Tecnologia de vigilância na América Latina:

Feita no exterior, implantada em cas

A Access Now defende e amplia os direitos digitais dos usuários em risco em todo o mundo. Combinando suporte técnico direto, amplo engajamento político, divulgação global, concessão de subsídios de base, intervenções legais e convocações como a RightsCon, lutamos pelos direitos humanos na era digital.

Artigo atualizado em 10 de agosto de 2021

Este artigo é uma publicação da Access Now. É escrito por Gaspar Pisanu e Verónica Arroyo do Access Now, Leandro Ucciferri e Eduardo Ferreyra da Asociación por los Derechos Civiles (Argentina), Thiago Moraes e José Renato Laranjeira, Eduarda Costa Almeida, Fernando Fellows Dourado, Carolina Reis e Felipe Rocha da Silva do Laboratório de Políticas Públicas e Internet (Brasil), e Jonathan Finlay e Anais Córdova-Páez do LaLibre.net (Equador). Gostaríamos de agradecer aos membros da equipe Access Now que nos apoiaram, incluindo Ángela Alarcón, Hinako Sugiyama, Isedua Oribhabor, Juliana Castro, Sage Cheng, Marwa Fatafta, Daniel Leufer, Estelle Massé, Peter Micek, Natalia Krapiva, Javier Pallero, Gustaf Bjorksten, Raman Jit Singh Chima, Leanna Garfield e Donna Wentworth. Gostaríamos também de agradecer a todos os jornalistas, pesquisadores e ativistas que nos ajudaram a oferecer uma visão e informações essenciais para esta publicação. Esperamos receber feedback e outras contribuições de especialistas em direitos digitais, vigilância e privacidade.

A Access Now (https://www.accessnow.org) defende e amplia os direitos digitais dos usuários em risco em todo o mundo. Combinando suporte técnico direto, amplo engajamento político, divulgação global, concessão de subsídios de base, intervenções legais e convocações como a RightsCon, lutamos pelos direitos humanos na era digital.

Agosto de 2021

Para saber mais, fale com:
Gaspar Pisanu
(gaspar@accessnow.org)
Verónica Arroyo
(veronica@accessnow.org)
Ángela Alarcón
(angela@accessnow.org)

ÍNDICE

ÍNDICE **3**

SUMÁRIO EXECUTIVO **4**

I. INTRODUÇÃO: UMA COLABORAÇÃO PARA EXPOR OS FORNECEDORES **7**

II.: AS EMPRESAS: QUEM LUCRA COM VIOLAÇÕES DE DIREITOS HUMANOS? **8**

⇛ AnyVision 8

⇛ Hikvision e Dahua 10

⇛ Cellebrite 15

⇛ Huawei e ZTE 20

⇛ NEC 23

⇛ IDEMIA 29

⇛ Verint 32

Outras empresas que fornecem tecnologia de vigilância na América Latina 34

III. ESTUDOS DE CASOS: COMO A TECNOLOGIA É UTILIZADA **39**

ESTUDO DE CASO: Argentina **39**

Tecnologia utilizada 39

Enquadramento jurídico 41

Casos locais 42

ESTUDO DE CASO: Brasil **44**

Tecnologia utilizada 46

Enquadramento jurídico 47

Casos locais 48

ESTUDO DE CASO: Equador **50**

Tecnologia utilizada 53

Enquadramento jurídico 54

Casos locais 55

IV. CONCLUSÃO E RECOMENDAÇÕES **56**

SUMÁRIO EXECUTIVO

Deslizar para a esquerda, deslizar para a direita, dar um like, compartilhar, repetir. Estamos cada vez mais conscientes do impacto da tecnologia digital sobre nossos direitos. Os legisladores de todo o mundo estão voltando sua atenção para empresas como Google, Facebook, Amazon, Microsoft e Apple, e em muitos casos estão desenvolvendo novas leis e políticas para regular esses guardiães de direitos fundamentais. Mas outras empresas estão voando abaixo do radar, vendendo tecnologia de vigilância utilizada em toda a América Latina sem transparência ou escrutínio público suficientes. Isso está corroendo os processos democráticos, nos privando da privacidade e minando a liberdade de expressão e outros direitos humanos básicos.

Muitas vezes ouvimos que funcionários públicos enquadram a aquisição e o uso de ferramentas de vigilância como reconhecimento facial como um avanço tecnológico e uma medida positiva de "combater ao crime". No entanto, as ferramentas para nos identificar, destacar e rastrear em todos os lugares que vamos são **inerentemente incompatíveis com nossos direitos humanos e liberdades civis**. Além disso, as pesquisas mostram que os sistemas de reconhecimento facial e outras formas de identificar pessoas remotamente por suas características físicas - ou "biométricas" - são muitas vezes profundamente falhos, racialmente tendenciosos e discriminatórios. É por isso que há um movimento crescente ao redor do mundo para proibir o uso de IA para vigilância biométrica em massa.[1]

Infelizmente, muitos governos latino-americanos estão se movendo na direção oposta, comprando avidamente essa tecnologia e acelerando a implementação da vigilância biométrica de massa.[2] Notadamente, como revelamos neste relatório, a maior parte da tecnologia de vigilância implantada na América Latina é adquirida da Ásia (Israel, China e Japão), Europa (Reino Unido e França) e Estados Unidos, diretamente ou indiretamente através de uma rede de revendedores. Entre esses fornecedores estão a **AnyVision, Hikvision, Dahua, Cellebrite, Huawei, ZTE, NEC, IDEMIA,** e **VERINT**.

Considere a crescente infraestrutura de vigilância biométrica na **Argentina**, **Brasil** e **Equador**, os países que destacamos neste relatório.

Em 2011, a **Argentina** introduziu um enorme banco de dados biométricos chamado **SIBIOS**. Ao longo da última década, ele passou a ser a infraestrutura de muitas outras tecnologias de vigilância utilizadas a nível nacional e local que vão desde balões de vigilância na cidade autônoma de Buenos Aires até câmeras de reconhecimento facial na província de Córdoba, passando por câmeras térmicas nos principais aeroportos.

No **Brasil**, tanto o setor público quanto o privado estão usando tecnologias de vigilância citando razões como segurança pública, detecção de fraudes e acompanhamento da frequência escolar. Estados das regiões Nordeste e Sudeste, duas das regiões mais populosas do país, têm promovido intensamente o uso de tecnologias de reconhecimento facial como uma medida de aumento da segurança pública sem fornecer evidências que sustentem essas alegações. Mais preocupantes do ponto de vista da segurança

[1] Access Now. “Banimento da Vigilância Biométrica.” Junho de 2021. https://www.accessnow.org/ban-biometric-surveillance/
[2] Access Now. “Em vez de banir o reconhecimento facial, alguns governos da América Latina querem torná-lo oficial.” Dezembro de 2020. https://www.accessnow.org/facial-recognition-latin-america/

são as tecnologias de vigilância "doadas" por empresas privadas aos governos locais, às vezes usadas no público como população de teste.

Em 2010, o **Equador** implementou o "Serviço Integrado de Segurança **ECU911**", desenvolvendo uma infraestrutura nacional de vigilância policial que atualmente tem mais de 6.600 câmeras, algumas das quais com tecnologia de reconhecimento facial. Em 2019, soubemos que o governo utilizou essa mesma infraestrutura para espionar adversários políticos e cidadãos que as autoridades pretendiam coagir.

Por que a tecnologia de vigilância está sendo adotada tão rapidamente, apesar da ameaça aos direitos fundamentais das pessoas? O público confia na vigilância da mídia, aumentando a conscientização quando há riscos aos nossos direitos e liberdades democráticas. Infelizmente, na América Latina, quando a imprensa e os políticos abordam a questão muito real e sensível da violência e do crime nas ruas, em muitos casos, eles retratam de forma acrítica essas ferramentas como a solução para o problema. Os governos enfrentam a pressão do público para encontrar "soluções", e as empresas de tecnologia capitalizam esta dinâmica para obter lucro, apesar de seu dever de garantir que seus produtos não sejam utilizados para violar os direitos humanos.

Quando nem funcionários do governo nem o público entendem como essas tecnologias funcionam de fato, e ninguém incorporou ou reforçou a transparência e a responsabilidade necessárias para proteger as pessoas, **temos a receita perfeita para a expansão contínua e o uso generalizado dessas tecnologias.**

Este relatório é um esforço para **expor as empresas por trás desses produtos perigosos e as políticas e práticas governamentais de compra e distribuição que estão minando os direitos das pessoas**. Em muitos países da América Latina, o processo pelo qual as autoridades firmam acordos para adquirir tecnologia de vigilância é pouco divulgado e opaco. Os governos fazem acordos com pouco ou nenhum debate público ou supervisão, e muitas vezes com pouco respeito às leis de transparência e ao dever de comunicação com o público. Os países que permitem a exportação desses produtos de vigilância para a América Latina também são culpáveis. As empresas que deixam de ter a devida diligência e facilitam o abuso dos direitos humanos devem ser responsabilizadas.

Para esse fim, trabalhamos com nossos parceiros na **Asociación por los Derechos Civiles (ADC)**, no **Laboratório de Políticas Públicas e Internet (LAPIN)**, e na **LaLibre.net (Tecnologías Comunitarias)** para **investigar as empresas fornecedoras da tecnologia**, examinando seus históricos sobre direitos humanos. **Analisamos o impacto da tecnologia** sobre os direitos das pessoas na **Argentina**, no **Brasil**, e no **Equador**, fornecendo exemplos de casos para cada país. Ao final, **fizemos recomendações** para **legisladores**, **governos**, **empresas**, a **mídia**, e o **público em geral**, encorajando todas as partes interessadas a tomarem uma ação.

Os países da América Latina têm uma longa história de perseguição a dissidentes e pessoas em comunidades marginalizadas, e as autoridades continuam a abusar do poder público. A pandemia da

COVID-19 deu agora aos governos uma nova desculpa para empregar ferramentas perigosas de vigilância em nome da segurança pública, mesmo que elas não protejam os direitos humanos. Esperamos que este relatório estimule as organizações da sociedade civil, os meios de comunicação e os cidadãos a **fazer perguntas, investigar empresas e exigir que seus governos protejam e promovam os direitos humanos**. Como nossos estudos de caso demonstram, o que está em jogo não poderia ser mais valioso.

I. INTRODUÇÃO:
UMA COLABORAÇÃO PARA EXPOR OS FORNECEDORES

A Access Now, a Asociación por los Derechos Civiles (ADC), o Laboratório de Políticas Públicas e Internet (LAPIN) e a LaLibre.net colaboraram na pesquisa para este relatório, que representa o resultado final de uma investigação abrangente feita na Argentina, no Brasil e no Equador no último trimestre de 2020.

É bem conhecido que os governos nacionais e locais de cada um desses países estão implementando cada vez mais tecnologias de vigilância em massa. Entretanto, há pouca ou nenhuma informação disponível sobre quem está fornecendo essa tecnologia, que tipo de tecnologia está sendo comprada e sob que condições ela está sendo implantada. Essa opacidade frustra a oportunidade da sociedade civil de entender o que está acontecendo e responder adequadamente. Assim, nossas organizações decidiram mapear os fornecedores e as tecnologias que estão sendo vendidas e descobrir as relações entre governos e empresas. Este relatório visa esclarecer essas operações, expor os danos aos direitos humanos e colocar as empresas que vendem de forma irresponsável a Tecnologia de Vigilância na América Latina sob o escrutínio público.

Para obter o máximo de informações possíveis, enviamos pedidos com base na liberdade de informação, analisamos relatórios de notícias e conseguimos nos aproximar de representantes das empresas, obter informações e conduzir entrevistas. Descobrimos que muitas empresas de tecnologia de vigilância com mau histórico de direitos humanos das encontraram nos países latino-americanos os clientes "técnico-solucionistas" perfeitos para os quais podem vender tecnologia prejudicial aos direitos sem grandes obstáculos. Também identificamos padrões nas relações entre governos e essas empresas, mostrando um desrespeito ao cumprimento de padrões fundamentais de transparência e responsabilidade.[3] Essas e outras descobertas nos permitem concluir que na Argentina, Brasil e Equador, a ameaça aos direitos humanos está se expandindo juntamente com o crescente arsenal de tecnologias adquiridas no escuro e utilizadas por governos com pouco respeito aos direitos humanos. Por essa razão, concluímos este relatório com um aviso de que a situação atual deve mudar, e oferecemos recomendações urgentes aos governos e empresas.

Nossa metodologia de pesquisa compreende três estágios:

1) **Investigação**: Cada organização coletou informações de sites de compras públicas/orçamento, comunicados oficiais, artigos da imprensa, respostas a nossos pedidos com base em liberdade de informação por parte de escritórios públicos específicos e entrevistas com representantes de empresas, jornalistas e pesquisadores.
2) **Relatórios locais:** Preparamos uma explicação e análise do contexto jurídico e político e do estado atual do uso de vigilância em cada país.
3) **Análise transversal**: Examinamos o comportamento e os modelos comerciais de cada fornecedor que vende tecnologia de vigilância (diretamente ou através de representantes locais) e avaliamos seu histórico global de direitos humanos.

[3] Alto Comissariado das Nações Unidas para Direitos Humanos, “Princípios Orientadores sobre Empresas e Direitos Humanos” Junho de 2011. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

II. AS EMPRESAS:
QUEM LUCRA COM VIOLAÇÕES DE DIREITOS HUMANOS?

Iniciamos este relatório nos voltando para as empresas fornecedoras das tecnologias de vigilância que os governos estão utilizando na Argentina, no Brasil e no Equador. Destacamos as empresas com participação expressiva no mercado desses países ou que vendem uma tecnologia particularmente perigosa para os direitos humanos. Fornecemos informações sobre seu histórico, tecnologias que vendem e sua posição nos mercados desses países latino-americanos. Finalmente, avaliamos seu histórico de direitos humanos, como elemento essencial para entender os perigos que seus produtos representam na América Latina. Após fornecer informações detalhadas sobre as empresas, procedemos aos estudos de caso que demonstram os danos que já estão sendo causados aos direitos fundamentais dos indivíduos.

Obtivemos a maior parte das informações sobre as empresas a partir de declarações oficiais de autoridades públicas e representantes de empresas, reportagens na mídia, mídia social e entrevistas diretas. Na grande maioria dos casos, não fomos capazes de estabelecer uma comunicar direta com as empresas.

É especialmente desafiador obter informações sobre como as tecnologias estão sendo utilizadas quando elas são adquiridas através de fornecedores locais e não diretamente dos fabricantes. Essa é outra forma das empresas de vigilância permanecerem no escuro e evitar o escrutínio público, além de ignorarem consultas e não ser comunicativas e transparentes.

⇛ AnyVision

Nome da Empresa	**AnyVision Interactive Technologies Ltd**
Matriz	Holon, Israel
Países onde Atua	Israel, Reino Unido, Estados Unidos
Países onde suas tecnologias de vigilância são utilizadas entre Argentina, Brasil e Equador	Argentina
Fundada em	2015
Capital Aberto / Fechado	Capital Fechado
Acionistas Principais	DFJ Growth, OG Technology Partners, LightSpeed Venture Partners, Qualcomm Ventures, Bosch Building Technologies SVP [em 2020]

Número de Funcionários	240 em 2020
Receita Anual	Não disponível

A **AnyVision** é uma empresa israelense especializada em tecnologia de reconhecimento facial para segurança pública, além de aplicações para a saúde, cassinos e bancos.[4] Somente através de anúncios públicos e cobertura da mídia[5] foi possível descobrir que AnyVision é a empresa fornecedora do "software de reconhecimento biométrico" adquirido pela Província de Córdoba na **Argentina.**

AnyVision também parece ser a fornecedora do software utilizado no Aeroporto Internacional de Ezeiza, na Província de Buenos Aires, Argentina. A partir dos registros oficiais, descobrimos que as autoridades adquiriram um sistema de reconhecimento facial através de negociações diretas com uma revendedora local da AnyVision no país, a empresa **RC International**. O primeiro contrato direto entre a Polícia de Segurança Aeroportuária (PSA) e a RC International data de dezembro de 2017, e foi de aproximadamente US$48.000,00. O contrato envolveu a aquisição de quatro licenças de reconhecimento facial da AnyVision, juntamente com quatro câmeras IP (Internet Protocol) e um servidor, com a capacidade de escanear e comparar rostos com um registro de 2,5 milhões de rostos.[6] Um ano depois, a PSA assinou outro contrato direto com a RC International por cerca de US$ 54.000,00 para adquirir cinco licenças e melhorar a infraestrutura de processamento.[7]

Em 17 de julho de 2020, quando perguntado sobre a implementação da tecnologia da AnyVision, o gerente de Negócios e Estratégia da RC International, Pablo Marcovich, confirmou[8] que a PSA tinha usado a tecnologia de reconhecimento facial da AnyVision em Ezeiza por dois anos.

Histórico de direitos humanos da AnyVision

De acordo com uma investigação publicada pela NBC em março de 2020, as autoridades israelenses utilizaram a tecnologia da AnyVision em um esquema secreto de vigilância para monitorar o movimento de palestinos na Cisjordânia, um projeto chamado "Google Ayosh" em referência à capacidade da tecnologia de procurar e encontrar pessoas.[9] O projeto ganhou um prêmio da indústria de defesa em 2018 pela "prevenção de centenas de ataques terroristas" com o uso de "grandes quantidades de dados"[10], ainda que não esteja claro como exatamente o projeto evitou tais ataques.

[4] Veja mais informações no site da AnyVision em https://www.anyvision.co/
[5] Conta da El Doce YouTube. “O reconhecimento facial já está funcionando em Córdoba” (em espanhol) Novembro de 2019. https://www.youtube.com/watch?v=xC2Y_T2KxCo
[6] Processo número 279-0032-CDI17 https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhxpHQh1a9rqmrswnHE0fbV4WFyYSFDE6lxSvc3QcWHT4/5pakrCnV2dPCYEG/6/s7e/f0naaJmGFnfhrFxNdKQpW67nH3a2C04dnq|8jmWDuQ==
[7] Processo número 279-0035-CDI18 https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhzSOD16bvFoRxEndMm7PHzAtBPeqYP9/qDb7KvHTHIh0obV8V5uXVQalfN9iRQ6t0NyEcvs|vrVYCJ5StXEPkNZXp61l5600xzpoafNPUDbtt6dkX1N7sUlXsW/U3fjsZr4FM|ahmgldAmKnOzjXjiP3OSXKNWySBJ/gR9toZ5IZaihRjc3OgmkchygiKgU9i4=
[8] https://digital.practia.global/cuando-tu-foto-se-convierte-en-tu-huella-digital/
[9] Access Now. “Expostos e explorados: Proteção de dados no Oriente Médio e Norte da África.” Janeiro de 2021. https://www.accessnow.org/mena-data-protection-report
[10] NBC News. “Por que a Microsoft financiou uma empresa israelense que fiscaliza os palestinos da Cisjordânia?” Outubro de 2019. https://www.nbcnews.com/news/all/why-did-microsoft-fund-israeli-firm-surveils-west-bank-palestinians-n1072116

Além de descobrir o projeto confidencial, a NBC diz[11] ter provas de que a polícia israelense está usando a tecnologia da AnyVision para rastrear o movimento de palestinos em toda Jerusalém Oriental.

A tecnologia em questão é um dos produtos centrais da AnyVision, "Better Tomorrow". O sistema usa câmeras de reconhecimento facial instaladas e um sistema automatizado de alerta de lista de monitoramento para identificar os rostos dos "suspeitos" nas multidões, e rastrear e categorizar veículos. A AnyVision também fornece tecnologia de reconhecimento facial utilizada em 27 postos de controle militares israelenses na Cisjordânia para autenticar a identidade dos palestinos que cruzam para Israel.

Notavelmente, após anos de pressão de defensores dos direitos humanos, a **Microsoft** vendeu sua participação na AnyVision.[12] Em 2019, um estudo do Instituto Nacional de Padrões e Tecnologia dos EUA (NIST)[13] sobre o viés racial no software de reconhecimento facial descobriu que o algoritmo da AnyVision, como muitos dos outros algoritmos testados, teve um desempenho pior em rostos africanos ou do leste asiático do que em rostos do leste europeu.

⇛ Hikvision e Dahua

Nome da Empresa	**Hangzhou Hikvision Digital Technology Co Ltd**
Matriz	Hangzhou, República Popular da China
Países onde Atua	Global
Países onde suas tecnologias de vigilância são utilizadas entre Argentina, Brasil e Equador	Argentina, Brasil, Equador
Fundada em	2001
Capital Aberto / Fechado	Cotada na Bolsa de Valores de Shenzhen
Acionistas Principais	China Electronics Technology Group Corporation (estatal chinesa) (38.88%), Gong Hongjia, conselheiro da Hikvision e investidor de capital de risco (13.43%) [em 2019]
Número de Funcionários	40,403 em 2019
Receita Anual	RMB 57.66 bilhões (US$8.8 bilhões) em 2019

[11] NBC News. “Por que a Microsoft financiou uma empresa israelense que fiscaliza os palestinos da Cisjordânia?” Outubro de 2019. https://www.nbcnews.com/news/all/why-did-microsoft-fund-israeli-firm-surveils-west-bank-palestinians-n1072116
[12] The Verge. “Microsoft vai encerrar os investimentos em empresas de reconhecimento facial após controvérsia com a AnyVision.” Março de 2020.
https://www.theverge.com/2020/3/27/21197577/microsoft-facial-recognition-investing-divest-anyvision-controversy
[13] NIST. “Estudo do NIST avalia os efeitos da raça, idade, sexo em software de reconhecimento facial.” Dezembro de 2019.
https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software

Nome da Empresa	Zhejiang Dahua Technology Co., Ltd.
Matriz	Hangzhou, República Popular da China
Países onde Atua	Global
Países onde suas tecnologias de vigilância são utilizadas entre Argentina, Brasil e Equador	Argentina, Brasil
Fundada em	2001
Capital Aberto / Fechado	Cotada na Bolsa de Valores de Shenzhen
Acionistas Principais	Fu Liquan (35.97%) em 2019
Número de Funcionários	10.197 em 2019
Receita Anual	RMB 26,15 bilhões (US$4 bilhões) em 2019

Hikvision e **Zhejiang Dahua** são duas das maiores fabricantes de equipamentos de vigilância. Sua presença na América Latina cresceu exponencialmente em 2020, já que as empresas fornecem a vários governos soluções tecnológicas para enfrentar a pandemia da COVID-19.

Segundo fontes oficiais, o Ministério dos Transportes da **Argentina** autorizou o teste de câmeras térmicas da Hikvision dentro do terminal ferroviário de Retiro, para identificar passageiros com febre.[14] As autoridades utilizaram a mesma tecnologia, desta vez desenvolvida pela Dahua, no Aeroporto Internacional de Ezeiza e no transporte público, incluindo duas linhas de ônibus,[15] assim como em dois aeroportos **brasileiros**: o aeroporto de Guarulhos, em São Paulo[16] (o maior da América do Sul), e o aeroporto do Galeão, no Rio de Janeiro.[17]

A presença de Dahua na Argentina não é novidade. Em 2017, Cutral-Có, uma importante cidade produtora de petróleo, implantou um abrangente sistema da Dahua, incluindo um Sistema de Vigilância Profissional (PSS) como núcleo do projeto, e um software conectado simultaneamente a 256

[14] Telam. “Duas linhas de ônibus instalam câmeras térmicas para medir a temperatura de passageiros” (em espanhol) Maio de 2020. https://www.telam.com.ar/notas/202005/469479-camaras-termicas-colectivos-pasajeros.html

[15] Infobae. “Duas linhas de ônibus instalam câmeras térmicas para medir a temperatura de passageiros” (em espanhol) Maio de 2020. https://www.infobae.com/sociedad/2020/05/28/dos-lineas-de-colectivos-instalaron-camaras-termicas-para-medir-la-temperatura-de-los-pasajeros/

[16] Guarulhos Online. “Aeroporto de Guarulhos instala câmeras térmicas para medir a temperatura de passageiros” (em português). Junho de 2020. https://guarulhosonline.com.br/cidade/aeroporto-de-guarulhos-instala-cameras-termicas-para-medir-a-temperatura-dos-passageiros/

[17] Vinicius Novaes. “RIO galeão reforça medidas preventivas com câmeras térmicas” (em português). Dezembro de 2020. https://www.panrotas.com.br/aviacao/aeroportos/2020/12/riogaleao-reforca-medidas-de-prevencao-com-cameras-termicas_178330.html

dispositivos, de acordo com o material da Dahua divulgado para a imprensa.[18]

Nossa busca por fontes disponíveis ao público, incluindo a cobertura da iniciativa pela mídia, não produziu qualquer detalhe adicional.

O projeto em Cutral-Có envolveu a instalação de 242 câmeras de vídeo. Ainda que não haja qualquer confirmação oficial, a própria Dahua afirma que a infraestrutura implementada oferece flexibilidade para expandir seu uso, por exemplo, utilizando imagens de vídeo gravadas com software de reconhecimento facial e ferramentas para identificar números de placas de carro.

Testes independentes de câmeras térmicas, em particular produtos Hikvision, mostram que essa tecnologia é altamente imprecisa.[19] A sua temperatura corporal real pode ser ocultada apenas pelo cabelo sobre a sua testa. Pior, quando as câmeras Dahua foram instaladas em duas linhas de ônibus em Buenos Aires, a instalação não seguiu os padrões da indústria (padrões da Comissão Eletrotécnica Internacional[20]) e seu uso não obedeceu às instruções da própria empresa.[21]

Como parte da pesquisa para este relatório, fizemos dois pedidos com base na liberdade de informação ao Ministério Nacional de Transportes e sua contraparte na Cidade de Buenos Aires, em 3 de novembro de 2020. Esses pedidos incluíam perguntas sobre a implementação dessas tecnologias e a relação da cidade com ambas as empresas. Até de agosto de 2021 nossas perguntas não foram respondidas.

Além disso, tentamos diversas vezes falar com a Dahua através de vários canais, inclusive via e-mail e mensagens do LinkedIn, e entrevistar representantes que trabalham na região ou em sua matriz global. Também, até agosto de 2021, ainda aguardávamos a resposta oficial de um representante da Dahua. A Hikvision, por sua vez, tratou nosso pedido de entrevista com um sistema de suporte técnico automatizado, e o nosso pedido caiu num beco sem saída.

A preferência por essas empresas parece estar relacionada ao seu preço competitivo, como declararam alguns representantes brasileiros das autoridades públicas entrevistadas. Segundo um relatório da IPVM, os produtos HikVison ou Dahua podem custar até 10 vezes menos do que alguns de seus concorrentes.[22]

Em Mogi Das Cruzes no Brasil, a Dahua foi além de fornecer tecnologia de vigilância a um custo mais baixo — **ela fez isso de graça**. A empresa doou equipamentos para testar sua tecnologia nas ruas durante a Festa do Divino, implantando câmeras de reconhecimento facial e equipamentos de monitoramento para veículos, incluindo gravadores, microfones, telas sensíveis ao toque e até mesmo

[18] Security Worldmarket. "Cutral-Có se transforma numa Cidade Segura em 30 dias com a Dahua." Maio de 2017. https://www.securityworldmarket.com/int/Newsarchive/cutral-co-transforms-into-a-safe-city-with-dahua-solution-in-30-days
[19] IPVM. "Triagem de Temperatura da Hikvision é Testada." Maio de 2020 https://ipvm.com/reports/hikvision-temperature-test
[20] I*nternational Electrotechnical Commission*. "Desenvolvimento de Normas." https://www.iec.ch/standards-development
[21] IPVM. "*Triagem de ônibus em Buenos Aires viola Normas da IEC e as próprias instruções da Dahua*." Junho de 2020. https://ipvm.com/reports/buenos-aires-bus
[22] Enquanto câmeras Axis (Suécia) custam em média US$372, câmeras Hikvision (China) custam cerca de US$37. Veja mais informações em: IPVM. "*Montagem no Brasil Alavanca Expansão Local da Hikvision.*" Julho de 2020. https://ipvm.com/reports/hik-brazil?code=allow

drones.[23]

Em São Paulo, o governador João Doria recebeu pelo menos R$ 8,5 milhões (cerca de US$ 1,5 milhões) como "presentes" para o programa Câmeras Municipais. As doações vieram de várias empresas chinesas: **Huawei, Hikvision, Dahua**, e **ZTE**. Através dessas doações, funcionários implantaram pelo menos 4.000 câmeras de vigilância. Não está claro se elas integram a tecnologia de reconhecimento facial.[24]

A penetração dessas empresas no mercado brasileiro vem sendo particularmente notável. A Hikvision é atualmente a única fabricante estrangeira de vigilância por vídeo com operação de montagem na zona franca de Manaus.[25] Além disso, de acordo com uma entrevista realizada com uma autoridade local, em 2020 a Hikvision suplantou a empresa britânica **Facewatch** para implementação da tecnologia de reconhecimento facial em Campina Grande (Paraíba, Brasil).

Além disso, algumas empresas brasileiras que fornecem equipamentos de vigilância usam essas empresas como suas fabricantes. Um bom exemplo é a empresa **Intelbras**, que é líder no Brasil em tecnologias de vigilância por vídeo. Desde 2018, ela tem um contrato com Dahua, no qual esta última tem prioridade no fornecimento de equipamentos de CFTV.[26]

Algo semelhante está acontecendo no **Equador**. A **Full Tecnologia FullTec CIA. LTDA.** é uma empresa local que ganhou mais de US$ 1 milhão vendendo produtos Hikvision para o governo nacional e os governos municipais. As vendas da Hikvision são direcionadas a grandes cidades, como Guayaquil e Quito, e municípios vizinhos, como Nayón, Pedro Moncayo, e Daule. Também descobrimos que ela vende para outras cidades do Equador, como Quevedo, Ambato, Pelileo, Guano, Salcedo, Santa Elena e Rumiñahui, todas pertencentes ao circuito descentralizado.[27][28][29][30]

---

[23] Departamento de Segurança. “Segurança para a festa do Divino terá câmeras de reconhecimento facial” (em português) Maio de 2019.
http://www.mogidascruzes.sp.gov.br/noticia/seguranca-para-a-festa-do-divino-tera-cameras-com-reconhecimento-facial#:~:text=A%20quermesse%20da%20Festa%20do,custos%20para%20a%20administra%C3%A7%C3%A3o%20municipal

[24] Bruno Ribeiro. “Doações chinesas para Dória somam R$8.5 milhões” (em português). Julho de 2017.
https://sao-paulo.estadao.com.br/noticias/geral,doacoes-de-chineses-a-sp-somam-r-8-5-mi,70001912058

[25] Robert Gordon. “Montagem no Brasil potencializa a expansão local da Hikvision ". Julho de 2020.
https://ipvm.com/reports/hik-brazil

[26] Contrato social da Intelbras também declaram que a Dahua tem atualmente 10% dos ativos da empresa brasileira. Veja mais informações em: Intelbras. “Prospecto Preliminar da Oferta Pública de Distribuição Primária e Secundária de Ações Ordinárias de Emissão da Intelbras” (em português). 2020.
https://ww69.itau.com.br/fileserver/relatorios/intelbras-sa-ind-telecom-eletro-bra-prospecto-pre.pdf

[27] Sistema de Compras Públicas Oficial. SIE-GADMPM-020-2018. Dezembro de 2018.
https://www.compraspublicas.gob.ec/ProcesoContratacion/compras/PC/informacionProcesoContratacion2.cpe?idSoliCompra=BRlmsq33mpYSQbPbDK9oJTzqZSQXsCmgrOSChp_ddnA,

[28] Sistema de Compras Públicas Oficial. SIE-GADMA-118-2018. Novembro de 2018.
https://www.compraspublicas.gob.ec/ProcesoContratacion/compras/PC/informacionProcesoContratacion2.cpe?idSoliCompra=iL00ryPdwU_lpDLbghrZNhbEP-6oyJtDtUbINhNnX98,

[29] Sistema de Compras Públicas Oficial. SIE-GADPN-02-2019N. Dezembro de 2019.
https://www.compraspublicas.gob.ec/ProcesoContratacion/compras/PC/informacionProcesoContratacion2.cpe?idSoliCompra=SSGg5qeThJ2cPtAXO6hZeeB7BB8WojteF3tmWYZYM2s,

[30] Sistema de Compras Públicas Oficial. SIE-GADMQ-006-2019. Dezembro de 2019.
https://www.compraspublicas.gob.ec/ProcesoContratacion/compras/PC/informacionProcesoContratacion2.cpe?idSoliCompra=bCDa1cd5ztLy9wcH_d5PXToQ4JsCMfZg_iiQ1xdj-zQ,

Em 2019, a empresa **ANDEANTRADE S.A.** forneceu ao centro histórico do Distrito Metropolitano de Quito as câmeras de vigilância por vídeo da Hikvision com reconhecimento facial, por mais de US$602.976,00.[31]

Histórico de direitos humanos da Hikvision e Dahua

É essencial que a Hikvision e a Dahua sejam transparentes por muitas razões. Como já discutimos, essas empresas têm uma presença ampla na região da América Latina, vendendo com sucesso tecnologia altamente controversa para governos nacionais e locais a preços baixos. Como observado acima, algumas dessas tecnologias podem não ter um bom desempenho [32]ou atender os padrões das empresas ou os padrões básicos da indústria.[33] Mesmo assim, **governos da América Latina estão comprando delas, apresentando tecnologia invasiva e imprecisa ao público em geral como uma solução para o crime, um argumento que é, na melhor das hipóteses, enganoso.**

Hikvision e Dahua também ganharam uma vantagem competitiva na região oferecendo produtos e serviços gratuitos, aproveitando a frágil economia de muitos países da América Latina para testar seus sistemas de vigilância junto aos cidadãos. Embora nosso objetivo neste relatório não seja analisar as práticas de concorrência desleal, a questão merece atenção devido aos recentes escândalos associados ao comportamento monopolista e explorador das empresas da Big Tech.

Ambas as empresas estão implicadas em violações dos direitos humanos. Cada uma delas recebeu contratos de mais de US$ 1 milhão para projetos de vigilância apoiados pelo governo em Xingjian, na China[34], desde 2016. De acordo com uma investigação do The Wall Street Journal,[35] autoridades de Xingjian estão usando tecnologia de vigilância para perseguir a etnia muçulmana uyghur,[36] o que levou a sanções e críticas dos governos da Noruega,[37] da Dinamarca,[38] e dos Estados Unidos.[39]

---

[31] Sistema de Compras Públicas Oficial. SIE-EMS-003-2019. Agosto de 2019. https://www.compraspublicas.gob.ec/ProcesoContratacion/compras/PC/informacionProcesoContratacion2.cpe?idSoliCompra=FcPNLZ70povlg7KbsiZ-AnBh7MrENuiMXThS2d0Y4fI,

[32] IPVM. "Triagem de Temperatura Hikvision Testada." Maio de 2020. https://ipvm.com/reports/hikvision-temperature-test

[33] IPVM. "Triagem da Dahua em Ônibus de Buenos Aires Viola as Normas da CEI e as Instruções da Própria Dahua." Junho de 2020. https://ipvm.com/reports/buenos-aires-bus

[34] IPVM. "*Dahua e Hikvision recebem mais de US$1 bilhão em projetos apoiados pelo governo em Xingjian*." Abril de 2018. https://ipvm.com/reports/xinjiang-dahua-hikvision

[35] The Wall Street Journal. "Doze dias em Xingjian: Como o Estado de Vigilância da China supera a vida cotidiana." Dezembro de 2019. https://www.wsj.com/articles/twelve-days-in-xinjiang-how-chinas-surveillance-state-overwhelms-daily-life-1513700355

[36] Veja mais informações em: https://campaignforuyghurs.org/

[37] Business & Human Rights Resource Centre. "*O conselho de ética do fundo soberano norueguês recomendou a venda das ações da Hikvision por questões de direitos humanos sobre o papel da empresa na vigilância de massa.*" Setembro de 2020 https://www.business-humanrights.org/en/latest-news/norwegian-wealth-funds-ethics-council-recommends-divestment-from-hikvision-based-on-human-rights-concerns-over-co-role-in-mass-surveillance/

[38] Business & Human Rights Resource Centre. "*O fundo de pensão dinamarquês AkademikerPension vende a sua participação na Hikvision devido às preocupações com os direitos humanos sobre o papel da empresa na vigilância em massa.*" Novembro de 2020 https://www.business-humanrights.org/fr/derni%C3%A8res-actualit%C3%A9s/danish-pension-fund-akademikerpension-divests-from-chinese-surveillance-equipment-maker-over-human-rights-concerns/

[39] Business & Human Rights Resource Centre. "EUA: Onze empresas chinesas acrescentadas à lista negra econômica por causa de alegações de uso de trabalho forçado de minorias étnicas." Julho de 2020 https://www.business-humanrights.org/en/latest-news/usa-eleven-chinese-firms-added-to-economic-blacklist-over-allegations-of-using-forced-labour-of-ethnic-minorities/

Além disso, a Dahua já teve várias vulnerabilidades em seu sistema de nuvem.[40]Um pesquisador independente descobriu uma porta dos fundos para sistemas Dahua que permitia o acesso remoto não autorizado através da web. A Hikvision teve uma vulnerabilidade semelhante em 2017 com suas câmeras IP.[41] A Comissão Federal de Comunicações dos EUA recentemente adicionou a Hikvision e a Dahua a uma lista de empresas que representam uma ameaça à segurança nacional dos EUA, encorajando as empresas americanas a evitar o uso de produtos por essas empresas.[42]

⇛ Cellebrite

Nome da Empresa	**Cellebrite DI Ltd.**
Matriz	Petah Tikva, Israel
Países onde Atua	Global
Países onde suas tecnologias de vigilância são utilizadas entre Argentina, Brasil e Equador	Argentina
Fundada em	1999
Capital Aberto / Fechado	Private
Acionistas Principais	Suncorporation Ltd. (71.5%) Israel Growth Partners (24.41%)
Número de Funcionários	452 em 2019
Receita Anual	US$71.1 milhões em 2019

A **Cellebrite** é uma empresa israelense de inteligência digital e uma subsidiária da Suncorporation Ltd., uma empresa japonesa (cotada na Bolsa de Valores de Tóquio).[43] Ainda que seja complicado apontar uma data específica na qual as autoridades na **Argentina** começaram a utilizar a tecnologia da empresa, a presença da Cellebrite no país tem crescido de forma constante nos últimos cinco anos. Seus produtos são obtidos na Argentina através de dois dos principais revendedores locais: **Security Team Network S.A.** e **IAFIS Argentina S.A.** A Argentina ocupa a terceira posição nas Américas como mercado para o uso das licenças do Universal Forensic Extraction Device (UFED) da Cellebrite, que são exportadas para mais de 150 jurisdições.

[40] IPVM. "Vulnerabilidades Críticas na Nuvem da Dahua." Maio de 2020. https://ipvm.com/reports/dahua-cloud-vuln
[41] IPVM. "Exploração de backdoor da Hikvision." Setembro de 2017. https://ipvm.com/reports/hik-exploit
[42] *Federal Communications Commission*. "O GABINETE DE SEGURANÇA PÚBLICA E SEGURANÇA INTERNA ANUNCIA PUBLICAÇÃO DA LISTA DE EQUIPAMENTOS E SERVIÇOS COBERTOS PELA SEÇÃO 2 DA LEI DE REDES SEGURAS." WC *Arquivo número. 18-89*. Março de 2021 https://docs.fcc.gov/public/attachments/DA-21-309A1.pdf
[43] Veja mais informações no website da Suncorporation em https://www.sun-denshi.co.jp/eng/

Durante o início dos anos 2010, o Ministério da Justiça alocou fundos para dar início ao desenvolvimento de uma rede de Laboratórios Regionais de Investigação Forense em colaboração com o Ministério Público em todo o país. Em 2014, já existiam 13 laboratórios forenses utilizando a tecnologia da Cellebrite, especificamente a linha de produtos UFED[44] para extração de dados. De acordo com um documento oficial do Ministério da Justiça, entre as jurisdições que utilizavam esta tecnologia estão: Oficina de Gestão de Informação Tecnológica (OFITEC), Mercedes, Província de Buenos Aires; Laboratorio Forense de Comunicaciones Complejas, Mar del Plata, Província de Buenos Aires; Ciudad Autónoma de Buenos Aires; Entre Ríos; Mendoza; San Juan; San Luis; Formosa; Neuquén; Chubut; La Pampa; Corrientes; e Misiones.[45] No caso de La Pampa, além do UFED, eles tinham implementado o *add-on* CHINEX,[46] desenvolvido para realizar a extração de dados de telefones chineses não-padrão.

O uso dos produtos da Cellebrite se expandiu desde então para outras províncias. Em 2018, o Ministério Público em Salta atualizou suas licenças UFED 4PC e Touch por um total de US$23.000,00 em um contrato direto com a Security Team Network.[47]

Um dos principais usuários da tecnologia da Cellebrite a nível nacional na Argentina é a Gendarmerie Nacional (GNA). Dada sua competência federal, a GNA implantou produtos da Cellebrite em todo o país para equipar os laboratórios forenses.

Em Setembro de 2019, a GNA fechou um contrato direto com a Security Team Network S.A. totalizando US$643.900,00 para adquirir uma estação de trabalho para o desbloqueio de smartphones de alto nível. O produto UFED é mencionado apenas uma vez no detalhamento das especificações técnicas.[48] Em novembro, a Diretoria de Criminalística e Estudos Forenses da Gendarmerie adquiriu quatro licenças para o software "UFED 4PC". Segundo a Cellebrite, esse produto é usado para "extração, decodificação, análise, leitura e capacidade de gerenciamento" e pode ser executado em hardware personalizável pelo usuário.[49] A Gendarmerie adquiriu essas licenças por meio de concorrência pública, e acabou contratando novamente a Security Team Network por um valor total de 9.587.400 pesos (cerca de US$159.000,00 na época).[50]

Mais recentemente, a Gendarmerie atualizou essas licenças em junho de 2020, contratando

[44] Cellebrite. UFED: "O padrão da indústria para acesso aos dados de dispositivos digitais." https://cf-media.cellebrite.com/wp-content/uploads/2020/06/ProductOverview_Cellebrite_UFED_A4.pdf
[45] Ministério da Justiça e Direitos Humanos. "Laboratórios Regionais de Pesquisa Forense" (em espanhol). Agosto de 2014 http://www.saij.gob.ar/docs-f/ediciones/libros/Laboratorios_Regionales_de_Invest._Forense.pdf
[46] Cellebrite. "Telefones chineses for a do padrão agora acessíveis com o Kit UFED Chinex." Setembro de 2019 https://www.cellebrite.com/en/blog/non-standard-chinese-phones-now-accessible-with-ufed-chinex-kit/
[47] Ministério Público, Província de Salta. Arquivo número 130-17.933/17
[48] Arquivo número 37/105-0815-CDI19. https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhwbeNKAPenXR8IR3ih5YSXR79Wk8x7mmrwOCg9|4XRUnx0kCgm3oU8Rx5zyjpByUn|6t4HsX9ox3IM|fHZHcPGbahOwPe58NWP7IaFH5JcDkQ==
[49] Cellebrite. 4PC. https://cf-media.cellebrite.com/wp-content/uploads/2019/06/DataSheet_4PC_A4-print.pdf
[50] Diretoria de Criminalística e Estudos Forenses. "AQUISIÇÃO DE SOFTWARE UFED 4PC PARA A DIRETORIA DE CRIMINALÍSTICA E ESTUDOS FORENSES." File Nº 37/105-0041-LPU19. Julho de 2018 https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhy5xycgc2RiGO0seBx38Zrkqrf44NYcUHOQXWAZSx|FbiACHf8VyMdhxK5ugYZKg/ha7EWhWl7fjuQEoJmuXixefeg9/er7CV2Q|P|HNndQKg==

diretamente a Security Team Network por um total de US$ 132.116,00.[51]

De acordo com um jornalista que preferiu permanecer anônimo, forças federais de segurança (incluindo a Gendarmerie Nacional, a Polícia de Segurança Aeroportuária, a Polícia Federal e a Guarda Costeira) têm no total 35 produtos UFED e, contando todos os Ministérios Públicos e outros órgãos de aplicação da lei ("Law Enforcement Agencies – LEAs"), há 350 licenças sendo utilizadas no país.[52] O principal usuário é a Gendarmerie, que trabalha em todas as províncias e está atualmente melhorando seus laboratórios forenses digitais, usando produtos como O UFED Cloud da Cellebrite, o Pathfinder UFED e o Analisador Físico UFED.[53] A GNA também empresta seus equipamentos quando colabora em investigações criminais, por exemplo, no caso da província de Entre Ríos.[54]

Em Buenos Aires, o Ministério Público adquiriu uma licença UFED 4PC junto com o software Physical Analyzer[55]em 2019, através de um contrato direto com a Security Team Network no valor de 440.109,00 pesos (cerca de US$10.500,00 na época). Esses produtos foram cedidos ao Centro de Investigações Judiciais.[56] Esse centro já havia renovado uma licença para outro produto, o UFED Cloud Analyzer, em 2017, também contratado diretamente com a mesma empresa local.[57]

Em Agosto de 2020, o Ministério Público na província de Santa Fé assinou um contrato direto com a empresa local IAFIS Argentina S.A. para renovar quatro licenças UFED Touch 2 por um ano e adquirir três novas licenças para UFED 4PC, no total de US$96.226,00.[58]

Em dezembro de 2020, a Polícia de Segurança Aeroportuária assinou um contrato direto com a IAFIS Argentina S.A. para atualizar e modernizar suas licenças UFED, no valor de 8.057.111,00 pesos (cerca de US$90.784,00). O contrato incluiu a renovação de duas licenças UFED 4PC Ultimate e duas UFED Touch 2 Ultimate[59] por dois anos, bem como uma troca de hardware de dois dispositivos Touch I por dois

[51] Diretoria de Criminalística e Estudos Forenses. "SERVIÇO DE RENOVAÇÃO E ATUALIZAÇÃO DE LICENÇA DE SOFTWARE FORENSE UFEC TOUCH I PARA UFED 4PC." Arquivo número 37/105-0422-CDI20. Março de 2020 https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhyrV/4BRRj7a9qf3aG8azk|h3K/KAn7jb/h6aPDkgsy3caJklV5dh/l98fSQHDGyecUZqnGVTQz3UXLzeKrU0hskSjg8CnHW3bp5dO0tjSzbg==

[52] Clarín. "Detectives telefônicos: segredos do sistema que abre os telefones celulares e resolve as causas mais complexas" (em espanhol). Novembro de 2020 https://web.archive.org/web/20201114090956/https://www.clarin.com/policiales/detectives-telefonos-secretos-sistema-abre-celulares-resuelve-causas-complejas_0_U-d0fZd2m.html

[53] Cellebrite. "A Gendarmaria Nacional da Argentina está superando barreiras de tempo e distância com a inteligência digital" (em espanhol). Julho de 2020 https://www.cellebrite.com/es/blog-es/la-gendarmeria-nacional-de-argentina-esta-superando-las-barreras-de-tiempo-y-distancia-con-inteligencia-digital/

[54] El Entre Ríos. "Os dispositivos UFED, os novos equipamentos disponíveis para a polícia de Concordia e a Gendarmerie no Paraná" (em espanhol). Fevereiro de 2019 https://www.elentrerios.com/actualidad/dispositivos-ufed-el-nuevo-equipamiento-con-el-que-cuenta-la-polica-de-concordia-y-la-gendarmera-en-paran.htm

[55] Cellebrite. *Physical Analyzer*. https://www.cellebrite.com/en/physical-analyzer/

[56] Governo da Cidade Autônoma de. Provimento número 65/UOA/19. Julho de 2019. https://documentosboletinoficial.buenosaires.gob.ar/publico/ck_PJ-DIS-MPF-UOA-65-19-5660.pdf

[57] Ministério Público da Província de Buenos Aires. Provimento UOA número 45/2017. Setembro de 2017. https://mpfciudad.gob.ar/storage/archivos/Disposici%C3%B3n%20UOA%20N%C2%BA%2045-17%20AI%2030-00036938%20Adjudicacion%20SECURITY%20TEAM%20NETWORK%20S.A.%20-Ufed%20Cloud-.pdf

[58] Ministério Público da Província de Santa Fé. Arquivo número FG-000303-2020. Agosto de 2020 https://www.mpa.santafe.gov.ar/regulations_files/5f328fd04126a_Resoluci%C3%B3n%20N%C2%B0%20274.pdf

[59] Cellebrite. *UFED Ultimate*. https://www.cellebrite.com/en/ufed-ultimate/

UFED Touch 2.[60]

O Ministério da Segurança começou a assinar acordos de cooperação com mais de 15 empresas de tecnologia, incluindo a Cellebrite, no final de 2020. Esses acordos incluem treinamentos e compartilhamento de informações para melhorar a capacidade dos LEAs nas investigações judiciais que envolvem provas digitais.[61] Em 3 de novembro de 2020, apresentamos um pedido com base na liberdade de informação ao Ministério para que este se pronunciasse sobre esses contratos. A resposta oficial que o Ministério deu em dezembro de 2020 afirma que "não foi feita qualquer assinatura de qualquer dos acordos referidos no pedido de informações públicas em exame, razão pela qual há documentos sobre a mesma que possam ser levados ao conhecimento da parte interessada".

Histórico de direitos humanos da Cellebrite

A Cellebrite afirma vender sua tecnologia exclusivamente a governos e agências de aplicação da lei e, declaradamente, comercializa com as autoridades governamentais que interrogam pessoas que pedem asilo.[62] [63]

Em 2016, a Diretoria Geral Anticorrupção e Segurança Econômica e Eletrônica de Bahrain e a Diretoria de Investigações Criminais, declaradamente, utilizaram o UFED da Cellebrite para investigar e processar dissidentes.[64] Segundo uma investigação conduzida pelo advogado Eitay Mack em Israel, a empresa vendeu tecnologia forense aos governos da Venezuela, Belarus, Rússia, bem como para a Indonésia, que são conhecidos por reprimir a dissidência política da comunidade LGTBQ.[65]

Após o vazamento de documentos internos em 2017, foi revelado que Cellebrite também estava conversando com órgãos de aplicação da lei (LEAs) na Turquia e nos Emirados Árabes Unidos.[66] Além disso, a polícia de Mianmar usou a mesma tecnologia para prender dois jornalistas em 2019[67] e a polícia de Hong Kong supostamente a usou para assediar e investigar os manifestantes pró-democracia em

[60] Polícia de Segurança Aeroportuária. "Renovação de licenças e melhoria dos equipamentos UFED 4PC e UFED TOUCH, para Exclusividade." Arquivo número 279-0027-CDI20. Novembro de 2020
https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhy3iTxQqkwwChRpn2XPxXCSk5uij|LSdq2DmF5S3lGnqlsUbG2uGBeZPrbB8BhNUcLFrujs6LrFUaU3GDH8dDYrJv/eOuj/ve1TCcZ2AXWpaw==
[61] Governo da Argentina. "*Acciones para mayor eficiencia en la investigación criminal en el ámbito digital*." Outubro de 2020.
https://www.argentina.gob.ar/noticias/acciones-para-mayor-eficiencia-en-la-investigacion-criminal-en-el-ambito-digital
[62] Privacy International. "A empresa de vigilância Cellebrite encontra uma nova oportunidade de exploração: Espionagem de candidatos a asilo." Abril de 2019.
https://privacyinternational.org/long-read/2776/surveillance-company-cellebrite-finds-new-exploit-spying-asylum-seekers
[63] Access Now. "O que a empresa espiã Cellebrite não pode esconder dos investidores." Maio de 2021.
https://www.accessnow.org/what-spy-firm-cellebrite-cant-hide-from-investors/
[64] The Intercept. "*Phone-Cracking Cellebrite Software Used to Prosecute Tortured Dissident.*" Dezembro de 2016.
https://theintercept.com/2016/12/08/phone-cracking-cellebrite-software-used-to-prosecute-tortured-dissident/
[65] Haaretz. "Invasão do Grindr? A Cellebrite de Israel vendeu a tecnologia de invasão de telefones para a Indonésia." Novembro de 2020. https://www.haaretz.com/israel-news/tech-news/.premium.HIGHLIGHT-hacking-grindr-israel-s-cellebrite-sold-phone-s py-tech-to-indonesia-1.9281160
[66] Vice. "Dados Sugerem que Cellebrite Vendeu Tecnologia de Invasão de Telefones para Regimes Repressivos." Janeiro de 2017. https://www.vice.com/en/article/aekqjj/cellebrite-sold-phone-hacking-tech-to-repressive-regimes-data-suggests
[67] *The Washington Post*. "Empresas de tecnologia de segurança chegaram à Mianmar. Ferramentas de uma empresa foram usadas contra dois jornalistas." Maio de 2019.
https://www.washingtonpost.com/world/asia_pacific/security-tech-companies-once-flocked-to-myanmar-one-firms-tools-were-used-against-two-journalists-/2019/05/04/d4e9f7f0-5b5d-11e9-b8e3-b03311fbbbfe_story.html

2020.[68] O Comitê para Proteção de Jornalistas revelou recentemente que o governo de Botswana está usando a tecnologia da Cellebrite para revistar aparelhos de jornalistas e procurar fontes.[69] Alguns jornalistas dizem ter sido torturados.[70] Relatos adicionais revelam que ferramentas da Cellebrite estão sendo vendidas para a Nigéria, Bangladesh, Índia, Arábia Saudita, e Vietnã.[71]

Defensores dos direitos humanos apresentaram uma petição judicial para que o Ministério da Defesa de Israel suspenda a exportação da Cellebrite para Hong Kong, Rússia e Belarus.[72]Em outubro de 2020, a Cellebrite anunciou que deixará de vender sua tecnologia para a China e Hong Kong.[73] Em março de 2021, a Cellebrite também anunciou que ainda vai parar de vender para a Rússia e Bielorrússia. [74]

⇛ Huawei e ZTE

Nome da Empresa	**Huawei Technologies Co., Ltd.**
Matriz	Shenzhen, República Popular da China
Países onde Atua	Global
Países onde suas tecnologias de vigilância são utilizadas entre Argentina, Brasil e Equador	Argentina, Brasil
Fundada em	1987
Capital Aberto / Fechado	Capital Fechado
Acionistas Principais	Controle total dos seus funcionários
Número de Funcionários	194.000 funcionários
Receita Anual	RMB 858.8 bilhões (US$132 bilhões) em 2019

[68] *The Jerusalem Post*. "Ativistas a favor da democracia em Hong Kong em Israel: Parem de exportar tecnologia para a polícia." Julho de 2020. https://www.jpost.com/israel-news/hong-kong-democracy-activists-to-israel-stop-exporting-tech-to-police-636918#/
[69] Comitê para Proteção de Jornalistas, "Equipada por empresas israelenses nos EUA, a polícia de Botswana revista telefones à procura de fontes." Maio 2021. https://cpj.org/2021/05/equipped-us-israeli-firms-botswana-police/; Comitê para Proteção de Jornalistas, "Polícia de Botswana usa a tecnologia israelense Cellebrite para revistar telefone de outro jornalista." Julho de 2021. https://cpj.org/2021/07/botswana-cellebrite-search-journalists-phone/
[70] Id.
[71] Access Now. "O quê a empresa de espionagem Cellebrite não consegue esconder dos investidores." Maio de 2021. https://www.accessnow.org/what-spy-firm-cellebrite-cant-hide-from-investors/; Haaretz, "O quê o Vietnã está fazendo com a tecnologia israelense de invasão de telefones." Julho de 2021. https://www.haaretz.com/israel-news/tech-news/.premium-what-vietnam-is-doing-with-israel-s-phone-hacking-tech-1.10003831
[72] *MIT Technology Review*. "Empresa israelense de invasão de telefones em briga judicial para vendas a Hong Kong." Agosto de 2020.https://www.technologyreview.com/2020/08/25/1007617/israeli-phone-hacking-company-faces-court-fight-over-sales-to-hong-kong/; Haaretz, "Empresa israelense de invasão de telefones Cellebrite suspende vendas para Rússia, Bielorrússia, após Relatório Haaretz Report." Março de 2021. https://www.haaretz.com/israel-news/.premium-israeli-phone-hacking-firm-cellebrite-halts-sales-to-russia-after-haaretz-report-1.9633312
[73] Cellebrite. "Cellebrite deixará de vender seus produtos de inteligência digital em Hong Kong e na China." Outubro de 2020. https://www.cellebrite.com/en/cellebrite-to-stop-selling-its-digital-intelligence-offerings-in-hong-kong-china/
[74] Cellebrite, "Cellebrite Suspende a Venda de seus Produtos de Inteligência Digital na Federação Russa e Bielorrússia." Março de 2021. https://www.cellebrite.com/en/cellebrite-stops-selling-its-digital-intelligence-offerings-in-russian-federation-and-belarus/

Nome da Empresa	ZTE Corporation
Matriz	Shenzhen, República Popular da China
Países onde Atua	Global
Países onde suas tecnologias de vigilância são utilizadas entre Argentina, Brasil e Equador	Argentina, Brasil
Fundada em	1985
Capital Aberto / Fechado	Cotada nas Bolsas de Valores tanto de Hong Kong como de Shenzhen
Acionistas Principais	ZTE Holdings (21.85%), Hong Kong Securities Clearing Company Limited (16.31%)
Número de Funcionários	70.066 funcionários considerando o grupo (60.514 funcionários considerando a empresa) em 2019
Receita Anual	RMB 90.737 bilhões (US$13.94 bilhões) em 2019

Ambas as empresas chinesas, **Huawei Technologies Co.** e **ZTE Corporation**, oferecem uma ampla gama de soluções tecnológicas. Um dos serviços que elas oferecem é a tecnologia e os sistemas para a construção do que é conhecido como "cidades inteligentes". Cada uma delas se envolve ativamente com governos locais em toda a América Latina para fornecer ferramentas para segurança pública.

Em Julho de 2020, a ZTE desembarcou na província de Jujuy, **Argentina**. O governador, Gerardo Morales, recebeu o vice presidente da ZTE Corporation e o gerente geral da ZTE Argentina, Hua Xinhai e Dennis Wang. Eles chegaram a um acordo para implantar um programa chamado "Jujuy Seguro e Interconectado", para o qual a província recebeu em março de 2020 um empréstimo do banco BBVA de Hong Kong de US$24.146.142,00[75]. A ZTE fechou o acordo por US$30 milhões para cumprir parte dessa agenda, fornecendo a instalação de câmeras, centros de monitoramento, serviços de emergência e infraestrutura de telecomunicações.[76] De acordo com o governador Morales, agora Jujuy "será tão segura quanto a China". Com base na lei de liberdade de informação pedimos mais detalhes em 11 de novembro de 2020, mas não recebemos uma resposta apesar de termos cumprido o prazo legal.

Em Abril de 2018, Alfredo Cornejo, governador da província de Mendoza, Argentina, reuniu-se com o vice-presidente de vendas da Huawei, Tony Sze.[77] O objetivo da reunião, de acordo com reportagens da

[75] Diário Oficial. Decreto 207/2019. Março de 2019 https://www.boletinoficial.gob.ar/detalleAviso/primera/203703/20190320
[76] Reuters. “Seguro como a China': Na Argentina, a ZTE encontra um comprador ávido por tecnologia de vigilância.” Julho de 2019. https://www.reuters.com/article/us-argentina-china-zte-insight-idUSKCN1U00ZG
[77] Website oficial de Mendoza. “O governador se reuniu com representantes da Huawei na América Latina” (em espanhol). Abril de 2018. https://www.mendoza.gov.ar/prensa/el-gobernador-se-reunio-con-representantes-de-huawei-en-latinoamerica/

mídia, era discutir a aquisição de tecnologia para reconhecimento facial, geolocalização e gestão de big data para segurança pública. Organizações da sociedade civil incluindo a Access Now e ADC responderam com uma carta ao governador[78] pedindo o fim das negociações privadas e uma discussão pública sobre o assunto. Infelizmente, o governador não divulgou mais informações.

A Huawei também está presente na região através de uma rede de concessionários e revendedores. Um exemplo está na Bahia no **Brasil**, onde as autoridades escolheram a filial brasileira da rede espanhola **El Corte Ingles** para uma "disposição contratual adicional" para o "Consórcio Bahia Segura 2014" fornecer o hardware (câmeras) e software de reconhecimento facial da Huawei. O provedor brasileiro de telecomunicações "**Oi**" também assinou um contrato com a Huawei para vender tecnologia de reconhecimento facial no Brasil.[79] As autoridades testaram esta tecnologia no público durante os carnavais no Rio de Janeiro em 2019. O sistema captou aproximadamente três milhões de imagens faciais, mas apenas 10 prisões foram feitas com base no uso do sistema, segundo o porta-voz da Polícia Militar do Rio de Janeiro, Coronel Mauro Fliess.[80]

Para acelerar a aquisição de sua tecnologia e testar suas capacidades, a Huawei também doou a Campinas, no estado de São Paulo, os equipamentos necessários para um projeto de "cidade inteligente". Campinas é agora conhecida por seu "laboratório aberto", que inclui tecnologia de reconhecimento facial invasora da privacidade, levando à sua designação como a "cidade mais inteligente" do Brasil.[81]

Histórico de direitos humanos da ZTE e Huawei

ZTE e Huawei há muito tempo são conhecidas por trabalharem com regimes que violam os direitos humanos. Em 2013, quando o grupo de defesa Bolo Bhi pediu a ambas as empresas para não participarem na construção de um firewall de censura na internet contra o governo do **Paquistão**, elas optaram por ignorar os impactos dos direitos humanos de seus produtos e emitir declarações sumárias sobre a priorização das leis "locais" em relação às leis e normas internacionais de direitos humanos.[82] Naquele mesmo ano, a Reflets.Info relatou que a ZTE, juntamente com a Hewlett Packard, estavam colaborando com a Telecommunications Infrastructure Co. (TCI), provedor de serviços de Internet estatal do Irã, para ajudar a limitar o tipo de informação que os iranianos podem acessar on-line.[83]

---

[78] ADC. " Defensores dos direitos fundamentais pedem ao governo de Mendoza que interrompa a compra de tecnologia de vigilância em massa " (em espanhol). Julho de 2018. https://adc.org.ar/2018/07/13/defensores-de-derechos-fundamentales-piden-al- gobierno-de-mendoza-que-detenga-la-compra-de-tecnologia-de-vigilancia-masiva/

[79] Folha de S. Paulo. “Chinesa Huawei faz Parceria com a Oi para Câmeras de Reconhecimento Facial” (em português). Outubro de 2018. https://www1.folha.uol.com.br/tec/2018/10/chinesa-huawei-faz-parceria-com-oi-para-cameras-de-reconhecimento-facial.shtml

[80] Defesanet. “Reconhecimento Facial - No Carnaval do Rio identificou 8 mil pessoas de interesse” (em português). Maio de 2019. https://www.defesanet.com.br/tecdi/noticia/32851/Reconhecimento-Facial---No-Carnaval-do-Rio-identificou-8-mil-pessoas-de-interesse/

[81] The Rio Times. “Campinas é a cidade mais "inteligente" e mais conectada do Brasil, segundo ranking não-oficial.” Setembro de 2019. https://riotimesonline.com/brazil-news/brazil/life-brazil/campinas-is-the-smartest-and-most-connected-city-in-brazil/

[82] Access Now. “Promessas quebradas: Paquistão anuncia planos para lançar um firewall de censura, possivelmente com tecnologia chinesa.” Janeiro de 2013. https://www.accessnow.org/broken-promises-pakistan-announces-plans-to-launch-censorship-firewall-poss/

[83] Reflets.Info. “ZTE e HP unidas para uma internet Halal na terra dos mulás” (em francês). Junho de 2013. https://reflets.info/articles/zte-et-hp-unis-pour-un-halalternet-au-pays-des-mollahs

Em 2008, o então presidente venezuelano Hugo Chávez enviou funcionários do Ministério da Justiça para visitar a ZTE. Eles aprenderam como a China, através do uso de cartões inteligentes, estava desenvolvendo um sistema que ajudaria Pequim a monitorar o comportamento social, político e econômico dos indivíduos. Após 10 anos, o **governo venezuelano** contratou a ZTE por US$ 70 milhões para implantar um programa similar, o "carnet de la patria", ou licença da pátria. Os cartões estão sendo usados em campanhas para influenciar as decisões de votação,[84] dar subsídios para alimentos, fornecer assistência médica e administrar outros programas sociais dos quais a maioria dos venezuelanos depende para sobreviver.[85] Esse sistema de cartões inteligentes despertou o alarme de cidadãos e ativistas e organizações de direitos humanos devido ao risco claro de abuso do governo, invasão de privacidade e controle da comunidade. Após sua implementação, o banco de dados "carnet de la patria" foi invadido,[86] e, em 2018, o governo utilizou os cartões da pátria e os dados por trás deles para identificar as pessoas que não votaram. Também tornou os cartões obrigatórios para obter benefícios do governo e para comprar combustível a preços subsidiados.

A Huawei também tem estado sob muito escrutínio da mídia nos últimos anos. Em 2019, uma investigação *do Wall Street Journal*[87] mostrou que técnicos da empresa, em pelo menos dois casos, ajudaram pessoalmente os governos de **Uganda** e **Zâmbia** a espionar seus opositores políticos, inclusive interceptando suas comunicações codificadas e mídias sociais, e usando dados de telefones celulares para rastrear seu paradeiro.

Em junho de 2020, uma investigação conduzida pela *Reuters* mostrou que a Huawei vendeu ao governo iraniano pelo menos 1,3 milhões de euros em equipamentos de computador embargados da Hewlett-Packard e se esforçaram muito para esconder isso.[88] Em dezembro do mesmo ano, a IPVM encontrou um documento "confidencial" hospedado publicamente no próprio site europeu da Huawei, que foi apagado pouco tempo depois. Esse documento mostrou como a Huawei testou um software de reconhecimento facial que poderia enviar "alarmes Uighur" automatizados às autoridades **governamentais chinesas** quando seus sistemas de câmera identificassem membros desse grupo minoritário oprimido.[89]

Esse e outros casos preocupantes levaram a **Suécia** a proibir equipamentos de telecomunicações da Huawei e da ZTE em sua rede 5G,[90] e outras nações europeias tomaram ou estão considerando tomar medidas semelhantes.

---

[84] BBC News. “Eleições na Venezuela: quais são os pontos vermelhos e por que Henri Falcón acusa Maduro de "comprar votos" (em espanhol). Maio de 2018. https://www.bbc.com/mundo/noticias-america-latina-44192915

[85] Reuters. “Como a ZTE ajuda a Venezuela a implementar o controle social no estilo chinês” (em espanhol). Novembro de 2018. https://www.reuters.com/investigates/special-report/venezuela-zte-es/

[86] AlbertoRodNews conta no Twitter. https://twitter.com/AlbertoRodNews/status/1070733400372326401

[87] *The Wall Street Journal*. “Técnicos Huawei ajudaram os governos africanos a espionar os opositores políticos.” Agosto de 2019. https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017

[88] Reuters. “Exclusivo: Huawei escondeu operação comercial no Irã depois que a Reuters relatou ligações com o CFO.” Junho de 2020. https://www.reuters.com/article/us-huawei-iran-probe-exclusive-idUSKBN23A19B

[89] IPVM. “*Huawei / Megvii Uyghur Alarms*.” Dezembro de 2020. https://ipvm.com/reports/huawei-megvii-uygur

[90] Reuters. “A Suécia proíbe a Huawei, ZTE das próximas redes 5G.” Outubro de 2020. https://www.reuters.com/article/sweden-huawei-int-idUSKBN2750WA

⇛ NEC

Nome da Empresa	NEC Corporation
Matriz	Tóquio, Japão
Países onde Atua	Global
Países onde suas tecnologias de vigilância são utilizadas entre Argentina, Brasil e Equador	Argentina, Brasil
Fundada em	1899
Capital Aberto / Fechado	Cotada na Bolsa de Valores de Tóquio
Acionistas Principais	N/A
Número de Funcionários	Aproximadamente 110.000 em 2020
Receita Anual	JPY 3.095,2 bilhões (US$28.35 bilhões) em 2020

A **NEC** é um dos principais players da indústria de identificação biométrica digital global. Ela uma empresa com 122 anos de existência e mais de 110.000 funcionários. O gigante japonês da tecnologia (cotado na Bolsa de Valores de Tóquio) se apresenta[91] como a escolha para múltiplas agências governamentais em todo o mundo. Ela vem desenvolvendo tecnologia biométrica, como tecnologia facial, de íris, impressão digital, pareamento vascular do dedo e reconhecimento de voz, há mais de 50 anos, vendendo para 70 jurisdições.[92] As tecnologias da NEC formam a espinha dorsal do maior sistema biométrico do mundo, o Aadhaar da **Índia**, que registrou 1,3 bilhões de pessoas.[93] Nos **EUA**, mais de um terço das polícias estaduais e órgãos de aplicação da lei utilizam os sistemas biométricos da NEC desde 2019.[94]

Os serviços de alfândega e proteção de fronteiras dos EUA (*United States Customs and Border Protection - CBP*) usam o software de reconhecimento facial da NEC nos aeroportos,[95] e a tecnologia também tem

[91] NEC. Relatório Integrado 2020. https://www.nec.com/en/global/ir/pdf/annual/2020/ar2020-e_two.pdf
[92] NEC. Autenticação Biométrica. https://www.nec.com/en/global/solutions/biometrics/index.html
[93] NEC. "Identificação Biométrica para Mais de 1 Bilhão de Pessoas." Novembro de 2018. https://www.nec.com/en/case/uidai/index.html
[94] OneZero. "Cruzeiros de Carnaval, Delta e 70 países Usam uma empresa de reconhecimento facial da qual você nunca ouviu falar." Fevereiro de 2020 https://onezero.medium.com/nec-is-the-most-important-facial-recognition-company-youve-never-heard-of-12381d530510
[95] EFF. "Evite a Vigilância Optando pelo não Reconhecimento Facial nos Aeroportos." Abril de 2014. https://www.eff.org/deeplinks/2019/04/skip-surveillance-opting-out-face-recognition-airports
NEC. "A NEC testa o reconhecimento facial com o CBP (U.S. Customs and Border Protection) em voos selecionados do Aeroporto Internacional de Dulles (IAD)." Junho de 2017. https://www.nec.com/en/press/201706/global_20170627_03.html
Ventura Beat. "A Segurança Interna dos EUA usou o reconhecimento facial em mais de 43,7 milhões de pessoas." Fevereiro de 2020. https://venturebeat.com/2020/02/06/u-s-homeland-security-has-used-facial-recognition-on-over-43-7-million-people/

se expandido para estádios esportivos na **Colômbia**[96]e **Taiwan**.[97] A presença da NEC na América Latina está crescendo à medida que mais governos locais adotam a retórica de "cidade inteligente".

A NEC estabeleceu suas operações na **Argentina** em 1978, para realizar negócios no país e na região através de sua própria subsidiária local. **Em 2004, a empresa escolheu a NEC Argentina S.A. como Centro Regional de Desenvolvimento de Software para o mercado latino-americano da empresa**.[98] Desde 2006, a NEC tem sido a fornecedora oficial de tecnologia biométrica do Ministério do Interior e do Registro Nacional de Cidadãos (RENAPER). Graças a essa tecnologia, a RENAPER expandiu o uso de seu banco de dados biométricos para verificação e identificação para outros órgãos públicos, tais como a Secretaria de Migração, a Diretoria Nacional de Reincidência e o Ministério de Segurança, entre outros, o que também foi resultado da expansão do Sistema Federal de Identificação Biométrica para Segurança (SIBIOS).

Em 2017, o Departamento Nacional de Migração (DNM) assinou um contrato direto com a NEC para implementar portais automatizados de controle de passaportes, comumente chamados de "eGates", nos aeroportos internacionais da Argentina, no valor total de US$ 3.309.318,00.[99] Segundo os documentos de compra oficiais a NEC foi escolhida, uma vez que o Departamento Nacional de Migração já estava utilizando produtos AFIS[100] e NeoFace[101] da empresa para o reconhecimento de impressões digitais e facial, respectivamente.

Os portais eletrônicas foram implementados e utilizados pelo público em 2018 no aeroporto de Ezeiza, mas posteriormente foram expandidos para o aeroporto Aeroparque e o porto marítimo, ambos na Cidade de Buenos Aires.[102] O controle de fronteira utiliza esses pontos de verificação dos portais eletrônicos para substituir algumas interações humanas, usando impressões digitais e software de verificação facial para comparar uma varredura com os dados biométricos coletados de qualquer pessoa que entre ou saia do país. Os dados cadastrais do eGates são mantidos pela RENAPER.

Em 2019, o DNM assinou outro contrato direto com a NEC para um sistema biométrico de identificação de pessoas a partir de uma lista de vigilância (por exemplo, pessoas com restrições de viagem, aquelas procuradas pela INTERPOL, etc.), no valor total de 145.189.000 pesos (cerca de US$ 3 milhões de dólares na época).[103]

---

[96] NEC. “NEC contribui para a segurança dos estádios de futebol na Colômbia.” Outubro de 2016. https://www.nec.com/en/press/201610/global_20161012_03.html

[97] *Find Biometrics.* “Tecnologia de Reconhecimento Facial NEC Utilizada para proteger o estádio desportivo em Taipei.” Novembro de 2017. https://findbiometrics.com/nec-facial-recognition-sports-stadium-taipei-411022/

[98] NEC. History (em espanhol). https://ar.nec.com/es_AR/about/history/index.html

[99] Diretoria Geral de Administração. “FORNECIMENTO DE SOLUÇÃO AUTOASSISTIDA PARA PROCESSO DE IMIGRAÇÃO.” Arquivo número 21-0028-CDI17. Setembro de 2017. https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhxKmqLque6kMW1chJuEHzB2LvnmYI6tmgdCyJ7Ep7d490YZKW8ptaXbZVpysEhjsnNcElgEeF4JDcgYQh41LgX8fcn98cZ8e12qM5BlL50fqw==

[100] NEC. Fingerprint Identification. https://www.nec.com/en/global/solutions/biometrics/fingerprint/index.html

[101] NEC. NeoFace Watch. https://www.nec.com/en/global/solutions/biometrics/face/neofacewatch.html

[102] Home Office. “O Governo Nacional lançou os portões biométricos no aeroporto de Ezeiza” (em espanhol). Abril de 2018. http://www.migraciones.gov.ar/accesible/novedad.php?i=4019

[103] Diretoria Geral de Administração. “SOLUÇÃO INTEGRAL PARA IDENTIFICAÇÃO DE ESTRANGEIROS E CONTROLE BIOMÉTRICO DE RESTRIÇÕES.” File Nº 21-0002-LPU19. Fevereiro de 2019. https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhwfHN|0dYheEGyNBwGGvH3GL6jBhnOAiv5hg9nZ3JQi1tBQTuogGzD12zCv6XuNwuBmJTvQzJWApOOrz69pEW2MV9graYTQBzR11CtszG5T6w==

A solicitação especificou que o sistema deve ser compatível com o AFIS da RENAPER, para fazer consultas de identificação e verificação.

Entre 2017 e 2020, a RENAPER assinou vários contratos com a NEC para melhorar, atualizar e expandir ainda mais seus sistemas biométricos.[104]

Em dezembro de 2017, RENAPER e a antiga Secretaria de Modernização (atualmente a Secretaria de Inovação Pública, subordinada à Casa Civil) assinaram um acordo de cooperação para desenvolver um Sistema Nacional de Identidade Digital (SID).[105] O sistema usa o reconhecimento facial para validar a identidade das pessoas quando elas acessam certos serviços estatais e privados que utilizam sua Interface de Programação de Aplicações (API) e/ou kit de desenvolvimento de software (SDK). O SID foi lançado inicialmente em fase piloto, para testar seu uso por algumas empresas fintech para o processo de ativação de clientes e criação de conta bancária.[106] O elemento de reconhecimento facial do software do SID é o NeoFace Watch, adquirido com empréstimo do **Banco Mundial** no valor de US$ 834.403,90.

O Sistema de Identidade Digital da Argentina está sendo expandido para cobrir casos de uso múltiplo, além dos sistemas para serviços administrados pelo estado e fintechs. Em Julho de 2020, o Ministério do Interior assinou um acordo de cooperação com o Ministério da Educação para implementar o sistema nas universidades nacionais, para exigir que os estudantes validem suas identidades antes de fazer exames on-line.[107] Essa expansão está acontecendo apesar das preocupações com as falhas em seus algoritmos de reconhecimento facial.[108] Conforme este sistema se torna mais difundido, ele pode se tornar a principal maneira de validar a identidade, com risco de discriminação e exclusão de pessoas fora do sistema ou identificadas incorretamente, no acesso a serviços públicos. O governo tem minimizado essa ameaça, argumentando que o algoritmo de reconhecimento facial é configurado

[104] Divisão de Compras. “Contratação de serviços, licenças e produtos relacionados à plataforma biométrica RENAPER” Outubro de 2017. Arquivo número 78-0012-CDI17. https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhy7MmMdVUat6QKfRigU80UVxJmyaLvy67Tv2OgtO1qNBgGmFkKWbfpTnnfNopxo|oaRtWe20G7DjIP49UkgkEP896PfIoNb393/NEPZ2M5G7w== Divisão de Compras. “Solução abrangente de gestão centralizada de terminais para a gestão de licenças.” Arquivo número 78-0022-CDI18. Setembro de 2018. https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhzln331uwbedtWpuhJRVlkYFu5E0d6zTuIWgkUVrzCpo|kMsAHgU/dYCpNuyBnX9eXEW4riZstvHDV2ZqhmqPbCKquiSivEogUdA1Hk MNIlaA==Divisão de Compras. “EXPANSÃO E ATUALIZAÇÃO DA PLATAFORMA BIOMÉTRICA EXISTENTE RENAPER.” Arquivo nº 78-0028-CDI18. Dezembro de 2018.https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhzNiQxEvvRD1M4Hrw70Q0R4HTin1WArUVSpJfI4xYYgmiT77fvnNNo8g|PlFmMreDTagF|N6f4dFxdRnoYveFKYmjFSg8zlglzEUYmrvWH5MQ== Divisão de Compras. “SERVIÇO DE MANUTENÇÃO, SUPORTE E ASSISTÊNCIA TÉCNICA PARA O SISTEMA ABIS.” Arquivo nº 78-0029-CDI18. Dezembro de 2018. https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhyGzxXg3NEnQt|kEbGqFjvyvkPpcD27XbPjr B79ynaMSQETGHQanjODkHz9Nz64Gib/l6s/AI|E2d1ogkSzvDmTJdhqutPSEbqYs|rd|4j|BA== Divisão de Compras. “SERVIÇO INTEGRAL PARA MIGRAÇÃO E MANUTENÇÃO GERAL DE TODA A PLATAFORMA AFIS EXISTENTE.” Arquivo nº 78-0001-CDI20. Abril de 2020. https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhxz8ZzajHoNTGv6h2avQkrsmYw2yzxlp7rrnVp3vvETTUXRKICLVaNVdpDAhqicxls3LP/xxu4zp9sqDVtRdJGZ6ZJhpzdesliW7C8vB7JEGg==

[105] Home Office. “SID - Digital ID System” (em espanhol) https://www.argentina.gob.ar/interior/renaper/sid-sistema-de-identidad-digital

[106] "Fintech" ou tecnologia financeira, é um termo usado para designar novos negócios que desenvolvem serviços financeiros usando tecnologias digitais no núcleo dos seus produtos ou serviços.

[107] Ministério da Educação. “Novo sistema para validação da identidade de estudantes universitários” (em espanhol). Julho de 2020. https://www.argentina.gob.ar/noticias/nuevo-sistema-para-la-validacion-de-la-identidad-de-estudiantes-universitarios

[108] La Nación. “"Eu não vou com a sua cara": aplicativos discriminam?” (em espanhol). Setembro de 2019. https://www.lanacion.com.ar/tecnologia/no-me-gusta-tu-cara-discriminan-aplicaciones-nid2292711/

segundo as taxas padrão da NEC para falsos positivos e falsos negativos.[109]

A nível local, a NEC desenvolveu uma estreita relação com o governo de Tigre, cidade em Buenos Aires. O município tem usado a tecnologia da NEC para todo seu programa de vigilância urbana desde pelo menos 2016, começando com o CCTV, reconhecimento automático de placas (ALPR) e reconhecimento facial usando o NeoFace Watch.[110]

Em 2019, a Tigre reformulou sua infraestrutura de vigilância[111] ao lançar o NeoCenter, desenvolvido pela NEC para promover as possibilidades existentes na cidade.[112] Além das características mencionadas acima, o software de reconhecimento facial foi atualizado para rastrear as pessoas com mais precisão em espaços públicos, registrando caminhos de movimento para identificar onde alguém estava (seu histórico de viagens) e identificando "comportamentos suspeitos", através da análise do movimento tanto de pessoas quanto de veículos. A Tigre expandiu ainda mais sua tecnologia de vigilância em 2020, com a instalação de um totem com câmeras para reconhecimento facial.[113]

Quando Tigre anunciou o lançamento, a ADC apresentou[114] um pedido com base na liberdade de informação para saber mais sobre como a tecnologia está sendo utilizada e o enquadramento jurídico para seu uso. O governo local atrasou o processo e não respondeu, mesmo após vários acompanhamentos, indicando uma falta de transparência e responsabilidade.

Tigre tem sido um parceiro tão próximo da NEC que a empresa utiliza a cidade como um estudo de caso de marketing, mostrando as soluções que eles fornecem à cidade, incluindo tecnologia para colaboração do cidadão na segurança pública, análise de placas, reconhecimento facial, detecção de comportamento, construção de mapa de crime e coleta de provas e tecnologias de aprendizado de máquinas para análise de dados. A NEC afirma que Tigre está se tornando "um modelo de cidade segura na América Latina".[115]

A NEC também se envolveu na implantação de equipamentos de vigilância em aeroportos no **Brasil**.

O serviço aduaneiro federal do Brasil (Receita Federal), por exemplo, adquiriu a tecnologia de reconhecimento facial da NEC para identificar passageiros suspeitos de evasão de impostos de importação.[116] O sistema já está em operação em 14 aeroportos brasileiros desde 2016.[117]

---

[109] ADC. “Seu eu digital: Descobrindo as narrativas sobre identidade e biometria na América Latina” (em espanhol). Abril de 2019.https://adc.org.ar/informes/tu-yo-digital-descubriendo-las-narrativas-sobre-identidad-y-biometria-en-america-latina/
[110] NEC Corporation, canal corporativo no YouTube. “A cidade de Tigre” (em espanhol). Setembro de 2016. https://www.youtube.com/watch?v=5Lp9PWv0EQ0
[111] Município de Tigre. “Os Olhos de Tigre” (em espanhol). https://www.tigre.gob.ar/seguridad/cot
[112] Ámbito. “Tigre lançou um novo sistema de reconhecimento facial” (em espanhol). Maio de 2019. https://www.ambito.com/municipios/municipios/tigre-lanzo-un-nuevo-sistema-reconocimiento-facial-n5030978
[113] Município de Tigre. “Novo totem de segurança com câmera de reconhecimento facial em El Talar” (em espanhol). Setembro de 2020. http://www.tigre.gov.ar/novedades/detalle/1267
[114] ADC, conta no Twitter. https://twitter.com/adcderechos/status/1131556333466116096?s=20
[115] NEC. "Soluções Integradas de Segurança Urbana na Cidade de Tigre." https://www.nec.com/en/case/tigre/index.html Brochura da NEC para o estudo de caso Tigre: https://web.archive.org/web/20170321095617/http://www.nec.com/en/case/tigre/pdf/brochure.pdf
[116] NEC. “A Receita Federal utilizará a tecnologia de identificação facial da NEC em 14 aeroportos internacionais do país” (em português). 2016. https://br.nec.com/pt_BR/press/PR/20160409060302_11186.html
[117] Ministério da Economia. “Receita Federal lança o Sistema de Reconhecimento Facial” (em português). 2016.

Histórico de direitos humanos da NEC

Em dezembro de 2020, o **Justice for Myanmar**, um grupo de ativistas, conduziu uma investigação[118] sobre a corrupção e influência do exército de Mianmar no setor de informação e comunicação. O grupo descobriu evidências do roubo de bens públicos pelos militares, expôs novas redes de compras militares e revelou a rede global de empresas que estão permitindo aos militares continuar cometendo crimes de guerra e crimes contra a humanidade.

De acordo com a investigação, a **NEC** forneceu equipamentos de transmissão por microondas às forças militares de Myanmar através da **Viettel** (Vietnam Telecommunications Company) e **Mytel** (a mais nova operadora móvel de Myanmar). Ao fazer isso, a NEC e outras empresas que estão fornecendo tecnologia através da Mytel e Vittel correm o risco de contribuir para as graves violações dos direitos humanos em Mianmar.

O Business & Human Rights Resource Centre (BHRRC) convidou a NEC e outras 20 das empresas mencionadas no relatório a responder às acusações. Em sua resposta, a NEC disse que "se absteria de comentar casos individuais"[119] A empresa anteriormente não respondeu quando o BHRRC perguntou se as autoridades japonesas pediram ou não a ela que desenvolvesse drones para uso militar junto ao governo israelense.[120]

Em 2019, foi amplamente divulgado que o sistema de reconhecimento facial da NEC foi usado no primeiro caso de prisão injusta conhecida devido ao viés algorítmico.[121] A NEC respondeu afirmando que "uma correspondência usando apenas o reconhecimento facial não é um meio de identificação positiva" e não esclareceu como a empresa evitará que casos semelhantes aconteçam no futuro.

Esta conduta é diretamente conflitante com o compromisso declarado da NEC de respeitar os direitos humanos e a privacidade em seu Código de Conduta do Grupo,[122] e representa falha em proporcionar transparência conforme contemplado em seus próprios "Princípios de AI e Direitos Humanos do Grupo NEC".[123]

---

https://receita.economia.gov.br/noticias/ascom/2016/agosto/receita-federal-apresentou-hoje-1-8-em-coletiva-de-imprensa-detalhes-sobre-o-novo-sistema-de-reconhecimento-facial-1

[118] Justice for Myanmar. “Nodos de Corrupção, Linhas de Abuso.” Dezembro de 2020. https://www.justiceformyanmar.org/stories/nodes-of-corruption-lines-of-abuse-how-mytel-viettel-and-a-global-network-of-businesses-support-the-international-crimes-of-the-myanmar-military

[119] Business & Human Rights Resource Centre. “Resposta da NEC.” Janeiro de 2021. https://www.business-humanrights.org/en/latest-news/necs-response/

[120] Business & Human Rights Resource Centre. “Japão: Relatado desenvolvimento conjunto de drones com Israel.” Outubro de 2016. https://www.business-humanrights.org/es/%C3%BAltimas-noticias/japan-reported-joint-drone-development-with-israel/

[121] New York Times. “Acusado injustamente por um Algoritmo.” Junho de 2020. https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

[122] NEC. “Código de Conduta do Grupo.” Atualizado em Janeiro de 2019. https://www.nec-enterprise.com/documents?id=1432&hash=7c546360141e92ca5009db242402001dd7e393ef5198076b4f5e5a9f1c869f29

[123] NEC. “NEC Revela "Princípios de IA e Direitos Humanos do Grupo NEC." Abril de 2019. https://www.nec.com/en/press/201904/global_20190402_01.html

⇛ IDEMIA

Nome da Empresa	Idemia France SAS
Matriz	Courbevoie, França
Países onde Atua	Global
Países onde suas tecnologias de vigilância são utilizadas entre Argentina, Brasil e Equador	Argentina
Fundada em	2008
Capital Aberto / Fechado	Capital Fechado
Acionistas Principais	Advent International (acionista majoritária)
Número de Funcionários	Aproximadamente 15.000 em 2019
Receita Anual	€2.3 bilhões (US$2.7 bilhões) em 2019

Anteriormente conhecida como "Morpho Safran" e "Safran Identity and Security",[124] a empresa francesa **IDEMIA** é um dos principais fornecedores de tecnologia biométrica do mundo. Somente nos Estados Unidos, a empresa fornece soluções para o Federal Bureau of Investigation (FBI),[125] INTERPOL,[126] o Departamento de Polícia de Nova York,[127] e a Administração de Segurança de Transportes dos Estados Unidos, entre outros.

Em nossa pesquisa para este relatório, não conseguimos encontrar qualquer conexão recente entre os governos argentino, equatoriano ou brasileiro e a empresa sob a marca IDEMIA. A IDEMIA tem um escritório em Buenos Aires, Argentina, mas está voltada para o mercado de operadoras móveis. Ainda que não esteja claro quando as autoridades argentinas compraram a tecnologia do IDEMIA pela primeira vez, os órgãos de aplicação da lei (LEAs) na Argentina começaram a usar os produtos Morpho

[124] IDEMIA, "OT-Morpho passa a ser IDEMIA, a líder global em identidades confiáveis." Setembro de 2017. https://www.idemia.com/press-release/ot-morpho-becomes-idemia-global-leader-trusted-identities-2017-09-28.
[125] Morpho. "Tecnologia MorphoTrak Passa a ser Operacional para o FBI." Abril de 2011. http://web.archive.org/web/20150607084516/http://www.morpho.com/actualites-et-evenements/presse/morphotrak-technology-goes-operational-for-the-fbi?lang=en
[126] Morpho. "Sagem Sécurité irá fornecer à Interpol e seus 186 estados-membros o Sistema mais recente de Identificação de Impressões Digitais Automatizado AFIS." Fevereiro de 2008. http://web.archive.org/web/20150607090048/http://www.morpho.com/news-events-348/press/sagem-securite-to-provide-interpol-and-its-186-member-states-with-latest-afis-automated-fingerprint-identification-system?lang=en
Morpho. "Safran Identity & Security é a parceira exclusiva da INTERPOL para reconhecimento facial." Novembro de 2016: http://www.morpho.com/en/media/safran-identity-security-exclusive-partner-interpol-facial-recognition-20161123
[127] Morpho. "Morpho Trak Utiliza o Sistema de Identificação Biométrica da Morpho no NYPD." Setembro de 2012: http://web.archive.org/web/20150607084015/http://www.morpho.com/news-events-348/press/morphotrak-deploys-morpho-biometric-identification-system-at-nypd?lang=en

antes de 2010.[128] O uso da tecnologia decolou então com a introdução, e posterior expansão, do **SIBIOS**, um banco de dados biométricos maciço de propriedade do estado.

Como destacaremos em nosso estudo de caso sobre a Argentina neste relatório, o uso dos produtos Morpho está intimamente relacionado ao SIBIOS. Esses produtos são utilizados pelo Ministério Nacional de Segurança e pela Polícia Federal. Em 2014 e 2015, o Ministério gastou mais de US$ 7 milhões em contratos com Morpho S.A. para tecnologia biométrica.[129] A Polícia Federal emprega dispositivos Morpho RapID no campo, para realizar a identificação de impressões digitais de indivíduos,[130] bem como "Morpho Face Detective" para reconhecimento facial para identificar pessoas em multidões.[131]

Com a competência da Polícia Federal é nacional, o uso da tecnologia Morpho se expandiu por todo o país, como nas cidades de Campana,[132] Luján,[133] Balcarce,[134] Córdoba,[135] Chaco,[136] e várias cidades da Província de Buenos Aires.[137]

As agências estatais dependem de um dos principais revendedores da tecnologia da IDEMIA, a **IAFIS Argentina S.A.**, a mesma empresa que vende os produtos da Cellebrite. Este revendedor indica várias forças policiais de várias províncias da Argentina como seus clientes,[138] assim como o Ministério Público e outras instituições públicas, embora não especifique quais produtos está fornecendo.

A Cidade de Buenos Aires adquiriu o software Morpho Face Investigate da IAFIS Argentina S.A. em 2011

---

[128] Zona Norte. “O sistema de segurança Morpho Touch já é aplicado em Tigre" (em espanhol). Agosto de 2008. https://www.zonanortediario.com.ar/05/08/2008/el-sistema-de-seguridad-morpho-touch-ya-se-aplica-en-tigre/

[129] Superintendência de Administração da Polícia Federal Argentina, Divisão de Compras, Contratação Direta nº 25/2014, Arquivo nº 581-01-000726-14: https://www.boletinoficial.gob.ar/detalleAviso/tercera/2134795/20150119
Superintendência de Administração da Polícia Federal Argentina, Divisão de Compras, Contratação Direta nº 26/2014, Arquivo nº 581-01-000640-14: https://www.boletinoficial.gob.ar/detalleAviso/tercera/2134792/20150119
Arquivo nº 550-01-001003-2014 y 563-01-001091-2014
https://www.boletinoficial.gob.ar/detalleAviso/tercera/2125517/20141024 Arquivo nº 581-01-000726/2014 y 563-01-001090/2014 https://www.boletinoficial.gob.ar/detalleAviso/tercera/2125518/20141024

[130] A Conta de Twitter oficial do Ministro anunciou o seu uso em 2018:
https://web.archive.org/web/20201230202624/https://twitter.com/MinSeg/status/1038127257401810944?s=20 e
https://web.archive.org/web/20201230202648/https://twitter.com/minseg/status/1033045304638156803
https://www.argentina.gob.ar/noticias/gdetuvimos-en-retiro-un-hombre-que-ten%C3%ADa-pedido-de-captura

[131] Conta de Twitter oficial da Polícia Federal, mostrando o uso do Morpho Face Detective na estação de trem de Retiro, Janeiro de 2019: https://web.archive.org/web/20201230203110/https://twitter.com/PFAOficial/status/1090673247161597952?s=20

[132] La Auténtica Defensa. " O sistema Morpho Rapid é aplicado em Campana " (em espanhol). Março de 2009. www.laautenticadefensa.net/62085

[133] El Civismo. "Equipamentos modernos para identificar pessoas" (em espanhol). Setembro de 2010. https://www.elcivismo.com.ar/notas/7191/

[134] "La Vanguardia. “Avanço: Operação da Polícia Federal em Balcarce” (em espanhol). Fevereiro de 2019. http://www.diariolavanguardia.com/noticias/21448--cobramos-por-lo-que-trabajamos--no-le-robamos-la-plata-a-nadie-/

[135] La Voz. " Eles recapturaram "Cañete", o fugitivo "mais procurado" de Córdoba " (em espanhol). Maio de 2017. https://www.lavoz.com.ar/sucesos/recapturaron-canete-el-profugo-cordobes-mas-buscado

[136] Departamento de Polícia de Chaco. " A polícia treina e testa novo sistema de identificação " (em espanhol). Março de 2013. https://web.archive.org/web/20201230210055/http://policia.chaco.gov.ar/index.php/ecmPagesView/view/id/101

[137] Primera Plana. " A Polícia Federal desembarca no interior de Buenos Aires com operações de controle e prevenção " (em espanhol). Maio de 2019.
http://primeraplana.com.ar/policia-federal-desembarca-en-el-interior-bonaerense-con-operativos-de-control-y-prevencion/

[138] IAFIS. Clientes.
https://web.archive.org/web/20201230205443/https://www.iafisgroup.com/quienes-somos/clientes-argentina/

por 33.198.500 pesos (mais de US$ 6 milhões à época), e começou a testar seu uso no metrô para identificar punguistas.[139]

De acordo com documentos oficiais sobre compras e concorrências públicos, a Polícia Metropolitana da Cidade de Buenos Aires utiliza tanto a tecnologia de reconhecimento de impressões digitais quanto a tecnologia de reconhecimento facial da Morpho para investigações judiciais. A IAFIS Argentina S.A. vem fornecendo apoio técnico a eles desde pelo menos 2015, com vários contratos de mais de US$ 6,5 milhões no total.[140]

Histórico de direitos humanos da IDEMIA

Em 2017, a Morpho (que mais tarde se tornou **IDEMIA**) foi responsabilizada por problemas com seus kits de registro e autenticação biométricos utilizados nas eleições gerais de 2017 no Quênia, resultando no cancelamento de seus contratos públicos pela Assembleia Nacional e bloqueio de quaisquer novos contratos.

Essa decisão foi contestada e anulada pelo Supremo Tribunal do Quênia.[141] A coalizão de oposição do Quênia acusou a empresa francesa de cumplicidade em fraude eleitoral, mas a empresa negou essas acusações. **A Safran (empresa anterior à incorporação da IDEMIA) também foi multada pela justiça francesa por ter pago propinas para garantir um negócio na Nigeria[142]**

Em setembro de 2020, a **Anistia Internacional** descobriu que três empresas europeias, uma das quais era a IDEMIA, vendia tecnologia de vigilância ao governo chinês.[143] Especificamente, a IDEMIA recebeu um contrato para fornecer equipamentos de reconhecimento facial diretamente ao Bureau de Segurança Pública de Xangai em 2015. Devido ao risco das autoridades chinesas utilizarem esse equipamento para vigilância em massa e outros abusos dos direitos humanos, a Anistia Internacional, a Access Now e outras organizações, bem como alguns países europeus, vêm solicitando à União Europeia que reforce as salvaguardas dos direitos humanos em suas decisões sobre exportação de vigilância e garanta que todas essas empresas façam uma avaliação do impacto dos direitos

[139] Infobae. " Avaliação de um software de identificação facial para localizar "pungas" no metrô" (em espanhol). Janeiro de 2013. https://www.infobae.com/2013/01/13/691102-evaluan-un-software-identificacion-facial-ubicar-pungas-el-subte/
[140] Departamento de Compras de Buenos Aires. Número de processos de compra: 2900-1047-CDI15 https://www.buenosairescompras.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhzAdZmPYqqZ4su3ScBBrBvMPHSPHPxZ74bjkpi4POk3iZKynCGKbKt|RDsvNlcW1mJISgBUffWWFY1vgdwt/W5yzl3PnouupiCeVWiQu ysmvw== Número de processos de compra: 2900-0858-CDI17. https://www.buenosairescompras.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhzjp0DPq1u2nI3iH|4rzqLn 9Phu5zQ6mkLN3u849mLkhWIq/6PJyo37gtSRaUyG3uJLK1ZE2CoQE3RKSJHwBng31I/q82/vv9su9cJDc2PG2g==
[141] Biometric Update. "Biometria na África esta semana: A suspensão da Idemia no Quênia foi derrubada, soluções locais procuradas para o crime cibernético." Abril de 2020. https://www.biometricupdate.com/202004/biometrics-in-africa-this-week-idemia-suspension-in-kenya-overturned-local-solutions-sought-for-cybercrime
[142] BBC. "Safran é multada em caso de suborno na Nigéria." Setembro de 2012. https://www.bbc.com/news/business-19498916
[143] Anistia Internacional. "Empresas da UE vendendo ferramentas de vigilância para os violadores dos direitos humanos da China." Setembro de 2020. https://www.amnesty.org/en/latest/news/2020/09/eu-surveillance-sales-china-human-rights-abusers/

humanos.[144] A França, onde a IDEMIA está sediada, tem resistido a esse apelo.[145]

⇛ Verint

Nome da Empresa	Verint Systems Inc.
Matriz	New York, the U.S.
Países onde Atua	Global
Países onde suas tecnologias de vigilância são utilizadas entre Argentina, Brasil e Equador	Equador
Fundada em	2002
Capital Aberto / Fechado	Cotada na Nasdaq
Acionistas Principais	N/A
Número de Funcionários	Aproximadamente 6.500 em 2019
Receita Anual	€2.3 bilhões (US$2.7 bilhões) em 2019

A **VERINT** é uma das poucas empresas sediadas nos Estados Unidos a ter entrado no mercado latino-americano. Aproximadamente metade de seus funcionários está localizada em Israel.

No **Equador**, a cidade de **Guayaquil** adquiriu a tecnologia de vigilância da VERINT da distribuidora **Union Electrica S.A.**, uma empresa que ganhou contratos milionários da **Corporation for Citizen Security**, uma entidade privada sem fins lucrativos criada para gerenciar a vigilância por vídeo e outros serviços de segurança para Guayaquil.[146] O objetivo era integrar 100 câmeras de vigilância com reconhecimento facial para segurança em instituições educacionais. A integração custou US$ 2.569.906,41 e incluiu produtos como câmeras com capacidade de captura facial, sistemas de reconhecimento facial, soluções de armazenamento de dados, licenças para câmeras e monitoramento e equipamentos periféricos de megafones, serviços e infraestrutura. Em 2020, essas câmeras e produtos foram integrados ao **ECU911** o programa de vigilância em massa do Equador.

Histórico de direitos humanos da VERINT

[144] Access Now. “Paradas de negócios e direitos humanos na Internet Apelo urgente ao Conselho da UE: os direitos humanos devem vir primeiro na minuta final de Duplo Uso.” Novembro de 2020. https://www.accessnow.org/urgent-call-to-council-of-the-eu-human-rights-must-come-first-in-dual-use-final-draft/
[145] Netzpolitik, “Exportações de vigilância: Como Estados-Membros da EU estão comprometendo as novas normas sobre direitos humanos.” Outubro de 2018. https://netzpolitik.org/2018/surveillance-exports-how-eu-member-states-are-compromising-new-human-rights-standards/
[146] Corporation for Citizen Security of Guayaquil. https://cscg.gob.ec/

Em 2014, uma investigação conduzida pela Privacy International[147] detalhou como a **VERINT** forneceu centros de monitoramento capazes de interceptação em massa de redes telefônicas, móveis e IP ao **Cazaquistão** e ao **Uzbequistão**. O Cazaquistão foi condenado por leis que restringem a liberdade de expressão e reunião, julgamentos parciais e tortura,[148] enquanto no Uzbequistão há relatos de advogados, jornalistas e blogueiros cujas comunicações foram interceptadas, e que depois foram perseguidos por motivos políticos.[149] Ambos os países são há muito conhecidos pela ampla vigilância digital dos seus cidadãos.[150]

A Privacy International também publicou um relatório especial sobre o estado da vigilância na **Colômbia**, em 2015.[151] De acordo com o relatório, o governo colombiano utiliza um sistema chamado Plataforma Única de Monitoramento e Análise ou **PUMA** (suas iniciais em espanhol). A PUMA tem a capacidade potencial de interceptar e armazenar todas as comunicações transmitidas pela infraestrutura de base da qual todos os colombianos dependem para conversar e enviar mensagens uns aos outros. A PUMA é alimentada por tecnologia própria da VERINT, utilizando principalmente sua plataforma de centro de monitoramento RELIANT.

Segundo relatos, técnicos da VERINT colocaram 16 sondas "IP-PROBER "[152] nas redes tronco para interceptar dados e encaminhá-los para os centros de monitoramento da PUMA. O Departamento Administrativo de Segurança (DAS) utilizou as mesmas para vigilância das redes de comunicação, e a agência foi posteriormente investigada por atividades ilegais e depois dissolvida devido a sua espionagem e assédio a políticos, jornalistas, ativistas e juízes da Suprema Corte que se opunham ao governo de Álvaro Uribe.

Em 2012, o Centro de Recursos Empresariais e de Direitos Humanos convidou empresas, inclusive a VERINT, a responder as acusações de que fornecem tecnologia de vigilância a regimes opressivos no Oriente Médio.[153] A VERINT não respondeu.

---

[147] Privacy International. “Interesses privados: Monitoramento da Ásia Central.” Novembro de 2014. https://privacyinternational.org/report/837/private-interests-monitoring-central-asia

[148] Human Rights Watch. “Cazaquistão.” https://www.hrw.org/europe/central-asia/kazakhstan Access Now, “Sociedade civil relata apagões da internet em duas cidades no Cazaquistão durante protestos em 28 de fevereiro.” Março de 2021. https://www.accessnow.org/internet-shutdowns-kazakhstan-feb-28-protests/

[149] Human Rights Watch. “Uzbequistão.” https://www.hrw.org/europe/central-asia/uzbekistan

[150] Access Now, “Commonwealth de estados de vigilância: Sobre a exportação e revenda de tecnologia russa para Ásia Central pós-soviética.” Junho de 2013. https://www.accessnow.org/cms/assets/uploads/archive/docs/Commonwealth_of_Surveillance_States_ENG_1.pdf

[151] Privacy International. “Um estado sombra: vigilância e ordem pública na Colômbia” (em espanhol). Agosto de 2015. https://www.privacyinternational.org/sites/default/files/2017-12/ShadowState_Espanol.pdf

[152] Diretoria de Administração e Finanças, Polícia Nacional da Colômbia. Arquivo nº06-7-10124- 10. Setembro de 2010. http://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=10-12-351033

[153] Business & Human Rights Resource Centre. “Human Rights First & OWNI Digital artigos sobre tecnologia de vigilância e regimes opressivos.” Janeiro de 2012 https://www.business-humanrights.org/es/%C3%BAltimas-noticias/human-rights-first-owni-digital-articles-on-surveillance-technology-oppressive-regimes/

Outras empresas que fornecem tecnologia de vigilância na América Latina

Como mencionamos na introdução a este relatório, nos concentramos nas empresas com informações mais publicamente disponíveis sobre seus negócios na América Latina, que representam uma ameaça particular aos direitos humanos, e que são pervasivas devido às suas relações com órgãos governamentais. No entanto, há várias empresas que merecem ser mencionadas que estão mantendo um perfil mais discreto e merecem uma investigação mais aprofundada.

BGH Tech Partner

Nome da Empresa	BGH Tech Partner S.A.
Matriz	Buenos Aires, Argentina
Países onde Atua	[Não disponível]
Países onde suas tecnologias de vigilância são utilizadas entre Argentina, Brasil e Equador	Argentina
Fundada em	1913
Capital Aberto / Fechado	Capital Fechado
Acionistas Principais	[Não disponível]
Número de Funcionários	[Não disponível]
Receita Anual	[Não disponível]

A **Boris Garfunkel e Hijos**, ou **BGH**, é uma empresa **argentina** que começou vendendo uma ampla gama de produtos mas ao longo da última década concentrou-se parcialmente no desenvolvimento de soluções tecnológicas. A empresa é responsável pela utilização de tecnologia para o "Laboratório de Análise de Vídeo Forense" na província de **San Juan**.[154]

Ainda que a empresa afirme que só está fornecendo soluções de aplicação da lei para comunicações criptografadas e serviços de mapeamento de localização, de acordo com relatórios da mídia,[155] esse laboratório em breve será equipado com software de reconhecimento facial para identificar pessoas e detectar e classificar objetos, atributos e comportamentos, bem como reconhecer placas de veículos.

[154] BGH. "San Juan implementa tecnologia no estado da arte para polícia provincial" (em espanhol). Setembro de 2020. https://www.bghtechpartner.com/2020/09/11/san-juan-implementa-tecnologia-de-comunicaciones-de-ultima-generacion-para-la-policia-provincial/

[155] Serviço de Informações do Governo de San Juan. "Acordo de San Juan: tecnologia aplicada à segurança" (em espanhol). Outubro de 2020. https://sisanjuan.gob.ar/seguridad/2020-10-22/26837-acuerdo-san-juan-tecnologia-aplicada-a-la-seguridad

Tentamos obter informações sobre a implantação da tecnologia BGH, tanto do governo quanto da própria empresa, mas sem sucesso. É possível que a tecnologia venha da **Hikvision**, já que em 2018, a BGH começou a vender produtos Hikvision.[156] As soluções BGH agora incluem câmeras de reconhecimento térmico, veicular, portátil e facial, bem como tecnologias como drones e robôs.[157]

Danaide S.A. e NTechLab

Nome da Empresa	**Danaide S.A.**
Matriz	Buenos Aires, Argentina
Países onde Atua	Argentina
Países onde suas tecnologias de vigilância são utilizadas entre Argentina, Brasil e Equador	Argentina
Fundada em	1999
Capital Aberto / Fechado	Capital Fechado
Acionistas Principais	[Não disponível]
Número de Funcionários	[Não disponível]
Receita Anual	[Não disponível]

Nome da Empresa	**N-Tech.Lab Ltd.**
Matriz	Nicósia, Chipre
Países onde Atua	Rússia
Países onde suas tecnologias de vigilância são utilizadas entre Argentina, Brasil e Equador	Argentina
Fundada em	2015
Capital Aberto / Fechado	Capital Fechado

[156] BGH. "BGH Tech Partner suma Hikvision a su portfolio." Fevereiro de 2018. https://www.bghtechpartner.com/2018/02/02/bgh-tech-partner-suma-hikvision-su-portfolio/
[157] Canal AR. "BGH amplia seu portfólio de vigilância por vídeo com a Hikvision" (em espanhol). Janeiro de 2018. https://canal-ar.com.ar/25431-BGH-impulsa-su-porfolio-de-videovigilancia-con-Hikvision.html

Acionistas Principais	[Não disponível] Entre acionistas minoritários, o Russian Direct Investment Fund e principais fundos soberanos de países do Oriente Médio totalizaram um investimento de capital de RUB 1 bilhão (US$13 milhões) em 2020.
Número de Funcionários	[Não disponível]
Receita Anual	[Não disponível]

De acordo com alguns relatos independentes,[158] a empresa **argentina** local **Danaide**, contratada por Buenos Aires para implementar seu sistema de reconhecimento facial,[159] pode estar utilizando o software Find Face[160] desenvolvido pela empresa russa **NTechLab**. Apesar de nossas diversas tentativas de obter mais detalhes com base na liberdade de informação, o governo só viria a confirmar que a Danaide ganhou um contrato numa concorrência, recusando-se a esclarecer se ela própria desenvolveu o algoritmo de reconhecimento facial.

Na versão russa do site da NTechLab,[161] o software **UltraIP**[162] da Danaide, que é vendido na Argentina, aparece na seção de parceiros. Em resposta ao pedido da ADC com base na liberdade de informação feito em Junho de 2019,[163] funcionários de Buenos Aires confirmaram que UltraIP é o nome do software licenciado.

Em outubro de 2020, a Human Rights Watch alertou o público sobre falhas no sistema da NTechLab e seu uso indevido pelo governo para identificar e direcionar crianças para processo criminal em violação dos direitos humanos.[164] Em **Moscou**, a NTechLab fornece o software para um programa de vigilância que grupos de direitos humanos dizem que o governo abusou ao vigiar as pessoas durante a pandemia COVID-19 para impor um lockdown.[165]

IBM

[158] One Zero. “Os EUA Temem o Reconhecimento Facial ao Vivo. Em Buenos Aires, é um Fato da Vida.” Março de 2020. https://onezero.medium.com/the-u-s-fears-live-facial-recognition-in-buenos-aires-its-a-fact-of-life-52019eff454d
[159] ADC. "#ConMiCaraNo: Reconhecimento facial na Cidade de Buenos Aires " (em espanhol). Maio de 2019. https://adc.org.ar/2019/05/23/con-mi-cara-no-reconocimiento-facial-en-la-ciudad-de-buenos-aires/
[160] NTechLab. Site oficial Find Face. https://findface.pro/en/
[161] NTechLab. Partners (em russo). https://web.archive.org/web/20200511205745/https:/findface.pro/partners/
[162] Danaide. Desenvolvimento de software. https://danaide.com.ar/desarrollos/desarrollossoftware.html
[163] ADC. FOIA solicitação NO-2019-21065074-GCABA-DGAYCSE. Julho de 2019. https://adc.org.ar/wp-content/uploads/2019/07/Respuesta-PAIP-reconocimiento-facial-GCBA-V2.pdf
[164] Human Rights Watch. “Argentina: Dados particulares de crianças suspeitas publicados online.” Outubro de 2020. https://www.hrw.org/news/2020/10/09/argentina-child-suspects-private-data-published-online
[165] Reuters. “As medidas de vigilância de bloqueio da Rússia precisam ser regulamentadas, dizem os grupos de direitos.” Abril de 2020. https://uk.reuters.com/article/uk-health-coronavirus-russia-facial-reco-idUKKCN2253CG

Nome da Empresa	International Business Machines Corporation
Matriz	New York, U.S.
Países onde Atua	Global
Países onde suas tecnologias de vigilância são utilizadas entre Argentina, Brasil e Equador	Argentina
Fundada em	1911
Capital Aberto / Fechado	Cotada na Bolsa de Valores de Nova York
Acionistas Principais	N/A
Número de Funcionários	Aproximadamente 350.000 em 2020 (considerando o grupo)
Receita Anual	US$45 bilhões em 2020

Em dezembro de 2016, o Ministério Nacional de Segurança da Argentina assinou um contrato direto com a empresa local **Unitech S.A.**, descrito como a aquisição de "software avançado para investigações criminais", no valor total de US$3.515.518,77.[166] Dentre os documentos da compra, as especificações técnicas declaram que os produtos e serviços do contrato incluíam: nove licenças para IBM i2 Enterprise Insight Analysis,[167] um add-on IBM i2 Collaborate e gráfico de texto IBM i2, e serviços de suporte técnico múltiplo.

Há precedentes da tecnologia IBM utilizada nas Filipinas durante a violenta "guerra às drogas". De acordo com uma investigação conduzida em 2009 pela Human Rights Watch[168] , há evidências de que funcionários do governo e a polícia foram cúmplices dos esquadrões da morte que assassinaram crianças de rua, traficantes de drogas e pequenos criminosos durante o mandato de Rodrigo Duterte como prefeito na cidade de Davao.

Em 2012, a IBM fez um acordo com Sara Duterte, filha de Rodrigo Duterte e prefeito da cidade naquela época, para atualizar o centro de comando policial de Davao a fim de "melhorar ainda mais as operações de segurança pública na cidade", enquanto a violência nas ruas continuava. De acordo com um relatório da The Intercept,[169] a IBM recusou-se a responder a perguntas sobre seu histórico de

[166] Diretoria Geral de Administração. “ADQ. DE LICENÇAS DE SOFTWARE AVANÇADO PARA ANÁLISE CRIMINAL COM A UNITECH S.A. FIRM.” Arquivo nº 347-0066-CDI16. Dezembro de 2016.
https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhxZR|eGCUUs0CDTFEc5IK6|8mooLYATqyEzFwVde9PPWAMi|0jPJGKn6pHkBSQAUfnO3onZZEr5bCGawx17losLJTLKoi9VrlOdxyH6GqsNTw==
[167] IBM. i2 Enterprise Insight Analysis 2.3.0.
https://www.ibm.com/support/knowledgecenter/SSXVXZ_2.3.0/com.ibm.i2.landing.doc/eia_welcome.html
[168] Human Rights Watch. “Você pode morrer a qualquer momento.” Abril de 2009.
https://www.hrw.org/sites/default/files/reports/philippines0409webwcover_0.pdf
[169] The Intercept. “Dentro do Programa de Vigilância por Vídeo IBM Construído para o homem forte filipino Rodrigo Duterte.”

direitos humanos na cidade de Davao. O porta-voz da IBM, Edward Barbini, fez uma observação curta de que a empresa "não fornece mais tecnologia para o Centro de Operações Inteligentes em Davao, e não o faz desde 2012", embora tenha se recusado a esclarecer se a IBM prestou serviços referentes à tecnologia após essa ocasião, e os arquivos públicos da IBM mencionam o programa como contínuo após essa data.

Johnson Controls

Nome da Empresa	Johnson Controls International PLC
Matriz	Cork, Irlanda
Países onde Atua	Global
Países onde suas tecnologias de vigilância são utilizadas entre Argentina, Brasil e Equador	Brasil
Fundada em	1885
Capital Aberto / Fechado	Cotada na Bolsa de Valores de Nova York
Acionistas Principais	Dodge & Cox Stock Fund (11.3%) em 2020
Número de Funcionários	Aproximadamente 97,000 em 2020 (considerando o grupo)
Receita Anual	US$22.317 milhões em 2020

Em São Paulo, a tecnologia de reconhecimento facial instalada no metrô foi fornecida pela Johnson Controls, uma empresa sediada na Irlanda. Esse é outro caso em que as autoridades não utilizaram o sistema de aquisição tradicional[170]. Em vez disso, elas adquiriram a tecnologia de reconhecimento facial através de uma licitação internacional, o que permite aos concorrentes estrangeiros mais oportunidades de fazer suas ofertas.

Março de 2019. https://theintercept.com/2019/03/20/rodrigo-duterte-ibm-surveillance/

[170] IDEC. “Ação questiona a falta de transparência na licitação do metrô de SP” (em português). Fevereiro de 2020. https://idec.org.br/noticia/acao-questiona-falta-de-transparencia-e-solicita-informacoes-sobre-licitacao-do-metro-de-sp

III. ESTUDOS DE CASOS: COMO A TECNOLOGIA É UTILIZADA

ESTUDO DE CASO: Argentina

Pela Asociación por los Derechos Civiles (ADC)

Desde 2015, o uso de tecnologias de vigilância na Argentina tem crescido de forma gradual, mas constante, abrindo grandes riscos para o direito à privacidade em todo o país. Em todos os casos, o setor privado tem desempenhado um papel fundamental na implantação de tecnologias, nutrindo relações estreitas com órgãos governamentais a nível local, provincial e nacional.

Estamos agora enfrentando o auge de uma tendência que começou há mais de uma década, em 2008, quando os governos locais começaram a usar tecnologias como câmeras de vigilância por vídeo (ou CCTV) para apoiar suas campanhas políticas,[171] promovendo uma imagem de progresso em direção a uma maior segurança pública.

Segundo um estudo realizado pela Faculdade de Psicologia da Universidade de Buenos Aires,[172] uma alta porcentagem da população considera a situação da segurança pública e da segurança na Argentina "muito grave" ou "extremamente grave", e nove em cada dez pessoas pensam que "bastante ou muito provavelmente" serão vítimas de um crime a curto prazo. Devido a esse medo, a segurança pública tem estado na vanguarda da narrativa dos oficiais do governo para justificar os meios para um fim. Ao mesmo tempo, esses oficiais citaram a segurança pública como um motivo para evitar compartilhar detalhes sobre seus acordos com empresas de tecnologia, como as informações pessoais das pessoas são processadas e quaisquer especificações sobre equipamentos adquiridos.

Embora a Argentina tenha tanto fortes proteções constitucionais para os direitos humanos, inclusive o direito à privacidade, e uma estrutura abrangente de proteção de dados, a aquisição e implementação de tecnologias de vigilância é geralmente realizada com pouca ou nenhuma supervisão ou transparência.[173]

Tecnologia utilizada

Descobrir a extensão dos mecanismos e sistemas de vigilância utilizados pelos vários níveis de governo não é um feito fácil, pois as informações não estão prontamente disponíveis através dos canais públicos, a menos que a mídia divulgue informações a respeito ou que seja realizada uma pesquisa independente.

[171] Natalia Zuazo, Revista Anfibia. “A vida dos outros” (em espanhol). http://revistaanfibia.com/cronica/la-vida-de-los-otros/
[172] Faculdade de Psicologia, Universidade de Buenos Aires. "Monitor de Insegurança". (em espanhol). Dezembro de 2020. http://www.psi.uba.ar/opsa/informes/monitor_inseguridad_pais_2.pdf
[173] Veja mais informações sobre a situação mais ampla da privacidade na Argentina em: https://privacyinternational.org/state-privacy/57/state-privacy-argentina

Além do CCTV, as autoridades introduziram lentamente tecnologias mais invasivas na sociedade durante a última década. **Um ponto de virada em particular foi marcado pela introdução do SIBIOS em 2011.**

Através do Decreto Executivo 1766/11,[174] o governo nacional criou o Sistema Federal de Identificação Biométrica para a Segurança (**SIBIOS**), administrado pela Polícia Federal sob a autoridade do Ministério da Segurança.

Um dos principais objetivos da SIBIOS era fundir e digitalizar as bases de dados independentes mantidas pela Polícia Federal e pelo Registro Nacional de Cidadãos (**RENAPER**, em espanhol). O SIBIOS representou o auge do trabalho que começou alguns anos antes de seu lançamento, quando o Ministério do Interior começou a coletar, processar e armazenar dados biométricos para a emissão de carteiras de identidade (DNI) e passaportes. Desde 2009, o RENAPER está autorizado a utilizar tecnologias digitais para identificar cidadãos, residentes e visitantes. A partir de então, eles vêm coletando dados biométricos de cada cidadão, incluindo impressões digitais, impressões palmares e fotos de rosto, assim como de todos que entram no país.[175]

O SIBIOS é um sistema nacional, portanto todas as províncias do país assinaram acordos de cooperação com o governo nacional, juntamente com o Ministério da Segurança (incluindo suas quatro forças de segurança federais) e o Ministério do Interior (incluindo RENAPER e a Secretaria Nacional de Migração). Esses acordos garantem que suas forças policiais locais possam atualizar e acessar o banco de dados. Em 2017, através do Decreto Executivo 243/17,[176] o governo ampliou o acesso ao SIBIOS a qualquer órgão público dentro dos poderes Executivo ou Judiciário a nível nacional e provincial, e deu acesso à Cidade Autônoma de Buenos Aires (capital da Argentina). Os usuários do SIBIOS não são obrigados a obter mandado ou autorização judicial antes de executar consultas no banco de dados biométricos.

O Ministério de Segurança contou com um grande fornecedor para sua infraestrutura ligada ao SIBIOS, a empresa francesa Morpho Safran, que como resultado de uma fusão se tornou **IDEMIA**. A IDEMIA é responsável pela instalação e configuração do Sistema de Identificação Automática de Impressões Digitais (AFIS) do Ministério. O Ministério adquiriu e utilizou outros produtos da empresa, incluindo o Morpho Face Investigate Pilot, para reconhecimento facial a partir de arquivos de foto e vídeo, e o Morpho RapID,[177] para verificações de identificação de impressões digitais no local em todo o país.

Outra parte da infraestrutura do SIBIOS foi construída pelo Ministério do Interior, que nutre uma estreita relação com sua contraparte em Cuba, particularmente entre 2011 e 2015. O Ministério adquiriu sua tecnologia biométrica da empresa estatal cubana **DATYS**, que desenvolveu um conjunto de

[174] Decreto 1766/2011. Argentina. http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/189382/texact.htm
[175] ADC. "A Identidade que não podemos mudar: Como a biometria prejudica nossos direitos humanos." 2017. https://adc.org.ar/wp-content/uploads/2019/11/0027-B-The-identity-we-can%C2%B4t-change-12-2017.pdf
[176] Ministério da Segurança Argentino. Decreto 243/2017. http://servicios.infoleg.gob.ar/infolegInternet/anexos/270000-274999/273446/norma.htm
[177] La Capital. "Identidade instantânea e histórico em operações de saturação" (em espanhol). Junho de 2016. https://www.lacapitalmdp.com/identidad-y-antecedentes-al-instante-en-los-operativos-de-saturacion/

produtos para identificação biométrica[178] e verificação,[179] baseado no reconhecimento facial, impressões digitais, impressões palmares, DNA e voz. Em outubro de 2015, o Ministério atualizou sua tecnologia biométrica através de um contrato de US$1.080.000,00 com a DATYS, mais US$180.000,00 anuais de suporte técnico, por um período de cinco anos.

Desde a introdução do SIBIOS em 2011, o uso de tecnologias biométricas tem crescido exponencialmente em todo o país. **Além de sua utilização para segurança pública e imigração, a biometria é utilizada para verificação de identidade em contextos como programas de previdência social (por exemplo, para acesso a fundos de aposentadoria e pensão), bancos, impostos e taxas fiscais, educação, eleições e esportes.[180]**

Além da biometria, o governo argentino acrescentou outras tecnologias de vigilância ao seu repertório. As forças militares nacionais - incluindo o Exército, a Marinha e a Força Aérea - realizaram projetos para desenvolver seus próprios Veículos Aéreos Não Tripulados (UAVs), já em 1996, com desenvolvimento adicional entre 2011 e 2014. As forças policiais federais confiaram num grande fornecedor de aeronaves comerciais para atender suas necessidades, a empresa chinesa **DJI** (Dà-Jiang Innovations Science and Technology Co.). Além disso, em meados de 2017, a Cidade Autônoma de Buenos Aires adquiriu um balão de vigilância, o Skystar 180, produzido pela empresa israelense **RT**.[181]

Mais recentemente, as autoridades têm feito cada vez mais uso do reconhecimento facial e leitores automáticos de placas em todo o país, como parte do que parece ser uma corrida entre os oficiais de governo para implementar o máximo de tecnologia possível para fins de segurança pública.

Enquadramento jurídico

Como observamos acima, a Argentina possui amplas proteções para a privacidade. A Constituição nacional consagra esse direito fundamental nos artigos 18 e 19, e a Argentina ratificou tratados internacionais de direitos humanos[182], como o Pacto Internacional de Direitos Civis e Políticos e a Convenção Americana de Direitos Humanos.

Além disso, a Argentina possui um regime robusto - embora desatualizado - de proteção de dados, através do artigo 43 da Constituição e da Lei Nacional nº 25.326 sobre a proteção de dados pessoais. É também signatária da Convenção 108+[183] e a Comissão Europeia reconheceu a Argentina como tendo um nível adequado de proteção de dados em 2003, através da Decisão 2003/490 CE.[184]

---

[178] Identificação facial,(1:n) é o processo para analisar se uma imagem facial detectada corresponde a uma das imagens faciais armazenadas em um banco de dados. Aqui o sistema está tentando comparar as pessoas com um banco de dados de identidades.

[179] Verificação ou autenticação facial: (1:1) é o processo para analisar se uma imagem facial detectada coincide com uma imagem facial específica já armazenada. Normalmente, o sistema tenta responder à pergunta "a pessoa nesta imagem é a pessoa que diz ser?

[180] ADC. “Quantificando identidades na América Latina” (em espanhol). Maio de 2017. https://adc.org.ar/informes/cuantificando-identidades-en-america-latina/

[181] RT. “SKYSTAR 180” https://www.rt.co.il/skystar-180

[182] Nações Unidas. Status de Ratificação para a Argentina. https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?CountryID=7&Lang=EN

[183] Conselho da Europa. Convenção 108 e Protocolos. https://www.coe.int/es/web/data-protection/convention108-and-protocol

[184] EUR-Lex. Documento 32003D0490. 2003. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32003D0490

Infelizmente, essas leis provaram ser insuficientes para proteger os cidadãos da vigilância do Estado. **Os governos utilizam as exceções dessas leis como bases legais para a implantação de programas de vigilância para o exercício normal das funções estatais, melhoria dos serviços e segurança pública.** Até o momento, tem havido muito poucos questionamentos sobre privacidade ou proteção de dados e decisões judiciais ou administrativas para proteger as pessoas da coleta em massa de dados biométricos e uso de tecnologias de vigilância invasivas.

Essa deficiência nas decisões legais para salvaguardar direitos individuais piorou em outubro de 2020, quando o poder legislativo da Cidade Autônoma de Buenos Aires estabeleceu um perigoso precedente ao aprovar uma emenda à Lei nº 5688 que aprova o uso do reconhecimento facial para identificar fugitivos incluídos numa lista de vigilância nacional.[185]

Casos locais

A tendência de crescente implantação de tecnologias difundidas, que começou com CCTVs e o SIBIOS, é ainda mais prevalente a níveis local e provincial na Argentina. É complicado obter informações atualizadas sobre todas as autoridades do país, particularmente quando os usuários destas tecnologias são os Órgãos de Aplicação da Lei (LEAs) locais, por isso nos concentraremos nos casos mais abrangentes e naqueles para os quais, como parte deste projeto, fizemos mais pesquisas para obter informações mais detalhadas.

Identificamos as câmeras de vigilância com capacidade de reconhecimento facial e software como a tecnologia mais amplamente utilizada em todos os níveis de governo na Argentina. Em abril de 2019, o Governo da Cidade Autônoma de Buenos Aires anunciou a implementação de um software de reconhecimento facial para as câmeras de segurança (CCTV) e centros de monitoramento da cidade. Em maio do mesmo ano, a Cidade de Tigre, na província de Buenos Aires, criou o Centro de Operações de Tigre[186] para utilizar câmeras e software de reconhecimento facial, procurar pessoas desaparecidas e identificar pessoas com antecedentes criminais.

Em 15 de outubro de 2019, o governo provincial de Córdoba anunciou, através da mídia social, a introdução de um "software de reconhecimento biométrico" implantado em uma SUV policial, com quatro câmeras montadas e duas câmeras fixas.[187] Devido à falta de informações mais detalhadas disponíveis ao público, enviamos dois pedidos com base na liberdade de informação, em 7 de novembro de 2019 e 11 de novembro de 2020. Em ambos os casos, o governo não respondeu.

Isso se soma ao longo histórico de não conformidade da província com a lei local de acesso a informações públicas, sendo estimado, de acordo com dados fornecidos por organizações da sociedade civil como Red Ciudadana Nuestra Córdoba, Fundeps, Foro Ambiental e Córdoba de Todos,

[185] Telam. “A Legislatura aprovou o uso de reconhecimento facial para a prisão de fugitivos” (em espanhol). Outubro de 2020. https://www.telam.com.ar/notas/202010/527676-la-legislatura-aprobo-el-uso-de-reconocimiento-facial-para-la-detencion-de-profugos.html

[186] Ámbito. “Tigre lançou um novo sistema de reconhecimento facial” (em espanhol). Maio de 2019. https://www.ambito.com/municipios/municipios/tigre-lanzo-un-nuevo-sistema-reconocimiento-facial-n5030978

[187] Conta de Twitter do Governo de Córdoba. Outubro de 2019. https://twitter.com/gobdecordoba/status/1184116108665729025?s=20

que as autoridades respondem apenas 10% dos pedidos que recebem por ano.[188]

Em meados de 2017, a província de Mendoza começou a implementar um dos programas de vigilância mais invasivos da Argentina. Os órgãos policiais da província possuem câmeras móveis de reconhecimento facial e carros equipados com a mesma tecnologia, bem como scanners de impressões digitais e leitores de placas.[189] Apesar de nossos esforços para obter informações detalhadas do governo, eles forneceram só os nomes dos fornecedores dos quais adquiriram o equipamento (3M Argentina, INTEMA Comunicaciones S.A, Express Software, e Hardware S.A.), e não as especificações do software e hardware. O Ministério de Segurança da província argumentou que isto se deve ao fato de "as informações necessárias afetarem a segurança pública".

Seguindo essa tendência, o governo da Província de San Juan anunciou o "Acuerdo San Juan", um acordo para implementar mais tecnologia para a segurança pública. O programa inclui a implantação de câmeras de CFTV e tecnologia de reconhecimento facial, além de um "Laboratório de Análise de Vídeo Forense" para processamento de big data, localização imediata de pessoas, veículos e outros itens de interesse, através da busca de objetos com atributos particulares.[190]

Infelizmente, não encontramos muitas informações sobre o acordo de San Juan utilizando fontes públicas disponíveis. San Juan não tem lei sobre pedidos de acesso a informações públicas, mas de qualquer forma conseguimos fazer nossas perguntas chegarem aos oficiais de governo. Até agosto de 2021, eles não haviam respondido qualquer uma de nossas perguntas.

Notadamente, durante a pandemia da COVID-19 em 2020, governos locais começaram a ver a tecnologia como uma forma de mitigar a propagação do vírus. As autoridades instalaram câmeras térmicas em linhas de ônibus e metrô, aeroportos e estações de transporte público. O governo nacional introduziu o aplicativo "CuidAr,"[191] e as províncias usaram aplicativos móveis para impor quarentenas obrigatórias, controlar multidões e monitorar sintomas, gerando controvérsia sobre o propósito e usos desses aplicativos.[192] Como a análise técnica e o relatório da ADC mostraram, aplicativos em várias províncias, implantados como resposta à emergência de saúde pública, trouxeram sérias preocupações com a segurança e a privacidade das informações das pessoas.[193]

[188] La Voz del Interior. “Resposta a pedidos de informação, uma conta pendente da Província e do município” (em espanhol). Novembro de 2019.
https://www.lavoz.com.ar/ciudadanos/responder-pedidos-de-informacion-una-cuenta-pendiente-de-provincia-y-municipio
[189] El Sol. “Reconhecimento facial: foram encontradas mais de 100 pessoas com mandado de prisão” (em espanhol). Maio de 2019. https://www.elsol.com.ar/reconocimiento-facial-hallaron-a-mas-de-100-personas-con-pedido-de-captura
[190] Website oficial de San Juan. “Acordo de San Juan: tecnologia aplicada à segurança” (em espanhol). Outubro de 2020.
https://sisanjuan.gob.ar/seguridad/2020-10-22/26837-acuerdo-san-juan-tecnologia-aplicada-a-la-seguridad
[191] Conselho da Europa. “”Soluções Digitais para Combater a COVID-19.” Outubro de 2020.
https://rm.coe.int/report-dp-2020-en/16809fe49c
[192] La Capital. “Eles vão controlar quem violou o isolamento com um App em seus telefones celulares” (em espanhol). Março de 2020.
https://www.lacapital.com.ar/la-ciudad/controlaran-quienes-incumplieron-elaislamiento-una-app-sus-celulares-n2572740.html
[193] ADC. “Em caso de emergência: baixe um aplicativo - Parte II” (em espanhol). Dezembro de 2020.
https://adc.org.ar/2020/12/22/en-caso-de-emergencia-descargue-una-app-parte-ii/

ESTUDO DE CASO: Brasil

Pelo Laboratório de Políticas Públicas e Internet (LAPIN)

No Brasil, tanto o setor público quanto o privado estão utilizando tecnologias de vigilância por diversas razões, incluindo segurança pública e segurança, detecção de fraudes e gestão de frequência escolar. Dentre as tecnologias de vigilância disponíveis, as autoridades públicas têm interesse crescente em tecnologias de reconhecimento facial.

O uso dessa tecnologia não é uma grande novidade no Brasil. Um relatório de 2019 do Instituto Igarapé mostra que ela vem sendo implementada desde pelo menos 2011.[194] Desde então, houve um aumento dos casos de uso, e os legisladores têm proposto projetos de lei para regulamentar a tecnologia, que vem avançando tanto nas câmaras federais quanto nas estaduais.

Dentre os inúmeros usos do setor público de reconhecimento facial, destacamos o uso que mais se destaca no Brasil: o reconhecimento facial para **segurança pública**. Autoridades que implantam a tecnologia sob esta lógica estão usando a mesma em diversos espaços públicos, incluindo eventos públicos e festividades. Um fator essencial citado para justificar sua implementação são os números relativos à violência e ao crime no país. Por exemplo,

- ➔ em 2018, o número de homicídios foi de 57.956, uma taxa de 27,8 assassinatos por 100 mil habitantes;[195]
- ➔ naquele mesmo ano, o Brasil tinha uma população carcerária de mais de 720.000 indivíduos;[196] e
- ➔ hoje continua sendo um dos países mais importante para o tráfico internacional de drogas.[197]

A tecnologia também está sendo utilizada para fins como **detecção de fraudes no acesso a serviços públicos, incluindo subsídios de transporte público gratuito e outros benefícios sociais.** No Estado de Alagoas, a tecnologia é utilizada em 102 municípios para verificar a identidade dos beneficiários de programas sociais, como mulheres grávidas e famílias de crianças desnutridas.[198] A cidade de São Paulo utiliza um mecanismo semelhante no sistema de transporte urbano para verificar a identidade das pessoas que utilizam o cartão de entrada gratuita. No entanto, a tecnologia implantada capta imagens na tela de cada indivíduo que entra em um ônibus, não apenas dos portadores do cartão, e mais de 1,5 milhões de pessoas usam ônibus a cada dia em São Paulo.[199] Finalmente, na capital, Brasília,

[194] Instituto Igarapé. "Reconhecimento Facial no Brasil" (em português). 2019. https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/

[195] Instituto de Pesquisa Econômica Aplicada. "Atlas da Violência" (em português). 2020. https://www.ipea.gov.br/atlasviolencia/download/24/atlas-da-violencia-2020

[196] Bueno, S., & Lima, R. S. de. "Anuário Brasileiro de Segurança Pública 2019. Fórum Brasileiro de Segurança Pública" (em português). 2019. https://www.forumseguranca.org.br/wp-content/uploads/2019/10/Anuario-2019-FINAL_21.10.19.pdf

[197] Gabinete das Nações Unidas para o Controle das Drogas e Prevenção do Crime. "Relatório Mundial sobre Drogas 2020." Junho de 2020. https://wdr.unodc.org/wdr2020/field/WDR20_BOOKLET_1.pdf

[198] Renata Bello. "A tecnologia de reconhecimento facial trará mais segurança para o Programa de Complementação Alimentar e Nutricional" (em português). Março de 2018. http://reconhecimentofacial.com.br/2018/03/11/alagoas-tecnologia-de-reconhecimento-facial-trara-mais-seguranca-ao-programa-de-complementacao-alimentar-e-nutricional/

[199] Diário do Transporte. "A demanda de passageiros nos ônibus de São Paulo ultrapassou 1,5 milhões de pessoas por dia útil desde 7 de julho" (em português). Julho de 2020. https://diariodotransporte.com.br/2020/07/27/demanda-de-passageiros-

aproximadamente 2.000 ônibus estão equipados com câmeras de reconhecimento facial.

A empresa que fornece a tecnologia, **PRODATA**, afirma que sua solução é desenvolvida inteiramente em casa. Entretanto, de acordo com informações obtidas através de uma entrevista privada com um representante, vários componentes são importados, como a tecnologia da **Anders** (EUA) e **Compulab** (Israel).

A mesma tecnologia está sendo implementada para a **gestão da frequência escolar** em algumas instituições públicas. A pretexto de melhorar a gestão de recursos, as instituições educacionais estão usando a tecnologia de reconhecimento facial para permitir aos pais rastrear os alunos, monitorar e controlar automaticamente o comparecimento às aulas e oferecer merenda escolar.[200] O uso do reconhecimento facial nas escolas é difundido em todo o Brasil, com exemplos de norte a sul, incluindo escolas municipais,[201] escolas particulares de elite,[202] e até mesmo na maior universidade brasileira, a Universidade de São Paulo.[203] Ainda que a maioria dos programas piloto para esta tecnologia tenha começado entre 2018 e 2020, houve iniciativas mesmo antes de 2014.[204]

Neste relatório, apresentamos 33 pedidos com base na liberdade de informação a várias administrações locais, incluindo secretarias de segurança pública estaduais, forças policiais, prefeituras e serviços de transporte público. A nível federal, fizemos perguntas ao SERPRO, empresa pública responsável pelo processamento de dados do governo, e à Receita Federal, a agência federal de serviços de receita, sobre os serviços de reconhecimento facial que eles prestam no contexto de suas atividades. Recebemos respostas à maioria dessas solicitações, mas elas não tinham detalhes e eram genéricas.[205] Assim, em algumas situações, apresentamos recursos administrativos.[206]

Tecnologia utilizada

Vale notar que não identificamos qualquer caso em que as autoridades tenham utilizado o sistema de compras tradicional, de concorrência aberta. **Os casos mais preocupantes foram aqueles em que as**

nos-onibus-de-sao-paulo-tem-ultrapassado-a-15-milhao-de-pessoas-por-dia-util-desde-07-de-julho/

[200] Revista de Segurança Eletrônica. “As escolas usam o reconhecimento facial para controlar frequência e desperdício de merenda” (em português). Abril de 2018. https://revistasegurancaeletronica.com.br/escolas-usam-reconhecimento-facial-para-controlar-frequencia-e-desperdicio-de-merenda/

[201] Diário do Aço. “Sistema de Reconhecimento Facial já funciona nas escolas de Ipatinga” (em português). Fevereiro de 2020. https://www.diariodoaco.com.br/noticia/0075842-sistema-de-reconhecimento-facial-ja-funciona-nas-escolas-de-ipatinga

[202] Reconhecimento Facial. “A Escola Maple Bear de Porto Alegre começa a usar 2BFACE!” (em português). Junho de 2017. http://reconhecimentofacial.com.br/2017/06/07/escola-maple-bear-porto-alegre-passa-utilizar-o-2bface/

[203] Estadão. “Poli-USP testa câmera de monitoramento facial” (em português). Julho de 2017. https://sao-paulo.estadao.com.br/noticias/geral,poli-usp-testa-novo-sistema-de-seguranca-com-cameras-de-monitoramento-facial,70001900605

[204] Baguete. “Rua lança sistema de reconhecimento facial” (em português). Dezembro de 2015. https://www.baguete.com.br/noticias/09/12/2015/rua-lanca-sistema-de-reconhecimento-facial

[205] Quando este relatório foi concluído, apenas cinco instituições não haviam respondido aos pedidos de liberdade de informação: a Secretaria de Segurança Pública do Estado do Ceará, a Secretaria Pública do Estado do Piauí e as prefeituras de Anápolis, Pilar e Arapiraca.

[206] Um caso que merece destaque é o da SERPRO. Após apresentarmos todos os recursos administrativos possíveis, a empresa recusou-se a compartilhar informações importantes sobre os fornecedores de equipamentos de reconhecimento facial ou o nível de precisão para o sistema, alegando segredos comerciais. Quando esta publicação foi concluída, a LAPIN estava considerando um litígio estratégico para tratar deste caso no Judiciário.

autoridades governamentais locais implantaram tecnologias de vigilância "doadas" para testar na população. Demos vários exemplos desses cenários quando nos dirigimos a cada empresa.

Infelizmente, quando se deparam com uma solicitação com base na liberdade de informação, as autoridades públicas raramente fornecem informações sobre as especificações técnicas destas tecnologias. As principais razões citadas foram reclamações de proteção de propriedade intelectual/ segredos comerciais e falta de conhecimento. Nas poucas vezes em que obtivemos informações sobre especificidades técnicas, as informações eram muito superficiais.

Por exemplo, quando perguntamos sobre a precisão de um sistema de reconhecimento facial, as Secretarias da Segurança Pública da Bahia (SSPS), responderam observando que o sistema alerta as forças policiais quando a identificação de um suspeito atinge uma taxa de probabilidade de 90%. Por sua vez, o governo de Campina Grande nos informou que o sistema tem uma precisão acima de 85% e a câmera tem um alcance de zoom de 2 km. Entretanto, eles não forneceram o número de falsos positivos ou negativos. Também não abordaram a precisão do sistema sob condições de luz diferente ou em pessoas com cores de pele diferentes.

Nossas perguntas sobre a eficiência do sistema na identificação de criminosos também ficaram sem resposta. Os casos reportados pela mídia dão motivos para duvidar da eficácia do sistema. Na Bahia, a polícia prendeu mais de 200 pessoas com base no uso de tecnologias de reconhecimento facial de dezembro de 2018 a agosto de 2020,[207] mas não está claro quantas dessas prisões foram falsos positivos. Houve uma notícia sobre um caso falso positivo, no qual a polícia se aproximou de um menino de 25 anos com necessidades especiais, confundindo-o com um homem procurado por agressão.[208]

No Rio de Janeiro, a força policial alegou que, utilizando tecnologia em torno da área do Estádio do Maracanã, foi possível cumprir 63 mandados de prisão durante a Copa América em 2019. A imprensa relatou dois falsos positivos na época. Um suspeito foi confundido com um indivíduo que já estava preso.[209] Outro, era um homem que ficou preso por vários dias antes da polícia descobrir seu erro.[210]

Ainda mais preocupante do que a falta de precisão é o fato de que os sistemas de reconhecimento facial podem atingir desproporcionalmente as pessoas de cor, como revelou um estudo de um instituto

[207] G1 Bahia. “Homem preso em Salvador após ser identificado pelo sistema de reconhecimento facial” (em português). Março de 2021. https://g1.globo.com/ba/bahia/noticia/2021/03/14/homem-e-preso-em-salvador-apos-ser-identificado-pelo-sistema-de-reconhecimento-facial.ghtml.

[208] Redação 4P. “O sistema de reconhecimento facial de Salvador confunde homens com necessidades especiais com arrombadores” (em português). Janeiro de 2020. https://midia4p.cartacapital.com.br/sistema-de-reconhecimento-facial-de-salvador-confunde-homem-com-necessidades-especiais-com-assaltante/

[209] O Globo Rio. “O reconhecimento facial falha no segundo dia, e uma mulher inocente é confundida com uma criminosa já presa” (em português). Julho de 2019. https://oglobo.globo.com/rio/reconhecimento-facial-falha-em-segundo-dia-mulher-inocente-confundida-com-criminosa-ja-presa-23798913

[210] Band News. “O homem é preso por engano em Copacabana” (em português). Julho de 2019. https://bandnewsfmrio.com.br/editorias-detalhes/homem-e-preso-por-engano-em-copacabana

de pesquisa brasileiro, "Redes de Observatórios de Segurança".[211] Isso traz preocupação com essas tecnologias identificando erroneamente as pessoas que já enfrentam discriminação no Brasil.

Enquadramento jurídico

Assim como a Argentina, o Brasil possui um arcabouço legal que protege a privacidade. A Constituição Federal do Brasil consagra esse direito fundamental nos artigos 5º, X e XII, e o Brasil reconhece tratados internacionais de direitos humanos como o Pacto Internacional de Direitos Civis e Políticos e a Convenção Americana de Direitos Humanos. Além disso, o Brasil possui uma legislação ampla e única em matéria de Internet, o "Marco Civil da Internet", que estabelece regras específicas para a proteção do direito à privacidade no contexto on-line através dos artigos 3º, 8º e 11º. Finalmente, o país estabeleceu um precedente com a adoção da Lei Geral de Proteção de Dados (LGPD), que foi aprovada após anos de engajamento de múltiplas partes interessadas e consagra padrões legais modernos para a proteção de dados.

A legislação relacionada à vigilância do Estado também está em alta. De acordo com o Instituto Igarapé e a associação Data Privacy Brasil,[212] a partir de junho de 2020, **pelo menos quatro leis estaduais abordam tecnologias de reconhecimento facial em algum nível**; três delas, a Lei nº 16.873/2019, do **Ceará**, a Lei nº 21.737/2015, de **Minas Gerais**, e a Lei nº 8.113/2019, de **Alagoas**, regulamentam seu uso nos estádios. Por sua vez, a Lei nº 7.123/2015, do **Rio de Janeiro**, enfoca a implantação da tecnologia no sistema de transporte intermunicipal. Infelizmente, todas as leis acima mencionadas oferecem pouca ou nenhuma proteção legal ao implantar a tecnologia. Mais recentemente, em novembro de 2020, o **Distrito Federal** aprovou a Lei nº 6.712/2020, que regulamenta o uso da tecnologia para fins de segurança pública em espaços públicos na capital brasileira.[213] A Lei nº 6.712 segue algumas boas práticas, tais como tornar obrigatória uma revisão humana quando o sistema identifica uma pessoa antes que qualquer decisão seja tomada. Entretanto, a lei não determina medidas de ciber-segurança, nem procedimentos para o exercício dos direitos da pessoa em questão. Além disso, ela permite o uso da tecnologia para investigações de crimes. Apesar da lei já estar em vigor, não há registro da tecnologia utilizada para fins de segurança pública no Distrito Federal até agora.

Várias iniciativas legislativas têm sido propostas nos Estados nos últimos dois anos. Alguns exemplos são o Projeto de Lei nº 391/2019 - **Minas Gerais**;[214] o Projeto de Lei nº 318/2019 - **Rio de Janeiro**;[215] o

[211] No estudo, 151 casos de uso da tecnologia de reconhecimento facial foram identificados entre quatro estados federais. Em 42 desses casos, havia dados sobre a identidade racial. Desses 42, 38 dos indivíduos rastreados eram negros. Veja mais informações em: Rede de Observatórios da Segurança. “Retratos da Violência” (em português). 2019. https://www.ucamcesec.com.br/wp-content/uploads/2019/11/Rede-de-Observatorios_primeiro-relatorio_20_11_19.pdf

[212] Instituto Igarapé e Pesquisa de Privacidade de Dados. “Regulamentação do reconhecimento facial no setor público: avaliação das experiências internacionais” (em português). Junho de 2020. https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf

[213] Diário Oficial. Lei nº 6.712. Novembro de 2020. https://www.tjdft.jus.br/institucional/relacoes-institucionais/arquivos/lei-no-6-712-de-10-de-novembro-de-2020.pdf

[214] Assembleia Legislativa de Minas Gerais. Projeto nº 391/2019. 2019. https://www.almg.gov.br/atividade_parlamentar/tramitacao_projetos/interna.html?a=2019&n=391&t=PL

[215] Assembleia Legislativa do Rio de Janeiro. Projeto nº 218/2019. 2019. http://alerjln1.alerj.rj.gov.br/scpro1923.nsf/0c5bf5cde95601f903256caa0023131b/d9e71e222a9c8e1c832583d0006d6f05?OpenDocument&Highlight=0,318%2F2019

Projeto de Lei nº 148/2019 - **Paraná**;[216] e o Projeto de Lei nº 865/2019 - **São Paulo**.[217] Outro que merece destaque é o Projeto de Lei nº 42/2020 - **Ceará**.[218] Embora não focalize o reconhecimento facial, a lei permite à polícia coletar dados de câmeras privadas em áreas públicas, ampliando os olhos curiosos do Estado. Finalmente, há também propostas em nível federal, como o Projeto de Lei nº 4.612/2019 e o Projeto de Lei nº 4.858/2020. Embora não haja previsão para que estas propostas sejam incluídas na agenda do Congresso Nacional, o número de projetos de lei referentes à implantação de tecnologias de vigilância nos últimos anos revela o crescente interesse pelo tema.

Em dezembro de 2019, o Ministério da Justiça e Segurança Pública brasileiro publicou a Portaria nº 793/2019.[219] entre outras disposições, promove a implementação de "sistemas de vídeo monitoramento com soluções de reconhecimento facial, Reconhecimento de Caracteres Óticos, uso de inteligência artificial, ou outros".

Embora a **Lei Geral de Proteção de Dados, ou LGPD, tenha entrado em vigor recentemente, ela não se aplica a contextos de segurança pública e segurança**. Este fato prejudica a eficácia da LGPD para tratar do uso da tecnologia de reconhecimento facial em vários casos atuais no Brasil.[220] Uma equipe de especialistas propôs recentemente um projeto de lei "LGPD Penal" que trata dos princípios e obrigações de proteção de dados para o processamento de dados pessoais pelas autoridades de aplicação da lei,[221] mas não sabemos se ou quando será promulgada.

Casos locais

Destacaremos duas regiões onde as tecnologias de reconhecimento facial são fortemente promovidas para a segurança pública: o **Nordeste** (NE) e o **Sudeste** (SE), duas das regiões mais populosas do país.[222] Esse fato em si já causa alguma desaprovação porque mostra como as **áreas populosas podem se tornar laboratórios perfeitos para os testes das tecnologias de reconhecimento facial**.

Muitos dos casos foram implementados por Secretarias de Segurança Pública estaduais ou municipais. Entretanto, as forças policiais (civis e militares) também utilizaram diretamente a tecnologia.

---

[216] Assembleia Legislativa do Paraná. Projeto nº 148/2019. 2019. http://portal.assembleia.pr.leg.br/modules/mod_legislativo_arquivo/mod_legislativo_arquivo.php?leiCod=82332&tipo=I

[217] Assembleia Legislativa of São Paulo. Projeto nº 865/2019, 2019. https://www.al.sp.gov.br/propositura/?id=1000278098

[218] Assembleia Legislativa of Ceará. Projeto nº 42/2019, 2019. https://www2.al.ce.gov.br/legislativo/tramit2020/8531.htm

[219] Diário Oficial da União. Portaria nº 793. Outubro de 2019. https://www.in.gov.br/en/web/dou/-/portaria-n-793-de-24-de-outubro-de-2019-223853575

[220] Embora não se aplique no contexto da segurança pública, no artigo 4, parágrafo 1, a LGPD afirma que a legislação futura para tratar do tema deve prever medidas proporcionais e estritamente necessárias para servir ao interesse público, e deve observar o devido processo legal, bem como os princípios da LGPD sobre proteção de dados e direitos das pessoas envolvidas.

[221] Câmara dos Deputados. Projeto de Lei Criminal LGPD. 2020. https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf

[222] De acordo com o Instituto Brasileiro de Geografia e Estatística, IBGE, a estimativa da população destas duas regiões em 2020 totaliza mais de 146 milhões de pessoas, 69% da população do país. Veja mais informações em: https://ftp.ibge.gov.br/Estimativas_de_Populacao/Estimativas_2020/POP2020_20201030.pdf

A começar pela **Região Nordeste**, três estados devem ser abordados. No estado da **Bahia**, as tecnologias de reconhecimento facial são estrategicamente e amplamente utilizadas em locais públicos como aeroportos, metrôs, estádios, ruas e praças. A tecnologia também tem sido empregada em eventos públicos significativos, como os carnavais de 2020. Em Salvador, as câmeras capturaram 4,3 milhões de registros faciais e a polícia deteve 42 pessoas.[223] Em Feira de Santana, 1,3 milhões de pessoas tiveram seus rostos capturados, com 33 detidas.[224]

O estado do **Ceará** adota uma abordagem diferente e não incorpora a tecnologia em câmeras de rua, mas em smartphones da força policial que capturam rostos quando as autoridades se aproximam de suspeitos. Quando a polícia tira uma foto, eles podem compará-la com as imagens faciais em um banco de dados das Secretarias de Segurança Pública.[225]

O terceiro exemplo no NE é o estado da **Paraíba**. Segundo a Secretaria de Segurança Pública da Paraíba, a tecnologia ainda está em sua fase inicial de implementação, com um contrato assinado em 2020. Portanto, ainda não está claro onde a tecnologia de reconhecimento facial será instalada. Entretanto, o município de Campina Grande utilizou a tecnologia durante as festividades tradicionais de São João, às quais compareceram 1,8 milhões de pessoas, vindas de várias regiões do país.[226]

Na **Região Sudeste**, chamamos a atenção para suas duas maiores capitais do estado, bem como outras duas grandes cidades da região.

No **Rio de Janeiro**, a polícia testou a tecnologia em dois eventos públicos. No Carnaval de 2019, espalharam câmeras por toda a região de Copacabana, onde se estimava a presença de 1,6 milhões de pessoas.[227] Também, durante a Copa América de 2019, evento de futebol que aconteceu entre 6 de julho e 19 de outubro, havia câmeras de reconhecimento facial nas proximidades do estádio do Maracanã. Em entrevistas com as autoridades públicas, foi revelado que há planos de instalar permanentemente essas câmeras em espaços públicos.

Na cidade de **São Paulo**, as tecnologias de reconhecimento facial também foram utilizadas durante o Carnaval de 2020, utilizando câmeras ao vivo instaladas em áreas onde ocorreram eventos

[223] Bahia. “Sistema de Reconhecimento Facial registrou mais de 4,3 milhões de imagens” (em português). Fevereiro de 2019. http://www.bahia.ba.gov.br/2020/02/noticias/carnaval/sistema-de-reconhecimento-facial-ja-registrou-mais-de-43-milhoes-de-imagens/

[224] G1 BA. “Feira de Santana registra 33 prisões por reconhecimento facial durante a micareta” (em português). Abril de 2019. https://g1.globo.com/ba/bahia/noticia/2019/04/29/feira-de-santana-registra-33-prisoes-por-reconhecimento-facial-durante-micareta.ghtml

[225] Daniel Praciano. “Departamento de Segurança analisa parceria com empresa chinesa de tecnologia para implementar novas soluções” (em português). Agosto de 2019. http://blogs.diariodonordeste.com.br/narede/seguranca/secretaria-de-seguranca-analisa-parceria-com-empresa-chinesa-de-tecnologia-para-implantar-novas-solucoes/12531

[226] Viva Campina. “Balanço geral da maior São João do mundo de 2019 tem os melhores resultados das últimas edições” (em português). Julho de 2019. https://www.vivacampina.com.br/noticia/balanco-geral-do-maior-sao-joao-do-mundo-2019-conta-com-os-melhores-resultados-das-ultimas-edicoes

[227] Jornal do Brasil. “Carnaval traz 1,6 milhões de turistas e R$ 3,5 bilhões em receitas para o Rio” (em português). Março de 2019. https://www.jb.com.br/rio/carnaval_2019 rio/2019/03/987757-carnaval-traz-1-6-milhao-de-turistas-e-receita-de-r--3-5-bilhoes-para-o-rio.html

carnavalescos.[228] Além disso, há um projeto contínuo da polícia civil para utilizar a tecnologia para registro de identificação pessoal em tempo real.[229] Ao mesmo tempo, as autoridades realizarão investigações criminais utilizando a captura de tela obtida a partir de várias câmeras instaladas tanto em espaços públicos quanto privados. A tecnologia de reconhecimento facial também será implantada nas estações do metrô, onde cerca de 3,5 milhões de pessoas utilizam o sistema de transporte diariamente.

Outra cidade do estado de São Paulo, **Campinas**, é conhecida por seu "laboratório aberto" sobre o uso de várias tecnologias de "cidade inteligente", incluindo a tecnologia de reconhecimento facial. Lá, 30 câmeras já foram instaladas em várias estações de transporte público e imediações.[230] Com esse tipo de iniciativa, Campinas foi premiada como a cidade mais "inteligente" do Brasil em 2019.[231]

Finalmente, destacamos o caso de **Mogi das Cruzes**, outra cidade do estado de São Paulo conhecida por implementar tecnologia de reconhecimento facial para fins de segurança. Durante a "Festa do Divino Espírito Santo"[232], a polícia criou um banco de dados de pessoas procuradas, como criminosos procurados e crianças perdidas, utilizando imagens raspadas de imagens de perfil de redes sociais.[233] O sistema opera como parte de uma parceria entre o município e a **Dahua Technology**, onde a tecnologia foi entregue gratuitamente às autoridades e, de acordo com a cidade, pode ser utilizada em outros espaços públicos, uma vez que seu mainframe foi instalado em veículos.[234]

[228] Tilt. Helton Simões Gomes. “Pela 1ª vez, SP tem monitoramento facial em tempo real no Carnaval; entenda” (em português) Fevereiro de 2020. https://www.uol.com.br/tilt/noticias/redacao/2020/02/19/folia-vigiada-sp-tera-reconhecimento-facial-ao-vivo-no-carnaval-entenda.htm

[229] Tilt. Helton Simões Gomes. “Grande Irmão Urbano? Como será o reconhecimento facial da polícia de SP” (em português). Novembro de 2019. https://www.uol.com.br/tilt/noticias/redacao/2019/11/15/big-brother-urbano-como-vai-funcionar-o-reconhecimento-facial-em-sao-paulo.htm

[230] Correio. “As câmeras espiãs começam a fase de testes” (em português). Dezembro de 2019. https://correio.rac.com.br/_conteudo/2019/12/campinas_e_rmc/888175-cameras-espias-iniciam-fase-de-testes.html

[231] Prefeitura de Campinas. “Campinas é a cidade mais inteligente e mais conectada do Brasil” (em português). Setembro de 2019. http://www.campinas.sp.gov.br/noticias-integra.php?id=37205

[232] "Festa do Divino Espírito Santo" é uma festa religiosa em Mogi das Cruzes celebrada anualmente, na qual as pessoas se reúnem em espaços públicos para assistir a procissões e concertos, entre outras coisas. No ano passado, foram recebidos cerca de 200.000 participantes durante os sete dias do festival. Veja mais informações em: http://www.festadodivino.org.br/

[233] Diário TV 1ª Edição. “Sistema de reconhecimento facial reforça a segurança na Festa do Divino em Mogi das Cruzes” (em português). Junho de 2019. https://g1.globo.com/sp/mogi-das-cruzes-suzano/festa-do-divino/2019/noticia/2019/06/07/sistema-de-reconhecimento-facial-reforca-seguranca-na-quermesse-da-festa-do-divino-em-mogi-das-cruzes.ghtml

[234] Prefeitura de Mogi das Cruzes. “A segurança para a Festa do Divino terá câmeras de reconhecimento facial” (em português). Maio de 2019. https://www.mogidascruzes.sp.gov.br/noticia/seguranca-para-a-festa-do-divino-tera-cameras-com-reconhecimento-facial

ESTUDO DE CASO: Equador

Por LaLibre.net

O uso de sistemas de vigilância por vídeo em espaços públicos no Equador remonta a 2002, ano em que os prefeitos de Quito e Guayaquil, duas das cidades mais populosas do país, lançaram os primeiros programas piloto do "Sistema Ojos de Águila" (Eagle Eyes System). O projeto foi conduzido inicialmente nos dois municípios e festejado como uma ferramenta para redução da criminalidade[235] e melhoria da percepção de segurança da população. Então, as autoridades instalaram oito[236] câmeras de vídeo vigilância da marca **PELCO** em Quito e 20[237] em Guayaquil, nas áreas centrais de cada cidade.

Outros municípios rapidamente seguiram o exemplo dessas duas grandes cidades, apesar de **não haver estudos conclusivos para demonstrar a eficácia desse tipo de vigilância sobre a segurança do cidadão, redução da criminalidade ou prevenção de mortes violentas**.[238] Entretanto, os meios de comunicação nacionais e locais utilizaram imagens tiradas das câmeras para mostrar o que consideram ser "realizações" de segurança pública.

Entre 2010 e 2014, o governo de Rafael Correa definiu novas políticas para "reduzir a criminalidade e construir uma coexistência social pacífica". Isto consistiu em criar um modelo descentralizado para a Polícia Nacional, com um novo modelo de zoneamento e gestão. As políticas foram concebidas e implementadas principalmente pelo Ministério da Justiça, o Ministério da Coordenação de Segurança e o Ministério do Interior, sob direção de seu ministro José Serrano. Há pesquisas que sugerem que as mudanças podem ter dado a aparência de redução da criminalidade, mas não tiveram impacto significativo. De acordo com os pesquisadores Castro, Jácome e Mancero (2015), os funcionários realmente queriam melhorar os indicadores de criminalidade e exibiram taxas reduzidas em 2014, o mesmo ano em que o preço do petróleo diminuiu e o boom econômico desacelerou.[239] Mas a redução da criminalidade pode não ter sido o resultado do uso de equipamentos de reconhecimento facial, mas um reflexo da categorização da criminalidade de uma nova forma, como parte das modificações do novo Código Penal Orgânico Compreensivo e um trabalho estatístico meticuloso.[240] Em 2010, os novos funcionários da administração criaram o serviço nacional chamado **“Serviço de Segurança Integrado ECU911.”**.

---

[235] Castro, D., Jácome, J.C., Mancero, J. “Segurança Cidadã no Equador: Política Ministerial e Avaliação de Impacto, Anos 2010-2014” (em espanhol). Nova Criminis 9. Pp.111-148. 2015

[236] El Universo. " Oito câmeras para o plano Eagle Eyes” (em espanhol). Abril de 2002. https://www.eluniverso.com/2002/04/22/0001/10/2388C8238A14459AB2ADE998D58D7FFB.html

[237] El Universo. "Controvérsia sobre o uso e gestão do sistema 'Ojos de Águila” (em espanhol). Dezembro de 2007. https://www.eluniverso.com/2007/12/16/0001/10/B3296480B7784A66AA773C39D74E9B3A.html

[238] Ethnodata. “Uma exploração da relação entre o ganho em infraestrutura de segurança e o índice de mortes violentas no Equador” (em espanhol). 2020. https://www.ethnodata.org/es-es/muertes-violentas/upc/

[239] El Universo. "77.530 milhões de dólares que o Equador recebeu em 7 anos pela exportação de petróleo” (em espanhol). Janeiro de 2015. https://www.eluniverso.com/noticias/2015/01/05/nota/4399061/77530-millones-recibio-pais-7-anos-exportacion-petrolera

[240] Ethnodata. “Uma exploração da relação entre o ganho em infraestrutura de segurança e o índice de mortes violentas no Equador.” 2020. https://www.ethnodata.org/es-es/muertes-violentas/upc/

O serviço ECU911 é administrado por um órgão público, subordinado ao Presidente, que direciona todas as chamadas de emergência (polícia, bombeiros, ambulâncias, etc.) para um único número -911- que implica na implantação de vários centros de monitoramento e vigilância por vídeo em todo o país, interligados entre si e reunindo informações de diferentes territórios.

A implementação desse "Serviço Integrado" não tem sido isenta de críticas. Em 2019, o atual Presidente do Equador, Lenin Moreno, revelou que ele tem sido utilizado para espionagem. Ele disse que o trabalho da instituição foi "diversificado para outra tarefa perversa: espionagem de adversários políticos e cidadãos que eles (o governo) pretendiam coagir "[241]. Também houve relatos sobre corrupção no processo de uso e implantação.[242] Apesar disso, o Serviço Integrado continuou a ser desenvolvido e expandido sem questionamentos.

Em 2012, a Secretaria de Planejamento e Desenvolvimento estabeleceu uma nova divisão para unidades de planejamento administrativo: nacional, zona, distritos e circuitos. Eles representam uma unidade de vigilância de acordo com "subcircuitos"de monitoramento e controle. Antes disso, os mecanismos de controle nunca haviam sido tão centralizados. Durante os sete anos seguintes, as autoridades priorizaram a melhoria dos equipamentos da Polícia Nacional e, com base na nova ordem das unidades, elas tinham melhor representação no território. Em 2017, quando Rafael Correa terminou seu mandato, o governo investiu US$ 781 milhões em infraestrutura e equipamentos para a Polícia Nacional.[243]

Ao final desta pesquisa, o antigo governo equatoriano era um dos menos populares na América Latina,[244] talvez devido a sua polícia agressiva e suas forças de segurança e a um histórico sombrio de violações dos direitos humanos.[245] O Ministério do Governo (Interior e Polícia) era administrado por um Comandante Geral da Polícia, o Ministério da Defesa por um Major-General de Divisão do Exército e o Diretor do Serviço Integrado de Segurança ECU911 é um Tenente-Coronel da Polícia do Estado-Maior General. Todos eles foram nomeados diretamente pelo executivo, sem competição ou oposição.

Para de obter informações para este relatório, apresentamos vários pedidos formais baseados no direito de acesso a informações públicas estabelecido na Lei Orgânica de Transparência e Acesso a Informações Públicas, Art. 1 e Art. 18 (números 1 e 2) e Art. 66 da Constituição da República do Equador. Apresentamos os pedidos a várias instituições, mas obtivemos muito poucas respostas.

---

[241] El Comercio. “Lenín Moreno diz que ECU 911 foi usado de forma "perversa" para espionagem” (em espanhol). Abril de 2019. https://www.elcomercio.com/actualidad/lenin-moreno-ecu-911-espionaje.html

[242] Vistazo. "ECU-911: Contratos que entram em pânico" (em espanhol). Maio de 2019, https://www.vistazo.com/seccion/pais/ecu-911-contratos-que-dan-panico

[243] Nota do Relatório Presidencial. “781 milhões de dólares é o investimento do governo em infraestrutura e equipamentos para a polícia” (em espanhol). Acessado em janeiro de 2020. https://www.presidencia.gob.ec/781-millones-de-dolares-es-la-inversion-del-gobierno-en-infraestructura-y-equipamiento-para-la-policia/

[244] Mitofsky. " Aprovação dos líderes da América e do mundo " (em espanhol). Março de 2021. http://www.consulta.mx/index.php/encuestas-e-investigaciones/el-mundo/item/download/1209_7300384f47710f38dd84cec8765dd463

[245] OEA. " A CIDH apresenta observações sobre sua visita ao Equador" (em espanhol). Janeiro de 2020. https://www.oas.org/es/cidh/prensa/comunicados/2020/008.asp

Quando perguntamos sobre a implementação da tecnologia de vigilância por vídeo, o uso de tecnologias de reconhecimento facial e o enquadramento jurídico para a sua utilização, a Assembleia Nacional respondeu apenas a algumas de nossas perguntas. Soubemos que o debate sobre o atual projeto de lei de proteção de dados ainda estava em andamento e não há enquadramento jurídico para o uso de tecnologias de vigilância por vídeo e reconhecimento biométrico.[246]

Em alguns casos, as autoridades solicitaram mais tempo para fornecer informações adicionais para complementar a resposta inicial.

Também enviamos um pedido ao ECU911 na esperança de obter informações sobre como os dados das pessoas são tratados, quem pode acessar esses dados, a existência de protocolos de segurança, se realizaram uma avaliação do impacto sobre os direitos humanos e os nomes dos produtos e dispositivos implantados, entre outras questões. Infelizmente, a instituição se dispensou de fornecer informações, alegando que se trata de um segredo de Estado. **O ECU911 disse que eles não possuem câmeras com capacidade de reconhecimento facial, mas vários anúncios oficiais indicam o contrário.[247]**

Até a conclusão deste relatório, em agosto de 2021, não recebemos respostas de outras instituições relevantes, incluindo o Ministério do Governo, o Ministério das Telecomunicações e Sociedade da Informação e a Direção Nacional de Registro de Dados Públicos. (DINARDAP).

Tecnologias utilizadas

Em abril de 2019, o New York Times publicou uma investigação sobre o uso pelo Equador da tecnologia de vigilância por vídeo desenvolvida por empresas chinesas.[248] Ela revelou o funcionamento de 4.300 câmeras utilizadas para tarefas de inteligência sem regulamentação. Neste relatório, levamos em conta a infraestrutura de vigilância por vídeo controlada diretamente pelo ECU911, mas existem centenas de dispositivos de vigilância por vídeo que funcionam de forma autônoma nos municípios de Quito e Guayaquil. Em 2020, essas cidades foram conectadas ao Serviço Integrado de Segurança ECU911 para aumentar suas capacidades.

Para obter o número real de "Olhos de Águia" instalados no país, pedimos ao Diretor do Serviço Integrado de Segurança ECU911, Juan Zapata, que fornecesse informações a este respeito. Mesmo ele tendo se recusado a responder, suas declarações anteriores indicam que em outubro de 2019 (antes da integração com os sistemas municipais de Quito e Guayaquil), o Serviço tinha 4.638 dispositivos ativos para vigilância por vídeo.[249] Havia 890[250] câmeras no Município de Quito que foram integradas em

[246] Resposta da Assembleia Nacional. Dezembro de 2020. https://nube.cyberzen.ec/s/qjto9dZwmmW9GRT

[247] Serviço de Segurança Integrado ECU911. “O ECU 911 apresentou um relatório relacionado aos mecanismos e ferramentas de cooperação internacional” (em espanhol). Outubro de 2019. https://www.ecu911.gob.ec/ecu-911-presento-informe-relacionado-con-mecanismos-y-herramientas-de-cooperacion-internacional/

[248] New York Times. “Fabricado na China e exportado para o Equador: o aparelho de vigilância estatal” (em espanhol). Abril de 2020. https://www.nytimes.com/es/2019/04/24/espanol/america-latina/ecuador-vigilancia-seguridad-china.html

[249] Serviço de Segurança Integrado ECU911. " Na Smart City 2019, foi anunciado o plano de modernização do sistema de vigilância por vídeo ECU 911” (em espanhol). Outubro de 2019. https://www.ecu911.gob.ec/en-smart-city-2019-se-anuncio-el-plan-de-modernizacion-del-sistema-de-videovigilancia-del-ecu-911/

[250] Serviço de Segurança Integrado ECU911. "1.518 câmeras do ECU 911 e da Prefeitura interconectadas para a segurança de

Janeiro de 2020 e 1.100 câmeras do Município de Guayaquil em setembro. Com base nessas informações, **há mais de 6.600[251] câmeras controladas pelo ECU911.**

A pandemia da COVID-19 resultou em maior controle e vigilância, o que uma grande parte do público vê como positivo e aceita. Embora essa vigilância seja vista como justificável devido ao medo que uma crise sanitária e humanitária gera, essas ferramentas não têm sido utilizadas apenas para medir o distanciamento social ou fornecer segurança aos cidadãos. Segundo o Presidente Lenin Moreno, estes instrumentos também são utilizados para espionagem e assédio político, estabelecendo a possibilidade de reincidência.[252]

Vale mencionar que em julho de 2020 o **Banco Interamericano de Desenvolvimento** contribuiu para o desenvolvimento do governo equatoriano de um software chamado "**Distancia2**" para uso com as câmeras de vigilância por vídeo já instaladas nas ruas. O software, que as autoridades e a mídia têm promovido amplamente, utiliza inteligência artificial para medir a distância física entre as pessoas, alertando as agências de monitoramento quando as regras de distanciamento da COVID-19 não estão sendo seguidas.[253]

As tecnologias de vigilância implementadas no Equador são fornecidas principalmente pelas seguintes empresas: **Axis** (Suécia), **Hikvision** (China) e **VERINT** (Israel e Estados Unidos). Entretanto, há uma implantação em pequena escala utilizando produtos da **Intelligent Security Systems** (Rússia), **Pelco Corporations** (EUA) e **Tiandy** e **ZKTeco** (China). A maioria deles opera em conjunto por meio de protocolos e padrões desenvolvidos pela **OVNIF**,[254] uma organização dedicada ao desenvolvimento de padrões para a interoperabilidade de dispositivos de segurança.

Enquadramento jurídico

O Equador tem algumas disposições na lei relativas à privacidade a nível constitucional e internacional. A Constituição do Equador consagra o direito fundamental à privacidade no Artigo 66, e o Equador reconhece os tratados internacionais de direitos humanos, como o Pacto Internacional sobre Direitos Civis e Políticos e a Convenção Americana sobre Direitos Humanos. **Entretanto, em contraste com o Brasil e a Argentina, o Equador carecia de um regulamento específico sobre proteção e privacidade de dados até 2021.** Após o vazamento de dados pessoais de 20 milhões de equatorianos em 2019.[255] o Presidente e várias instituições se comprometeram a desenvolver uma lei de proteção de

Quito" (em espanhol). Janeiro de 2020.
https://www.ecu911.gob.ec/1-518-camaras-del-ecu-911-y-del-municipio-interconectadas-para-la-seguridad-de-quito/

[251] Serviço de Segurança Integrado ECU911. " As câmeras 911 ECU registram indisciplina e não conformidade com os cidadãos em várias cidades do país" (em espanhol). Maio de 2020. https://www.ecu911.gob.ec/camaras-del-ecu-911-registran-indisciplina-e-incumplimiento-ciudadanos-en-varias-urbes-del-pais/

[252] El Comercio. "Lenín Moreno diz que o ECU 911 foi usado de forma "perversa" para espionagem" (em espanhol). Abril de 2019. https://www.elcomercio.com/actualidad/lenin-moreno-ecu-911-espionaje.html

[253] El Comercio. " Câmeras de segurança irão monitorar o distanciamento físico no Equador" (em espanhol). Junho de 2020. https://www.elcomercio.com/actualidad/camaras-vigilaran-distanciamiento-fisico-covid19.html

[254] Veja mais informações em: https://www.onvif.org/

[255] BBC News. " Violação de dados no Equador: a "falha grave do computador" que expôs as informações pessoais de quase toda a população do país sul-americano " (em espanhol). Setembro de 2019.
https://www.bbc.com/mundo/noticias-america-latina-49721456

dados a curto prazo para responder às preocupações do público.[256] Em Maio de 2021, a Assembleia Nacional aprovou uma lei moderna de proteção de dados.[257] Ainda será determinado se esta lei será suficiente para proteger os cidadãos de tecnologias de vigilância intrusivas, uma vez que não há nenhuma regulamentação específica planejada a este respeito.

Casos locais

Em 2019, os prefeitos de Quito e Guayaquil empreenderam projetos paralelos com o objetivo semelhante de adquirir câmeras e licenças de análise de vídeo para o reconhecimento facial com inteligência artificial.

Em janeiro de 2020, as autoridades assinaram um acordo interinstitucional para a integração da infraestrutura de vigilância dos centros de monitoramento de Quito com os da ECU911, aumentando a capacidade total de vigilância para 1.518.[258] dispositivos de vigilância por vídeo para a cidade. As 628 câmeras do Serviço Integrado ECU911 e as 890 câmeras da Prefeitura de Quito, assim como quaisquer novas câmeras, estão agora acessíveis a ambas as instituições.

Mais tarde, em 2020, os dispositivos de vigilância por vídeo de Guayaquil foram integrados ao ECU911, assim como o sistema de Quito e de outras regiões haviam sido nos meses anteriores. O governo construiu um novo centro operacional do ECU911 na cidade por aproximadamente US$13 milhões, incluindo US$1 milhão para a aquisição de software para análise de vídeo e várias câmeras para integração no sistema nacional de vigilância por vídeo. Existem, portanto, mais de 2.000 dispositivos que monitoram esta cidade.

Com base em comunicados de imprensa e contratos públicos, concluímos que o sistema integrado de vigilância é utilizado principalmente em Guayaquil e Quito, mas a tecnologia é instalada em todo o país, mesmo em pequenos municípios, como Shushufindi[259] [260] e Quevedo.[261]

[256] El Universo. " O Projeto de Lei de Proteção de Dados Pessoais no Equador " (em espanhol). Agosto de 2020. https://www.eluniverso.com/larevista/2020/08/24/nota/7953820/datos-personales-ley-ecuador

[257] Registro Oficial. Quinto Suplemento nº 459. https://www.registroficial.gob.ec/index.php/registro-oficial-web/publicaciones/suplementos/item/14857-quinto-suple mento-al-registro-oficial-no-459

[258] Serviço de Segurança Integrado ECU911. "1.518 câmeras do ECU 911 e da Prefeitura interconectadas para a segurança de Quito " (em espanhol). Janeiro de 2020. https://www.ecu911.gob.ec/1-518-camaras-del-ecu-911-y-del-municipio-interconectadas-para-la-seguridad-de-quito/

[259] Sistema de Compras Públicas Oficial. SIE-GADMSFD-012-2016. Agosto de 2016. https://www.compraspublicas.gob.ec/ProcesoContratacion/compras/PC/informacionProcesoContratacion2.cpe?idSoliCompra=lIWn6R6_KAorcEHiMtHkUdaqUHKgoWj2Xc9ws8xEKOY,

[260] Sistema de Compras Públicas Oficial. SIE-GADMSFD-2018-059. Dezembro de 2018. https://www.compraspublicas.gob.ec/ProcesoContratacion/compras/PC/informacionProcesoContratacion2.cpe?idSoliCompra=6N1fWVKkcDQjCErudz79IPThdQYl2SDKXJgMZHkNfh0,

[261] Sistema de Compras Públicas Oficial. SIE-GADMQ-006-2019. Dezembro de 2019. https://www.compraspublicas.gob.ec/ProcesoContratacion/compras/PC/informacionProcesoContratacion2.cpe?idSoliCompra=bCDa1cd5ztLy9wcH_d5PXToQ4JsCMfZg_iiQ1xdj-zQ,

IV. CONCLUSÃO E RECOMENDAÇÕES

As tecnologias discutidas neste relatório representam uma ameaça crescente aos nossos direitos humanos: elas dão às autoridades a capacidade de identificar, seguir, destacar e rastrear pessoas onde quer que elas vão, minando nossos direitos à privacidade e proteção de dados, o direito à livre reunião e associação (levando à criminalização do protesto e induzindo um efeito inibidor), e os direitos à igualdade e à não-discriminação. Grupos da sociedade civil em todo o mundo têm lançado o alarme sobre o uso do reconhecimento facial e outras tecnologias de vigilância biométrica, e há movimentos e campanhas para proibir a aplicação dessas tecnologias na União Europeia,[262] nos Estados Unidos,[263] na Índia,[264] na Rússia,[265] e em muitos outros lugares.

O objetivo deste relatório não é apenas mostrar que estas tecnologias ameaçam nossos direitos, mas expor a falta de transparência e responsabilidade das empresas que negociam com governos sua implementação. Em alguns casos, estas empresas fornecem essa perigosa tecnologia gratuitamente para testá-la na população, ignorando o impacto sobre os direitos fundamentais das pessoas. Enquanto esperamos que este relatório motive organizações de direitos, jornalistas e ativistas a continuar fazendo perguntas e investigando empresas e governos, o ônus de evitar danos não deve recair apenas sobre a sociedade civil. Os governos têm o dever de proteger os direitos fundamentais dos cidadãos, e as empresas devem respeitar esses direitos. Precisamos de que **legisladores tomem medidas ousadas e concretas para impedir a disseminação desta tecnologia, banindo uma tecnologia que permite a vigilância em massa** e apresentem salvaguardas para proteger as pessoas, como a tutela daqueles cuja privacidade é violada, e medidas robustas para **aumentar a responsabilidade e a transparência - tanto para as empresas que desenvolvem essa tecnologia quanto para as autoridades que a utilizam.** Permitir amplas exceções para o uso da tecnologia por razões de "segurança pública" abre a porta para o abuso desses sistemas. A segurança pública também não é uma desculpa legítima para manter cidadãos, jornalistas e outros na sociedade civil no escuro.

Ao utilizar qualquer tipo de tecnologia, e ainda mais nos casos em que os direitos fundamentais estão em jogo, os **governos** devem realizar avaliações de impacto sobre os direitos humanos antes de tomar uma decisão ou implantar o sistema, e recusarem-se a comprar ou utilizar tecnologia de empresas com um histórico de direitos humanos precário. Os órgãos públicos devem melhorar sua transparência comunicando e compartilhando os documentos relacionados às reuniões e acordos para a aquisição de tecnologia de vigilância, e consultando a sociedade civil sobre o potencial impacto adverso.

Enquanto isso, as **empresas** devem se comprometer a cumprir as normas de transparência, responsabilidade e respeito aos direitos humanos.

---

[262] Para mais informações visite https://reclaimyourface.eu/

[263] Para mais informações visite https://banthescan.amnesty.org/

[264] Internet Freedom Foundation. "*FF propõe uma moratória de três anos sobre o uso da Tecnologia de Reconhecimento Facial na Índia #ProjectPanoptic.*" Março de 2020. https://internetfreedom.in/we-have-written-to-the-government-seeking-a-3-year-moratorium-on-government-use-of-facial-recognition-technology-in-india-projectpanoptic/

[265] Para mais informações visite https://bancam.ru/en

Para fazer isso, elas precisam melhorar sua comunicação quando recebem pedidos de informações sobre produtos e serviços com implicações para os direitos humanos, implementar procedimentos sólidos de *due diligence* em matéria de direitos humanos, produzir relatórios de transparência, buscando de forma proativa e contínua informações para compreender e tomar ciência do impacto de suas tecnologias sobre os direitos humanos, e fornecer remédios adequados às vítimas dos abusos que elas facilitam.[266]

O público e a mídia tradicional têm um papel fundamental na criação de conscientização e debate, mudando a narrativa sobre a tecnologia de vigilância de "uma solução mágica" para ferramentas que requerem uma ampla discussão pública e um compromisso de cumprimento às leis e princípios de direitos humanos.

[266] Alto Comissariado das Nações Unidas para Direitos Humanos, "Princípios Orientadores sobre Empresas e Direitos Humanos" Junho de 2011. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf