos na base de dados da biometria facial por tempo indeterminado. Quanto às imagens capturadas nos veículos, caso não haja indício de fraude, são excluídas, em regra, após um período que varia entre 30 e 90 dias. As imagens que indicam fraudes, porém, são armazenadas por um ano.

AEROPORTOS

1. Receita Federal

No Brasil, outro uso comum de tecnologia de RF ocorre em aeroportos. Desde 2016, a Receita Federal (RFB) utiliza o sistema de reconhecimento facial da empresa **NEC** em 14 aeroportos internacionais, como o de Brasília, Guarulhos, Recife, Rio de Janeiro e Salvador.[133] A contratação ocorreu via licitação, pela modalidade de pregão eletrônico, e o valor do contrato foi de R$ 7.576.090,72.[134] O objeto do contrato foi o fornecimento de solução de tecnologia de RF para localizar viajantes com risco aduaneiro identificado. Dessa forma, "os servidores dos órgãos de controle podem **identificar inequivocamente os indivíduos de potencial interesse** (previamente selecionados pelo sistema de gerenciamento de risco) e encaminhá-los para fiscalização minuciosa".[135]

Para tanto, a RFB informou que "a solução tecnológica se processa exclusivamente de forma interna no ambiente computacional da RFB, que é acessado apenas por servidores públicos cadastrados com certificado digital. A RFB **não compartilha** os dados da solução de reconhecimento facial nem com a iniciativa privada nem com outro órgão público."[136] Ainda, a RFB afirmou que não existem mecanismos no sistema para extrair os dados coletados mediante solicitação do titular.

---

[133] NEC. Receita Federal utilizará tecnologia de identificação facial da NEC em 14 aeroportos internacionais do País. 2016. Disponível em: https://br.nec.com/pt_BR/press/PR/20160409060302_11186.html. Acesso em 5 fev. 2020.

[134] Contrato RFB-Copol n. 22-2015. Disponível em: http://receita.economia.gov.br/sobre/licitacoes-e-contratos/contratos-de-ti/2015/contrato-rfb-copol-no-22-2015-nec.pdf/view. Acesso em: 5 fev. 2021.

[135] Edital de Pregão Eletrônico RFB/Sucor/Copol n. 16/2014. Disponível em: http://compras.dados.gov.br/pregoes/doc/pregao/17001000001620 14/itens. Acesso em: 5 fev. 2021.

[136] RFB, pedido de informação via Lei de Acesso à Informação, 25 nov. 2020.

1. Serviço Federal de Processamento de Dados (SERPRO)

O Serviço Federal de Processamento de Dados (SERPRO) é uma empresa pública vinculada ao Ministério da Economia que presta serviços na área de tecnologia da informação para a Administração Pública e para empresas privadas. Um dos principais produtos do SERPRO é o **DataValid**, uma Interface de Programação de Aplicações (API) que valida e verifica diversas informações pessoais dos cidadãos por meio de uma consulta às bases originais do governo.

É possível que qualquer empresa valide informações de seus clientes, a exemplo de dados cadastrais como nome, CPF, RG, data de nascimento e número da CNH, mas também dados biométricos, como a digital e o rosto de uma pessoa, por meio da **comparação das informações de rostos coletados pela empresa e disponibilizados na CNH** com o uso de ferramentas de tecnologia de RF.[137]

Para que este produto funcione, a empresa contratante coleta as informações ou a foto de seus próprios clientes a serem validadas, as envia para o SERPRO[138] e este compara tais dados com as informações constantes nas diversas bases de dados originais do governo. O SERPRO informou **que não possui banco de dados próprio**, já que todas as informações são validadas nas bases de dados oficiais do governo, como o banco da Secretaria Especial da Receita Federal[139] e do Departamento Nacional de Trânsito.[140]

---

[137] SERPRO. DataValid. Disponível em: https://www.loja.serpro.gov.br/datavalid. Acesso em: 5 fev. 2021.

[138] SERPRO, pedido de informação via Lei de Acesso à Informação, 28 set. 2020. O pedido e as respostas podem ser acessadas na plataforma do e-sic ou no endereço eletrônico http://www.consultaesic.cgu.gov.br/busca/dados/Lists/Pedido/Item/displayifs.aspx?List=0c839f31-47d7-4485-ab65-ab0cee9cf8fe&ID=1408743&Source=http://www.consultaesic.cgu.gov.br/busca/SitePages/resultadopesquisa.aspx?k=ALL(biom%25C3%25A9trico)%23k=ALL(biom%25C3%25A9trico)%2520(facial)&Web=88cc5f44-8cfe-4964-8ff4-376b5ebb3bef.

[139] Portaria RFB n. 1384/2016, que disciplina a disponibilização de dados não protegidos por sigilo fiscal sob tutela da Receita Federal; e Portaria RFB n. 2189/2017, que autoriza o Serpro a disponibilizar para terceiros dados e informações sob tutela da Receita Federal.

[140] Portaria DENATRAN n. 215, de 06/08/2018; - Portaria DENATRAN n. 72, de 12/05/2017; e autorização do Denatran ao SERPRO publicada no Diário Oficial da União em 03/08/2017. Discorre do Termo de Autorização emitido pelo Denatran ao Serpro para

Quando perguntado sobre os impactos de proteção de dados do DataValid na sociedade, o SERPRO afirmou que foi elaborado um relatório de impacto à proteção de dados (RIPD) com relação à Lei Geral de Proteção de Dados (LGPD) para avaliação dos riscos do DataValid. No entanto, afirmou que o RIPD realizado seria **sigiloso**. Além disso, o SERPRO se negou a conceder informações sobre os fornecedores dos componentes da tecnologia da solução e sobre as empresas e órgãos públicos que têm acesso ao serviço **DataValid**, diante de argumento de suposto segredo comercial.

O SERPRO se coloca apenas como um **intermediário** de validação dos dados, e afirmou não se configurar como controlador de dados. Dessa forma, a empresa pública afirmou que qualquer alteração ou direito a ser exercido pelo titular deveria ser feito perante o órgão controlador.

Porém, em contradição ao explicitado a respeito dos mecanismos disponíveis para o exercício dos direitos dos titulares, o SERPRO informou que o portal Privacidade Digital do Cidadão deveria ser acessado para que o titular exerça direitos previstos na LGPD. Durante o período de envio dos pedidos e recursos de informação, esse portal estava com seu certificado digital desatualizado, apresentando riscos de segurança e à privacidade do usuário. Após ser avisado pelo LAPIN, o SERPRO corrigiu a falha.

Diante de pedidos de informação feitos pelo LAPIN respondidos de forma incompleta ou não respondidos, o requerimento de acesso à informação foi levado à Controladoria-Geral da União (CGU) em recurso. Este foi conhecido e provido para que o SERPRO adote providências para franquear acesso às informações de conteúdo obrigatório sobre os contratos, as quais seriam, conforme o próprio SERPRO, disponibilizadas em transparência ativa em seu Portal da Transparência.

Ainda, deverá ser possível acessar o documento denominado "Aviso de Privacidade da solução DataValid" diretamente ou por meio do link onde se encontra a informação em transparência ativa, com correspondente passo a passo, nos termos do art. 17 do Decreto no 7.724/2012. O conteúdo deste documento deve trazer informações claras e objetivas relativas ao contexto de tratamento de dados pessoais. O SERPRO teve o prazo de 60 dias, a contar de janeiro de 2020, para fazer as alterações determinadas pela CGU, porém o LAPIN não conseguiu confirmar a ocorrência desta mudança.

LAPIN

LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET

JULHO | 2021