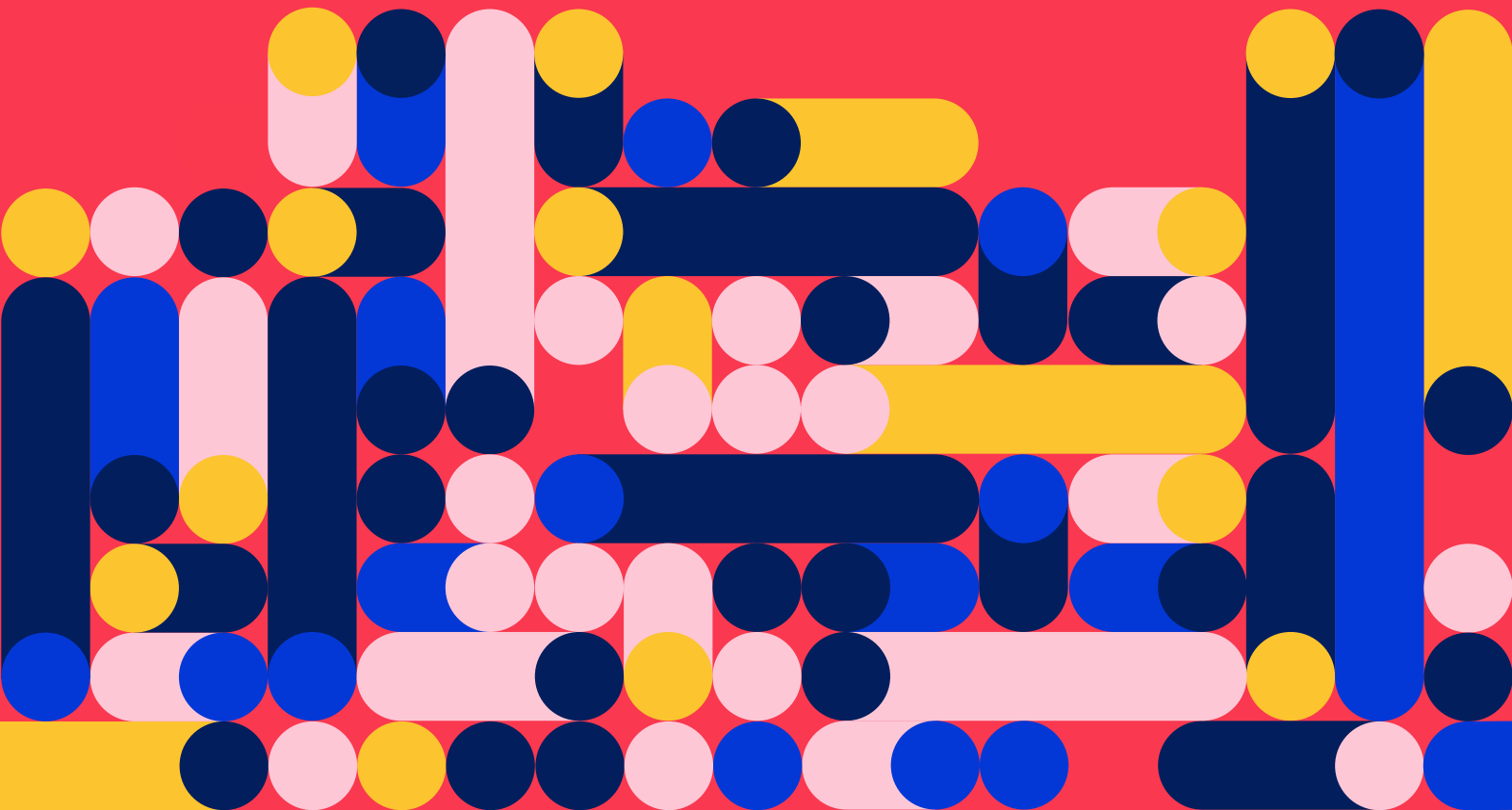
Reconhecimento facial na América Latina

Tendências na implementação de uma tecnologia perversa

AlSur



Reconhecimento facial na América Latina: tendências na implementação de uma tecnologia perversa

Texto: Jamila Venturini y Vladimir Garay (Derechos Digitales)
Revisão: María Paz Canales (Derechos Digitales), Juan Diego Castañeda (Fundación Karisma) e Cristin León (Al Sur).
Tradução para o português: Dafne Melo.
Tradução para o inglês: Pedro Nogueira.
Diagramação: Rocío Rubio.
Gráficos: Data Sketch.

Coleta de dados: Abdías Zambrano (Ipandetec), Alejo Kiguel (ADC), Bárbara Simão (Internet Lab), Dilmar Villena (Hiperderecho), Joana Varon y Vanessa Koetz (Coding Rights), Juliana Valdés, Juan Diego Castañeda y Joan López (Fundación Karisma), Luã Cruz (IDEC), Maricarmen Sequera (TEDIC), Michele Bordachar (Derechos Digitales), Santiago Narváez (R3D).

Com apoio do

NED NATIONAL ENDOWMENT FOR DEMOCRACY
SUPPORTING FREEDOM AROUND THE WORLD

A modo de introdução

O reconhecimento facial é uma tecnologia de identificação biométrica que, por meio da análise de alguns traços característicos do rosto, busca estabelecer a identidade de uma pessoa. Apesar de ser menos precisa que outras formas de identificação biométrica, como impressão digital ou leitura da íris, não requer contato físico. Isso permite sua implementação, por exemplo, em espaços públicos para fins de vigilância em larga escala e sem que aqueles que estão sendo submetidos ao seu escrutínio necessariamente tenham conhecimento disso.

Embora sua introdução remonte à década de 1960, vários avanços técnicos recentes foram fundamentais para sua aplicação nos últimos anos. O desenvolvimento de novas tecnologias de captura e processamento de imagens, avanços no campo de "big data" – associados à coleta, armazenamento e processamento de grandes volumes de dados – bem como avanços em técnicas de "aprendizagem profunda" (Deep Learning) no "treinamento" de algoritmos, têm facilitado a adoção cada vez maior de sistemas de reconhecimento facial em diferentes âmbitos. Hoje, o reconhecimento facial tem aplicações variadas que vão desde o desbloqueio de dispositivos móveis até tentativas de "ler" intenções e emoções, um uso que está relacionado a técnicas e teorias frenológicas desenvolvidas no século XIX.

Embora os sistemas de reconhecimento facial possam ser diversos, todos requerem pelo menos três elementos para funcionar: uma forma de capturar as imagens, um software encarregado de analisar as imagens e um banco de dados com rostos para fazer a comparação. A precisão do sistema vai depender do acesso a um banco de dados que permita a identificação das imagens com sujeitos previamente catalogados, depende também de que as imagens atendam a determinados padrões mínimos de qualidade exigidos pelo software para sua análise (tamanho, brilho, que a imagem capture os pontos de análise utilizado pelo sistema, etc.), da forma como os algoritmos foram "treinados" para fazer as associações entre os dados capturados e os do banco de dados que permite a comparação, bem como o próprio design do software, que indicará os parâmetros precisos de acordo com os quais as comparações serão feitas para produzir a identificação. Problemas em qualquer um desses níveis podem impedir que o sistema execute corretamente a função para a qual foi implementado, o que pode levar a reconhecimentos falhos, discriminações arbitrárias e falsos positivos, todas situações – infelizmente – comuns associadas ao uso de sistemas de reconhecimento facial, especialmente quando é usado para monitorar o espaço público e resguardar o acesso a direitos sociais.

Esse problema aumenta dramaticamente quando as pessoas sujeitas a essa tecnologia pertencem a grupos historicamente vulneráveis, como mulheres, pessoas não brancas ou pessoas trans. Assim, a implantação de sistemas de reconhecimento facial acarreta a reprodução técnica do viés de exclusão social e, quando utilizada para fins de vigilância, ameaça o direito à dignidade, ao devido processo e à presunção de inocência, entre outros.

Por se tratar de uma tecnologia de identificação biométrica, ou seja, que processa informações relacionadas ao nosso corpo, o reconhecimento facial é uma técnica altamente intrusiva que força a coleta e armazenamento de dados extremamente íntimos, retirando o controle sobre nosso rosto e dando aval a seu uso, potencialmente contra nosso próprios interesses e benefícios.

Quando utilizado para vigilar o espaço público e combater o crime comum, o reconhecimento facial corrói a autonomia das pessoas em prol de um sistema que busca o controle absoluto, por meio da gestão técnica das identidades, reproduzindo as desigualdades e exclusões que historicamente têm prejudicado as comunidades não hegemônicas.

O objetivo desta pesquisa é estimular o debate público sobre a forma como os sistemas de reconhecimento facial têm avançado na América Latina, a partir da iniciativa do Estado. Tais desenvolvimentos têm sido marcados por uma opacidade excessiva e por escassos compromissos por parte das autoridades que garantam condições mínimas na sua implantação, para mitigar os impactos no exercício dos direitos fundamentais.

Quais são as tecnologias de reconhecimento facial presentes na região? Para que são usadas? Quem as fornece? Como estão regulamentadas? Como são auditadas? Estas são algumas das questões que esta pesquisa tenta responder.

O relatório se inicia com uma explicação da metodologia utilizada na coleta de informações sobre as iniciativas, seguida de um panorama das tendências observadas na região e uma análise mais detalhada das empresas que fornecem tecnologias de reconhecimento facial. Concluímos com algumas considerações sobre os impactos das iniciativas identificadas e observadas.

Mapeando o reconhecimento facial na América Latina

Este relatório apresenta uma análise qualitativa a partir dos resultados do levantamento de informações sobre a implantação de sistemas de reconhecimento facial em nove países da América Latina, realizado entre abril e maio de 2021. A pesquisa foi desenvolvida pelas organizações que integram o Consorcio Al Sur, baseado em uma metodologia proposta pelas seguintes organizações: Coding Rights, Ipandetec, InternetLab, R3D, Derechos Digitales, Tedic e Fundación Karisma.

O objetivo da pesquisa foi mapear detalhadamente as iniciativas existentes na região, com especial ênfase na identificação das empresas que fornecem tecnologias biométricas dominantes e seus países de origem, o tipo de relação que se estabelece com os Estados, as áreas em que sua presença predomina, e suas potenciais consequências sociais, econômicas e políticas. Por esse motivo, a análise se centra nas iniciativas desenvolvidas por iniciativa do Estado, embora se reconheça a existência de um conjunto de aplicações de sistemas de reconhecimento facial promovidos pelo setor privado com grande potencial para afetar direitos fundamentais. Além disso, essa pesquisa é considerada o primeiro passo em um esforço mais amplo para mapear tecnologias de identificação biométrica na América Latina.

Este relatório é complementado pelo site https://estudio.reconocimientofacial.info/, onde é possível encontrar mais detalhes sobre cada uma das iniciativas encontradas, os fornecedores de tecnologia e mais informações sobre as tendências regionais na implementação de sistemas de reconhecimento facial na região. Além disso, em reconocimientofacial.info é possível encontrar notícias e atualizações sobre ações de resistência à implementação desses sistemas, modelos de solicitação de acesso às informações, entre outras informações.

Metodologia

O exercício de identificação e caracterização dos sistemas de reconhecimento facial presentes na região e das entidades responsáveis por fornecer e implementar a referida tecnologia foi efetuado através da preparação de fichas padronizadas, que dão conta de informação rele-

vante, incluindo área de aplicação, situação atual de funcionamento da iniciativa, país de origem dos fornecedores e setor a que pertencem, características do contrato, existência de estudos de impacto e auditorias posteriores à implementação do sistema, entre outros. O objetivo era poder tipificar as informações, de forma que fossem comparáveis para facilitar a identificação de tendências regionais.

Foram considerados os sistemas de reconhecimento facial desenvolvidos no marco de políticas públicas, especialmente aqueles sistemas implementados para auxiliar a vigilância do espaço público e a autenticação de identidade, particularmente como medida de acesso a direitos e benefícios sociais. Não foram considerados sistemas implantados em espaços privados como lojas, shopping centers ou bancos privados; tampouco estão inclusos sistemas implementados em áreas como comércio eletrônico ou acesso a dispositivos ou aplicativos digitais quando não constituem uma condição para o acesso a um serviço público.

A informação coletada nas fichas considera os seguintes aspectos:

- País
- Nome da iniciativa
- Descrição do sistema
- Área de aplicação
- Tipo de uso
- Data de implementação
- Status atual da iniciativa
- Fornecedores de tecnologia envolvidos
    - Nome
    - País
    - Setor (governamental, privado, acadêmico, sociedade civil)
    - Sitio web
    - Tipo de contrato (direto, licitação, doação)
    - Detalhes de contratação
- Existe alguma base legal ou normativa que dê aval a implementação?
- Existe algum processo de participação pública antes da implementação?
- O processo de implementação considerou a realização de um estudo de impacto em privacidade e/ou direitos humanos?
- Está prevista alguma auditoria externa da implementação?
- Existem registros de incidentes de segurança, usos discriminatórios ou outros tipos de abusos relacionados com a iniciativa desde sua implementação?
- Organização que preencheu a ficha

A informação foi compilada a partir das seguintes fontes:

- Solicitações de acesso à informação.
- Entrevistas semiestruturadas com agentes chave: empresas, agentes públicos, etc.
- Busca por palavras-chave em mecanismos de busca: buscadores diversos na internet, meios de comunicação, portais de transparência, webs de governos, etc.
- Consulta a organizações de direitos humanos, movimentos sociais, jornalistas e ativistas em cada país.

O que, como e onde? Tendências regionais sobre a implementação de reconhecimento facial na América Latina?

No âmbito desta pesquisa, foram mapeadas 38 iniciativas de uso do reconhecimento facial, distribuídas por nove países latino-americanos e implementadas sob diferentes políticas públicas. Embora essa não seja uma lista exaustiva da totalidade dos sistemas existentes na região, os números servem para dar uma ideia geral do panorama latino-americano quanto ao avanço dessa tecnologia e seu desenvolvimento.

A maioria dos sistemas de reconhecimento facial documentados na pesquisa datam dos últimos três anos, com apenas sete deles implementados antes de 2018. Dos 38 sistemas listados, 22 estão ativos atualmente, cinco foram desativados, três estão em fase piloto e oito estão em processo de implantação. Em relação aos cinco sistemas desativados, em dois casos foi uma ordem judicial que impediu a continuidade de seu funcionamento e uso, ambos no Brasil ("ViaQuatro"[1] e "Edital de Licitação do Metrô de São Paulo").[2] Em outros dois casos, os sistemas nunca foram implantados (o "Sistema Integrado de Vigilância Inteligente para Transmilênio na Colômbia"[3] e "Fórmula Antievasão do Metrô Transantiago e Valparaíso" no Chile) e um foi desativado por falhas, interrupções e falta de medidas de segurança ("Aplicativo móvel de reconhecimento facial para entregar a Senha Única" no Chile).[4]

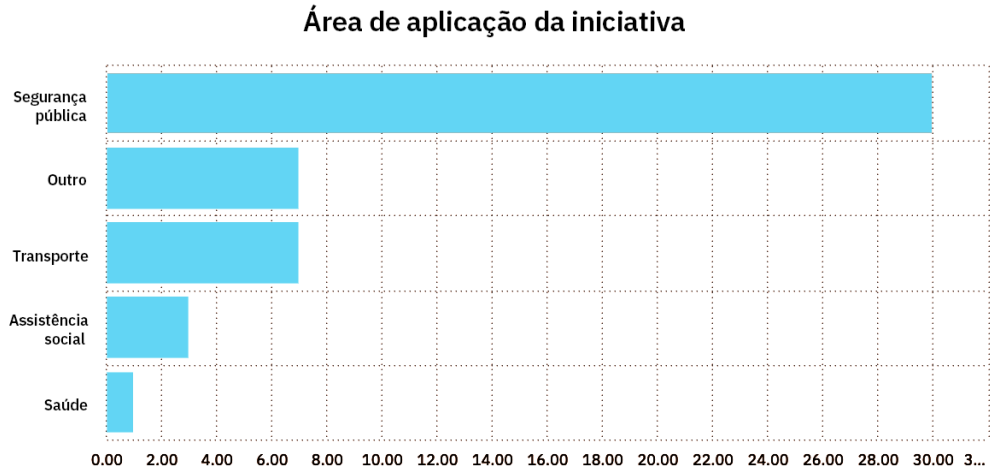
Com relação às áreas de aplicação dos sistemas, de longe o uso mais recorrente é "segurança pública" (30 sistemas listados) e "vigilância de espaços públicos" (31 sistemas listados). Seguem transporte (7 sistemas listados), assistência social e migração (3 sistemas cada). No âmbito desta investigação, não foi possível documentar os sistemas de reconhecimento facial implementados no campo da educação ou nos processos eleitorais, apesar de se tratarem de áreas em que, sobretudo no contexto de uma pandemia – as suas implementações cresceram. Por sua vez, assinalamos que 10 iniciativas são utilizadas para controlar o acesso aos direitos econômicos, sociais e culturais, tais como benefícios sociais concedidos pelo Estado, enquanto a utilização de seis delas está relacionada ao controle de acesso aos direitos civis e políticos, como acesso à identificação por parte dos cidadãos.

1 Ver https://reconocimientofacial.info/reconhecimento-facial-a-banalizacao-de-uma-tecnologia-controversa/

2 Ver https://reconocimientofacial.info/justicia-brasilena-condena-empresa-de-metro-por-uso-de-reconocimiento-facial-sin-consentimiento-en-sao-paulo/

3 Ver https://digitalid.karisma.org.co/2021/07/01/SIVIT-reconocimiento-facial/

4 Ver https://www.biobiochile.cl/noticias/nacional/chile/2020/03/29/registro-civil-anuncio-que-bajo-la-app-para-obtener-clave-unica-hubo-denuncia-sobre-su-seguridad.shtml



Com relação às bases normativas que regulam a implementação da tecnologia de reconhecimento facial, é importante mencionar que em mais de 60% dos casos não existe uma base jurídica específica que suporte a implementação. Apenas 14 dos 38 casos documentados indicam a existência de uma regulamentação que apoiaria a implantação desse tipo de tecnologia. No entanto, é surpreendente que na maioria dos casos os padrões citados não sejam especificamente para o uso de reconhecimento facial ou dados biométricos, mas sim uma ampla interpretação dos regulamentos referentes ao uso de outros tipos de tecnologias (por exemplo, a operação de vídeo câmeras de vigilância) que desejam análogo o reconhecimento facial com argumentos duvidosos ou poderes específicos que poderiam ser cumpridos por meio do uso de reconhecimento facial ("supervisionar o cumprimento das disposições sobre evasão em transporte público", "funções de verificação migratória, de estrangeiros e controle migratório", etc.)

Poucos são os casos em que é indicada uma regulamentação específica referente ao reconhecimento facial ou outras tecnologias de identificação biométrica. Exemplo disso seria a Portaria nº 1.515, de 18 de dezembro de 2018 do Departamento Nacional de Trânsito – Denatran do Brasil, que possibilitaria a implantação da coleta e armazenamento de dados biométricos para a concessão da carteira nacional de habilitação,[5] a normativa que regula o Sistema Público Integral de Videovigilância instituído pela lei da Cidade de Buenos Aires n. 5688, na Argentina,[6] e o projeto de lei 234 na Colômbia,[7] que estabelece que o Registro Nacional de Estado Civil pode identificar e autenticar nacionais em meios digitais na Colômbia por meio de "todos tipos de biometria" e que está por ser revisto pelo Tribunal Constitucional. Mesmo ao nível da proteção de dados pessoais, nos países em que existem regras gerais, as referências à regulamentação específica da utilização de dados biométricos são escassas. Na opinião dos diversos especialistas locais, nenhuma das normativas utilizadas para justificar a implementação de sistemas de reconhecimento facial oferece um tratamento adequado do ponto de vista dos direitos humanos.

Esse contexto regulatório deficiente agrava os riscos que esse tipo de tecnologia apresenta para o exercício dos direitos fundamentais. Também é necessário mencionar que a maioria das tentativas de regulamentar as tecnologias de identificação biométrica parecem estar mais preocupadas em validar sua implementação do que em equilibrar seus objetivos com relação aos direitos dos cidadãos. Nesse sentido, embora seja verdade que um regulamento específico pode ser benéfico quando procura corrigir deficiências nos regulamentos gerais de proteção de

5 Ver https://www.legisweb.com.br/legislacao/?id=372479

6 Ver http://www2.cedom.gob.ar/es/legislacion/normas/leyes/ley5688.html

7 Ver http://leyes.senado.gov.co/proyectos/index.php/textos-radicados-senado/p-ley-2020-2021/2021-proyecto-de-ley-234-de-2020

dados pessoais, isso só será possível quando a sua formulação considerar uma abordagem para prevenir riscos de impacto sobre o exercício de direitos fundamentais, nomeadamente privacidade e não discriminação.

Na grande maioria dos casos, os sistemas de reconhecimento facial identificados no marco deste estudo foram implementados sem qualquer tipo de consulta ou participação pública, com exceção de um sistema de vigilância no Chile, iniciativa cuja discussão contou com a presença dos conselheiros regionais, representantes eleitos popularmente que fazem parte da estrutura de governo regional descentralizada do país. Na discussão da lei que rege o Sistema de Reconhecimento Facial de Foragidos, em Buenos Aires, diferentes organizações tiveram a oportunidade de apresentar cartas expressando suas preocupações,[8] mas não houve discussão na Comissão de Direitos Humanos do Legislativo da Cidade de Buenos Aires como originalmente planejado, o que gerou uma grande reclamação da sociedade civil.[9] Nas iniciativas restantes, não houve qualquer tipo de consulta aberta ou qualquer instância de participação pública no que se refere à concepção e implementação de sistemas de reconhecimento facial.

Também não houve estudos de impacto sobre privacidade ou direitos humanos, os primeiros entendidos como avaliações que contemplam os riscos da utilização de dados pessoais por um sistema de autodeterminação informacional e a privacidade de seus titulares, enquanto os últimos podem ser definidos como um processo para identificar, compreender, avaliar e abordar os efeitos adversos de uma atividade ou política pública no usufruto dos direitos humanos dos titulares de direitos afetados.

A única exceção é o Sistema de Reconhecimento Facial de Fugitivos de Buenos Aires, que – em resposta a um pedido de acesso à informação pública feito pela Associação dos Direitos Civis – declara ter realizado "exames correspondentes para reduzir ao máximo admissível taxa de erro, juntamente com outras restrições impostas em torno da conformação do cadastro de dados e das medidas de controle do pessoal com acesso ao sistema", e desta forma minimizar os "impactos negativos em termos de direitos humanos".

Em geral, o desenvolvimento de auditorias externas ao funcionamento dos sistemas implementados também não é uma prática comum. Auditorias externas do funcionamento de sistemas técnicos que impactam o exercício de direitos são uma boa prática que permite obter informações de forma independente sobre o funcionamento do sistema e os riscos potenciais que sua concepção ou implementação podem representar para o exercício de direitos de usuários ou pessoas impactadas por uma tecnologia específica. A sua ausência impede processos de melhoria iterativos nos quais a visão dos operadores do sistema é complementada por visões externas que contribuem para a sua melhoria e evitam os impactos negativos da implementação de um sistema.

Apenas três das 38 iniciativas mapeadas respondem pela realização de algum tipo de auditoria, duas na Colômbia e uma na Argentina. Em relação aos sistemas colombianos, há um anúncio do Prefeito de Bogotá sobre a eventual realização de auditorias externas à Ágata, a Agência de Análise de Dados;[10] no caso do Sistema Integrado de Vídeo Vigilância Inteligente para Trans

8 Ver https://adc.org.ar/2020/09/18/avanza-la-regulacion-del-reconocimiento-facial-en-la-legislatura-portena

9 Ver https://www.telam.com.ar/notas/202010/527676-la-legislatura-aprobo-el-uso-de-reconocimiento-facial-para-la-detencion-de-profugos.html

10 Ver http://www.sdp.gov.co/noticias/agata-la-nueva-agencia-analitica-de-datos-hara-de-bogota-lider-global-transparencia-e-inteligencia

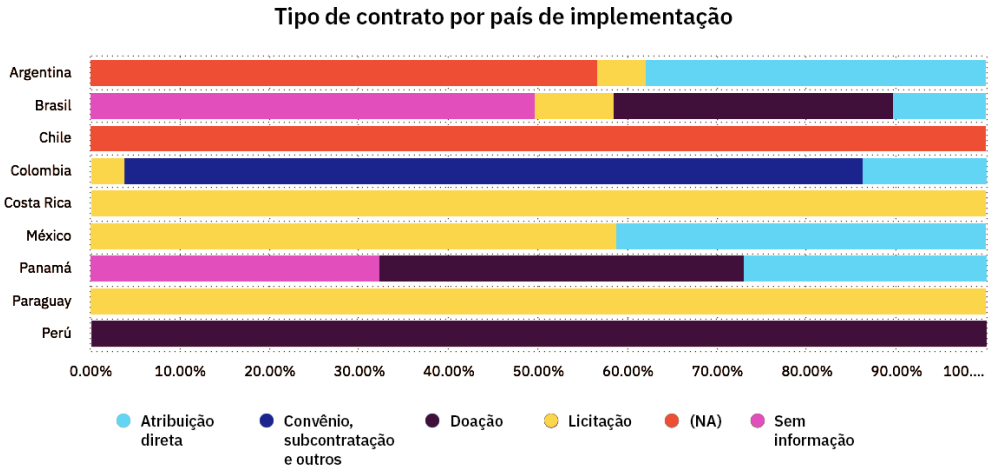
milênio – atualmente desativado – houve uma auditoria pela Universidade Francisco José de Caldas-IDEXUD para a instalação e operação do equipamento biométrico.[11]

Em relação ao caso argentino, a lei que regulamenta o funcionamento do Sistema de Reconhecimento Facial de Foragidos em Buenos Aires prevê a criação de uma Comissão Especial de Acompanhamento de Sistemas de Videovigilância, composta pelos Presidentes das Comissões de Justiça e Segurança, três deputados indicados pela Vice-Presidência Primeira do órgão, abrindo também a possibilidade de convocar especialistas e organizações da sociedade civil para análise e proposição.[12]

Provedores

Diversas empresas estão envolvidas na prestação de serviços para a implementação de iniciativas que utilizam tecnologia de reconhecimento facial em nossa região. Elas cumprem diferentes funções que vão desde a implantação da infraestrutura necessária para a operação desses sistemas até o fornecimento de tecnologia de análise biométrica. Embora a participação de empresas locais seja relevante, deve-se destacar que, em geral, elas não são responsáveis pelo desenvolvimento do software. Em alguns casos, eles se especializam na venda de sistemas desenvolvidos no exterior.

É importante destacar a presença de empresas questionadas internacionalmente por seu suposto envolvimento em violações de direitos humanos. O caso das empresas chinesas Dahua e Hikvision é particularmente ilustrativo, proibidas de operar nos Estados Unidos, embora tenham contratos milionários no México. A francesa IDEMIA (ex-Morpho Safran), presente em pelo menos quatro países da região, e a inglesa FaceWatch, cujo software é utilizado em uma das iniciativas identificadas no Brasil, também têm sido alvo de preocupações de organismos internacionais.



As empresas locais, por sua vez, costumam ser grandes prestadoras de serviços ao Estado e, em vários casos, têm alguma relação com figuras políticas ou escândalos de corrupção.

11 Ver https://www.yumpu.com/es/document/read/55729155/informe20de20gestic3b3n202015

12 Ver http://www2.cedom.gov.ar/es/legislacion/normas/leyes/ley6339.html

Argentina

Na Argentina, foram identificadas quatro iniciativas para o uso de sistemas ativos de reconhecimento facial. Todos contam com a participação de empresas argentinas ou multinacionais estrangeiras, em alguns casos por meio de seus representantes locais

- DANAIDE SA, contratada por 1.511.300 dólares para oferecer o serviço completo de análise de vídeo no Sistema de Reconhecimento Facial de Foragidos (SRFP, na sigla em espanhol) implantado na Cidade Autônoma de Buenos Aires, ativo desde 2019;
- NEC Argentina SA – parte do grupo global NEC CORPORATION de origem japonesa –, contratada por 44.906.400 pesos argentinos (aproximadamente 462.702 dólares)[13] em licitação para oferta de hardware, software e serviços de manutenção no Sistema de Reconhecimento Facial da Tigre NeoCenter, na cidade de Tigre, província de Buenos Aires, também ativa desde 2019;
- Nubicom, contratada para a implementação do sistema de Reconhecimento Facial de Salta, na cidade de Salta, capital da província, e ativa desde 2018;
- Morpho Safran (atualmente IDEMIA), francesa, e DATYS, cubana, contratadas para fornecer a tecnologia do Sistema Federal SIBIOS de Identificação Biométrica para Segurança, ativa desde 2011.

Além das empresas identificadas, o software de reconhecimento facial utilizado no SRFP e denominado UltraIP seria desenvolvido pela empresa russa NtechLab. De acordo com fontes jornalísticas, o sistema seria usado em mais de 3 mil câmeras de vigilância por vídeo na Rússia.[14]

A modalidade de contratação das empresas, nos casos em que os dados estavam disponíveis, era a contratação direta na Cidade de Buenos Aires e Salta. Segundo a imprensa local, a contratação da DANAIDE SA havia sido denunciada pela atual vice-presidente argentina Cristina Fernández de Kirchner por espionagem em 2018.[15]

No caso de Salta, a empresa inicialmente contratada para oferecer os dispositivos de videovigilância e software ao sistema de Reconhecimento Facial Salta foi a DATANDHOME FORNECEDOR SA. A Nubicom era a provedora do serviço de conectividade. No entanto, o contrato com a primeira foi rescindido em 2019 devido a "violações graves" na instalação das câmeras comprometidas. Por isso, foi firmado contrato direto com a Nubicom, que também se responsabilizou pela conectividade e manutenção das câmeras e softwares.

De acordo com reportagens da imprensa, a contratação da Nubicom foi marcada por uma série de vícios, incluindo um procedimento abreviado por motivos emergenciais que não foram explicitados. O custo mensal cobrado pela empresa pela prestação dos serviços chegaria a 440 mil dólares, segundo a mesma fonte. Por sua vez, a DATANDHOME moveu uma ação de 6 milhões de dólares contra a província de Salta por incumprimento de pagamentos.[16]

---

13 A conversão dos valores em moeda local a dólares estadunidenses implica uma estimação para fins de referência. Foi feita a partir da consulta em https://www.xe.com em agosto de 2021 e não corresponde ao montante equivalente no momento da contratação.

14 Ver https://onezero.medium.com/the-u-s-fears-live-facial-recognition-in-buenos-aires-its-a-fact-of-life-52019eff454d e https://www.hrw.org/es/news/2020/10/09/argentina-publica-en-linea-datos-personales-de-ninos-y-ninas-acusados-de-cometer

15 Ver https://realpolitik.com.ar/nota/37024/larreta-le-dio-el-control-del-reconocimiento-facial-a-una-empresa-denunciada-por-espiar-a-cfk/

16 Ver https://www.eltribuno.com/salta/nota/2021-5-9-1-45-0-el-sistema-de-camaras-cuesta-mas-de-440-mil-dolares-por-mes

No caso do município de Tigre, a empresa NEC Argentina SA foi vencedora de um concurso público para fornecer uma "Plataforma de Segurança Integral" em 2018 e novamente em 2019, desta vez sob o conceito de "Aquisição de totens inteligentes de segurança". Em 2020, a empresa foi vencedora de um novo concurso público para "serviço de manutenção de sessenta (60) unidades de Totens de Segurança Inteligente (TSI)". Na Argentina, o grupo japonês NEC Corporation foi estabelecido desde 1978 e desde então obteve vários contratos com o Estado. Morpho Safran, agora denominado IDEMIA, e DATYS são os fornecedores do Sistema Federal de Identificação Biométrica para Segurança, SIBIOS. A primeira é uma multinacional francesa que se dedica ao desenvolvimento de tecnologias, voltada principalmente para a venda de produtos de reconhecimento facial. A empresa foi criticada pela Anistia Internacional por exportar tecnologias de vigilância digital para a China, devido ao risco para os direitos humanos envolvido.[17] A IDEMIA foi responsabilizada pelos problemas com as eleições gerais no Quênia em 2017, que resultaram no cancelamento dos contratos atuais pela Assembleia Nacional e na proibição de que novos fossem assinados. A decisão foi revogada pela Suprema Corte do país.[18]

A DATYS, por sua vez, é uma empresa cubana fundada em 2005. Segundo informações obtidas pela Associação pelos Direitos Civis (ADC), a ferramenta contratada pelo DATYS permite a identificação automática de pessoas por meio da comparação de impressões digitais e, como método secundário, de rostos.[19]

Brasil

No Brasil foram identificadas seis iniciativas de uso de sistemas de reconhecimento facial com os seguintes provedores de tecnologias envolvidos:

- Admobilize, dos Estados Unidos, contratada para o desenvolvimento de tecnologias em um sistema de reconhecimento facial e emocional instalado nas estações de metrô do consórcio ViaQuatro, na cidade de São Paulo, ativo entre março e setembro de 2018.
- Equipe da Security Technologies do Brasil Software Ltda, empresa brasileira que importou o software Facewatch da Inglaterra para implementar um sistema de identificação facial na edição 2019 do tradicional festival de São João, que acontece anualmente na cidade de Campina Grande, Paraíba.
- Brisanet Telecomunicações, empresa brasileira que ofereceu infraestrutura para o sistema implantado na festa de São João em Campina Grande em 2019.
- Tecway, empresa brasileira vencedora de processo de licitação para desenvolver tecnologias biométricas para o Centro Integrado de Câmaras de Monitoramento de Itacoatiara, província do Amazonas, atualmente em fase de implantação.
- Engie Brasil Soluções Integradas Ltda., empresa brasileira integrante do consórcio Engie Ineo Johnson, que recebeu a atribuição para a implantação de um sistema de reconhecimento facial no metrô de São Paulo em 2019.
- Ineo Infracom, empresa francesa integrante do consórcio Engie Ineo Johnson, que recebeu a atribuição para a implantação de um sistema de reconhecimento facial no metrô de São Paulo em 2019.

---

17 Anistia Internacional, "Out of control: failling EU laws for digital surveillance export" (2020). Ver https://www.amnesty.org/en/documents/eur01/2556/2020/en/

18 Ver https://www.biometricupdate.com/202101/criticism-sparked-by-delay-of-biometric-election-systems-unveiling-in-uganda-procurement-in-kenya

19 Asociación por los Derechos Civiles, "La identidad que no podemos cambiar: cómo la biometría afecta nuestros derechos humanos" (2017), ver https://adc.org.ar/wp-content/uploads/2019/06/027-A-la-identidad-que-no-podemos-cambiar-04-2017.pdf. E "Tu yo digital – Descubriendo las narrativas sobre identidad y biometría en América Latina: los casos de Argentina, Brasil, Colombia y México" (2019), ver https://adc.org.ar/wp-content/uploads/2020/06/050-tu-yo-digital-04-2019.pdf

- Johnson Controls BE do Brasil Ltda, empresa americana integrante do consórcio Engie Ineo Jonhson, que recebeu a atribuição para implantação de um sistema de reconhecimento facial no metrô de São Paulo em 2019.

No caso de Campina Grande, as tecnologias foram obtidas por meio de uma doação dos fornecedores à empresa Medow Entertainment, responsável pela organização do festival São João em 2019. A empresa Staff da Security Technologies do Brasil Software Ltda, responsável pela importação do software Facewatch tem ligações com uma figura política envolvida em vários escândalos de corrupção em todo o país.[20]

Segundo informações da Privacy International, a empresa Facewatch teria distribuidores locais tanto no Brasil quanto na Argentina. No Reino Unido, seus sistemas têm sido adotados por diferentes tipos de comércios com o objetivo de identificar pessoas consideradas indesejáveis nesse tipo de comércio (por comportamento antissocial, tentativa de roubo etc.) e sua inclusão em uma lista. Ao passar por uma câmera para entrar no negócio ou evento, o sistema identifica se a pessoa está ou não na lista e, caso esteja, envia um alerta. O sistema gerou polêmica no país em relação à legalidade de seu uso e às implicações para a privacidade, segundo a BBC.[21]

De acordo com a Privacy International, em 2019 o sistema Facewatch era usado em pelo menos três centros comerciais no Brasil. Sobre a investigação de uma possível colaboração entre a empresa e a polícia de Londres para troca de dados, a entidade alerta para a anunciada intenção do governador do Rio de Janeiro de permitir que a polícia local troque sua própria lista de suspeitos de ter cometido crimes com empresas de reconhecimento facial.[22]

Por sua vez, a empresa brasileira Tecway, contratada para desenvolver o Centro Integrado de Câmaras de Monitoramento de Itacoatiara, tem entre seus antecedentes uma investigação do Ministério Público da província do Amazonas devido a possível irregularidade em concurso público e uma indicação por parte de comissão instalada no Senado brasileiro de apuração de irregularidades durante a gestão da pandemia de Covid-19.[23] Um dos sócios da empresa é parente de deputado nacional e tentou disputar um cargo local em Manaus, capital do Amazonas.[24]

Duas iniciativas contam com serviços do provedor público de tecnologia: o Serviço Federal de Processamento de Dados (SERPRO), que oferece a base e armazenamento de dados biométricos e está envolvido na implementação da validação da carteira nacional de habilitação por meio de dados biométricos e dos "testes de vida", uma exigência anual obrigatória para que não haja interrupção do pagamento das pensões pelo sistema previdenciário brasileiro. Nesse caso, o objetivo é substituir o processo presencial por um aplicativo, no qual o beneficiário envia uma "selfie" que é comparada com a foto cadastrada nos bancos de dados do sistema.

O Serpro é uma empresa pública vinculada ao Ministério da Fazenda e tem por objeto a execução de serviços de informação e processamento de dados, incluindo teleprocessamento e comunicação de dados, voz e imagem, atividades necessárias, de forma limitada e especializada. O

---

20 Ver https://agenciasportlight.com.br/index.php/2019/06/11/o-governador-witzel-e-as-caras-ocultas-no-milionario-negocio-de-reconhecimento-facial/.

21 Ver https://www.bbc.com/news/technology-55259179

22 Ver https://privacyinternational.org/long-read/4216/facewatch-reality-behind-marketing-discourse

23 Ver https://amazonasatual.com.br/promotora-chama-de-esdruxula-forma-como-ssp-am-iniciou-negocio-de-r-427-milhoes-para-aluguel-de-viaturas-2/ e https://www.metropoles.com/colunas/igor-gadelha/cpi-pede-quebra-de-sigilo-de-empresa-de-parente-do-lider-do-mdb

24 Ver https://simenao.com.br/simenao/autor-de-post-que-viralizou-teve-candidatura-indeferida-pela-ficha-limpa

órgão máximo do Serpro é o Conselho de Administração, composto por seis membros indicados pelo Presidente da República e recomendados pelo Ministro da Fazenda.

Duas iniciativas recentes questionam na Justiça o uso indevido dos dados armazenados pelo Serpro. A primeira pede a suspensão da troca de dados com a Agência Brasileira de Inteligência (Abin).[25] A segunda questiona a legalidade da utilização da base de dados de carteiras de habilitação para a oferta de serviços de reconhecimento facial para os setores público e privado.[26]

Chile

No Chile, embora tenham sido identificadas dez iniciativas de uso de sistemas de reconhecimento facial no setor público, das quais seis estão ativas, não foi possível identificar os provedores envolvidos em sua implantação, em geral devido à lentidão de resposta dos órgãos públicos aos pedidos de acesso à informação apresentados para esta investigação.

Somente no caso do município de San Joaquín foi possível identificar as empresas Enel Distribución Chile SA e Sistema de Seguridad y Tecnología SpA como vencedoras de uma licitação pública, cujos resultados foram publicados em 2019, para a melhoria do sistema de televigilância do município.[27] O valor oferecido pelas obras contratadas foi de 789.888.183 pesos chilenos, o equivalente hoje a cerca de 1.023.965 dólares.

A Enel Distribución Chile SA foi contratada para a prestação de serviços de "controle de energia ou sistemas de vigilância". A empresa faz parte do Grupo Enel, multinacional de origem italiana, responsável pela distribuição de energia elétrica em várias localidades do país, mas entrou no negócio de câmeras de segurança em 2018.

Colombia

Na Colômbia, foram identificadas cinco iniciativas para o uso de sistemas de reconhecimento facial, nas quais estão envolvidos os seguintes provedores:

- A empresa colombiana de serviços públicos mistos EMTEL, contratada por meio de um acordo interadministrativo pela Prefeitura de Bogotá por 11.758.251.357 pesos colombianos (aproximadamente 3.100.000 dólares), assinado em 2015, para reunir os esforços necessários para o comissionamento do Sistema de Vigilância por Vídeo Inteligente Integrado para Transmilênio (SIVIT), desativado em 2021.
- Inversiones Tecnológicas de América, também colombiana, subcontratada pela EMTEL para o fornecimento de equipamentos que permitiriam o funcionamento do SIVIT: câmeras, iluminação, interruptores e telas, entre outros.
- Compañía Internacional de Integración S.A. e TecniDidácticos IND S.A.S (Unión Temporal Tecnocom), colombiana, contratada por 11.298.307.350,00 pesos colombianos (aproximadamente 2.865.268 dólares) para liderar a implantação do Sistema Multibiométrico ABIS da Polícia Nacional e do Ministério do Interior, ativo desde 2017.

25 Ver https://theintercept.com/2020/06/06/abin-carteira-motorista-serpro-vigilancia/ e https://www.jota.info/stf/do-supremo/psb-aciona-stf-contra-compartilhamento-de-dados-da-cnh-entre-serpro-e-abin-1606202

26 Ver https://computerworld.com.br/plataformas/ministerio-publico-acusa-serpro-de-oferecer-servico-ilegal/

27 Ver https://www.mercadopublico.cl/Procurement/Modules/RFB/DetailsAcquisition.aspx?qs=/qaUKJpnZ48L4WtkI40xyg==

- IDEMIA, empresa francesa, subcontratada pela primeira para o desenvolvimento do cadastro de impressões digitais do sistema e para a migração do sistema anteriormente utilizado pela polícia para o ABIS. O valor do contrato era de 1.000.000.000 pesos colombianos (aproximadamente 253.603 dólares). A mesma empresa está envolvida na implementação do "Cartão de Identidade Digital", nomeadamente o motor multibiométrico Morpho Biometric Search Service.[28]
- HERTA Security, espanhola, também subcontratada pela Tecnocom Temporary Union para migrar fotografias para o banco de dados digital e instalar seus aplicativos no sistema ABIS (Biodata, BioFinder e Biogenerator).
- Bogotá Telecommunications Company, empresa pública colombiana encarregada de desenvolver testes de implementação em câmeras de reconhecimento facial da Data Analytics Agency (Ágata) de Bogotá, ativa desde 2020.
- BYTTE SAS, da Colômbia, vencedora de licitação pública no valor de 13.994.000.000 pesos colombianos (3.549.058 dólares aproximadamente) para liderar a implantação do Sistema Integrado de Informação Multibiométrica atualmente em processo de implantação.

A impossibilidade de acionar as câmeras de reconhecimento biométrico fornecidas pelo SIVIT e contratadas pela EMTEL levou a autoridade judiciária de Bogotá a investigar dois gestores adjuntos do Fundo de Segurança e Vigilância daquela cidade.[29] Embora a investigação tenha sido encerrada em 2021,[30] foram instauradas ações contra os ex-subgerentes por negligência na contratação, pois não levaram em consideração as advertências de que tal sistema só poderia funcionar caso não existisse um banco de dados fotográfico.

Em 2019, o prefeito de Popayán e o ex-secretário de Trânsito Municipal foram investigados por possíveis atos de corrupção, como a prestação irregular de serviços de trânsito a uma empresa chamada Quipux através da Emtel.[31]

A Unión Temporal Tecnocom, por sua vez, enfrentou quatro processos em 2017 por supostas violações no desenvolvimento do contrato que foi firmado com a Polícia Nacional para o desenvolvimento do sistema ABIS. As decisões foram favoráveis à empresa. Tanto a TecniDidácticos quanto a Compañía Internacional de Integración S.A. celebraram vários contratos com o Estado colombiano. A francesa IDEMIA, por sua vez, é a empresa com a qual o Registro Civil Nacional mantém contratos há mais de 10 anos. A TecniDidácticos é investigada desde 2020 por supostas irregularidades em um contrato com a Prefeitura de Medellín para o fornecimento de máscaras N95 durante a pandemia de Covid-19.[32]

No caso de Ágata, existem vários investidores e facilitadores da iniciativa, entre os quais estão a Bogotá Sewer Aqueduct Company, o Bogotá Energy Group, a Unidade Administrativa Especial de Cadastro Distrital, a Secretaria de Planejamento Distrital, Transmilenio SA e a Bogotá Metro Company. No entanto, a Bogotá Telecommunications Company (ETB) tem uma participação majoritária de 51% na Agência. Além disso, conduziu seu processo de formação junto a entidades da

28 Ver https://www.idemia.com/mbss

29 Ver https://www.personeriabogota.gov.co/sala-de-prensa/notas-de-prensa/item/578-inhabilitado-exsubgerente-de-fondo-de-vigilancia-y-seguridad

30 Secretaría de Seguridad, Convivencia y Justicia, "Cierre de investigación disciplinaria del proceso 015-2019". 4 jan. 2021, Disponível em: https://scj.gov.co/sites/default/files/notificaciones_control_interno_disciplinario/ESTADO%20001%20Firmado%7D.pdf

31 Ver https://caracol.com.co/emisora/2019/01/29/popayan/1548787323_962726.html

32 Ver https://www.kienyke.com/crimen-y-corrupcion/denuncias-corrupcion-contratos-coronavirus-alcaldia-medellin

Prefeitura de Bogotá.[33] A empresa possui diversos contratos com diversas instituições públicas da cidade de Bogotá.

A ETB foi punida por violar o direito de livre escolha de seus usuários por não cumprirem a rescisão dos contratos nos prazos estabelecidos e se envolveu em algumas irregularidades relacionadas ao descumprimento na execução dos contratos.[34]

Por fim, a Bytte S.A.S tem contratos com entidades públicas e privadas para adaptação de software de controle de acesso e suporte a sistemas de identificação. Os clientes incluem Aeronáutica Civil e Universidade Pedagógica e Tecnológica da Colômbia, sede em Tunja. Em 2010 a empresa desenvolveu uma aliança com a Safran Morpho, hoje IDEMIA.[35]

Costa Rica

Três iniciativas que envolvem o uso de sistemas de reconhecimento facial foram identificadas na Costa Rica. A francesa IDEMIA - que tem fábrica na Costa Rica - foi contratada em conjunto com um consórcio por meio de licitação no valor de 3.674.203 dólares para o desenvolvimento do software utilizado no Sistema de Identificação Biométrica Automatizado (ABIS) que inclui diversos elementos de identificação biométrica, incluindo o reconhecimento facial.[36] O sistema foi implementado no final de 2020, com particular destaque para a emissão de cédulas e cartões de identidade para menores (12 a 18 anos).

Também é membro do consórcio IAFIS, empresa criada na Argentina para comercializar sistemas Morpho (atualmente IDEMIA) na América Latina.[37] Quem participa da ABIS e faz parte do consórcio é a Componentes El Orbe S.A, empresa costarriquenha com atuação em diversos países da América Central. Todos os envolvidos no contrato trabalharam em outros projetos com o Estado da Costa Rica. No caso da IAFIS, é responsável pelo Sistema Automatizado de Identificação de Impressões Digitais do Tribunal Supremo Eleitoral.

No caso do Sistema Migratório de Identificação Biométrica, em processo de implementação, em fevereiro de 2020 foi encerrado o prazo de recepção de propostas no âmbito do concurso público de contratação. O orçamento estimado é de 3.317.389.479,96 colóns (equivalente a cerca de 5.344.276,41 dólares). De acordo com o sistema de contratação pública, a atribuição ainda está em avaliação. No entanto, de acordo com a Direção-Geral de Migração e Estrangeiros, o projeto foi atribuído ao consórcio GSI-Dinamica-Veridos-Sertracen. Tanto o Grupo de Soluciones Informáticas SA (GSI) como a Sertracen são empresas com presença significativa na América Central.

O consórcio também se beneficiou da contratação para implantação do Passaporte Biométrico do Bicentenário, que prevê a integração do reconhecimento facial como mecanismo de autenticação até março de 2022. Nesse caso, o valor do contrato foi de 5.501.308.159 dólares. Fazem

---

33 Ver https://www.valoraanalitik.com/2020/12/14/bogot-lanza-gara-nueva-agencia-de-anal-tica-de-datos/ https://bogota.gov.co/mi-ciudad/administracion-distrital/que-es-la-agencia-analitica-de-datos-de-la-alcaldia-de-bogota e https://gestor.etb.net.co/mp4/ABECE.pdf

34 Ver https://www.eltiempo.com/bogota/sancion-superintendencia-de-industria-y-comercio-impone-millonaria-sancion-a-la-etb-522846

35 Ver https://repository.urosario.edu.co/bitstream/handle/10336/13091/PedrozoBoada-MullerJose-2017.pdf?sequence=1&isAllowed=y

36 O contrato pode ser encontrado em https://www.sicop.go.cr/moduloPcont/pcont/ctract/es/CE_COJ_COQ038_O.jsp?contract_no=CE201905000256&contract_mod_seq=00&typeExp=Y

37 Ver https://www.linkedin.com/company/iafisgroup/about/

parte do consórcio a Dinámica Consultores Internacional S.A, também da Costa Rica, e a Veridos da Alemanha.

México

No México, foram identificadas três iniciativas para implementar sistemas de reconhecimento facial para a vigilância de espaços públicos. Os fornecedores envolvidos são os seguintes:

- Dahua, empresa de origem chinesa, contratada por meio de atribuição direta no valor de 600 milhões de pesos mexicanos (aproximadamente 29.494.148 dólares) para a implantação e manutenção do Sistema de Vídeo-Inteligência do Estado de Coahuila. Atualmente em fase piloto, a iniciativa envolve a instalação de 300 câmeras de vigilância com capacidade de reconhecimento facial em 11 municípios do Estado.
- A empresa mexicana Teléfonos de México S.A.B. de C.V. foi vencedora de licitação pública nacional no valor total de 197.564.863,80 pesos mexicanos (cerca de 9.702.029 dólares) para a implementação do Centro de Comando e Controle C2 da Central de Abastecimentos da Cidade do México.
- Na mesma licitação, Hanwa, da Coréia do Sul, também foi contratada para o desenvolvimento de tecnologias biométricas; e a empresa de engenharia estadunidense Intelligent Security Systems, também dedicada ao desenvolvimento de tecnologias biométricas.
- Empresa SYM Servicios Integrales, S.A. de CV, do México, foi contratada pelo valor total de 728.010.176 pesos mexicanos (aproximadamente 36.118.859 dólares) para a implantação e manutenção do Centro de Comando, Controle, Comunicação, Informática e Coordenação "C5 SITEC" – ativo desde maio de 2021. A iniciativa inclui a instalação de 40 câmeras com capacidade de reconhecimento facial, instaladas em 20 pontos do município de Aguascalientes no estado de mesmo nome.

Em relação ao Sistema de Vídeo-Inteligência Coahuila, Dahua declarou à imprensa que os algoritmos fornecidos foram "tropicalizados" para identificar o "fenótipo mexicano", o que sugere que a empresa tinha alguma possibilidade de acessar dados de mexicanos para treinar seus sistemas de reconhecimento facial. A iniciativa foi apresentada ao público logo após uma visita do governador de Coahuila à China, na qual se reuniu com a empresa. Durante o lançamento do sistema, seu CEO, Zhijie Li, esteve presente.

A empresa, uma das mais importantes do mercado global de videovigilância, foi sancionada pelos Estados Unidos em 2019 por violações de direitos humanos devido à sua participação em campanhas de assédio contra uma minoria islâmica.[38] A empresa mantém contratos para projetos de vigilância em Xinjiang, onde o governo chinês é acusado de genocídio contra a população Uighur. Segundo informações publicadas pela imprensa americana no início de 2021, seu software de reconhecimento facial seria capaz de identificar pessoas dessa etnia.[39]

Hikvision, uma das que recebeu a atribuição no Projeto Comprehensive Urban Video Surveillance with Analytical Technology, sofreu sanções nos Estados Unidos em 2019 e na Noruega em 2020 por abusos de direitos humanos.[40] Suas tecnologias de vigilância também seriam usadas pelo governo chinês para reprimir pessoas de minorias muçulmanas.

---

38 Ver https://www.icij.org/investigations/china-cables/us-blacklists-chinese-companies-linked-to-uighur-abuses/

39 Ver https://www.latimes.com/business/technology/story/2021-02-09/dahua-facial-recognition-china-surveillance-uighur

40 Ver https://www.dw.com/en/us-blacklists-28-chinese-companies-over-xinjiang-rights-abuses/a-50732014

Já a mexicana Teléfonos de México se encarregou da grande maioria dos projetos relacionados à instalação de câmeras de vigilância na Cidade do México. Essa empresa é propriedade de Carlos Slim, que conquistou projetos milionários e teve importante participação em projetos de infraestrutura nas três últimas administrações da Cidade do México. Em um dos projetos com a participação da empresa, foram constatadas diversas irregularidades, como pagamentos indevidos, falta de comprovação de gastos, extravio de notas fiscais, entre outros.[41]

No caso de Aguascalientes, a forma de contratação por atribuição direta pode violar o disposto na Lei de Aquisições, Arrendamentos e Serviços do Estado de Aguascalientes. No contrato declaram que se baseia nos incisos I e VII do artigo 63 da referida Lei, que estabelecem que a atribuição direta pode ser feita se não houver substitutos ou bens equivalentes aos oferecidos pela empresa ou mesmo de outra natureza do procedimento de contratação pode comprometer informações confidenciais e/ou reservadas. No entanto, iniciativas equivalentes têm sido contratadas por meio de licitações públicas, o que embasa a versão de possível violação do disposto na referida lei.

A contratada, SYM Servicios Integrales, tem uma longa história de abastecimentos a governos na área de sistemas e equipamentos de segurança, incluindo sistemas de videovigilância para espaços públicos e sistemas de vigilância.[42] De acordo com e-mails vazados pelo Wikileaks, a empresa vendeu sistemas de vigilância fabricados pela empresa Hacking Team para governos locais no México (incluindo os de Tamaulipas, Campeche, Puebla e Jalisco). SYM Servicios Integrales S.A. de C.V. é uma das subsidiárias do Grupo Kabat, que também comercializa sistemas Hacking Team para governos de outros estados do México. Segundo o New York Times, esses sistemas foram usados pelo governo de Puebla para espionar adversários políticos no contexto eleitoral.[43]

Panamá

No Panamá, foram mapeadas três iniciativas de uso de reconhecimento facial, nas quais estão envolvidas duas empresas estrangeiras. Uma delas é a Huawei Technologies, contratada para desenvolver tecnologias biométricas para o Centro de Operaciones de Seguridad y Emergencias C2, iniciativa que está ativa desde 2018. O valor do contrato, 9,3 milhões de dólares, foi pago por meio de um empréstimo não reembolsável da China, o que significa que os serviços foram doados pelo governo chinês ao país. Deve-se observar que a Huawei Technologies mantém uma corporação que representa seus interesses no Panamá, todas as pessoas em seu Conselho de Administração são cidadãos chineses e não vivem no Panamá.

A outra empresa envolvida no fornecimento de tecnologias biométricas no Panamá é a Canadian General Dynamics Mission Systems, contratada para o Projeto de Reconhecimento Facial Biométrico do Aeroporto de Tocumen e do Centro de Operações Nacionais, ambos ativos desde 2019. Os contratos alcançaram o valor de 4.786.388 e 27,5 milhões de dólares, respectivamente. A empresa mantém diversos contratos com o governo panamenho no âmbito da cooperação do país com a Câmara de Comércio do Canadá.

41 Ver https://poderlatam.org/2020/01/el-negocio-de-slim-en-el-centro-historico-de-la-cdmx/

42 Ver https://www.quienesquien.wiki/es/empresas/sym-servicios-integrales-sa-de-cv?collection=all&name=SYM+-SERVICIOS+INTEGRALES+SA+DE+CV&tipo-entidad=&pais=&estado=&ciudad=&fuente=&size=&sort-all=#summary-supplier_contract

43 Ver https://r3d.mx/2017/01/05/nyt-documenta-uso-de-malware-para-espionaje-politico-en-puebla/

Paraguay

No Paraguai, foram identificadas três iniciativas de uso do reconhecimento facial. Em todos eles estão envolvidos dois fornecedores nacionais, responsáveis pela implementação e manutenção dos sistemas. A primeira é Tecnología, Seguridad y Vigilancia del Paraguay SRL, contratada a partir de uma licitação de 3 milhões de dólares no âmbito do projeto de reconhecimento facial em espaços públicos urbanos que se realiza atualmente em Assunção, Encarnación, San Ignacio, Caaguazú, Coronel Oviedo e Ciudad del Este. A empresa atende a polícia paraguaia desde pelo menos 2011, de acordo com a imprensa local, que também tem levantado dúvidas quanto ao efetivo funcionamento das tecnologias de reconhecimento facial implementadas.[44]

Também a paraguaia Asunción Comunicaciones S.A. venceu concurso para Ampliação de Capacidades, Garantias e Facial do Sistema AFIS (*Automated Fingerprint Identification System*). O contrato resultou em uma receita de 1.676.303 dólares em 2017 e 1.813.215 dólares em 2019. Como parte do serviço, a empresa forneceu licenças de software biométrico para telefones móveis, licenças de middleware central biométrico móvel, licença registrada AFIS criminal, licença de atualização de software central facial e licença de atualização estação de trabalho de software facial.

Asunción Comunicaciones S.A. também recebeu atribuição por concurso público para a implementação do Sistema AFIS em um evento esportivo, no âmbito de uma ação conjunta com a Associação Paraguaia de Futebol e a Polícia Nacional, liderada pelo Ministério do Interior. A ação piloto realizada em 2019 resultou em um investimento de aproximadamente 1.642.093 dólares.

Peru

No Peru, uma única iniciativa de implantação de sistemas de reconhecimento facial foi identificada no Gamarra, um dos mais importantes centros comerciais do país, localizado na região metropolitana de Lima. O sistema está em processo de implantação desde 2019. A iniciativa contou com a participação da empresa peruana Desarrollos Terrestres, responsável pela instalação das câmeras.

O mecanismo de contratação neste caso é particular: a empresa Desarrollos Terrestres vem firmando convênios com diversos municípios distritais de Lima. Assim, de acordo com esses convênios, a empresa era obrigada a instalar as câmeras e disponibilizar um sistema de monitoramento ao Município. Em troca, o Município prometeu facilitar a instalação de redes de telecomunicações no distrito.

44 Ver https://www.abc.com.py/edicion-impresa/economia/2019/11/11/tsv-srl-es-la-eterna-proveedora-tecnologica-del-911-de-la-policia/

A modo de conclusão: o reconhecimento facial não nos protege, nos deixa vulneráveis

Diferentes governos ao redor do mundo começaram a impor proibições e moratórias sobre a implementação e uso do reconhecimento facial e algumas empresas de desenvolvimento de software se comprometeram a restringir as vendas desse tipo de sistema em determinadas situações. É o caso da Amazon,[45] Microsoft[46] e IBM,[47] que se manifestaram expressamente nesse sentido após os episódios de protestos por justiça racial nos Estados Unidos em 2020. Essas manifestações ocorrem ao mesmo tempo que se descobrem traços de preconceito racial nessas tecnologias.[48]

Especialistas internacionais também se posicionaram favoravelmente à imposição desse tipo de medida,[49] considerando que os sistemas de reconhecimento facial implicam em uma série de impactos sobre o exercício dos direitos humanos.[50]

Por que não? Impacto nos direitos humanos e riscos associados ao uso de reconhecimento facial

É importante lembrar que a tecnologia de reconhecimento facial permite a identificação individualizada de qualquer pessoa e, com isso, o acompanhamento de suas viagens e hábitos pessoais em tempo real. A transformação dessas informações em metadados que podem, por sua vez, ser armazenados e analisados de forma agregada, implica na possibilidade adicional de inferir uma série de comportamentos e até de tentar prever ações futuras.

Especialmente quando são implementados em espaços públicos – como é o caso da maioria das iniciativas identificadas a partir deste mapeamento – os sistemas de reconhecimento facial consistem em uma tecnologia de vigilância em massa encoberta que atinge todas as pessoas que circulam em um determinado espaço, sem ter conhecimento ou a possibilidade de consentir na coleta de informações pessoais sensíveis, como seus dados biométricos. Isso inclui, por exemplo, crianças e adolescentes, cuja privacidade goza de proteção especial devido ao enorme impacto que o uso abusivo ou o vazamento dessas informações extremamente sensíveis podem ter no livre desenvolvimento de sua personalidade. Organizações da sociedade civil identificaram a inclusão indevida de dados de menores nas bases de dados do Sistema de Reconhecimento Facial

45 El País. Amazon suspende indefinidamente la venta de su tecnología de reconocimiento facial a la policía. Ver https://elpais.com/tecnologia/2021-05-21/amazon-suspende-indefinidamente-la-venta-de-su-tecnologia-de-reconocimiento-facial-a-la-policia.html

46 The Washington Post. Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM. Ver https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/.

47 El País, IBM abandona la tecnología de reconocimiento facial por las dudas éticas sobre su uso. Ver https://elpais.com/tecnologia/2020-06-09/ibm-abandona-la-tecnologia-de-reconocimiento-facial-por-las-dudas-eticas-sobre-su-utilizacion.html.

48 Ver Buolamwini J.; Gebru T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research 81:1–15, 2018. Recuperado http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

49 Ver https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736

50 Moratorium call on surveillance technology to end "free-for-all" abuses: UN expert. En UN News [Internet]. 25 de junho de 2019 [citado 18 de febrero de 2020]. Recuperado: https://news.un.org/en/story/2019/06/1041231

de Foragidos (SRFP) implementado em algumas estações do metrô da Cidade Autônoma de Buenos Aires.[51]

A instalação de sistemas de reconhecimento facial para vigilância de espaços públicos, portanto, implica necessariamente restrições ao direito à livre circulação, uma vez que quem não quiser que o sistema recolha os seus dados biométricos terá que procurar caminhos ou meios de transporte alternativos. Por outro lado, o grau de intrusão típico deste tipo de tecnologia implica uma violação do direito à privacidade e, de forma associada, do direito à proteção dos dados pessoais.[52]

Além disso, as capacidades de monitoramento e previsão de comportamentos comprometem o exercício do direito à liberdade de associação, expressão e reunião pacífica, pois permitem traçar perfis de participantes em movimentos que contradizem interesses políticos ou econômicos estabelecidos, violando seu anonimato e facilitando a criminalização ou perseguição de expressões legítimas de caráter distinto.[53] Mais que um exercício imaginativo, é um risco concreto em países marcados por uma história de autoritarismo e inúmeros exemplos recentes de abusos, por exemplo, na vigilância de opositores políticos, como é o caso na maioria dos países analisados. A possibilidade de estar sob vigilância constante também incentiva o silenciamento e a autocensura e representa um risco gravíssimo para as sociedades democráticas.

As implicações da vigilância individualizada de pessoas em tempo real não afetam apenas as pessoas envolvidas na defesa dos direitos humanos ou em diferentes formas de ativismo. Em uma região particularmente marcada pelo racismo, machismo e homofobia de forma estrutural, esse tipo de sistema facilita a violência sexual por quem tem acesso ao funcionamento do sistema. Embora se espere que as operadoras estejam sujeitas a regras e controles rígidos, episódios de abuso e discriminação por parte de policiais na região não são incomuns.

O direito à não discriminação, reconhecido nos artigos 1 e 24 da Convenção Americana sobre Direitos Humanos, também está diretamente ameaçado pelos altos índices de falsos positivos produzidos pelos sistemas de reconhecimento facial, problema que aumenta exponencialmente quando as pessoas que estão sendo vigiadas pertencem a grupos historicamente vulneráveis, como mulheres, pessoas não brancas ou pessoas trans.[54] Os sistemas implantados na região já registraram erros que resultaram em graves consequências para as pessoas afetadas.

---

51 Ver https://www.hrw.org/es/news/2020/10/09/carta-al-lic-horacio-rodriguez-larreta-sobre-el-sistema-de-reconocimiento-facial-de

52 Ver, por exemplo: Assembleia Geral das Nações Unidas. 20 de novembro de 2013. El derecho a la privacidad en la era digital. A/RES/68/167. Recuperado https://undocs.org/pdf?symbol=es/A/RES/68/167 y Naciones Unidas, resolución del Consejo de Derechos Humanos, 'El derecho a la privacidad en la era digital', A/HRC/34/L.7/Rev.1, Naciones Unidas, Nueva York, 2017.

53 Ver Alto Comissariado das Nações Unidas para os Direitos Humanos, relatório "Impacto de las nuevas tecnologías en la promoción y protección de los derechos humanos en el contexto de las reuniones, incluidas las protestas pacíficas", A/HRC/44/24, 24 de junio 2020, párrafo 31, disponível em https://undocs.org/es/A/HRC/44/24. Ver também Relator Especial sobre los derechos a la libertad de reunión pacífica y de asociación, Informe Derechos a la libertad de reunión pacífica y de asociación, 17 de maio de 2019, parágrafo 56, disponível em https://undocs.org/es/A/HRC/41/41. Sobre as implicações da vigilância ao direito à liberdade de expressão ver: Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos. Estándares para una Internet Libre, Abierta e Incluyente. OEA/Ser.L/V/II CIDH/RELE/INF.17/17. Organização dos Estados Americanos; mar. 2017. Recuperado http://www.oas.org/es/cidh/expresion/docs/publicaciones/INTERNET_2016_ESP.pdf e Conselho de Direitos Humanos, Assembleia Geral das Nações Unidas. El derecho a la privacidad en la era digital. A/HRC/28/L.27. Organização das Nações Unidas; 24 de março de 2015. Recuperado: https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_28_L27.pdf.

54 Alto Comissariado das Nações Unidas para os Direitos Humanos, Informe "Impacto de las nuevas tecnologías en la promoción y protección de los derechos humanos en el contexto de las reuniones, incluidas las protestas pacíficas", A/HRC/44/24, 24 de junho 2020, parágrafo 32, disponível em https://undocs.org/es/A/HRC/44/24

No Sistema de Reconhecimento Facial de Foragidos implantado na Cidade Autônoma de Buenos Aires, Argentina, há registros de pelo menos dois casos de falsos positivos, um dos quais envolveu a detenção de um inocente por seis dias.[55] Situações semelhantes também foram identificadas no Brasil,[56] onde organizações denunciaram que, de um total de 151 pessoas presas em decorrência do uso de sistemas de reconhecimento facial, 90% são afrodescendentes.[57]

A implementação de sistemas de reconhecimento facial acarreta, portanto, a reprodução técnica de vieses de exclusão social e, quando utilizada para fins de vigilância, ameaça o direito à dignidade, ao devido processo e à presunção de inocência.

Por fim, quando implementado como mecanismo de autenticação de identidade para condicionar o acesso aos serviços públicos, o reconhecimento facial (assim como outras tecnologias biométricas) pode representar uma barreira ao exercício dos direitos econômicos e sociais. Além disso, implica que algumas pessoas, principalmente as que dependem da assistência social, estão sujeitas a garantias inferiores em termos de proteção dos seus direitos fundamentais. Quando aplicadas dessa forma, as tecnologias reforçam e aprofundam as históricas desigualdades estruturais que afetam a região.[58]

Da falta de transparência pública à resistência cidadã

Por todas as razões aqui expostas, é fundamental que as decisões associadas à implementação de sistemas de reconhecimento facial estejam sujeitas a rígidos controles democráticos – que incluem critérios de legalidade, necessidade e proporcionalidade – e de fiscalização pública. No entanto, o atual mapeamento realizado pelas organizações membros da Al Sur mostra que tais critérios são pouco respeitados na América Latina.

Primeiro, as implementações carecem de discussão pública antes da implantação. Na maioria dos casos, as iniciativas são divulgadas através de comunicados em meios especializados e de circulação restrita, a partir da publicação nos meios oficiais de processos de compras públicas (sobretudo quando são realizadas através de licitações públicas, o que nem sempre ocorre) ou quando já há registros de abusos ou outros tipos de escândalos de corrupção. Mais grave é que, inclusive durante esse processo de investigação, surgiram barreiras para o acesso às informações nesses sistemas.

Em segundo lugar, apenas em duas das 38 iniciativas identificadas havia um mecanismo de participação pública previsto antes da implementação das tecnologias. Quando se trata da realização de estudos anteriores de impacto à privacidade ou aos direitos humanos, novamente apenas duas iniciativas os implementaram. Por fim, apenas três das iniciativas preveem a realização de uma auditoria externa que ofereça garantias mínimas de implementação adequada dos sistemas.

O contexto regional é complementado por regulamentações fracas no que diz respeito à proteção de dados pessoais e acesso à informação pública, controles insuficientes tanto nos gastos públicos como na implementação de tecnologias, um histórico de autoritarismo e desprezo pelos direitos humanos, elevada insegurança social, políticas de austeridade e a promessa eterna de desenvolvimento na forma de tecnologia importada. O resultado é que a América Latina se torna um campo fértil para a adoção do reconhecimento facial para fins múltiplos e sem qualquer tipo

55 Ver https://www.pagina12.com.ar/209910-seis-dias-arrestado-por-un-error-del-sistema-de-reconocimien

56 Ver https://gizmodo.uol.com.br/rio-de-janeiro-reconhecimento-facial-erra-mulher-detida/.

57 Ver https://reconocimientofacial.info/denuncian-sesgo-racial-en-tecnologias-de-reconocimiento-facial-brasilenas/.

58 Ver https://www.derechosdigitales.org/13900/vigilancia-control-social-e-inequidad/.

de salvaguardas, o que permite evitar um uso contrário aos princípios democráticos que regem cada um dos países da região.

Diante de tal situação, organizações da sociedade civil têm recorrido aos tribunais para obter mais informações e questionar a implantação desses sistemas em seus países ou cidades, devido aos riscos potenciais envolvidos. No Brasil, a Justiça confirmou a ilegalidade de um sistema de câmeras de reconhecimento emocional instalado em estações de metrô.[59] A sentença é resultado de ação coletiva do Instituto Brasileiro de Defesa do Consumidor (Idec). Além da interrupção da coleta de dados pelo sistema, já apurada em 2018,[60] é estabelecida uma indenização de 100 mil reais por danos morais coletivos.[61] Atualmente, outras ações estão sendo desenvolvidas em São Paulo para questionar a instalação de câmeras de reconhecimento facial no transporte público. [62]

Na Argentina existem atualmente dois processos judiciais em andamento contra o Sistema de Reconhecimento Facial de Foragidos: uma Ação Declarativa de Inconstitucionalidade (ADI) contra o Governo da Cidade de Buenos Aires, movida pela Associação pelos Direitos Civis (ADC),[63] e um caso de proteção coletiva promovido pelo Observatório Argentino de Direito Informático (ODIA) que buscam interromper a iniciativa.[64] Além disso, foi recentemente admitido um processo de amparo contra a operação de sistemas com tecnologia de reconhecimento facial em Coahuila, México.

No Peru, um grupo de alunos apresentou perguntas sobre a obrigatoriedade do uso do reconhecimento facial para participação em um exame de admissão em uma universidade pública.[65] E no Paraguai, a organização TEDIC apresentou uma ação de inconstitucionalidade, questionando a declaração do Estado paraguaio de que as informações relacionadas com a implementação de sistemas de reconhecimento facial no país são de segurança nacional e, portanto, reservadas.

Diante das tentativas dos Estados da região de ocultar, encobrir e omitir do debate público o aumento das capacidades de vigilância por meio das tecnologias de reconhecimento facial, suas falhas, deficiências, negligências e perigos, a sociedade civil resiste e denuncia suas ilegalidades e abusos. Não se trata de um problema técnico, é uma discussão política sobre o tipo de sociedade que queremos e o papel que as tecnologias devem ter nela: ferramentas para o desenvolvimento integral das pessoas e da sociedade como um todo ou forma de perpetuar as desigualdades sociais e históricas, por meio de um autoritarismo tecnicamente assistido.

Esta é uma batalha particularmente importante na América Latina, onde os direitos humanos e as noções de dignidade e autonomia das pessoas são frequentemente minados pelos interesses das elites políticas e econômicas, e onde a democracia deve resistir constantemente a ataques, produtos da corrupção e dos abusos de poder. Diante da opacidade que o despotismo protege, exigimos transparência; diante de imposições arbitrárias, exigimos o debate democrático e a participação plural nos processos de tomada de decisão quanto à implantação de tecnologias

---

59 Ver https://idec.org.br/noticia/idec-obtem-vitoria-contra-reconhecimento-de-emocoes-no-metro-de-sp.

60 Ver https://idec.org.br/noticia/justica-impede-uso-de-camera-que-coleta-dados-faciais-do-metro-em-sp.

61 Ver https://teletime.com.br/10/05/2021/justica-condena-viaquatro-por-reconhecimento-facial-de-passageiros-sem-consentimento/.

62 Ver https://reconocimientofacial.info/metro-tera-que-explicar-licitacao-de-cameras-de-reconhecimento-facial/.

63 Ver https://adc.org.ar/2019/11/06/el-reconocimiento-facial-para-vigilancia-no-pertenece-a-nuestro-espacio-publico/

64 Ver https://amicus.odia.legal/

65 Ver https://reconocimientofacial.info/peru-uso-de-reconocimiento-facial-en-examen-de-admision-a-universidad-publica-genera-cuestionamientos/

invasivas como o reconhecimento facial. Em face do tecnossolucionismo grosseiro, exigimos uma perspectiva de direitos humanos ampla, robusta e sofisticada. Diante das promessas vazias de modernidade, exigimos desenvolvimento e dignidade para todas as pessoas.

A depredação dos direitos fundamentais em prol dos interesses políticos e econômicos que sustentam a implementação dos diferentes sistemas de reconhecimento facial aqui listados exige uma resposta enérgica da sociedade civil contra os governos que não parecem dispostos a enfrentar o problema com a seriedade necessária. Esperamos que este relatório sirva de subsídio para a luta que diferentes pessoas já estão realizando, em diferentes locais da América Latina, bem como um incentivo para a preparação das lutas de amanhã.

www.alsur.lat

AlSur