[Possível SPAM - Prodasen - NÃO CLIQUE nos links] CARTA ABERTA PELO BANIMENTO TOTAL DO USO DAS TECNOLOGIAS DIGITAIS DE RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA

Secretaria Executiva <secretariaexecutiva@direitosnarede.org.br>

seg 20/06/2022 22:18

Para: CJSUBIA <CJSUBIA@senado.leg.br>;

Cc: ANPD@anpd.gov.br <ANPD@anpd.gov.br>;

Prezados, Encaminho a pedido a carta abaixo e deixo os canais da Coalizão Direitos na Rede abertos para aprofundar o diálogo sobre o tema. Atenciosamente, Fabricio Solagna Secretaria Executiva ----------

CARTA ABERTA PELO BANIMENTO TOTAL DO USO DAS TECNOLOGIAS DIGITAIS DE RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA

As organizações e pessoas que subscrevem esta carta requerem o banimento total do uso das tecnologias digitais de Reconhecimento Facial na Segurança Pública[1] no Brasil em razão dos motivos apresentados a seguir.

Primeiramente, essas ferramentas são capazes de identificar, seguir, destacar individualmente e rastrear pessoas em todos os lugares aonde elas vão, podendo violar direitos como: privacidade, proteção de dados, liberdade de reunião e de associação, igualdade e não-discriminação. Ainda, podem fazer com que as pessoas se sintam inibidas, prejudicando o direito de exercer sua liberdade de expressão.

Essas tecnologias têm ocasionado uma série de graves abusos e violações a direitos humanos em todo o mundo. Um exemplo, retratado no documentário Coded Bias, é o uso do reconhecimento facial pela polícia do Reino Unido e a associação incorreta (até o ano de 2018) de 98% dos rostos apontados como correspondentes a pessoas foragidas. Diante dessas preocupações, cidades como São Francisco e Oakland, nos Estados Unidos, baniram o uso de reconhecimento facial em locais públicos.

No Brasil, país com a terceira maior população encarcerada do mundo, o uso de tecnologias de reconhecimento facial na segurança pública levaria ao agravamento de práticas racistas que constituem o sistema penal. Todavia, apesar da gravidade desses prejuízos, essas tecnologias já estão na grande maioria dos estados brasileiros. Na Bahia, desde 2018, câmeras de

reconhecimento facial foram instaladas com a finalidade oficial de combate à criminalidade, mas sem a comprovação de se ter efetivamente atingido tal objetivo.

Nenhuma proteção técnica ou legal pode eliminar totalmente a ameaça que essas tecnologias representam. Até mesmo empresas como Amazon, IBM, Meta e Microsoft repensaram o uso dessas ferramentas em alguns contextos. Acreditamos, portanto, que elas nunca devem ser usadas em atividades de segurança pública – seja pelo governo ou mesmo pelo setor privado, por meio da delegação da execução de serviços públicos. O potencial de abuso é muito grande e as potenciais consequências, muito graves.

As tecnologias de vigilância nos trazem insegurança em razão da violação a nossos direitos, sem que nos sejam dadas chances de evitar ou mesmo consentir com sua implementação e com o fato de nos tornarmos seus alvos. Destacam-se as violações de nossa integridade, pela coleta e pelo processamento de dados pessoais biométricos; de nossa liberdade de ir e vir e de autodeterminação, pois podemos estar sob vigilância 24 horas por dia, 7 dias por semana, criando um contexto amedrontador; do nosso direito ao devido processo legal, pois a vigilância em massa considera todas as pessoas culpadas por princípio, minando a garantia constitucional da presunção de inocência como um pressuposto jurídico básico.

Independentemente das salvaguardas e correções que poderiam ser propostas para a criação de uma tecnologia alegada e supostamente "livre de erros", essa vigilância constante, massiva e indiscriminada é – em si mesma – uma violação dos direitos e das liberdades das pessoas. Por estarmos falando de mecanismos aplicados de forma incompatível com os direitos humanos, pedimos pelo banimento, e não apenas por uma moratória, do reconhecimento facial no contexto da segurança pública.

Muitas das unidades federativas brasileiras empregam o reconhecimento facial em políticas públicas, total ou parcialmente voltadas à segurança; e os veículos de comunicação repercutem sem questionamentos uma suposta eficácia desse tipo de projeto para a segurança pública. Por essas razões, esta campanha tem como foco o banimento do reconhecimento facial no âmbito da segurança pública. Apesar desse recorte, estamos cientes dos graves problemas decorrentes de outras formas de tecnovigilância que se valem de dados biométricos (incluindo voz, contagem de passos, temperatura, batimentos cardíacos, DNA etc.) e são alvo de outras tantas campanhas e comunicados importantes da sociedade civil e especialistas ao redor do mundo.

Ainda no âmbito da segurança pública, é importante destacar que, embora possa haver a impressão de que a coleta e o tratamento de dados biométricos são realizados somente pelo poder público, muitas dessas conduções são implementadas por meio de contratos com a iniciativa privada. Essas parcerias destinam-se à prestação de serviços que envolvem infraestrutura e ferramentas tecnológicas, podendo incluir o reconhecimento facial.

Com frequência, esses acordos público-privados são pouco transparentes e não proveem à população detalhes relativos ao processamento de dados — cenário que pode ter como consequência, dentre outras, usos secundários desses dados para finalidades de interesse

exclusivo das entidades da iniciativa privada. Em outras palavras, não é rara a ocorrência de desvio de finalidade dos dados pessoais utilizados nesse tipo de projeto.

Na maioria das vezes, as críticas e os protestos que se opõem a esse cenário são destinados ao poder público, responsável por sua implementação. Porém, parcerias público-privadas demandam atenção especial, pois o acesso a informações sobre esse tipo de iniciativa não pode ser dificultado sob o argumento de que elas estariam protegidas por segredo comercial ou empresarial, por exemplo. As empresas têm também a obrigação de respeitar os direitos humanos, independentemente do caráter de seu envolvimento em projetos desse tipo — o que pode ocorrer a partir do fornecimento de dados pessoais ao poder público, por exemplo.

Um caso conhecido internacionalmente e que exemplifica o uso de dados coletados pela iniciativa privada para fins de vantagem competitiva (sem a ciência da população) é o da empresa Axon (atual Taser). Ela utilizou dados gerados por câmeras corporais que havia doado previamente a departamentos de polícia estadunidenses no desenvolvimento interno de sua Inteligência Artificial. Imagine o impacto para a coletividade se uma situação como essa ocorrer no Brasil, atingindo dados biométricos coletados por meio de reconhecimento facial. Nesse sentido, é relevante destacar que um levantamento do Al Sur mostra que uma parcela significativa dessas tecnologias utilizadas no Brasil são oriundas de doações de empresas[2].

Como já mencionado, mesmo que o Brasil possuísse uma lei em vigor para a regulação do processamento de dados pessoais na segurança pública, ainda assim os perigos que o reconhecimento facial representa não seriam eliminados. Diante de um contexto em que fatores como racismo, classismo, misoginia e LGBTQIA+fobia impactam a maneira por meio da qual as pessoas, em sua diversidade, têm seu corpos percebidos, interpretados, abordados e até mesmo discriminados e reprimidos, mecanismos cujo funcionamento se baseia na análise de rostos trazem preocupações específicas.

Um grande problema das tecnologias de reconhecimento facial é que elas dependem da classificação dos corpos. Isso pode ocorrer em função de aspectos como sexo e gênero, por exemplo, trazendo uma visão binária e baseada em estereótipos que não reconhecem a diversidade de corpos, identidades e expressões – quadro ainda mais preocupante no Brasil, país que mais mata pessoas trans.

Além disso, há registros que mecanismos semelhantes tenham sido utilizados para o reconhecimento de emoções das pessoas – o que, além de correr o risco de produzir premissas racistas, não tem comprovação científica sólida de funcionamento. Nesse sentido, vale destacar que a ViaQuatro, concessionária do metrô de São Paulo, foi condenada judicialmente por ter aplicado esse tipo de mecanismo em seus usuários.

Seu rosto pode, sem você ter se dado conta, ter sido submetido ao reconhecimento facial para fins de segurança pública. Isso porque, no Brasil, já existem câmeras de monitoramento munidas com esse tipo de tecnologia em ruas de diversas cidades, inclusive em relógios públicos, e também no transporte público. Pessoas que transitam nesse tipo de espaço com frequência não notam que estão sendo submetidas a alguma identificação. Ainda, há registros de que o reconhecimento facial

é também utilizado em aplicativos de celulares de policiais em abordagens. A possibilidade de circular sem constrangimentos e exercer diversos direitos nesses espaços estará fortemente ameaçada enquanto esse tipo de projeto existir.

A presente campanha pede, então, o banimento do reconhecimento facial na segurança pública porque entende que os seus problemas não têm solução – ou seja, são inseparáveis do próprio uso desses mecanismos. Os algoritmos não funcionam de maneira neutra e podem reproduzir discriminações relacionadas ao ambiente e às pessoas que os formularam e, além disso, sua lógica de funcionamento não é facilmente explicável ao público. Também poderia haver o vazamento da enorme quantidade de dados necessária para o funcionamento dessas tecnologias, deixando vulnerável toda a população.

Mesmo que o funcionamento desses mecanismos fossem aprimorados – uma necessidade que é frequentemente apontada pelas narrativas que defendem sua implementação – isso não contornaria seus impactos negativos. A tentativa de redução desses erros e a programação da tecnologia de acordo com a diversidade das populações-alvo faria com que esses grupos fossem mapeados, identificados, vigiados e rastreados com maior facilidade, o que significa que esse uso seguiria sendo desproporcional. Isso, também, porque há o risco constante de que esse tipo de tecnologia possa ser instrumentalizado por governos para perseguir determinados grupos e pessoas.

Ainda que fossem comprovados “benefícios” dessas tecnologias para a coletividade, não seria proporcional restringir o direito à privacidade da população que transita naquele espaço sob a justificativa de impactos positivos pontuais – os quais são também questionáveis, dada a complexidade de fatores necessários à promoção de medidas de segurança pública não discriminatórias e que efetivamente levem em consideração a coletividade. Nesse contexto, é importante ainda questionar se os “benefícios” apontados nesses debates reproduzem e/ou camuflam violências institucionais em relação a grupos que já são histórica e socialmente perseguidos e oprimidos, como a população negra e indígena, imigrantes, pessoas trans e travestis.

Para além desses impactos diretos aos direitos humanos, também não é vantajoso despender o tanto de dinheiro público que esse tipo de projeto demanda; a pretexto de melhorar a segurança pública, milhões de reais já são (e ainda podem vir a ser) gastos na busca de objetivos que sequer seriam positivos para a população como um todo.

Adicionalmente, o uso dessas ferramentas de forma massiva não é consistente com tratados internacionais com os quais o Brasil está comprometido – incluindo a Declaração Universal dos Direitos Humanos (DUDH) e o Pacto Internacional de Direitos Civis e Políticos (PIDCP). O artigo 17 do PIDCP, por exemplo, protege as pessoas de sofrerem ingerências arbitrárias ou ilegais em suas vidas privadas. A respeito do direito à privacidade na era digital, o Conselho de Direitos Humanos da ONU recentemente apontou em resolução[3] que os crescentes usos de tecnologias como reconhecimento facial, sem as devidas salvaguardas, impactam o direito à privacidade e outros direitos humanos, incluindo a liberdade de opinião, de expressão e de reunião pacífica. O Conselho também apontou preocupação com a reprodução e agravamento de desigualdades raciais com o uso de reconhecimento facial, e conclamou os Estados a garantirem que tecnologias biométricas e de reconhecimento, inclusive reconhecimento facial, não levem à vigilância arbitrária ou ilegal.

Ainda, destaca-se a ameaça ao exercício do direito de protesto. Manifestações públicas nas ruas são expressões de grupos dos mais diferentes espectros políticos no Brasil. A possibilidade de ser alvo de vigilância permanente pode levar as pessoas a mudarem seus comportamentos, em postura de autocensura, e mobilizações legítimas podem ser inibidas. A autocensura pode atingir de maneira mais profunda grupos mais vulnerabilizados pela repressão e violência estatal. Em casos limites, o uso dessas tecnologias pode ensejar a criminalização do direito de protestos.

Apesar de alegações de um pretenso aprimoramento da segurança pública por meio do uso de tecnologias de reconhecimento facial, esse tipo de projeto reproduz a cultura do punitivismo e do encarceramento, em detrimento de privilegiar medidas de prevenção e restauração. Há evidências que mostram como essas tecnologias são usadas de modo abusivo e/ou implementadas com pouca ou nenhuma transparência – quadro que sequer permite que a população questione a maneira como elas funcionam.

Trata-se de um uso de tecnologias de vigilância que, por ser tão perigoso, deve ser rejeitado em um contexto que se pretenda democrático. É preciso banir o uso de tecnologias de vigilância que promovem a violação de direitos!

Pelas razões expostas, essa campanha tem por objetivo que, no âmbito da segurança pública, ocorra a:

1. **Proibição** do uso das tecnologias de reconhecimento facial, sendo adotadas normas para a sua respectiva proibição em qualquer das esferas da Federação, inclusive no que diz respeito às contratações de soluções privadas pela administração pública.

2. **Interrupção** de quaisquer projetos que utilizem, ainda que de forma secundária, reconhecimento facial para fins de segurança pública. Nos casos em que a tecnologia já foi utilizada na população, os governos responsáveis devem formular políticas públicas e planos de ação para que as pessoas que tiveram seus direitos humanos violados por esses mecanismos possam buscar a reparação adequada.

3. **Publicação** de relatórios de impacto do uso dessas tecnologias, desde o momento em que elas foram idealizadas até suas respectivas interrupções, incluindo dados sobre investimento, número e características das abordagens e prisões realizadas, índices de falsos positivos e negativos, documentação dos procedimentos implementados, riscos aos titulares de dados e as medidas que foram adotadas para minimizá-los, entre outras informações relevantes para mensurar o impacto da sua utilização. A Autoridade Nacional de Proteção de Dados (ANPD), em cumprimento das suas atribuições institucionais legalmente estabelecidas, deve exigir a realização e publicação desses relatórios sempre que necessário.

4. **Recusa do setor privado** em incentivar a implementação desse tipo de projeto pelo poder público. Agências de cooperação e bancos não devem fornecer recursos à administração pública para o desenvolvimento e implementação desse tipo de projeto. Empresas e *startups* que

desenvolvam mecanismos de reconhecimento facial não devem fornecer esse tipo de tecnologia para políticas que envolvam segurança pública, seja esse o objetivo principal ou subsidiário.

5. **Mobilização de instituições** que buscam defender direitos constitucionais – como a Defensoria Pública, o Ministério Público e a Autoridade Nacional de Proteção de Dados – em favor do banimento do uso do reconhecimento facial na segurança pública, o que pode envolver desde a realização de diligências administrativas até a tomada de medidas judiciais frente a governos.

Brasília, 08 de Março de 2022.

[1] Levando em conta que essas considerações se referem ao âmbito da segurança pública, vale mencionar que, segundo a Constituição Federal brasileira (1988), a segurança pública se destina a preservar a "ordem pública" e a "incolumidade das pessoas e do patrimônio", sendo exercida pelos órgãos policiais que atuam no país – o que inclui, além das polícias civis e militares, a polícia federal. Além disso, é relevante destacar que o texto do anteprojeto de lei que visa consolidar a legislação de proteção de dados brasileira para determinadas finalidades que não são diretamente abrangidas pela Lei Geral de Proteção de Dados Pessoais (2018), esta última já em vigor, aponta para um entendimento doutrinário de diferenciação entre a atividade de segurança pública e a atividade de persecução penal.

[2] https://www.alsur.lat/reporte/reconocimiento-facial-en-america-latina-tendencias-en-implementacion-una-tecnologia

[3] Resolução adotada pelo Conselho de Direitos Humanos na ONU em 7 de outubro de 2021. Disponível em: https://digitallibrary.un.org/record/3945627?ln=en

Mais detalhes em: https://tiremeurostodasuamira.org.br

ORGANIZAÇÕES QUE ASSINAM ESTA CARTA:

- Ação Educativa – Assessoria, Pesquisa e Informação
- Access Now
- AMAR – Associação de Mulheres Ambulantes de Recife
- AMARC Brasil – Associação Mundial de Rádios Comunitárias
- AqualtuneLab – Cruzando o Atlântico
- ARTIGO 19 Brasil e América do Sul
- Associação Data Privacy Brasil de Pesquisa

- Associação Pernambucana das Profissionais do Sexo – APPS
- AVABBV – Associação de Vendedores Ambulantes do Bairro da Boa Vista
- Casa da Cultura Digital Porto Alegre
- Centro Brasileiro de Estudos de Saúde
- Centro de Estudo de Segurança e CIdadania (CESeC)
- Centro Popular de Direitos Humanos – CPDH
- Coalizão Direitos na Rede
- Coding Rights
- Coletiva Periféricas
- data_labe
- Derechos Digitales
- Instituto Brasileiro de Defesa do Consumidor – IDEC
- Instituto de Pesquisa em Direito e Tecnologia do Recife – IP.rec
- Instituto Educadigital
- Instituto Sumaúma
- Instituto Vero
- Internet Freedom Foundation
- InternetLab

- Intervozes - Coletivo Brasil de Comunicação Social
- IRIS – Instituto de Referência em Internet e Sociedade
- Laboratório de Pesquisa em Políticas Públicas e Internet – LAPIN
- Lavits
- MariaLab
- MediaLab.UFRJ
- Movimento Passe Livre São Paulo
- O Projeto Tor / The Tor Project
- Observatório da Branquitude
- Observatório da Ética Jornalística – objETHOS
- Open Knowledge Brasil
- Palavra Escocesa
- Partido Pirata
- Pimentalab – Laboratório de Tecnologia, Política e Conhecimento da Unifesp
- Plataforma CIPÓ
- Raul Hacker Club
- Rede de Pesquisa em Governança da Internet
- SINTRACI – Sindicato dos Trabalhadores e Trabalhadoras Informais de Recife

- SOS Corpo – Instituto Feminista para Democracia
- Washington Brazil Office
- Witness Brasil

ASSINATURAS INDIVIDUAIS:

- Aderica Campos
- Aina Selles
- Alan Fernandes Xavier
- Ana Carolina Sousa Dias
- Ana Clara Souza
- Ana Gabriela Souza Ferreira
- Ana Lucia Pompermaye
- Ana Luisa Figueiredo de Melo
- Anamaria D Andrea Corbo
- Anderson Santos Mansano
- André Lucas Fernandes
- André Ramiro
-

Anna Bentes Bárbara Lorena e Silva Alves

- Bernardo Gomes Alevato
- Branda Camargo Rochwerger
- Brenda Cunha
- Brisca Bracchi
- Bruna Santos, pesquisadora visitante no Berlin Social Science Center – WZB
- Carla Azevedo de Aragao
- Carla Vieira – Engenheira de Software e pesquisadora
- Carolina Batista Israel – Pós-doutoranda pela Universidade de São Paulo
- Carolina Soares – Desenvolvedora de projetos Dados Livres
- Clara Ferraz
- Clara Marinho
- Claudiana Lelis
- Cynthia Picolo
- Davey
- Davi Neuskens
- Débora Pio
- Diego Cerqueira
-

Diogo Dal Magro

- Eduarda Costa
- Eduardo Gomes Mendonça
- Eliel Pinheiro
- Ênio Lourenço Leite da Silva
- Érico França Bonfim
- Fabianne batista Balvedi
- Gabriela MachadoVergili
- Geisa S. Silva – pesquisadora e raquerartivista
- Gu da Cei – Artista visual e produtor cultural
- Gustavo Furtado
- Gustavo Luz
- Helena Martins
- Hélio Aparecido
- Ines Aisengart Menezes
- Ingrid Lima dos Santos
- Isabela Maria Rosal Santos
- Isabelle Cristine Oliveira Ribeiro
-

Izabela Domingues da Silva

- Izabella Bittencourt
- Jamila Venturini
- Janaina Spode
- Jess Reia – University of Virginia
- Jessica Carmo
- João Guilherme Bastos dos Santos
- José Antonio
- José Germano Neto
- José Rolfran de Souza Tavares
- José Vitor Pereira Neto
- Julia D'Agostini
- Kaio Duarte Costa – Hackerativista
- Karina Moreira Menezes
- Katemari Rosa
- Katiana Ventura da Silva
- Kelly
- Kennedy Antônio Vasconcelos Ferreira Júnior
-

Laura Gabrieli Pereira da Silva

- Lauren – Coletivo Minha Nossa de luta contra as diversas violências que atingem as mulheres
- Leandro Araujo
- Leonardo Perseu
- Leticia Venturoti do Nascimento
- Lia Pereira de Araújo e Silva
- Luã Cruz
- Luciana Moherdaui
- Luiz Augusto Galicioli
- Marcella de Melo Silva
- Marcelo A Xaud
- Marcelo Fornazin
- Marcos Urupá
- Maria Aparecida da Vitória Neves
- Maria Luiza Duarte Sá
- Maria Luiza Freire Merces
- Mariana Canto Sobral
- Mariana Monteiro
-

Marina Meira

- Matheus Freitas
- Maurício Magalhães
- Mauro Beal
- Mônica Mourão
- Natalia Conceição Viana
- Natane Santos
- Nina Da Hora – Cientista da Computação
- Olga Lopes
- Otávio Santos Gomes
- Patricia Guernelli Palazzo Tsai
- Paula Cardoso
- Paulo Faltay
- Paulo Rená da Silva Santarém
- Pedro Amaral
- Pedro Diogo Carvalho Monteiro
- Pedro Henrique Martins dos Santos
- Pedro Martins
-

Pedro Paulo da Silva Neri

- R, Ramires – Educador popular em tecnologia na InfoCria, Instituto Bola Pra Frente e Redes da Maré
- Rafael Alves dos Santos
- Rafaela Batista
- Ramênia Vieira
- Raphael Rosa
- Raquel Lima Saraiva
- Raquel Rachid
- Renata Arruda
- Rhaiana Caminha Valois
- Ricardo Yuji Mise
- Roberta Sernagiotto Soares
- Rodrigo Murtinho – pesquisador em saúde pública
- Rodrigo P. R. Lopes
- Rogério Marques
- Rosa Maria Tubaki
- Rosana Pinheiro Nascimento
- Sheley Gomes

- Taís Oliveira – Instituto Sumaúma
- Tarcizio Silva – Tech + Society Fellow Mozilla
- Thaís Cruz
- Thallita Gabriele Lopes Lima
- Thayane Guimarães Tavares
- Trajano Pontes Neto
- Vanessa Gomes – desenvolvedora back-end e pesquisadora em segurança digital
- Veridiana Alimonti
- Vico Meirelles de Souza
- Waldo Almeida Ramalho
- Weverton dos Santos Ferreira
- Wilson Borges
- Yure Sousa Lobo