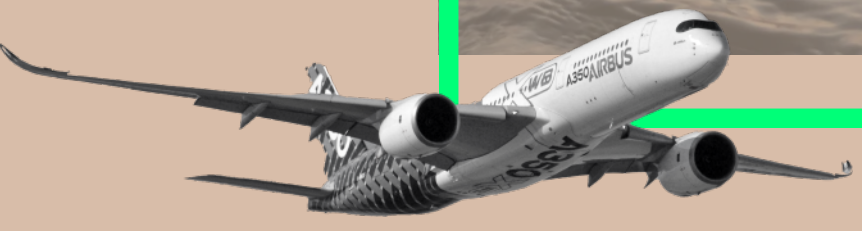
Tecnología de vigilancia en América Latina

Hecha en el exterior, utilizada en casa



accessnow

Access Now defiende y extiende los derechos digitales de los usuarios en riesgo alrededor del mundo. Mediante la combinación de apoyo técnico directo, campañas globales, el análisis integral de políticas públicas, el financiamiento a grupos locales emergentes, intervenciones judiciales y eventos como RightsCon, luchamos por los derechos humanos en la era digital.

Este documento se actualizó por última vez el 10 de agosto de 2021

Este documento es una publicación de Access Now. Fue escrito por Gaspar Pisanu y Verónica Arroyo de Access Now; Leandro Ucciferri y Eduardo Ferreyra de Asociación por los Derechos Civiles (Argentina); Thiago Morales, José Renato Laranjeira, Eduarda Costa Almeida, Fernando Fellows Dourado, Carolina Reis, y Felipe Rocha da Silva de Laboratório de Políticas Públicas e Internet (Brasil); y Jonathan Finaly y Anais Córdova-Páez de LaLibre.net (Ecuador). Agradecemos a miembros del equipo de Access Now que brindaron su apoyo: 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 y Donna Wentworth. También damos las gracias a periodistas, investigadores(as) y activistas que nos ayudaron a proporcionar los puntos y la información claves de esta publicación. Esperamos recibir comentarios y más contribuciones de especialistas en derechos digitales, vigilancia y privacidad.

Access Now (https://www.accessnow.org) defiende y extiende los derechos digitales de los usuarios en riesgo alrededor del mundo. Mediante la combinación de apoyo técnico directo, campañas globales, el análisis integral de políticas públicas, el financiamiento a grupos locales emergentes, intervenciones jurídicas y eventos como RightsCon, luchamos por los derechos humanos en la era digital.

Agosto del 2021

Para obtener más información, comuníquese con nosotros:
Gaspar Pisanu
(gaspar@accessnow.org)
Verónica Arroyo
(veronica@accessnow.org)
Ángela Alarcón
(angela@accessnow.org)

TABLA DE CONTENIDOS

RESUMEN EJECUTIVO

Desliza a la izquierda, desliza a la derecha, dale “me gusta”, comparte, hazlo otra vez. Cada vez somos más conscientes del impacto que tiene la tecnología digital en nuestros derechos. Quienes formulan las leyes alrededor del mundo están poniendo su atención en empresas como Google, Facebook, Amazon, Microsoft y Apple y, en muchos casos, elaboran nueves leyes y políticas para regular estos guardianes (*gatekeepers*) de los derechos fundamentales. Sin embargo, otras empresas están pasando inadvertidas, vendiendo tecnología de vigilancia que se utiliza en toda América Latina sin la transparencia ni el escrutinio público suficientes. Esto socava procesos democráticos, nos quita privacidad y debilita la libertad de expresión y otros derechos humanos básicos.

A menudo, escuchamos que personas en cargos públicos plantean que la compra y el uso de herramientas de vigilancia es un avance tecnológico y una medida positiva para “luchar contra el crimen”. Aun así, las herramientas usadas para identificarnos, individualizarnos y rastrearnos donde vayamos son **inherentemente incompatibles con los derechos humanos y las libertades civiles**. Además, investigaciones indican que los sistemas de reconocimiento facial y otras maneras de identificar personas de manera remota en función de sus características físicas —o datos biométricos— a menudo son muy defectuosos, tienen sesgos raciales y son discriminatorios. Es por esto que existe un movimiento que se está expandiendo en todo el mundo para prohibir el uso de la IA para la vigilancia biométrica masiva.[1]

Lamentablemente, muchos gobiernos latinoamericanos están moviéndose en dirección opuesta, ansiosos por comprar esta tecnología y acelerar la implementación de la vigilancia biométrica masiva.[2] Principalmente, como explicamos en este informe, la mayor parte de la tecnología de vigilancia desplegada en América Latina proviene de Asia (Israel, China y Japón), Europa (Reino Unido y Francia), y los EE. UU., ya sea de manera directa o a través de una red de distribuidores. Entre los proveedores, se encuentran **AnyVision, Hikvision, Dahua, Cellebrite, Huawei, ZTE, NEC, IDEMIA,** y **VERINT**.

Consideremos la creciente infraestructura de vigilancia biométrica en **Argentina**, **Brasil** y **Ecuador**, los países que destacamos en este informe.

En el 2011, **Argentina** introdujo una base de datos biométricos masiva llamada **SIBIOS**. Durante los últimos diez años, se ha convertido en la infraestructura de muchas tecnologías de vigilancia, desplegadas tanto a escala nacional como local, desde globos de vigilancia en la Ciudad Autónoma de Buenos Aires hasta cámaras de reconocimiento facial en la provincia de Córdoba y cámaras térmicas en los aeropuertos principales.

En **Brasil**, tanto en el sector público como en el privado, se están usando tecnologías de vigilancia, y los argumentos para su uso son la seguridad pública, la detección de fraudes y el seguimiento de la asistencia escolar, entre otros. Estados de la región noreste y sudeste, dos de las regiones más pobladas del país, han promocionado intensamente el uso de tecnologías de reconocimiento facial como una

[1] Access Now. “Ban Biometric Surveillance.” Junio del 2021. https://www.accessnow.org/ban-biometric-surveillance/
[2] Access Now. “Instead of banning facial recognition, some governments in Latin America want to make it official.” Diciembre del 2020. https://www.accessnow.org/facial-recognition-latin-america/

medida para aumentar la seguridad pública, sin presentar pruebas que respalden esos argumentos. Los casos más preocupantes desde el punto de vista de la seguridad son los de la tecnología de vigilancia "donada" a gobiernos locales por empresas privadas, la cual a veces se usa en el público como población de testeo.

En el 2010, **Ecuador** implementó el "Servicio Integrado de Seguridad **ECU911**", que desarrolló una infraestructura de vigilancia para las fuerzas del orden en todo el país con más de 6 600 cámaras, algunas de las cuales tienen integrada la tecnología de reconocimiento facial. En el 2019, descubrimos que el gobierno ha estado usando esa misma infraestructura para espiar a rivales políticos y coaccionar a ciertas partes de la ciudadanía.

¿Por qué se está adoptando tecnología de vigilancia tan rápidamente a pesar de la amenaza que supone para los derechos fundamentales de las personas? El público confía en que los medios funcionen como organismos de control que levanten la alarma cuando existan riesgos para los derechos y las libertades democráticas. Por desgracia, en América Latina, cuando la prensa comunica y el sector político habla de los problemas reales y delicados de la violencia y la delincuencia en las calles, en muchos casos y sin sentido crítico, describen estas herramientas como la solución a los problemas. Los gobiernos se ven presionados por la población para encontrar "soluciones", y las empresas de tecnología aprovechan esta dinámica para generar ganancias, a pesar de que tienen la responsabilidad de asegurar que sus productos no se usen para violar los derechos humanos.

Cuando ni el gobierno ni el público entienden cómo funcionan realmente estas tecnologías, y la transparencia y la rendición de cuentas necesarias no se integran ni se aplican para proteger a las personas, **se genera la receta perfecta para la expansión continua y el uso generalizado de estas tecnologías.**

Este informe procura **exponer a las empresas detrás de estos productos peligrosos, a los gobiernos que los compran, y las políticas y prácticas de despliegue que perjudican los derechos de las personas**. En muchos países latinoamericanos, el proceso por el que las autoridades celebran acuerdos para la adquisición de tecnología de vigilancia es solapado y poco transparente. Los gobiernos hacen tratos con poco o nulo debate público o supervisión, y a menudo con poca consideración en cuanto a transparencia y la responsabilidad de comunicarse con el público. Los países que permiten la exportación de estos productos de vigilancia a América Latina también son culpables. Las empresas que no actúan con la debida diligencia y que facilitan el abuso de los derechos humanos deben asumir su responsabilidad.

A tal efecto, hemos trabajado con nuestros socios de la **Asociación por los Derechos Civiles (ADC)**, el **Laboratório de Políticas Públicas e Internet (LAPIN)**, y **LaLibre.net (Tecnologías Comunitarias)** para **investigar a las empresas que proveen estas tecnologías**, examinando sus antecedentes en materia de derechos humanos. **Analizamos el impacto de la tecnología** en los derechos de las personas en **Argentina**, **Brasil** y **Ecuador**, y brindamos ejemplos concretos de cada país. Finalmente, **presentamos recomendaciones** para **legisladores(as)**, los **gobiernos**, las **empresas**, los **medios** y el **público general**, y alentamos a las partes interesadas a tomar acción.

Los países latinoamericanos cuentan con amplios antecedentes de persecución de disidencias y personas de comunidades marginalizadas, y las autoridades continúan abusando de su poder público. La pandemia de COVID-19 ha dado a los gobiernos una nueva excusa para desplegar herramientas de vigilancia peligrosas en nombre de la seguridad pública, aunque fallen en proteger los derechos humanos. Esperamos que este informe aliente a las organizaciones de la sociedad civil, los medios y la ciudadanía a **hacer preguntas, investigar a las empresas y exigir que sus gobiernos protejan y promuevan los derechos humanos**. Como lo demuestran nuestros casos de estudio, los riesgos son altísimos.

I. INTRODUCCIÓN:
UNA COLABORACIÓN PARA EXPONER A LOS PROVEEDORES

Access Now, la Asociación por los Derechos Civiles (ADC), el Laboratório de Políticas Públicas e Internet (LAPIN), y LaLibre.net colaboraron en la investigación llevada adelante para elaborar este informe, resultado final de una investigación exhaustiva centrada en Argentina, Brasil y Ecuador durante el último trimestre del 2020.

Como es sabido, los gobiernos nacionales y locales de estos países están implementando cada vez más tecnologías de vigilancia masiva. Sin embargo, por lo general hay poca o nula información disponible sobre quién brinda esta tecnología, qué tipo de tecnología se compra, y bajo qué condiciones se despliega. Esta falta de transparencia frustra la oportunidad de la sociedad civil de entender qué está sucediendo y responder de manera acorde. Así que, nuestras organizaciones decidieron mapear a los distribuidores y las tecnologías vendidas, y dejar al descubierto las relaciones entre los gobiernos y las empresas. Este informe tiene el objetivo de arrojar luz sobre estas transacciones, exponer el daño a los derechos humanos y someter a escrutinio público a las empresas que, irresponsablemente, venden tecnología de vigilancia a América Latina.

A fin de obtener la mayor cantidad de información posible, presentamos pedidos de acceso a la información, analizamos informes periodísticos, y nos comunicamos con representantes de las empresas para reunir datos y llevar a cabo entrevistas. Descubrimos que muchas empresas de tecnología de vigilancia con malos antecedentes de derechos humanos encontraron en los países latinoamericanos los clientes “tecnosolucionistas” perfectos para venderles, sin mayores obstáculos, tecnología perjudicial para nuestros derechos. Además, identificamos patrones en las relaciones entre los gobiernos y estas empresas, que demuestran una clara indiferencia en cuanto al cumplimiento de los estándares fundamentales de transparencia y rendición de cuentas.[3] Estos y otros hallazgos nos permiten concluir que, en Argentina, Brasil y Ecuador, las amenazas a los derechos humanos se están expandiendo junto con el creciente arsenal de tecnologías adquiridas solapadamente y desplegadas por los gobiernos con poca consideración por los derechos humanos. Por este motivo, concluimos este informe con una advertencia sobre que la situación actual debe cambiar, y ofrecemos recomendaciones urgentes para los gobiernos y las empresas.

Nuestra metodología de investigación consta de tres etapas:

1) **Investigación**: cada organización reunió información de sitios de compras/presupuestos públicos, comunicaciones oficiales, artículos de noticias, respuestas a nuestras solicitudes de acceso a la información de oficinas públicas específicas y entrevistas con representantes de empresas, periodistas e investigadores(as).
2) **Informes locales**: elaboramos una explicación y un análisis del contexto legal y político y el estado actual de utilización de la vigilancia en cada país.
3) **Análisis cruzado**: examinamos el comportamiento y los modelos de negocio de cada proveedor que vende tecnología de vigilancia (de manera directa o a través de representantes locales) y evaluamos sus antecedentes de derechos humanos a nivel mundial.

[3] Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. “Principios Rectores sobre las Empresas y los Derechos Humanos”. Junio del 2011. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_sp.pdf

II. LAS EMPRESAS: ¿QUIÉN SE BENEFICIA DE LAS VIOLACIONES DE DERECHOS HUMANOS?

Comenzamos este informe centrándonos en las empresas que proporcionan las tecnologías de vigilancia que los gobiernos están desplegando en Argentina, Brasil y Ecuador. Destacamos a las empresas que tienen una participación significativa en el mercado en estos países o que venden tecnología que es particularmente peligrosa para los derechos humanos. Brindamos información de contexto sobre sus historias, las tecnologías que venden, y su posición en los mercados de estos países latinoamericanos. Finalmente, revisamos sus antecedentes de derechos humanos como elemento clave para comprender los peligros que representan sus productos en América Latina. Tras exponer información detallada sobre las empresas, procedemos a los casos de estudio que demuestran el daño que ya se está provocando en los derechos fundamentales de las personas.

Obtuvimos la mayor parte de la información sobre las empresas a partir de declaraciones oficiales de autoridades públicas y representantes de las empresas, informes mediáticos, redes sociales y entrevistas directas. En la gran mayoría de los casos, no fuimos capaces de establecer una comunicación directa con las empresas.

Es muy difícil obtener información sobre cómo se están utilizando las tecnologías cuando estas fueron compradas a distribuidores locales en lugar de a los fabricantes. Esta es otra de las maneras en que las empresas de vigilancia pueden quedarse ocultas y evitar el escrutinio público, además de ignorar consultas y brindar nula comunicación y transparencia.

⇛ AnyVision

Nombre de la empresa	**AnyVision Interactive Technologies Ltd**
Sede principal	Jolón, Israel
Países en los que opera	Israel, Reino Unido y Estados Unidos
Países en los que se despliegan sus tecnologías de vigilancia entre Argentina, Brasil y Ecuador	Argentina
Fundación	2015
Pública/privada	Privada
Accionista(s) mayoritario(s)	DFJ Growth, OG Technology Partners, LightSpeed Venture Partners, Qualcomm Ventures, Bosch Building Technologies SVP [en el 2020]
Cantidad de empleados(as)	240 en el 2020
Ingresos anuales	No disponible

AnyVision es una empresa israelí que se especializa en tecnología de reconocimiento facial para la seguridad pública, así como también en aplicaciones para la atención de la salud, casinos y bancos.[4] Únicamente mediante anuncios públicos y cobertura mediática[5] pudimos descubrir que AnyVision es la empresa que proporciona el "software de reconocimiento biométrico" adquirido por la provincia de Córdoba en **Argentina.**

AnyVision también parece ser el proveedor del software que se utiliza en el Aeropuerto Internacional de Ezeiza de la provincia de Buenos Aires, Argentina. A partir de registros oficiales, hallamos que las autoridades adquirieron un sistema de reconocimiento facial a través de negociaciones directas con un revendedor local de AnyVision en el país: la empresa **RC International**. El primer contrato directo entre la Policía de Seguridad Aeroportuaria (PSA) y RC International data de diciembre del 2017 y tuvo un valor aproximado de USD 48 000. El contrato conllevó la adquisición de cuatro licencias de reconocimiento facial de AnyVision, junto con cuatro cámaras de Protocolo de Internet (IP) y un servidor, con la capacidad de escanear y comparar rostros con 2,5 millones de registros de rostros.[6] Un año después, la PSA firmó otro contrato directo con RC International de alrededor de USD 54 000 para adquirir cinco licencias para mejorar la infraestructura de procesamiento.[7]

El 17 de julio del 2020, cuando se le preguntó sobre la implementación de la tecnología de AnyVision, el gerente de negocios y estrategia de RC International, Pablo Marcovich, confirmó[8] que desde hace dos años que la PSA usaba la tecnología de reconocimiento facial de AnyVision en Ezeiza.

Antecedentes de derechos humanos de AnyVision

Según una investigación publicada por NBC en marzo del 2020, las autoridades israelíes usaban la tecnología de AnyVision en un esquema de vigilancia secreta para monitorear el movimiento de personas palestinas sobre el Banco Oeste, un proyecto denominado "Google Ayosh", en alusión a la capacidad de la tecnología de buscar y encontrar personas.[9] El proyecto hizo que la empresa ganara un premio de la industria de defensa en el 2018 por "evitar cientos de ataques terroristas" mediante el uso de "grandes cantidades de datos",[10] aunque no queda claro cómo el proyecto evitó tales ataques. Además de revelar el proyecto secreto, NBC indica[11] que tiene pruebas de que la policía israelí está

[4] Para obtener más información, visite el sitio web de AnyVision en https://www.anyvision.co/
[5] Canal de YouTube de El Doce. "Ya funciona el sistema de reconocimiento facial en Córdoba". Noviembre del 2019. https://www.youtube.com/watch?v=xC2Y_T2KxCo
[6] Número de procedimiento 279-0032-CDI17 https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhxpHQh1a9rqmrswnHE0fbV4WFyYSFDE6lxSvc3QcWHT4/5pakrCnV2dPCYEG/6/s7e/f0naaJmGFnfhrFxNdKQpW67nH3a2C04dnq|8jmWDuQ==
[7] Número de procedimiento 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. "Exposed And Exploited: Data Protection In The Middle East And North Africa." Enero del 2021. https://www.accessnow.org/mena-data-protection-report
[10] NBC News. "Why did Microsoft fund an Israeli firm that surveils West Bank Palestinians?" Octubre del 2019. https://www.nbcnews.com/news/all/why-did-microsoft-fund-israeli-firm-surveils-west-bank-palestinians-n1072116
[11] NBC News. "Why did Microsoft fund an Israeli firm that surveils West Bank Palestinians?" Octubre del 2019. https://www.nbcnews.com/news/all/why-did-microsoft-fund-israeli-firm-surveils-west-bank-palestinians-n1072116

usando tecnología de AnyVision para rastrear el movimiento del pueblo palestino en todo Jerusalén Este.

La tecnología en cuestión es uno de los productos principales de AnyVision: "Better Tomorrow". El sistema usa cámaras instaladas con reconocimiento facial y un sistema de alerta automatizado con una lista de seguimiento para identificar los rostros de "personas sospechosas" entre multitudes, y rastrear y categorizar vehículos. AnyVision también provee la tecnología de reconocimiento facial que se usa en los puntos de control militares israelíes en el Banco Oeste para autenticar la identidad de personas palestinas que ingresan a Israel.

Cabe notar que, tras años de presión por parte de defensores y defensoras de derechos humanos, **Microsoft** se desligó de AnyVision.[12] En el 2019, un estudio[13] del Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU. sobre el sesgo racial en el software de reconocimiento facial halló que el algoritmo de AnyVision, como muchos otros algoritmos que se han puesto a prueba, tenía un peor desempeño en rostros de personas de África o Asia del Este que en rostros de personas de Europa del Este.

⇛ Hikvision y Dahua

Nombre de la empresa	**Hangzhou Hikvision Digital Technology Co Ltd**
Sede principal	Hangzhou, República Popular China
Países en los que opera	En todo el mundo
Países en los que se despliegan sus tecnologías de vigilancia entre Argentina, Brasil y Ecuador	Argentina, Brasil, Ecuador
Fundación	2001
Pública/privada	Cotiza en la Bolsa de Valores de Shenzhen
Accionista(s) mayoritario(s)	China Electronics Technology Group Corporation (una empresa de propiedad del gobierno chino) (38,88 %), Gong Hongjia, director de Hikvision e inversor de capital de riesgo (13,43 %) [en el 2019]
Cantidad de empleados(as)	40 403 en el 2019
Ingresos anuales	RMB 57 660 millones (USD 8 800 millones) en el 2019

[12] The Verge. "Microsoft to end investments in facial recognition firms after AnyVision controversy." Marzo del 2020. https://www.theverge.com/2020/3/27/21197577/microsoft-facial-recognition-investing-divest-anyvision-controversy
[13] NIST. "NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software." Diciembre del 2019. https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software

Nombre de la empresa	Zhejiang Dahua Technology Co., Ltd.
Sede principal	Hangzhou, República Popular China
Países en los que opera	En todo el mundo
Países en los que se despliegan sus tecnologías de vigilancia entre Argentina, Brasil y Ecuador	Argentina, Brasil
Fundación	2001
Pública/privada	Cotiza en la Bolsa de Valores de Shenzhen
Accionista(s) mayoritario(s)	Fu Liquan (35,97 %) en el 2019
Cantidad de empleados(as)	10 197 en el 2019
Ingresos anuales	RMB 26 150 millones (USD 4 000 millones) en el 2019

Hikvision y **Zhejiang Dahua** son dos de los fabricantes de equipos de vigilancia más importantes. Su presencia en América Latina ha aumentado exponencialmente en el 2020, ya que estas empresas brindan a muchos gobiernos soluciones tecnológicas para abordar la pandemia de COVID-19.

Según fuentes oficiales, el Ministerio de Transporte de **Argentina** autorizó el testeo de cámaras térmicas de Hikvision dentro de la terminal de trenes de Retiro para identificar pasajeros(as) que tuvieran fiebre.[14] Las autoridades usaron la misma tecnología, esta vez desarrollada por Dahua, en el Aeropuerto Internacional de Ezeiza y en el transporte público, incluidas dos líneas de autobuses,[15] y también en dos aeropuertos de **Brasil**: el aeropuerto Guarulhos, en São Paulo[16] (el más grande de América del Sur), y el aeropuerto Galeão de Río de Janeiro.[17]

La presencia de Dahua en Argentina no es algo novedoso. En el 2017, Cutral-Có, una ciudad petrolera importante, desplegó un sistema integral de Dahua, con un sistema de vigilancia profesional (PSS) como núcleo del proyecto y un software conectado en simultáneo a 256 dispositivos, según los materiales de prensa de Dahua.[18] Nuestra investigación de fuentes disponibles al público, que incluye la cobertura de los medios sobre la iniciativa, no produjo detalles adicionales.

[14] Télam. "Dos líneas de colectivos instalan cámaras térmicas para medir la temperatura de los pasajeros". Mayo del 2020. https://www.telam.com.ar/notas/202005/469479-camaras-termicas-colectivos-pasajeros.html

[15] Infobae. "Dos líneas de colectivos instalan cámaras térmicas para medir la temperatura de los pasajeros". Mayo del 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. "El aeropuerto Guarulhos instala cámaras térmicas para medir la temperatura de los pasajeros" (en portugués). Junio del 2020. https://guarulhosonline.com.br/cidade/aeroporto-de-guarulhos-instala-cameras-termicas-para-medir-a-temperatura-dos-passageiros/

[17] Vinicius Novaes. "RIOgaleão refuerza las medidas preventivas con cámaras térmicas" (en portugués). Diciembre del 2020. https://www.panrotas.com.br/aviacao/aeroportos/2020/12/riogaleao-reforca-medidas-de-prevencao-com-cameras-termicas_178330.html

[18] Security Worldmarket. "Cutral-Có transforms into a Safe City in 30 days with Dahua." Mayo del 2017. https://www.securityworldmarket.com/int/Newsarchive/cutral-co-transforms-into-a-safe-city-with-dahua-solution-in-30-days

El proyecto de Cutral-Có implicó el despliegue de 242 cámaras de video. Si bien no hay confirmación oficial, la propia empresa, Dahua, afirma que la infraestructura implementada brinda la flexibilidad para expandir su uso, por ejemplo, mediante la utilización del material de video grabado con software de reconocimiento facial y herramientas para la identificación de números de matrículas de vehículos.

Las pruebas independientes de cámaras térmicas, particularmente de los productos de Hikvision, muestran que esta tecnología es altamente imprecisa.[19] Hasta usar flequillo puede esconder la temperatura real del cuerpo. Lo peor es que, cuando se implementaron las cámaras de Dahua en dos líneas de autobuses de Buenos Aires, la instalación no cumplió los estándares de la industria (estándares de la Comisión Electrotécnica Internacional[20]) y su uso no cumplió las instrucciones de la propia empresa.[21]

Como parte de la investigación para elaborar este informe, presentamos dos pedidos de acceso a la información ante el Ministerio de Transporte de la Nación y su equivalente de la ciudad de Buenos Aires, el 3 de noviembre del 2020. Los pedidos contenían preguntas sobre la implementación de estas tecnologías y la relación de la ciudad con ambas empresas. A agosto del 2021, aún no hemos obtenido respuesta.

Además, intentamos comunicarnos con Dahua en varias ocasiones y mediante varios canales, incluidos correos electrónicos y mensajes de LinkedIn, para entrevistar a representantes que trabajen en la región o en las sedes globales. Una vez más, a agosto del 2021, aún esperamos una respuesta oficial de algún representante de Dahua. Hikvision, por su parte, trató nuestra solicitud como un ticket de soporte técnico y terminó en un callejón sin salida.

La preferencia por estas empresas parece estar relacionada con sus precios competitivos, como señalaron en entrevistas representantes de autoridades públicas de Brasil. Según un informe de IPVM, los productos de Hikvision o Dahua pueden costar hasta 10 veces menos que los de sus competidores.[22]

En Mogi Das Cruzes en Brasil, Dahua dio un paso más allá de brindar tecnología a un precio más bajo: **la proporcionó de manera gratuita**. La empresa donó equipos para probar su tecnología en las calles durante la *Festa do Divino*, instalando cámaras de reconocimiento facial y equipos de monitoreo de vehículos, que incluyen grabadoras, micrófonos, pantallas táctiles y drones.[23] El gobernador João Doria, de São Paulo, recibió al menos BRL 8,5 millones (alrededor de USD 1,5 millones) como “regalo” para el programa de las cámaras de la ciudad. Las donaciones provinieron de varias empresas chinas:

[19] IPVM. “Hikvision Temperature Screening Tested.” Mayo del 2020. https://ipvm.com/reports/hikvision-temperature-test
[20] Comisión Electrotécnica Internacional. “Standards development.” https://www.iec.ch/standards-development
[21] IPVM. “Dahua Buenos Aires Bus Screening Violates IEC Standards and Dahua's Own Instructions.” Junio del 2020. https://ipvm.com/reports/buenos-aires-bus
[22] Mientras que las cámaras de Axis (Suecia) tienen un costo promedio de USD 372, las de Hikvision (China) cuestan alrededor de USD 37. Para obtener más información, consulte: IPVM. “Brazil Assembly Powers Hikvision Local Expansion.” Julio del 2020. https://ipvm.com/reports/hik-brazil?code=allow
[23] Departamento de Seguridad. “La seguridad para la Fiesta de lo Divino contará con cámaras de reconocimiento facial” (en portugués). Mayo del 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

Huawei, Hikvision, Dahua, y ZTE. Con estas donaciones, el gobierno desplegó al menos 4 000 cámaras de vigilancia. No está claro si tienen integrada tecnología de reconocimiento facial.[24]

La penetración de estas empresas en el mercado brasileño ha sido notable. Actualmente, Hikvision es el único fabricante extranjero de videovigilancia con operación de montaje en la Zona Franca de Manaus.[25] Asimismo, según una entrevista con una autoridad local, en el 2020, Hikvision suplantó a la empresa británica **Facewatch** en la implementación de tecnología de reconocimiento facial en Campina Grande (Paraíba, Brasil).

Por otra parte, algunas empresas brasileñas que ofrecen equipos de vigilancia tienen a estas empresas como sus fabricantes. Un buen ejemplo es la empresa **Intelbras**, líder en tecnologías de videovigilancia en Brasil. Desde el 2018, tiene un acuerdo con Dahua, bajo el cual esta última tiene prioridad en la prestación de equipos de CCTV.[26]

Algo similar sucede en **Ecuador**. **Full Tecnologia FullTec CIA. LTDA.** es una empresa local que ganó más de USD 1 millón en ventas de productos de Hikvision al gobierno nacional y municipios. Las ventas de Hikvision se centran en las grandes ciudades, como Guayaquil y Quito, y en los municipios aledaños, como Nayón, Pedro Moncayo y Daule. También descubrimos que vende a otras ciudades en Ecuador, como Quevedo, Ambato, Pelileo, Guano, Salcedo, Santa Elena, y Rumiñahui, las cuales pertenecen al circuito descentralizado.[27] [28] [29] [30]

En el 2019, la empresa **ANDEANTRADE S.A** proporcionó al centro histórico del Distrito Metropolitano de Quito cámaras de videovigilancia con reconocimiento facial de Hikvision, por más de USD 602 976.[31]

Antecedentes de derechos humanos de Hikvision y Dahua

Es esencial que Hikvision y Dahua sean transparentes, por muchos motivos. Como hemos señalado, estas empresas tienen una gran presencia en la región latinoamericana, donde venden exitosamente tecnología muy controvertida a gobiernos nacionales y locales a bajo precio. Como mencionamos

[24] Bruno Ribeiro. “Las donaciones chinas a Dória ascienden a los BRL 8,5 millones” (en portugués). Julio del 2017. https://sao-paulo.estadao.com.br/noticias/geral,doacoes-de-chineses-a-sp-somam-r-8-5-mi,70001912058

[25] Robert Gordon. “Brazil Assembly Powers Hikvision Local Expansion." Julio del 2020. https://ipvm.com/reports/hik-brazil

[26] El contrato social de Intelbras también señala que Dahua actualmente es propietaria del 10 % de los activos de la empresa brasileña. Para obtener más información, consulte: Intelbras. “Prospecto preliminar de oferta pública de distribución primaria y secundaria de acciones ordinarias de emisión de Intelbras” (en portugués). 2020. https://ww69.itau.com.br/fileserver/relatorios/intelbras-sa-ind-telecom-eletro-bra-prospecto-pre.pdf

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

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

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

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

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

anteriormente, algunas de estas tecnologías pueden no tener un buen desempeño[32] o no cumplir los estándares básicos de la industria o de las empresas.[33] Aun así, **los gobiernos latinoamericanos les están comprando de todas maneras, presentando al público una tecnología invasiva e imprecisa como solución a la delincuencia, argumento que, en el mejor de los casos, es engañoso.**

Hikvision y Dahua también ganaron una ventaja competitiva en la región al ofrecer productos y servicios de manera gratuita, aprovechando la frágil economía de muchos países de América Latina para probar sus sistemas de vigilancia en la ciudadanía. Si bien el objetivo de este informe no es analizar las injustas prácticas de competencia, este problema amerita atención dados los recientes escándalos en relación con el comportamiento monopólico y abusivo de las grandes empresas tecnológicas.

Ambas empresas están implicadas en violaciones de derechos humanos. Ambas han ganado contratos de más de USD 1 000 millones para proyectos de vigilancia respaldados por los gobiernos en Sinkiang, China,[34] desde el 2016. Según una investigación de *The Wall Street Journal*,[35] las autoridades de Sinkiang están usando tecnología de vigilancia para perseguir al grupo étnico minoritario musulmán uigur,[36] que ha resultado en sanciones y críticas por parte de los gobiernos de Noruega,[37] Dinamarca,[38] y EE. UU.[39]

Además, Dahua ha tenido una serie de vulnerabilidades en su sistema en la nube.[40] Una persona que realizó una investigación independiente descubrió una puerta trasera en los sistemas de Dahua que permitía el acceso remoto no autorizado a través de la web. Hikvision tuvo una vulnerabilidad similar en el 2017 en sus cámaras IP.[41] Recientemente, la Comisión Federal de Comunicaciones de los EE. UU. añadió a Hikvision y Dahua a una lista de empresas que representan una amenaza para la seguridad nacional del país, alentando a las empresas estadounidenses a evitar el uso de productos de estas dos empresas.[42]

---

[32] IPVM. "Hikvision Temperature Screening Tested." Mayo del 2020. https://ipvm.com/reports/hikvision-temperature-test

[33] IPVM. "Dahua Buenos Aires Bus Screening Violates IEC Standards and Dahua's Own Instructions." Junio del 2020. https://ipvm.com/reports/buenos-aires-bus

[34] IPVM. "Dahua and Hikvision Win Over $1 Billion In Government-Backed Projects In Xinjiang." Abril del 2018. https://ipvm.com/reports/xinjiang-dahua-hikvision

[35] The Wall Street Journal. "Twelve Days in Xinjiang: How China's Surveillance State Overwhelms Daily Life." Diciembre del 2019. https://www.wsj.com/articles/twelve-days-in-xinjiang-how-chinas-surveillance-state-overwhelms-daily-life-1513700355

[36] Para obtener más información, consulte: https://campaignforuyghurs.org/

[37] Business & Human Rights Resource Centre. "Norwegian wealth fund's ethics council recommended divestment from Hikvision for human rights concerns over co. role in mass surveillance." Septiembre del 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. "Danish pension fund AkademikerPension divests from Hikvision for human rights concerns over co. role in mass surveillance." Noviembre del 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. "USA: Eleven Chinese firms added to economic blacklist over allegations of using forced labour of ethnic minorities." Julio del 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/

[40] IPVM. "Dahua Critical Cloud Vulnerabilities." Mayo del 2020. https://ipvm.com/reports/dahua-cloud-vuln

[41] IPVM. "Hikvision Backdoor Exploit." Septiembre del 2017. https://ipvm.com/reports/hik-exploit

[42] Comisión Federal de Comunicaciones. "LA OFICINA DE SEGURIDAD PÚBLICA Y SEGURIDAD NACIONAL ANUNCIA LA PUBLICACIÓN DE LA LISTA DE EQUIPOS Y SERVICIOS CUBIERTOS POR LA SECCIÓN 2 DE LA LEY DE REDES SEGURAS". Expediente N° 18-89. Marzo del 2021. https://docs.fcc.gov/public/attachments/DA-21-309A1.pdf

⇛ Cellebrite

Nombre de la empresa	Cellebrite DI Ltd.
Sede principal	Petaj Tikva, Israel
Países en los que opera	En todo el mundo
Países en los que se despliegan sus tecnologías de vigilancia entre Argentina, Brasil y Ecuador	Argentina
Fundación	1999
Pública/privada	Privada
Accionista(s) mayoritario(s)	Suncorporation Ltd. (71,5 %) Israel Growth Partners (24,41 %)
Cantidad de empleados(as)	452 en el 2019
Ingresos anuales	USD 71,1 millones en el 2019

Cellebrite es una empresa de inteligencia digital israelí y una de las subsidiarias de la empresa japonesa Suncorporation Ltd. (que cotiza en la Bolsa de Valores de Tokio).[43] Aunque resulta difícil determinar una fecha específica en que las autoridades de **Argentina** comenzaron a usar la tecnología de esta empresa, la presencia de Cellebrite en el país ha aumentado continuamente durante los últimos cinco años. Sus productos se obtienen en Argentina mediante dos principales revendedores locales: **Security Team Network S.A.** e **IAFIS Argentina S.A.** Argentina está en el tercer puesto en el continente americano en el uso de licencias del dispositivo UFED (Universal Forensic Extraction Device) de Cellebrite, que se exporta a más de 150 jurisdicciones.

A principios de la década del 2010, el Ministerio de Justicia asignó fondos para iniciar el desarrollo de Laboratorios Regionales de Investigación Forense, en colaboración con la Fiscalía General en todo el país. En el 2014, ya había 13 laboratorios forenses que usaban la tecnología de Cellebrite, específicamente la línea de productos UFED[44] para la extracción de datos. Según un documento oficial del Ministerio de Justicia, las jurisdicciones que usaban esta tecnología incluían: Oficina de Gestión de Información Tecnológica (OFITEC), Mercedes, Provincia de Buenos Aires; Laboratorio Forense de Comunicaciones Complejas, Mar del Plata, Provincia de Buenos Aires; Ciudad Autónoma de Buenos Aires; Entre Ríos; Mendoza; San Juan; San Luis; Formosa; Neuquén; Chubut; La Pampa; Corrientes; y

[43] Para obtener más información, visite el sitio web de Suncorportation en https://www.sun-denshi.co.jp/en
[44] Cellebrite. UFED: "The industry standard for accessing digital device data."
https://cf-media.cellebrite.com/wp-content/uploads/2020/06/ProductOverview_Cellebrite_UFED_A4.pdf

Misiones.[45] En el caso de La Pampa, además del UFED, habían implementado el complemento CHINEX,[46] desarrollado para la extracción de datos de teléfonos chinos no estándares.

Desde entonces, el uso de los productos de Cellebrite se expandió a otras provincias. En el 2018, el Ministerio Público Fiscal de Salta actualizó sus licencias de UFED 4PC y TOUCH por un total de USD 23 000, mediante un contrato directo con Security Team Network.[47]

Uno de los principales usuarios de la tecnología de Cellebrite a escala nacional en el país es la Gendarmería Nacional Argentina (GNA). Debido a su jurisdicción federal, la GNA desplegó los productos de Cellebrite en todo el país para equipar los laboratorios forenses.

En septiembre del 2019, la GNA cerró un contrato directo con Security Team Network S.A. por un total de USD 643 900 para adquirir una estación de trabajo para desbloquear teléfonos inteligentes de alta gama. El producto UFED solo se menciona una vez en el desglose de especificaciones técnicas.[48] En noviembre, la Dirección de Criminalística y Estudios Forenses de Gendarmería adquirió cuatro licencias para el software "UFED 4PC". Según Cellebrite, este producto se utiliza para "capacidades de extracción, decodificación, análisis, lectura y administración" que pueden ejecutarse en hardware personalizable por el usuario.[49] Gendarmería adquirió estas licencias a través de una licitación pública, en la que, en última instancia, terminó nuevamente celebrando un contrato con Security Team Network por un total de ARS 9 587 400 (alrededor de USD 159 000 en ese momento).[50]

Más recientemente, Gendarmería actualizó esas licencias en junio del 2020, en un contrato con Security Team Network por un total de USD 132 116.[51]

Según una persona del ámbito periodístico que prefirió permanecer en el anonimato, las fuerzas federales de seguridad (integradas por Gendarmería Nacional, la Policía de Seguridad Aeroportuaria, la Policía Federal, y la Guardia Costera) cuentan con un total de 35 productos UFED y, al contar las Fiscalías y otros organismos de orden público, las licencias utilizadas en el país ascienden a 350.[52] El usuario principal es Gendarmería, que opera en todas las provincias y actualmente está mejorando sus laboratorios forenses digitales, usando productos como la nube UFED, UFED Pathfinder y UFED

---

[45] Ministerio de Justicia y Derechos Humanos. "Laboratorios Regionales de Investigación Forense". Agosto del 2014 http://www.saij.gob.ar/docs-f/ediciones/libros/Laboratorios_Regionales_de_Invest._Forense.pdf

[46]Cellebrite. "Non-standard Chinese Phones Now Accessible with UFED Chinex Kit." Septiembre del 2019 https://www.cellebrite.com/en/blog/non-standard-chinese-phones-now-accessible-with-ufed-chinex-kit/

[47] Ministerio Público, provincia de Salta. Expediente N° 130-17.933/17

[48] Expediente N° 37/105-0815-CDI19. https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhwbeNKAPenXR8IR3ih5YSXR79Wk8x7mmrwOCg9|4XRUnx0kCgm3oU8Rx5zvjpByUn|6t4HsX9ox3IM|fHZHcPGbahOwPe58NWP7IaFH5JcDkQ==

[49] Cellebrite. 4PC. https://cf-media.cellebrite.com/wp-content/uploads/2019/06/DataSheet_4PC_A4-print.pdf

[50] Dirección de Criminalística y Estudios Forenses. "ADQUISICIÓN DE SOFTWARE UFED 4PC PARA LA DIRECCIÓN DE CRIMINALÍSTICA Y ESTUDIOS FORENSES". Expediente N° 37/105-0041-LPU19. Julio del 2018 https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhy5xycgc2RiGO0seBx38Zrkqrf44NYcUHOQXWAZSx|FbiACHf8VyMdhxK5ugYZKg/ha7EWhWl7fjuQEoJmuXixefeg9/er7CV2Q|P|HNndQKg==

[51] Dirección de Criminalística y Estudios Forenses. "SERVICIO DE RENOVACIÓN Y ACTUALIZACIÓN DE LICENCIAS DE SOFTWARE FORENSE UFEC TOUCH I HACIA UFED 4PC". Expediente N° 37/105-0422-CDI20. Marzo del 2020 https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhyrV/4BRRj7a9qf3aG8azk|h3K/KAn7jb/h6aPDkgsy3caJklV5dh/l98fSQHDGyecUZqnGVTQz3UXLzeKrU0hskSjg8CnHW3bp5dO0tjSzbg==

[52] Clarín. "Detectives de teléfonos: secretos del sistema que abre los celulares y resuelve las causas más complejas". Noviembre del 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

Physical Analyzer de Cellebrite.[53] La GNA también presta su equipo cuando colabora en investigaciones penales, por ejemplo, en el caso de la provincia de Entre Ríos.[54]

En Buenos Aires, la Fiscalía adquirió una licencia de UFED 4PC junto con software Physical Analyzer[55] en el 2019, mediante un contrato directo con Security Team Network, por la suma de ARS 440 109 (alrededor de USD 10 500 en ese momento). Estos productos fueron destinados al Cuerpo de Investigaciones Judiciales.[56] Este centro ya había renovado una licencia de otro producto, UFED Cloud Analyzer, en el 2017, también mediante un contrato directo con la misma empresa local.[57]

En agosto del 2020, la Fiscalía General de la provincia de Santa Fe firmó un contrato directo con la empresa local IAFIS Argentina S.A. para renovar cuatro licencias de UFED Touch 2 por un plazo de un año, y adquirir tres licencias nuevas de UFED 4PC, por un total de USD 96 226.[58]

En diciembre del 2020, la Policía de Seguridad Aeroportuaria celebró un contrato directo con IAFIS Argentina S.A. para actualizar y mejorar sus licencias de UFED, por un total de ARS 8 057 111 (aproximadamente USD 90 784). El contrato incluía la renovación de dos licencias UFED 4PC Ultimate y dos de UFED Touch 2 Ultimate[59] por una duración de dos años, y también la permuta de hardware de dos dispositivos Touch I por dos UFED Touch 2.[60]

El Ministerio de Seguridad comenzó a celebrar contratos de cooperación con más de 15 empresas de tecnología, incluida Cellebrite, a fines del 2020. Estos acuerdos incluyen capacitaciones y compartición de información para mejorar la capacidad de las fuerzas del orden en investigaciones judiciales que involucren pruebas digitales.[61] El 3 de noviembre del 2020, presentamos una solicitud de acceso a la información ante el Ministerio para indagar sobre estos acuerdos. La respuesta oficial del Ministerio en diciembre del 2020 señala que “no se ha finalizado ninguna suscripción de ninguno de los acuerdos mencionados en la solicitud de acceso a la información pública en cuestión, por lo que no hay documentos sobre estos que puedan darse a conocer a la parte interesada”.

---

[53] Cellebrite. “La Gendarmería Nacional de Argentina está superando las barreras de tiempo y distancia con inteligencia digital”. Julio del 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. “Dispositivos UFED, el nuevo equipamiento con el que cuenta la Policía de Concordia y la Gendarmería en Paraná”. Febrero del 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] Gobierno de la Ciudad Autónoma de Buenos Aires. Disposición N° 65/UOA/19 Julio del 2019. https://documentosboletinoficial.buenosaires.gob.ar/publico/ck_PJ-DIS-MPF-UOA-65-19-5660.pdf

[57] Ministerio Público Fiscal de la Provincia de Buenos Aires. Disposición UOA N° 45/2017. Septiembre del 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] Ministerio Público de la Acusación de la Provincia de Santa Fe. Expediente N° FG-000303-2020. Agosto del 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/

[60] Policía de Seguridad Aeroportuaria. “Renovación de licencias y mejoramiento de equipos UFED 4PC y UFED TOUCH, por Exclusividad”. Expediente N° 279-0027-CDI20. Noviembre del 2020 https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhy3iTxQqkwwChRpn2XPxXCSk5uij|LSdq2DmF5S3lGnqlsUbG2uGBeZPrbB8BhNUcLFrujs6LrFUaU3GDH8dDYrJv/eOuj/ve1TCcZ2AXWpaw==

[61] Gobierno de Argentina. “Acciones para mayor eficiencia en la investigación criminal en el ámbito digital”. Octubre del 2020. https://www.argentina.gob.ar/noticias/acciones-para-mayor-eficiencia-en-la-investigacion-criminal-en-el- ambito-digital

Antecedentes de derechos humanos de Cellebrite

Cellebrite afirma vender su tecnología exclusivamente a gobiernos y agencias del orden público y, recientemente, a autoridades gubernamentales que interrogan a quienes buscan asilo.[62] [63]

En el 2016, la Dirección General Anticorrupción y Seguridad Económica y Electrónica y la Dirección de Investigaciones Penales de Baréin usaron el UFED de Cellebrite, según se informa, para investigar y perseguir a disidentes.[64] Según una investigación llevada a cabo por el abogado israelí Eitay Mack, la empresa vendió tecnología forense a los gobiernos de Venezuela, Bielorrusia, Rusia e Indonesia, conocidos por tomar medidas contra la disidencia política y perseguir a la comunidad LGTBQI.[65]

Después de que se filtraran documentos internos en el 2017, se reveló que Cellebrite también estaba en negociaciones con las fuerzas de seguridad de Turquía y los Emiratos Árabes.[66] Además, la policía de Myanmar usó la misma tecnología para arrestar a dos periodistas en el 2019[67] y la policía de Hong Kong la usó, aparentemente, para acosar e investigar a manifestantes prodemocráticos en el 2020.[68] El Comité para la Protección de Periodistas reveló, recientemente, que el gobierno de Botsuana está utilizando tecnología de Cellebrite para buscar dispositivos de periodistas para obtener fuentes.[69] Algunos(as) periodistas afirman haber sido objeto de torturas.[70] Informes adicionales revelan que se venden herramientas de Cellebrite a Nigeria, Bangladés, Arabia Saudí y Vietnam.[71]

Defensores y defensoras de derechos humanos presentaron una petición judicial para instar al Ministerio de Defensa de Israel a frenar la exportación de Cellebrite a Hong Kong, Rusia y Bielorrusia.[72]

---

[62] Privacy International. "Surveillance Company Cellebrite Finds a New Exploit: Spying on Asylum Seekers." Abril del 2019. https://privacyinternational.org/long-read/2776/surveillance-company-cellebrite-finds-new-exploit-spying-asylum-seekers

[63] Access Now. "What spy firm Cellebrite can't hide from investors." Mayo del 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." Diciembre del 2016. https://theintercept.com/2016/12/08/phone-cracking-cellebrite-software-used-to-prosecute-tortured-dissident/

[65] Haaretz. "Hacking Grindr? Israel's Cellebrite Sold Phone-hacking Tech to Indonesia." Noviembre del 2020. https://www.haaretz.com/israel-news/tech-news/.premium.HIGHLIGHT-hacking-grindr-israel-s-cellebrite-sold-phone-spy-tech-to-indonesia-1.9281160

[66] Vice. "Cellebrite Sold Phone Hacking Tech to Repressive Regimes, Data Suggests." Enero del 2017. https://www.vice.com/en/article/aekqjj/cellebrite-sold-phone-hacking-tech-to-repressive-regimes-data-suggests

[67] The Washington Post. "Security-tech companies once flocked to Myanmar. One firm's tools were used against two journalists." Mayo del 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

[68] The Jerusalem Post. "Hong Kong democracy activists to Israel: Stop exporting tech to police." Julio del 2020. https://www.jpost.com/israel-news/hong-kong-democracy-activists-to-israel-stop-exporting-tech-to-police-636918#/

[69] Comité para la Protección de Periodistas, "Equipped by US, Israeli firms, police in Botswana search phones for sources." Mayo del 2021. Https://cpj.org/2021/05/equipped-us-israeli-firms-botswana-police/; Comité para la Protección de Periodistas, "Botswana police use Israeli Cellebrite tech to search another journalist's phone." Julio del 2021. https://cpj.org/2021/07/botswana-cellebrite-search-journalists-phone/

[70] Id.

[71] Access Now. "What spy firm Cellebrite can't hide from investors." Mayo del 2021. https://www.accessnow.org/what-spy-firm-cellebrite-cant-hide-from-investors/; Haaretz, "What Vietnam Is Doing With Israeli Phone-hacking Tech." Julio del 2021.https://www.haaretz.com/israel-news/tech-news/.premium-what-vietnam-is-doing-with-israel-s-phone-hacking-tech-1.10003831

[72] Revisión de tecnología del MIT. "Israeli phone hacking company faces court fight over sales to Hong Kong." Agosto del 2020. https://www.technologyreview.com/2020/08/25/1007617/israeli-phone-hacking-company-faces-court-fight-over-sales-to-hong-kong/; Haaretz, "Israeli Phone-hacking Firm Cellebrite Halts Sales to Russia, Belarus in Wake of Haaretz Report." Marzo del 2021.

En octubre del 2020, Cellebrite anunció que dejaría de vender su tecnología a China y Hong Kong.[73] En marzo del 2021, Cellebrite también anunció que pondrá fin a las ventas a Rusia y Bielorrusia.[74]

⇛ Huawei y ZTE

Nombre de la empresa	**Huawei Technologies Co., Ltd.**
Sede principal	Shenzhen, República Popular China
Países en los que opera	En todo el mundo
Países en los que se despliegan sus tecnologías de vigilancia entre Argentina, Brasil y Ecuador	Argentina, Brasil
Fundación	1987
Pública/privada	Privada
Accionista(s) mayoritario(s)	Propiedad absoluta de sus empleados(as)
Cantidad de empleados(as)	194 000
Ingresos anuales	RMB 858 800 millones (USD 132 000 millones) en el 2019

Nombre de la empresa	**ZTE Corporation**
Sede principal	Shenzhen, República Popular China
Países en los que opera	En todo el mundo
Países en los que se despliegan sus tecnologías de vigilancia entre Argentina, Brasil y Ecuador	Argentina, Brasil
Fundación	1985
Pública/privada	Cotiza en las Bolsas de Valores de Hong Kong y de Shenzhen

https://www.haaretz.com/israel-news/.premium-israeli-phone-hacking-firm-cellebrite-halts-sales-to-russia-after-haaretz-report-1.9633312

[73] Cellebrite. “Cellebrite to Stop Selling Its Digital Intelligence Offerings in Hong Kong & China.” Octubre del 2020. https://www.cellebrite.com/en/cellebrite-to-stop-selling-its-digital-intelligence-offerings-in-hong-kong-china/

[74] Cellebrite, “Cellebrite Stops Selling Its Digital Intelligence Offerings in Russian Federation and Belarus.” Marzo del 2021. https://www.cellebrite.com/en/cellebrite-stops-selling-its-digital-intelligence-offerings-in-russian-federation-and-belarus/

Accionista(s) mayoritario(s)	ZTE Holdings (21,85 %), Hong Kong Securities Clearing Company Limited (16,31 %)
Cantidad de empleados(as)	70 066 empleados(as) en total como grupo (60 514 empleados(as) como empresa) en el 2019
Ingresos anuales	RMB 90 737 millones (USD 13 940 millones) en el 2019

Ambas empresas chinas, **Huawei Technologies Co**. y **ZTE Corporation**, ofrecen una amplia gama de soluciones tecnológicas. Uno de los servicios que prestan se basa en tecnología y sistemas para la construcción de lo que se conoce como "ciudades inteligentes". Cada una interactúa principalmente con gobiernos locales de América Latina para brindar herramientas para la seguridad pública.

En julio del 2020, ZTE llegó a la provincia de Jujuy, **Argentina**. El gobernador, Gerardo Morales, recibió al vice presidente de ZTE Corporation y al gerente general de ZTE Argentina, Hua Xinhai y Dennis Wang. Llegaron a un acuerdo para el despliegue de un programa denominado "Jujuy Seguro e Interconectado", para el cual la provincia recibió un préstamo en marzo del 2020 del banco BBVA con sede en Hong Kong por un monto de USD 24 146 142.[75] ZTE cerró el trato por USD 30 millones para completar parte de su agenda al ofrecer la instalación de cámaras, centros de monitoreo, servicios de emergencia e infraestructura para telecomunicaciones.[76] Según el gobernador Morales, ahora Jujuy será "tan segura como China". Enviamos una solicitud de acceso a la información para obtener más detalles el 11 de noviembre de 2020, pero no recibimos respuesta, a pesar de haber cumplido la fecha límite legal.

En abril del 2018, Alfredo Cornejo, el gobernador de la provincia de Mendoza, Argentina, se reunió con el vicepresidente de ventas de Huawei, Tony Sza.[77] El propósito de la reunión, según los informes periodísticos, era hablar sobre la adquisición de tecnología para el reconocimiento facial, la geolocalización y la gestión del big data para la seguridad pública. Organizaciones de la sociedad civil, incluidas Access Now y ADC, respondieron enviando una carta al gobernador,[78] en la que se pedía poner fin a las negociaciones privadas y llevar a cabo un debate público sobre el asunto. Lamentablemente, el gobernador no reveló ninguna otra información.

Huawei también tiene presencia en la región a través de una red de distribuidores y revendedores. Un ejemplo es Bahía, **Brasil**, donde las autoridades eligieron la sucursal brasileña de la cadena española **El Corte Inglés** para una "disposición contractual adicional" para el "Consorcio para

[75] Boletín Oficial. Decreto 207/2019. Marzo del 2019. https://www.boletinoficial.gob.ar/detalleAviso/primera/203703/20190320
[76] Reuters. "'Safe like China': In Argentina, ZTE finds eager buyer for surveillance tech." Julio del 2019. https://www.reuters.com/article/us-argentina-china-zte-insight-idUSKCN1U00ZG
[77] Sitio web oficial de Mendoza. "El Gobernador se reunió con representantes de Huawei en Latinoamérica". Abril del 2018. https://www.mendoza.gov.ar/prensa/el-gobernador-se-reunio-con-representantes-de-huawei-en-latinoamerica/
[78] ADC. "Defensores de derechos fundamentales piden al Gobierno de Mendoza que detenga la compra de tecnología de vigilancia masiva". Julio del 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/

Bahía Segura del 2014" para proporcionar hardware (cámaras) y software de reconocimiento facial de Huawei. El proveedor de telecomunicaciones brasileño **Oi** también firmó un contrato con Huawei para vender tecnología de reconocimiento facial en Brasil.[79] Las autoridades probaron esta tecnología en el público durante los carnavales de Río de Janeiro del 2019. El sistema capturó aproximadamente tres millones de imágenes de rostros, pero solo se efectuaron 10 arrestos en base al uso del sistema, según el vocero de la Policía Militar de Río de Janeiro, el coronel Mauro Fliess.[80]

Para acelerar la aceptación de su tecnología y probar sus capacidades, Huawei también donó a Campinas, en el estado de São Paulo, el equipo necesario para un proyecto de "ciudad inteligente". Actualmente, Campinas es conocida por su "laboratorio abierto", que incluye tecnología de reconocimiento facial invasora de la privacidad, lo que está resultando en su designación como "ciudad inteligente" en Brasil.[81]

Antecedentes de derechos humanos de ZTE y Huawei

Hace tiempo se conoce que ZTE y Huawei han trabajado con regímenes que violan los derechos humanos. En el 2013, cuando el grupo de defensa Bolo Bhi les pidió a ambas empresas que no participaran en la creación de un cortafuego de censura de internet para el gobierno de **Pakistán**, estas eligieron ignorar los impactos de sus productos en los derechos humanos y emitir declaraciones superficiales sobre priorizar las leyes "locales" por sobre las leyes y normas internacionales de derechos humanos.[82] Ese mismo año, Reflets.Info reportó que ZTE y Hewlett Packard estaban colaborando con Telecommunications Infrastructure Co. (TIC), el proveedor de servicios de internet del Estado iraní para ayudar a limitar el tipo de información a la que el pueblo iraní podía acceder en línea.[83]

En el 2008, el entonces presidente de Venezuela, Hugo Chávez, envió a representantes del Ministerio de Justicia para hacer una visita a ZTE. Descubrieron que China, mediante el uso de tarjetas inteligentes, estaba elaborando un sistema que ayudaría a Pekín a monitorear el comportamiento social, político y económico de las personas. Diez años después, el **gobierno venezolano** contrató a ZTE por USD 70 millones para desplegar un programa similar: el "carnet de la patria". Las tarjetas se están usando en campañas para influenciar las decisiones de votación,[84] dar subsidios para alimentos, brindar atención a la salud y administrar otros programas sociales de los que depende la mayor parte del pueblo

[79] Folha de S. Paulo. "Huawei de China se asocia a Oi para cámaras de reconocimiento facial" (en portugués). Octubre del 2018. https://www1.folha.uol.com.br/tec/2018/10/chinesa-huawei-faz-parceria-com-oi-para-cameras-de-reconhecimento-facial.shtml
[80] Defesanet. "Reconocimiento facial: en el carnaval de Río se identificaron a 8 mil personas de interés" (en portugués). Mayo del 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 is "Smartest" and Most Connected City in Brazil, per Unofficial Ranking." Septiembre del 2019. https://riotimesonline.com/brazil-news/brazil/life-brazil/campinas-is-the-smartest-and-most-connected-city-in-brazil/
[82] Access Now. "Broken promises: Pakistan announces plans to launch censorship firewall, possibly with Chinese tech." Enero del 2013. https://www.accessnow.org/broken-promises-pakistan-announces-plans-to-launch-censorship-firewall-poss/
[83]Reflets.Info. "ZTE y HP se unen por un internet halal en la tierra de los mulás" (en francés). Junio del 2013. https://reflets.info/articles/zte-et-hp-unis-pour-un-halalternet-au-pays-des-mollahs
[84] BBC News. "Elecciones en Venezuela: qué son los puntos rojos y por qué Henri Falcón acusa a Maduro de 'compra de votos'". Mayo del 2018. https://www.bbc.com/mundo/noticias-america-latina-44192915

venezolano para sobrevivir.[85] Este sistema de tarjetas inteligentes llamó la atención de la ciudadanía y de activistas y organizaciones de derechos humanos debido al claro riesgo de abuso gubernamental, invasión a la privacidad y control comunitario. Tras su implementación, la base de datos del carnet de la patria fue hackeada[86] y, en el 2018, el gobierno usó las tarjetas y los datos que estas contenían para identificar a las personas que no habían votado. También hizo que las tarjetas fueran obligatorias para obtener los beneficios ofrecidos por el gobierno y para comprar combustible a precios subsidiados.

Huawei también ha estado bajo el escrutinio de los medios durante los últimos años. En el 2019, una investigación[87] de *The Wall Street Journal* demostró que el plantel técnico de la empresa había ayudado personalmente, al menos en dos instancias, a los gobiernos de **Uganda** y **Zambia** a espiar a sus rivales políticos, lo que incluyó interceptar sus comunicaciones cifradas y sus redes sociales, y usar datos de teléfonos celulares para rastrear sus paraderos.

En junio del 2020, una investigación llevada adelante por *Reuters* señaló que Huawei vendió al menos EUR 1,3 millones en equipos de computadora de Hewlett-Packard embargados al gobierno iraní y se esforzó mucho por esconderlo.[88] En diciembre del mismo año, IPVM encontró un documento "confidencial" disponible al público en el propio sitio web europeo de Huawei, que poco después fue eliminado. Este documento explicaba que Huawei había probado un software de reconocimiento facial que podía enviar "alarmas uigures" automatizadas a autoridades del **gobierno chino** cuando sus sistemas de cámaras identificaran miembros de ese grupo minoritario oprimido.[89]

Este y otros casos preocupantes provocaron que **Suecia** prohibiera equipos de telecomunicaciones de Huawei y ZTE en su red 5G,[90] y otras naciones europeas han tomado medidas similares o están pensando hacerlo.

⇛ NEC

Nombre de la empresa	**NEC Corporation**
Sede principal	Tokio, Japón
Países en los que opera	En todo el mundo
Países en los que se despliegan sus tecnologías de vigilancia entre Argentina, Brasil y Ecuador	Argentina, Brasil

[85] Reuters. "Cómo ZTE ayuda a Venezuela a implementar un control social al estilo chino". Noviembre del 2018. https://www.reuters.com/investigates/special-report/venezuela-zte-es/
[86] Cuenta de Twitter AlbertoRodNews. https://twitter.com/AlbertoRodNews/status/1070733400372326401
[87] The Wall Street Journal. "Huawei Technicians Helped African Governments Spy on Political Opponents." Agosto del 2019. https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents- 11565793017
[88] Reuters. "Exclusive: Huawei hid business operation in Iran after Reuters reported links to CFO." Junio del 2020. https://www.reuters.com/article/us-huawei-iran-probe-exclusive-idUSKBN23A19B
[89] IPVM. "Huawei / Megvii Uyghur Alarms." Diciembre del 2020. https://ipvm.com/reports/huawei-megvii-uygur
[90] Reuters. "Sweden bans Huawei, ZTE from upcoming 5G networks." Octubre del 2020. https://www.reuters.com/article/sweden-huawei-int-idUSKBN2750WA

Fundación	1899
Pública/privada	Cotiza en la Bolsa de Valores de Tokio
Accionista(s) mayoritario(s)	N/A
Cantidad de empleados(as)	Aproximadamente 110 000 en el 2020
Ingresos anuales	JPY 3 095 200 millones (USD 28 350 millones) en el 2020

NEC es un actor muy importante en la industria de la identificación biométrica digital a escala mundial. Es una empresa fundada hace 122 años que cuenta con más de 110 000 empleados y empleadas. Este gigante tecnológico japonés (que cotiza en la Bolsa de Valores de Tokio) se presenta[91] como la elección inmediata para muchas agencias de gobierno en todo el mundo. Ha estado desarrollando tecnología biométrica, como tecnología de reconocimiento facial, del iris, de huellas dactilares, de venas de los dedos y de voz, durante más de 50 años y vendiéndola a 70 jurisdicciones.[92] Las tecnologías de NEC conforman la red troncal del sistema biométrico más grande del mundo, Aadhaar de la **India**, que ha inscrito a 1 300 millones de personas.[93] En **EE. UU.**, más de un tercio de las agencias del orden público y la policía estatal usan los sistemas biométricos de NEC desde el 2019.[94] Aduanas y Protección Fronteriza (CBP) de EE. UU. usa el software de reconocimiento facial en los aeropuertos,[95] y la tecnología también se abrió paso a los estadios deportivos en **Colombia**[96] y **Taiwán**[97]. La presencia de NEC en América Latina está creciendo a medida que más gobiernos locales adoptan la retórica de las "ciudades inteligentes".

NEC estableció sus operaciones en **Argentina** en 1978 para realizar sus actividades comerciales en el país y en la región mediante su propia subsidiaria local. **En el 2004, la empresa eligió a NEC Argentina S.A. como su Centro Regional de Desarrollo de Software para el mercado latinoamericano**.[98] Desde el 2006, NEC es el proveedor oficial de tecnología biométrica del Ministerio del Interior y el Registro

[91] NEC. Integrated Report 2020. https://www.nec.com/en/global/ir/pdf/annual/2020/ar2020-e_two.pdf
[92] NEC. Biometric Authentication. https://www.nec.com/en/global/solutions/biometrics/index.html
[93] NEC. "Biometric Identification for Over 1 Billion People." Noviembre del 2018. https://www.nec.com/en/case/uidai/index.html
[94] OneZero. "Carnival Cruises, Delta, and 70 Countries Use a Facial Recognition Company You've Never Heard Of." Febrero del 2020 https://onezero.medium.com/nec-is-the-most-important-facial-recognition-company-youve-never-heard-of-12381d530510
[95] EFF. "Skip the Surveillance By Opting Out of Face Recognition At Airports." Abril del 2014. https://www.eff.org/deeplinks/2019/04/skip-surveillance-opting-out-face-recognition-airports
NEC. "NEC tests facial recognition with U.S. Customs and Border Protection (CBP) on select Dulles International Airport (IAD) flights." Junio del 2017. https://www.nec.com/en/press/201706/global_20170627_03.html
Ventura Beat. "U.S. Homeland Security has used facial recognition on over 43.7 million people." Febrero del 2020. https://venturebeat.com/2020/02/06/u-s-homeland-security-has-used-facial-recognition-on-over-43-7-million-people/
[96] NEC. "NEC contributes to football stadium safety in Colombia." Octubre del 2016. https://www.nec.com/en/press/201610/global_20161012_03.html
[97] Find Biometrics. "NEC Facial Recognition Tech Used to Secure Sports Stadium in Taipei." Noviembre del 2017. https://findbiometrics.com/nec-facial-recognition-sports-stadium-taipei-411022/
[98] NEC. Historia. https://ar.nec.com/es_AR/about/history/index.html

Nacional de las Personas (RENAPER). Gracias a esta tecnología, el RENAPER ha expandido el uso de su base de datos biométricos para la verificación e identificación hacia otros organismos públicos, como la Oficina de Migraciones, el Registro Nacional de Reincidencia y el Ministerio de Seguridad, entre otros, lo que también fue una consecuencia de la expansión del Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS).

En el 2017, la Dirección Nacional de Migraciones (DNM) firmó un contrato con NEC para implementar puertas de control de pasaportes automatizadas, a las que se refiere comúnmente como "eGates", en los aeropuertos internacionales de Argentina, por un total de USD 3 309 318.[99] El documento de contratación oficial expone que se eligió a NEC porque la Dirección Nacional de Migraciones ya estaba utilizando los productos AFIS[100] y NeoFace[101] de la empresa, para el reconocimiento de huellas dactilares y el reconocimiento facial, respectivamente.

Las eGates se implementaron y usaron por primera vez en el público en el 2018, en el aeropuerto de Ezeiza, pero luego se expandieron al aeropuerto Aeroparque y al puerto marítimo, ambos en la Ciudad de Buenos Aires.[102] El control fronterizo utiliza estos puntos de control, eGates, para reemplazar algunas interacciones entre personas, utilizando software de verificación de huellas dactilares y rostros para comparar un escaneo con los datos biométricos reunidos de todas las personas que ingresan o dejan el país. El RENAPER mantiene los datos de inscripción de las eGates.

En el 2019, la DNM celebró otro contrato con NEC por un sistema biométrico para identificar a personas de una lista de seguimiento (por ejemplo, personas con restricciones de viaje, buscadas por la INTERPOL, etc.), por un total de ARS 145 189 000 (aproximadamente USD 3 millones en ese momento).[103] La solicitud especificaba que el sistema debía ser compatible con AFIS del RENAPER, para ejecutar consultas tanto de identificación como de verificación.

Entre el 2017 y el 2020, el RENAPER firmó múltiples contratos con NEC para mejorar, actualizar y expandir sus sistemas biométricos.[104]

---

[99] Dirección General de Administración. "PROVISIÓN DE SOLUCIÓN DE PROCESO MIGRATORIO AUTOASISTIDO". Expediente Nº 21-0028-CDI17. Septiembre del 2017. https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhxKmqLque6kMW1chJuEHzB2LvnmYl6tmgdCyJ7Ep7d490YZKW8ptaXbZVpysEhjsnNcElgEeF4JDcgYQh41LgX8fcn98cZ8e12qM5BlL50fqw==

[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] Ministerio del Interior. "El Gobierno Nacional puso en marcha las puertas biométricas en el aeropuerto de Ezeiza". Abril del 2018. http://www.migraciones.gov.ar/accesible/novedad.php?i=4019

[103] Dirección General de Administración. "SOLUCIÓN INTEGRAL PARA IDENTIFICACIÓN DE EXTRANJEROS Y CONTROL BIOMÉTRICO DE RESTRICCIONES". Expediente Nº 21-0002-LPU19. Febrero del 2019. https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhwfHN|0dYheEGyNBwGGvH3GL6jBhnOAiv5hg9nZ3JQi1tBQTuogGzD12zCv6XuNwuBmJTvQzJWApOOrz69pEW2MV9graYTQBzR11CtszG5T6w==

[104] División Compras. "Contratación de servicios, licencias y productos relativos a la plataforma biométrica del RENAPER". Octubre del 2017. Expediente Nº 78-0012-CDI17. https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhy7MmMdVUat6QKfRigU80UVxJmyaLvy67Tv2OgtO1qNBgGmFkKWbfpTnnfNopxo|oaRtWe20G7DjIP49UkgkEP896PfIoNb393/ NEPZ2M5G7w==
División Compras. "Solución integral de gestión centralizada de terminales para el manejo de licencias". Expediente Nº78-0022-CDI18. Septiembre del 2018. https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhzln331uwbedtWpuhJRVlkYFu5E0d6zTuIWgkUVrzCpo|kMsAHgU/dYCpNuyBnX9eXEW4riZstvHDV2ZqhmqPbCKquiSivEogUdA1HkMNIlaA== División Compras. "AMPLIACIÓN Y ACTUALIZACIÓN DE LA PLATAFORMA BIOMÉTRICA EXISTENTE DEL RENAPER". Expediente Nº 78-0028-CDI18. Diciembre del 2018.

En diciembre del 2017, el RENAPER y lo que era en su momento la Secretaría de Modernización (actualmente, la Secretaría de Innovación Pública, bajo la Jefatura de Gabinete) firmó un acuerdo de cooperación para desarrollar un Sistema de Identidad Digital (SID) nacional.[105] El sistema hace uso del reconocimiento facial para validar la identidad de las personas cuando acceden a ciertos servicios estatales y privados que implementan su Interfaz de Programación de Aplicaciones (API) o su kit de desarrollo de software (SDK). El SID se lanzó por primera vez en una fase piloto para probar su uso en algunas empresas *fintech* para el proceso de incorporación para crear una cuenta bancaria.[106] El elemento de reconocimiento facial del software del SID es NeoFace Watch, adquirido con un préstamo del **Banco Mundial** por USD 834 403,90.

El Sistema de Identidad Digital de Argentina se está ampliando para cubrir múltiples casos de uso, además de los sistemas para los servicios y las *fintechs* estatales. En julio del 2020, el Ministerio del Interior firmó un acuerdo de cooperación con el Ministerio de Educación para implementar el sistema en las universidades nacionales, para exigir que los y las estudiantes validen sus identidades antes de rendir exámenes en línea.[107] Esta ampliación está ocurriendo a pesar de las preocupaciones acerca de las fallas en sus algoritmos de reconocimiento facial.[108] La creciente expansión de este sistema puede convertirlo en la manera principal de validar la identidad de las personas, lo que puede provocar discriminación e impedir que personas que no estén en el sistema o que no puedan ser identificadas correctamente accedan a servicios públicos. El gobierno ha minimizado esta amenaza, argumentando que el algoritmo de reconocimiento facial está configurado en virtud de las tasas de falsos positivos y falsos negativos de NEC.[109]

A escala local, NEC ha estrechado una relación cercana con el gobierno de Tigre, una ciudad de Buenos Aires. La municipalidad usa la tecnología de NEC para todo su programa de vigilancia urbana desde al menos 2016, comenzando con CCTV, reconocimiento automatizado de matrículas de vehículos (ALPR) y reconocimiento facial mediante NeoFace Watch.[110]

---

https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhzNiQxEvvRD1M4Hrw70Q0R4HTin1WArUVSpJfI4xYYgmiT77fvnNNo8g|PlFmMreDTagF|N6f4dFxdRnoYveFKYmjFSg8zlglzEUYmrvWH5MQ==
División Compras. “SERVICIO DE MANTENIMIENTO, SOPORTE Y ASISTENCIA TÉCNICA PARA EL SISTEMA ABIS”. Expediente Nº 78-0029-CDI18. Diciembre del 2018. https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhyGzxXg3NEnQt|kEbGqFjvyvkPpcD27XbPjrB79ynaMSOETGHQanjODkHz9Nz64Gib/l6s/Al|E2d1ogkSzvDmTJdhqutPSEbqYs|rd|4j|BA==
División Compras. “SERVICIO INTEGRAL PARA LA MIGRACIÓN Y MANTENIMIENTO GENERAL DE TODA LA PLATAFORMA AFIS EXISTENTE”. Expediente Nº 78-0001-CDI20. Abril del 2020.
https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhxz8ZzajHoNTGv6h2avQkrsmYw2yzxlp7rrnVp3vvETTUXRKICLVaNVdpDAhqicxls3LP/xxu4zp9sqDVtRdJGZ6ZJhpzdesliW7C8vB7JEGg==
[105] Ministerio del Interior. “SID: Sistema de Identidad Digital”.
https://www.argentina.gob.ar/interior/renaper/sid-sistema-de-identidad-digital
[106] “*Fintech*” o tecnología financiera hace referencia a nuevos negocios que desarrollan servicios financieros utilizando tecnologías digitales como centro de sus productos y servicios.
[107] Ministerio de Educación. “Nuevo sistema para la validación de la identidad de estudiantes universitarios”. Julio del 2020. https://www.argentina.gob.ar/noticias/nuevo-sistema-para-la-validacion-de-la-identidad-de-estudiantes-universitarios
[108] La Nación. “‘No me gusta tu cara’: ¿discriminan las aplicaciones?” Septiembre del 2019. https://www.lanacion.com.ar/tecnologia/no-me-gusta-tu-cara-discriminan-aplicaciones-nid2292711/
[109] ADC. “Tu yo digital: Descubriendo las narrativas sobre identidad y biometría en América Latina”. Abril del 2019.https://adc.org.ar/informes/tu-yo-digital-descubriendo-las-narrativas-sobre-identidad-y-biometria-en-america-latina/
[110] Canal de YouTube de NEC Corporation. “La ciudad de Tigre”. Septiembre del 2016. https://www.youtube.com/watch?v=5Lp9PWv0EQ0

En el 2019, Tigre remodeló su infraestructura de vigilancia[111] lanzando NeoCenter, desarrollado por NEC para incrementar las capacidades existentes de la ciudad.[112] Además de las características mencionadas anteriormente, el software de reconocimiento facial se actualizó para seguir a las personas de manera más precisa en los espacios públicos, grabando los recorridos de movimiento para ubicar dónde ha estado una persona (su historial de recorrido) e identificar "comportamientos sospechosos" mediante el análisis del movimiento de las personas y los vehículos. Asimismo, Tigre amplió aún más su tecnología de vigilancia en el 2020 con la instalación de un tótem de cámaras para el reconocimiento facial.[113]

Cuando Tigre anunció el lanzamiento, ADC presentó[114] una solicitud de acceso a la información para obtener más datos sobre cómo se estaba usando la tecnología y cuáles eran los marcos legales de su uso. El gobierno local demoró el proceso y no respondió, incluso tras varios intentos de seguimiento, lo cual demostró su falta de transparencia y rendición de cuentas.

Tigre ha tenido una relación tan estrecha con NEC que la empresa usa la ciudad como un caso de estudio de marketing, exhibiendo las soluciones que le brinda a la ciudad, que incluyen tecnología para la colaboración ciudadana en la seguridad pública, el análisis de matrículas de vehículos, el reconocimiento facial, la detección de comportamiento, la elaboración de un mapa de delitos y la recopilación de pruebas, y tecnología de *machine learning* para el análisis de datos. NEC asegura que Tigre se está convirtiendo en "un modelo de ciudad segura para América Latina".[115]

NEC también estuvo involucrada en el despliegue de equipos de vigilancia en aeropuertos de **Brasil**. El Servicio Federal de Aduanas de Brasil (*Receita Federal*), por ejemplo, adquirió tecnología de reconocimiento facial de NEC para identificar personas viajeras sospechosas de evadir impuestos a la importación.[116] El sistema opera ya en 14 aeropuertos brasileños desde el 2016.[117]

Antecedentes de derechos humanos de NEC

En diciembre del 2020, **Justice for Myanmar**, un grupo de activistas, llevó adelante una investigación[118] sobre la corrupción del ejército de Myanmar y la influencia en el sector de la información y las

[111] Municipalidad de Tigre. "Ojos de Tigre". https://www.tigre.gob.ar/seguridad/cot
[112] Ámbito. "Tigre lanzó un nuevo sistema de reconocimiento facial". Mayo del 2019. https://www.ambito.com/municipios/municipios/tigre-lanzo-un-nuevo-sistema-reconocimiento-facial-n5030978
[113] Municipalidad de Tigre. "Nuevo tótem de seguridad con cámara de reconocimiento facial en El Talar". Septiembre del 2020. http://www.tigre.gov.ar/novedades/detalle/1267
[114] Cuenta de Twitter de ADC. https://twitter.com/adcderechos/status/1131556333466116096?s=20
[115] NEC. "Tigre City Integrated Urban Safety Solutions." https://www.nec.com/en/case/tigre/index.html NEC brochure for Tigre case study: https://web.archive.org/web/20170321095617/http://www.nec.com/en/case/tigre/pdf/brochure.pdf
[116] NEC. "El Servicio de Ingresos Federales usará la tecnología de identificación facial de NEC en 14 aeropuertos internacionales del país" (en portugués). 2016. https://br.nec.com/pt_BR/press/PR/20160409060302_11186.html
[117] Ministerio de Economía. "El Servicio de Ingresos Federales lanza sistema de reconocimiento facial" (en portugués). 2016. 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. "Nodes of Corruption, Lines of Abuse." Diciembre del 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

comunicaciones. El grupo reveló evidencia del robo de activos públicos por parte del ejército, expuso nuevas redes de adquisiciones militares y destapó la red global de negocios que está permitiendo que el ejército continúe cometiendo crímenes de guerra y de lesa humanidad.

Según la investigación, **NEC** proporcionó equipos de transmisión de microondas a las fuerzas armadas de Myanmar a través de **Viettel** (empresa de telecomunicaciones de Vietnam) y **Mytel** (el operador móvil más nuevo de Myanmar). Al hacerlo, NEC y otras empresas que brindan tecnología a través de Mytel y Viettel corren el riesgo de contribuir a las graves violaciones a los derechos humanos en Myanmar.

El Centro de Información sobre Empresas y Derechos Humanos (BHRRC) invitó a NEC y otras 20 de las empresas mencionadas en el informe a responder a las acusaciones. En su respuesta, NEC expresó que "se rehusaría a hacer comentarios sobre casos individuales".[119] Previamente, la empresa no había emitido respuesta cuando el BHRRC le preguntó si las autoridades japonesas le habían solicitado el desarrollo de drones para uso militar con el gobierno israelí.[120]

En el 2019, se difundió ampliamente que el sistema de reconocimiento facial de NEC había sido utilizado en el primer caso de detención ilegal debido a un sesgo algorítmico.[121] NEC respondió que "una coincidencia basada únicamente en el reconocimiento facial no es mecanismo para la identificación positiva" y no aclaró cómo la empresa evitará casos similares en el futuro.

Este accionar entra en conflicto directo con el compromiso expreso de NEC de respetar los derechos humanos y la privacidad establecido en su Código de Conducta del Grupo,[122] y representa un fracaso respecto de la transparencia tal como la recoge el documento de la empresa "IA y principios de derechos humanos del Grupo NEC".[123]

⇛ IDEMIA

Nombre de la empresa	**Idemia France SAS**
Sede principal	Courbevoie, Francia
Países en los que opera	En todo el mundo
Países en los que se despliegan sus tecnologías de vigilancia entre Argentina, Brasil y Ecuador	Argentina

[119] Business & Human Rights Resource Centre. "NEC's response." Enero del 2021. https://www.business-humanrights.org/en/latest-news/necs-response/
[120] Business & Human Rights Resource Centre. "Japan: Reported joint drone development with Israel." Octubre del 2016. https://www.business-humanrights.org/es/%C3%BAltimas-noticias/japan-reported-joint-drone-development-with-israel/
[121] New York Times. "Wrongfully Accused by an Algorithm." Junio del 2020. https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html
[122] NEC. "Group Code of Conduct." Actualizado en enero del 2019. https://www.nec-enterprise.com/documents?id=1432&hash=7c546360141e92ca5009db242402001dd7e393ef5198076b4f5e5a9f1c869f29
[123] NEC. "NEC Unveils "NEC Group AI and Human Rights Principles." Abril del 2019. https://www.nec.com/en/press/201904/global_20190402_01.html

Fundación	2008
Pública/privada	Privada
Accionista(s) mayoritario(s)	Advent International (accionista mayoritario)
Cantidad de empleados(as)	Aproximadamente 15 000 en el 2019
Ingresos anuales	EUR 2 300 millones (USD 2 700 millones) en el 2019

Conocida anteriormente como "Morpho Safran" y "Safran Identity and Security",[124] la empresa francesa **IDEMIA** es uno de los proveedores líderes de tecnología biométrica en todo el mundo. Solo en EE. UU., la empresa brinda soluciones para el Buró Federal de Investigaciones (FBI),[125] la INTERPOL,[126] el Departamento de Policía de Nueva York,[127] y la Administración de Seguridad del Transporte de EE. UU., entre otros.

En nuestra investigación para elaborar este informe, no pudimos encontrar conexiones recientes entre los gobiernos de Argentina, Brasil o Ecuador y la empresa bajo la marca IDEMIA. Esta empresa cuenta con una oficina en Buenos Aires, Argentina, pero se centra en el mercado de los proveedores móviles. Si bien no está claro cuándo las autoridades argentinas adquirieron por primera vez tecnología de IDEMIA, las fuerzas de aplicación de la ley comenzaron a usar productos de Morpho antes del 2010.[128] El uso de esta tecnología se incrementó exponencialmente con la introducción y consecuente expansión de **SIBIOS**, una base de datos biométricos masiva de propiedad del Estado.

Como destacaremos en nuestro caso de estudio sobre Argentina en este informe, el uso de productos de Morpho está estrechamente relacionado con SIBIOS. Tanto el Ministerio Nacional de Seguridad como la Policía Federal hacen uso de estos productos. En el 2014 y el 2015, el Ministerio destinó más de USD 7 millones a contratos con Morpho S.A. para adquirir tecnología biométrica.[129] La Policía Federal

[124] IDEMIA, "OT-Morpho becomes IDEMIA, the global leader in trusted identities." Septiembre del 2017. https://www.idemia.com/press-release/ot-morpho-becomes-idemia-global-leader-trusted-identities-2017-09-28
[125] Morpho. "MorphoTrak Technology Goes Operational for the FBI." Abril del 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 to provide Interpol and its 186 member states with latest AFIS, Automated FingerprintIdentification System." Febrero del 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 is the exclusive partner of INTERPOL for facial recognition." Noviembre del 2016. http://www.morpho.com/en/media/safran-identity-security-exclusive-partner-interpol-facial-recognition-20161123
[127] Morpho. "Morpho Trak Deploys Morpho Biometric Identification System at NYPD." Septiembre del 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
[128] Zona Norte. "El sistema de seguridad Morpho Touch ya se aplica en Tigre". Agosto del 2008. https://www.zonanortediario.com.ar/05/08/2008/el-sistema-de-seguridad-morpho-touch-ya-se-aplica-en-tigre/
[129] POLICÍA FEDERAL ARGENTINA, SUPERINTENDENCIA DE ADMINISTRACIÓN, DIVISIÓN CONTRATACIONES, CONTRATACIÓN DIRECTA N° 25/2014, Expediente N° 581-01-000726-14:
POLICÍA FEDERAL ARGENTINA, SUPERINTENDENCIA DE ADMINISTRACIÓN, DIVISIÓN CONTRATACIONES, CONTRATACIÓN

hace uso de dispositivos Morpho RapID en campo para llevar a cabo la identificación dactilar de individuos,[130] al igual que de Morpho Face Detective de reconocimiento facial para identificar personas en multitudes.[131]

Dado que la Policía Federal tiene jurisdicción en toda la nación, el uso de la tecnología de Morpho se expandió por todo el país, en ciudades como Campana,[132] Luján,[133] Balcarce,[134] Córdoba,[135] Chaco,[136] y múltiples municipios de la provincia de Buenos Aires.[137]

Las agencias estatales recurren a un revendedor principal de la tecnología de IDEMIA, **IAFIS Argentina S.A.**, la misma empresa que vende productos de Cellebrite. Este revendedor nombra como clientes a múltiples fuerzas policiales de varias provincias argentinas,[138] así como también Fiscalías y otras instituciones públicas, aunque no especifica qué productos les provee.

La Ciudad de Buenos Aires adquirió el software Morpho Face Investigate de IAFIS Argentina S.A. en el 2011 por ARS 33 198 500 (más de USD 6 millones en ese entonces), y comenzó a probar su funcionamiento en el subterráneo para identificar a carteristas.[139]

Según documentos oficiales de contratación y licitación pública, la Policía Metropolitana de la Ciudad de Buenos Aires usa tecnología de reconocimiento dactilar y facial de Morpho en investigaciones

---

DIRECTA N° 26/2014, Expediente N° 581-01-000640-14:
https://www.boletinoficial.gob.ar/detalleAviso/tercera/2134792/20150119
Expediente Nº 550-01-001003-2014 y 563-01-001091-2014
https://www.boletinoficial.gob.ar/detalleAviso/tercera/2125517/20141024
Expediente Nº 581-01-000726/2014 y 563-01-001090/2014
https://www.boletinoficial.gob.ar/detalleAviso/tercera/2125518/20141024

[130] La cuenta oficial de Twitter del Ministerio publicitó su uso en el 2018:
https://web.archive.org/web/20201230202624/https://twitter.com/MinSeg/status/1038127257401810944?s=20 y
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] Cuenta oficial de Twitter de la Policía Federal, mostrando el uso de Morpho Face Detective en la estación de trenes de Retiro, enero del 2019:
https://web.archive.org/web/20201230203110/https://twitter.com/PFAOficial/status/1090673247161597952?s=20

[132] La Auténtica Defensa. “El sistema Morpho Rapid ya se aplica en Campana”. Marzo del 2009.
www.laautenticadefensa.net/62085

[133] El Civismo. “Moderno equipo para identificar personas”. Septiembre del 2010. https://www.elcivismo.com.ar/notas/7191/

[134] La Vanguardia. “Adelanto: operativo de la Policía Federal en Balcarce”. Febrero del 2019.
http://www.diariolavanguardia.com/noticias/21448--cobramos-por-lo-que-trabajamos--no-le-robamos-la-plata-a-nadie-/

[135] La Voz. “Recapturaron a ‘Cañete’, el prófugo cordobés ‘más buscado’”. Mayo del 2017.
https://www.lavoz.com.ar/sucesos/recapturaron-canete-el-profugo-cordobes-mas-buscado

[136] Departamento de Policía de Chaco. “La policía capacita y prueba un nuevo sistema de identificación”. Marzo del 2013.
https://web.archive.org/web/20201230210055/http://policia.chaco.gov.ar/index.php/ecmPagesView/view/id/101

[137] Primera Plana. “Policía Federal desembarca en el interior bonaerense con operativos de control y prevención”. Mayo del 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/

[139] Infobae. “Evalúan un software de identificación facial para ubicar ‘pungas’ en el subte”. Enero del 2013.
https://www.infobae.com/2013/01/13/691102-evaluan-un-software-identificacion-facial-ubicar-pungas-el-subte/

judiciales. IAFIS Argentina S.A. les brinda soporte técnico desde, por lo menos, el 2015, con diferentes contratos por un total de más de USD 6,5 millones.[140]

Antecedentes de derechos humanos de IDEMIA

En el 2017, Morpho (que más adelante se convirtió en **IDEMIA**) fue culpada por problemas con sus kits de registro y autenticación biométricos usados en la elección general de Kenia del 2017, lo que causó que la Asamblea Nacional cancelara sus contratos públicos y bloqueara los contratos nuevos. Tal resolución fue impugnada y revocada por el Tribunal Superior de Kenia.[141] La coalición opositora de Kenia acusó a la firma francesa de complicidad en fraude electoral, pero la empresa negó dichas acusaciones. **Safran (entidad previa a la fusión de IDEMIA) también recibió una multa de la corte francesa por haber pagado sobornos para asegurar negocios en Nigeria.[142]**

En septiembre del 2020, **Amnistía Internacional** descubrió que tres empresas europeas, una de las cuales era IDEMIA, vendían tecnología de vigilancia al gobierno chino.[143] Específicamente, a IDEMIA se le adjudicó un contrato para proporcionar equipos de reconocimiento facial directamente al Buró de Seguridad Pública de Shanghái en el 2015. Debido al riesgo de que las autoridades chinas usaran los equipos para la vigilancia masiva y otros abusos a los derechos humanos, Amnistía Internacional, Access Now y otras organizaciones, así como también países europeos, han estado pidiendo a la Unión Europea que se fortalezcan las salvaguardas en materia de derechos humanos en las decisiones de exportación de vigilancia y se asegure que todas las empresas relevantes lleven a cabo evaluaciones de impactos en los derechos humanos.[144] Francia, donde se encuentra la sede central de IDEMIA, se ha resistido a esta petición.[145]

⇛ Verint

Nombre de la empresa	**Verint Systems Inc.**
Sede principal	Nueva York, EE. UU.
Países en los que opera	En todo el mundo

[140] Buenos Aires Compras. Número del proceso de compra: 2900-1047-CDI15 https://www.buenosairescompras.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhzAdZmPYqqZ4su3ScBBrBvMPHSPHPxZ74bjkpi4POk3iZKynCGKbKt|RDsvNIcW1mJISgBUffWWFY1vgdwt/W5yzl3PnouupiCeVWiQuysmvw== Número del proceso de compra: 2900-0858-CDI17. https://www.buenosairescompras.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhzjp0DPq1u2nI3iH|4rzqLn9Phu5zQ6mkLN3u849mLkhWIq/6PJyo37gtSRaUyG3uJLK1ZE2CoQE3RKSJHwBng31I/q82/vv9su9cJDc2PG2g==

[141] Biometric Update. "Biometrics in Africa this week: Idemia suspension in Kenya overturned, local solutions sought for cybercrime." Abril del 2020. https://www.biometricupdate.com/202004/biometrics-in-africa-this-week-idemia-suspension-in-kenya-overturned-local-solutions-sought-for-cybercrime

[142] BBC. "Safran fined in Nigerian bribery case." Septiembre del 2012. https://www.bbc.com/news/business-19498916

[143] Amnistía Internacional. "EU companies selling surveillance tools to China's human rights abusers." Septiembre del 2020. https://www.amnesty.org/en/latest/news/2020/09/eu-surveillance-sales-china-human-rights-abusers/

[144] Access Now. "Urgent call to Council of the EU: human rights must come first in Dual Use final draft." Noviembre del 2020. https://www.accessnow.org/urgent-call-to-council-of-the-eu-human-rights-must-come-first-in-dual-use-final-draft/

[145] Netzpolitik, "Surveillance exports: How EU Member States are compromising new human rights standards." Octubre del 2018. https://netzpolitik.org/2018/surveillance-exports-how-eu-member-states-are-compromising-new-human-rights-standards/

Países en los que se despliegan sus tecnologías de vigilancia entre Argentina, Brasil y Ecuador	Ecuador
Fundación	2002
Pública/privada	Cotiza en Nasdaq
Accionista(s) mayoritario(s)	N/A
Cantidad de empleados(as)	Aproximadamente 6 500 en el 2019
Ingresos anuales	EUR 2 300 millones (USD 2 700 millones) en el 2019

VERINT es una de las pocas empresas estadounidenses que se ha abierto camino en el mercado latinoamericano. Aproximadamente la mitad de su nómina reside en Israel.

En **Ecuador**, la ciudad de **Guayaquil** adquirió tecnologías de vigilancia de VERINT comprando al distribuidor **Unión Eléctrica S.A.,** una empresa que ha ganado millones en contratos a partir de la **Corporación para la Seguridad Ciudadana**, una entidad privada sin fines de lucro creada para gestionar la videovigilancia y otros servicios de seguridad en Guayaquil.[146] El propósito era integrar reconocimiento facial en 100 cámaras de vigilancia para la seguridad en instituciones educativas. Tal integración tuvo un costo de USD 2 569 906,41 e incluyó productos como cámaras con capacidades de captura de rostros, sistemas de reconocimiento facial, soluciones de almacenamiento de datos, licencias de cámaras y monitoreo, y equipos de megáfonos, servicios e infraestructura periféricos. En el 2020, estas cámaras y demás productos se incorporaron al programa de vigilancia masiva **ECU911** de Ecuador.

Antecedentes de derechos humanos de VERINT

En el 2014, una investigación de Privacy International[147] explicó en detalle cómo **VERINT** proporcionaba centros de monitoreo capaces de interceptación masiva de redes telefónicas, móviles y de IP a **Kazajistán** y **Uzbekistán**. Kazajistán ha sido condenado por leyes que restringen la libertad de expresión y de reunión, juicios deficientes, apagones de internet y torturas[148], mientras que en Uzbekistán ha habido testimonios de abogados(as), periodistas y blogueros(as) cuyas comunicaciones

[146] Corporación para la Seguridad Ciudadana de Guayaquil. https://cscg.gob.ec/
[147] Privacy International. "Private Interests: Monitoring Central Asia." Noviembre del 2014. https://privacyinternational.org/report/837/private-interests-monitoring-central-asia
[148] Human Rights Watch. "Kazakhstan." https://www.hrw.org/europe/central-asia/kazakhstan; Access Now, "Civil society reports internet shutdowns in two cities in Kazakhstan during February 28 protests." Marzo del 2021. https://www.accessnow.org/internet-shutdowns-kazakhstan-feb-28-protests/

fueron interceptadas, y quienes fueron luego objeto de persecución por motivos políticos.[149] Ambos países son conocidos por la extensa vigilancia digital de sus ciudadanos y ciudadanas.[150]

Privacy International también publicó un informe especial sobre el estado de la vigilancia en **Colombia** en el 2015.[151] Según el informe, el gobierno de Colombia usa un sistema llamado Plataforma Única de Monitoreo y Análisis (**PUMA**). La PUMA tiene la capacidad potencial de interceptar y almacenar todas las comunicaciones transmitidas a través de la infraestructura de red troncal de la que depende el pueblo colombiano para comunicarse y enviarse mensajes. Esta plataforma funciona con tecnología de propiedad exclusiva de VERINT, haciendo uso principalmente de la plataforma de centro de monitoreo RELIANT.

Al parecer, especialistas de VERINT colocaron 16 sondas "IP-PROBER"[152] en las redes troncales para interceptar datos y reenviarlos a los centros de monitoreo de la PUMA. El Departamento Administrativo de Seguridad (DAS) las usó para vigilar la red de comunicaciones; luego, se investigó a la agencia por actividades ilegales, y finalmente se disolvió debido al espionaje y acoso a personas del ámbito político y periodístico, activistas y jueces/juezas de la Corte Suprema que se oponían al gobierno de Álvaro Uribe.

En el 2012, el Centro de Información sobre Empresas y Derechos Humanos invitó a empresas, incluida VERINT, a responder a las acusaciones de prestación de tecnología de vigilancia a regímenes opresivos en Medio Oriente.[153] VERINT no emitió respuesta.

Otras empresas que proporcionan tecnología de vigilancia en América Latina

Como mencionamos en la introducción de este informe, nos hemos centrado en empresas con la mayor información disponible al público sobre sus negocios en América Latina, que plantean amenazas particulares a los derechos humanos y son dominantes debido a sus relaciones con organismos gubernamentales. Sin embargo, cabe mencionar que existen múltiples empresas que están manteniendo un perfil más bajo y que ameritan una investigación más profunda.

[149] Human Rights Watch. "Uzbekistan." https://www.hrw.org/europe/central-asia/uzbekistan
[150] Access Now, "Commonwealth of surveillance states: On the export and resale of Russian surveillance technology to post-Soviet Central Asia." Junio del 2013.
https://www.accessnow.org/cms/assets/uploads/archive/docs/Commonwealth_of_Surveillance_States_ENG_1.pdf
[151] Privacy International. "Un estado en la sombra: vigilancia y orden público en Colombia". Agosto del 2015.
https://www.privacyinternational.org/sites/default/files/2017-12/ShadowState_Espanol.pdf
[152] Dirección de Administración y Finanzas, Policía Nacional de Colombia. Expediente N° 06-7-10124-10. Septiembre del 2010.
http://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=10-12-351033
[153] Business & Human Rights Resource Centre. "Human Rights First & OWNI Digital articles on surveillance technology & oppressive regimes." Enero del 2012 https://www.business-humanrights.org/es/%C3%BAltimas-noticias/human- Rights - First-- - articles - on - surveillance - technology- oppressive - regimes/

BGH Tech Partner

Nombre de la empresa	BGH Tech Partner S.A.
Sede principal	Buenos Aires, Argentina
Países en los que opera	[No disponible]
Países en los que se despliegan sus tecnologías de vigilancia entre Argentina, Brasil y Ecuador	Argentina
Fundación	1913
Pública/privada	Privada
Accionista(s) mayoritario(s)	[No disponible]
Cantidad de empleados(as)	[No disponible]
Ingresos anuales	[No disponible]

Boris Garfunkel e Hijos, o **BGH**, es una empresa **argentina** que comenzó a vender una gran variedad de productos, pero que, durante la última década, se centró en parte en el desarrollo de soluciones tecnológicas. La empresa es responsable del despliegue tecnológico del Laboratorio de Análisis Forense de Videos de la provincia de **San Juan**.[154] Si bien la empresa afirma que solo brinda servicios de comunicaciones cifradas y de mapeo de ubicaciones a las agencias de aplicación de la ley, según informes de los medios,[155] este laboratorio pronto estará equipado con software de reconocimiento facial para la identificación de personas y la detección y clasificación de objetos, atributos y comportamientos, así como también el reconocimiento de matrículas de vehículos.

Hemos intentado obtener información sobre el despliegue tecnológico de BGH, tanto del gobierno como de la propia empresa, pero no hemos tenido éxito. Es posible que la tecnología provenga de **Hikvision**, dado que, en el 2018, BGH comenzó a vender productos de dicha empresa.[156] Las soluciones que ahora ofrece BGH incluyen cámaras térmicas, vehiculares, portátiles y de reconocimiento facial, así como tecnologías como drones y robots.[157]

Danaide S.A. y NTechLab

[154] BGH. "San Juan implementa tecnología de comunicaciones de última generación para la policía provincial". Septiembre del 2020. https://www.bghtechpartner.com/2020/09/11/san-juan-implementa-tecnologia-de-comunicaciones-de-ultima-generacion-para-la-policia-provincial/
[155] Servicio de información del Gobierno de San Juan. "Acuerdo San Juan: tecnología aplicada a la seguridad". Octubre del 2020. https://sisanjuan.gob.ar/seguridad/2020-10-22/26837-acuerdo-san-juan-tecnologia-aplicada-a-la-seguridad
[156] BGH. "BGH Tech Partner suma Hikvision a su portfolio." Febrero del 2018. https://www.bghtechpartner.com/2018/02/02/bgh-tech-partner-suma-hikvision-su-portfolio/
[157] Canal AR. "BGH impulsa su porfolio de videovigilancia con Hikvision". Enero del 2018. https://canal-ar.com.ar/25431-BGH-impulsa-su-porfolio-de-videovigilancia-con-Hikvision.html

Nombre de la empresa	Danaide S.A.
Sede principal	Buenos Aires, Argentina
Países en los que opera	Argentina
Países en los que se despliegan sus tecnologías de vigilancia entre Argentina, Brasil y Ecuador	Argentina
Fundación	1999
Pública/privada	Privada
Accionista(s) mayoritario(s)	[No disponible]
Cantidad de empleados(as)	[No disponible]
Ingresos anuales	[No disponible]

Nombre de la empresa	N-Tech.Lab Ltd.
Sede principal	Nicosia, Chipre
Países en los que opera	Rusia
Países en los que se despliegan sus tecnologías de vigilancia entre Argentina, Brasil y Ecuador	Argentina
Fundación	2015
Pública/privada	Privada
Accionista(s) mayoritario(s)	[No disponible] Entre sus accionistas minoritarios, el Fondo Ruso de Inversión Directa y fondos soberanos de inversión líderes de los países del Medio Oriente hicieron una inversión capital de RUB 1 000 millones (USD 13 millones) en el 2020.
Cantidad de empleados(as)	[No disponible]
Ingresos anuales	[No disponible]

Según algunos informes independientes,[158] la empresa **argentina** local **Danaide**, contratada por Buenos Aires para implementar su sistema de reconocimiento facial,[159] puede que esté usando el

[158] One Zero. “The U.S. Fears Live Facial Recognition. In Buenos Aires, It’s a Fact of Life.” Marzo del 2020. https://onezero.medium.com/the-u-s-fears-live-facial-recognition-in-buenos-aires-its-a-fact-of-life-52019eff454d
[159] ADC. "#ConMiCaraNo: Reconocimiento facial en la Ciudad de Buenos Aires”. Mayo del 2019. https://adc.org.ar/2019/05/23/con-mi-cara-no-reconocimiento-facial-en-la-ciudad-de-buenos-aires/

software Find Face[160] desarrollado por la empresa rusa **NTechLab**. A pesar de nuestros múltiples intentos por obtener más detalles a través de pedidos de acceso a la información, el gobierno solo confirma que Danaide ganó la licitación del contrato, rehusándose a aclarar si la propia empresa había sido la desarrolladora del algoritmo de reconocimiento facial.

En la versión rusa del sitio web de NTechLab,[161] el software **UltraIP**[162] de Danaide, que se vende en Argentina, figura en la sección de socios. Como respuesta al pedido de acceso a la información de ADC de junio del 2019,[163] autoridades de Buenos Aires confirmaron que UltraIP es el nombre del software que licenciaba.

En octubre del 2020, Human Rights Watch alertó al público acerca de fallas en el sistema de NTechLab y su uso indebido por parte del gobierno para identificar y usar de blanco a niños(as) por persecución penal en violación de derechos humanos.[164] En **Moscú**, NTechLab provee el software para un programa de vigilancia del que el gobierno ha abusado, según grupos de derechos humanos, mediante la vigilancia de personas durante la pandemia de COVID-19 para hacer cumplir un confinamiento.[165]

IBM

Nombre de la empresa	**International Business Machines Corporation**
Sede principal	Nueva York, EE. UU.
Países en los que opera	En todo el mundo
Países en los que se despliegan sus tecnologías de vigilancia entre Argentina, Brasil y Ecuador	Argentina
Fundación	1911
Pública/privada	Cotiza en la Bolsa de Valores de Nueva York
Accionista(s) mayoritario(s)	N/A
Cantidad de empleados(as)	Aproximadamente 350 000 en el 2020 (en total, como grupo)
Ingresos anuales	USD 45 000 millones en el 2020

[160] NTechLab. Sitio web oficial de Find Face. https://findface.pro/en/
[161] NTechLab. Socios (en ruso). https://web.archive.org/web/20200511205745/https:/findface.pro/partners/
[162] Danaide. Software developments. https://danaide.com.ar/desarrollos/desarrollossoftware.html
[163] ADC. Solicitud de acceso a la información NO-2019-21065074-GCABA-DGAYCSE. Julio del 2019. https://adc.org.ar/wp-content/uploads/2019/07/Respuesta-PAIP-reconocimiento-facial-GCBA-V2.pdf
[164] Human Rights Watch. "Argentina: Child Suspects' Private Data Published Online." Octubre del 2020. https://www.hrw.org/news/2020/10/09/argentina-child-suspects-private-data-published-online
[165] Reuters. "Russia's lockdown surveillance measures need regulating, rights groups say." Abril del 2020. https://uk.reuters.com/article/uk-health-coronavirus-russia-facial-reco-idUKKCN2253CG

En diciembre del 2016, el Ministerio Nacional de Seguridad de Argentina firmó un contrato con la empresa local **Unitech S.A.**, descripto como la adquisición de "software avanzado para investigaciones penales", por un total de USD 3 515 518,77.[166] Dentro de los documentos de contratación, las especificaciones técnicas indican que los productos y servicios del contrato incluían: nueve licencias de i2 Enterprise Insight Analysis[167] de IBM, un complemento i2 Collaborate de IBM, i2 Text chart de IBM, y múltiples servicios de soporte técnico.

Existen precedentes de tecnología de IBM utilizada en Filipinas durante la violenta "guerra contra las drogas". Según una investigación del 2009 liderada por Human Rights Watch,[168] existen pruebas de que autoridades del gobierno y la policía estaban en complicidad con escuadrones de la muerte que asesinaban a niños y niñas de la calle, traficantes de drogas, y delincuentes menores durante el mandato de Rodrigo Duterte como alcalde de Dávao. En el 2012, IBM celebró un acuerdo con Sara Duterte, hija de Rodrigo Duterte y alcaldesa de la ciudad en ese entonces, para actualizar el centro de comandos de la policía de Dávao para "mejorar las operaciones de seguridad pública en la ciudad" mientras continuaba la violencia en las calles. Según un informe de The Intercept,[169] IBM se rehusó a responder consultas sobre sus antecedentes de derechos humanos en la ciudad de Dávao. El vocero de IBM, Edward Barbini, observó brevemente que la empresa "ya no proporciona tecnología al Centro de Operaciones de Inteligencia de Dávao, y no lo ha hecho desde el 2012", aunque no aclaró si IBM hacía mantenimiento de las tecnologías luego de ese momento, y los expedientes públicos de IBM mencionan que es un programa continuo luego de esa fecha.

[166] Dirección General de Administración. "ADQ. DE LICENCIAS DE SOFTWARE AVANZADO PARA EL ANÁLISIS CRIMINAL CON LA FIRMA UNITECH S.A.". Expediente N° 347-0066-CDI16. Diciembre del 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. "You Can Die Any Time." Abril del 2009.
https://www.hrw.org/sites/default/files/reports/philippines0409webwcover_0.pdf
[169] The Intercept. "Inside the Video Surveillance Program IBM Built for Philippine Strongman Rodrigo Duterte." Marzo del 2019.
https://theintercept.com/2019/03/20/rodrigo-duterte-ibm-surveillance/

Johnson Controls

Nombre de la empresa	Johnson Controls International PLC
Sede principal	Cork, Irlanda
Países en los que opera	En todo el mundo
Países en los que se despliegan sus tecnologías de vigilancia entre Argentina, Brasil y Ecuador	Brasil
Fundación	1885
Pública/privada	Cotiza en la Bolsa de Valores de Nueva York
Accionista(s) mayoritario(s)	Fondo Dodge & Cox Stock Fund (11,3 %) en el 2020
Cantidad de empleados(as)	Aproximadamente 97 000 en el 2020 (en grupos)
Ingresos anuales	USD 22 317 millones en el 2020

En São Paulo, la tecnología de reconocimiento facial instalada en el subterráneo fue provista por Johnson Controls, una empresa con sede central en Irlanda. Este es otro caso en que las autoridades no usaron el sistema de contratación tradicional.[170] En cambio, adquirieron la tecnología de reconocimiento facial a través de una contratación pública internacional, que otorga a competidores extranjeros una mayor oportunidad de hacer sus ofertas.

[170] IDEC. "Acción alega falta de transparencia en licitación del metro de SP" (en portugués). Febrero del 2020. https://idec.org.br/noticia/acao-questiona-falta-de-transparencia-e-solicita-informacoes-sobre-licitacao-do-metro-de-sp

III. CASOS DE ESTUDIO: CÓMO SE DESPLIEGA LA TECNOLOGÍA

CASO DE ESTUDIO: Argentina

Por Asociación por los Derechos Civiles (ADC)

Desde el 2015, el uso de tecnologías de vigilancia en Argentina ha aumentado gradual y constantemente, dando paso a grandes riesgos para el derecho a la privacidad en todo el país. En todas las instancias, el sector privado ha cumplido un papel clave en el despliegue de las tecnologías, estrechando relaciones con organismos gubernamentales a escala local, provincial y nacional.

Actualmente, estamos ante el pico de una tendencia que comenzó hace más de diez años, en el 2008, cuando los gobiernos locales comenzaron a usar tecnologías como cámaras de videovigilancia (o CCTV) para apoyar sus campañas políticas,[171] promocionando una imagen de progreso hacia una mayor seguridad pública.

Según un estudio llevado adelante por la Facultad de Psicología de la Universidad de Buenos Aires,[172] un alto porcentaje de la población considera que la situación de la seguridad pública en Argentina es "muy grave" o "extremadamente grave", y nueve de cada 10 personas piensan que tienen "bastantes o muchas probabilidades" de ser víctimas de un delito en el corto plazo. Debido a estos miedos, la seguridad pública ha tomado un lugar protagónico en la narrativa de funcionarias y funcionarios públicos para argumentar que el *fin* justifica los *medios*. Las personas en estos cargos han citado, al mismo tiempo, la seguridad pública como razón para evitar compartir detalles sobres sus acuerdos con empresas tecnológicas, cómo se procesa la información personal y cualquier otra especificación sobre los equipos adquiridos.

Si bien Argentina cuenta con fuertes protecciones constitucionales para los derechos humanos, incluido el derecho a la privacidad, y un marco exhaustivo de protección de datos, la adquisición e implementación de tecnologías de vigilancia usualmente se lleva adelante con poca o nula supervisión o transparencia.[173]

Tecnología desplegada

No es tarea fácil descubrir la medida en que los distintos niveles de gobierno usan los mecanismos y sistemas de vigilancia, ya que la información no está disponible inmediatamente a través de canales públicos, a menos que los medios informen sobre el tema o que se lleve a cabo una investigación independiente.

Además de las CCTV, las autoridades han incorporado lentamente tecnologías más invasivas a lo largo de la última década. **La introducción de SIBIOS en el 2011 marcó un momento particularmente**

[171] Natalia Zuazo, Revista Anfibia. "La vida de los otros". http://revistaanfibia.com/cronica/la-vida-de-los-otros/
[172] Facultad de Psicología, Universidad de Buenos Aires. "Monitor de inseguridad". Diciembre del 2020. http://www.psi.uba.ar/opsa/informes/monitor_inseguridad_pais_2.pdf
[173] Para obtener más información sobre el estado de la privacidad en general en Argentina, visite: https://privacyinternational.org/state-privacy/57/state-privacy-argentina

decisivo. Mediante el Decreto Ejecutivo 1766/11,[174] el gobierno nacional creó el Sistema Federal de Identificación Biométrica para la Seguridad (**SIBIOS**), gestionado por la Policía Federal bajo la autoridad del Ministerio de Seguridad.

Uno de los principales objetivos de SIBIOS era fusionar y digitalizar las bases de datos independientes de la Policía Federal y el Registro Nacional de las Personas (**RENAPER**). SIBIOS marcó la culminación de un trabajo que comenzó años antes de su lanzamiento, cuando el Ministerio del Interior empezó a recopilar, procesar y almacenar datos biométricos para la emisión de documentos nacionales de identidad (DNI) y pasaportes. Desde el 2009, el RENAPER tiene permitido usar tecnologías digitales para identificar a personas ciudadanas, residentes y visitantes. Desde ese momento en adelante, ha estado recopilando datos biométricos, que incluyen huellas dactilares, huellas palmares y fotos del rostro, tanto de ciudadanos(as) como de todas las personas que ingresan al país.[175]

SIBIOS es un sistema nacional, así que todas las provincias del país firmaron acuerdos de cooperación con el gobierno nacional, junto con el Ministerio de Seguridad (incluidas sus cuatro fuerzas federales de seguridad) y el Ministerio del Interior (incluidos el RENAPER y la Dirección Nacional de Migraciones). Estos acuerdos garantizan que las fuerzas policiales locales puedan actualizar y acceder a la base de datos. En el 2017, mediante el Decreto Ejecutivo 243/17,[176] el gobierno amplió el acceso a SIBIOS a cualquier organismo público dentro del Poder Ejecutivo o Judicial a nivel nacional y provincial, al tiempo que otorgó acceso a la Ciudad Autónoma de Buenos Aires (ciudad capital de Argentina). Quienes usan SIBIOS no tienen la obligación de obtener una orden o autorización judicial antes de hacer consultas en la base de datos biométricos.

El Ministerio de Seguridad recurrió a un proveedor importante para la infraestructura conectada a SIBIOS: la empresa francesa Morpho Safran, que, como resultado de una fusión, se convirtió en **IDEMIA**. Esta empresa es la responsable de la instalación y configuración del Sistema Automatizado de Identificación de Huella Dactilar (AFIS) del Ministerio. El Ministerio adquirió y utilizó otros productos de la empresa, incluido Morpho Face Investigate Pilot, para el reconocimiento facial a partir de archivos de fotos y video, y Morpho RapID,[177] para verificaciones de identidad *in situ* mediante huellas dactilares en todo el país.

Otra porción de la infraestructura de SIBIOS fue construida por el Ministerio del Interior, lo que cultivó una estrecha relación con su equivalente cubano, particularmente entre el 2011 y el 2015. El Ministerio adquirió su tecnología biométrica de una empresa propiedad del Estado cubano, **DATYS**, que desarrolló una familia de productos para la identificación[178] y la verificación[179] biométrica, basados en

[174] Decreto 1766/2011. Argentina. http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/189382/texact.htm
[175] ADC. "The Identity We Can't Change: How biometrics undermine our human rights." 2017. https://adc.org.ar/wp-content/uploads/2019/11/0027-B-The-identity-we-can%C2%B4t-change-12-2017.pdf
[176] Ministerio de Seguridad de Argentina. Decreto 243/2017. http://servicios.infoleg.gob.ar/infolegInternet/anexos/270000-274999/273446/norma.htm
[177] La Capital. "Identidad y antecedentes al instante en los operativos de saturación". Junio del 2016. https://www.lacapitalmdp.com/identidad-y-antecedentes-al-instante-en-los-operativos-de-saturacion/
[178] La identificación facial (1:n) es el proceso para analizar si la imagen de un rostro detectado coincide con la imagen de un rostro almacenada en la base de datos. En este caso, el sistema intenta encontrar una coincidencia en una base de datos de identidades.
[179] La verificación o autenticación facial (1:1) es el proceso para analizar si la imagen de un rostro detectado coincide con una imagen específica almacenada anteriormente. Usualmente, el sistema intenta responder la pregunta "¿la persona de la imagen es quien dice ser?"

el reconocimiento facial, de huellas dactilares, de huellas palmares, de ADN y de voz. En octubre del 2015, el Ministerio actualizó su tecnología biométrica mediante un contrato de USD 1 080 000 con DATYS, más USD 180 000 anuales para soporte técnico, durante un plazo de cinco años.

A partir de la introducción de SIBIOS en el 2011, el uso de tecnologías biométricas ha crecido exponencialmente en todo el país. **Además de su uso para la seguridad pública y la inmigración, los datos biométricos se utilizan para verificar identidades en contextos como programas de seguridad social (por ejemplo, para el acceso a fondos de jubilación y pensión), responsabilidades bancarias, impositivas o fiscales, educación, elecciones y deportes**.[180]

Además de los datos biométricos, el gobierno argentino añadió otras tecnologías de vigilancia a su inventario. Las fuerzas militares nacionales, incluidos el ejército, la fuerza naval y la fuerza aérea, han llevado adelante proyectos para desarrollar sus propios Vehículos Aéreos No Tripulados (VANT), los cuales comenzaron en 1996 y se desarrollaron en más profundidad entre el 2011 y el 2014. La Policía Federal, mientras tanto, recurrió a un importante proveedor de drones comerciales para cubrir sus necesidades: la empresa china **DJI** (Dà-Jiang Innovations Science and Technology Co.). Asimismo, a mediados del 2017, la Ciudad Autónoma de Buenos Aires adquirió un globo de vigilancia, el Skystar 180, producido por la empresa israelí **RT**.[181]

Más recientemente, las autoridades han aumentado su uso de lectores de reconocimiento facial y de matrículas de vehículos en todo el país, como parte de lo que parece ser una carrera entre personajes políticos para implementar tanta tecnología como sea posible en pos de la seguridad pública.

Marco legal

Como observamos más arriba, Argentina cuenta con amplias protecciones para la privacidad. La Constitución Nacional recoge este derecho fundamental en los Artículos 18 y 19, y el país ha ratificado tratados internacionales de derechos humanos[182], como el Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana de Derechos Humanos.

Además, Argentina se jacta de un régimen de protección de datos robusto, aunque desactualizado, mediante el Artículo 43 de la Constitución y la Ley Nacional Nº 25.326 sobre la protección de datos personales. También firmó el Convenio 108+[183] y la Comisión Europea reconoció que Argentina tenía un nivel de protección de datos adecuado en el 2003, mediante la decisión 2003/490 CE.[184]

Lamentablemente, estas leyes han demostrado ser insuficientes para proteger a la ciudadanía de la vigilancia estatal. **Los gobiernos recurren a las excepciones contenidas en las leyes como base legal para el despliegue de programas de vigilancia para el ejercicio normal de las funciones estatales, la mejora de servicios y la seguridad pública.** Hasta el momento, ha habido muy pocas acciones

[180] ADC. “Cuantificando identidades en América Latina”. Mayo del 2017. https://adc.org.ar/informes/cuantificando-identidades-en-america-latina/
[181] RT. “SKYSTAR 180” https://www.rt.co.il/skystar-180
[182] Naciones Unidas. Ratification Status for Argentina. https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?CountryID=7&Lang=EN
[183] Consejo de Europa. Convenio 108 y 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

judiciales y resoluciones judiciales o administrativas en materia de protección de datos o privacidad que protejan a las personas de la recopilación constante y masiva de datos biométricos y el despliegue de tecnologías invasivas de vigilancia.

La deficiencia en las resoluciones judiciales para salvaguardar los derechos de las personas empeoró en octubre del 2020, cuando el Poder Legislativo de la Ciudad Autónoma de Buenos Aires sentó un precedente peligroso al enmendar la Ley N° 5688 para aprobar el uso de reconocimiento facial para identificar a personas fugitivas nombradas en una lista de seguimiento nacional.[185]

Casos locales

La tendencia de aumentar el despliegue de tecnologías ubicuas, que comenzó con las CCTV y SIBIOS, es aún más dominante a escala local y provincial en Argentina. Resulta difícil obtener información actualizada de cada jurisdicción del país, en especial cuando quienes usan estas tecnologías son las agencias de aplicación de la ley, por lo que nos centraremos en los casos más trascendentales y que, como parte de este proyecto, hemos investigado con mayor profundidad.

Identificamos que las cámaras de vigilancia con capacidades y software de reconocimiento facial son la tecnología más usada en todos los niveles gubernamentales de Argentina. En abril del 2019, el gobierno de la Ciudad Autónoma de Buenos Aires anunció la implementación de software de reconocimiento facial para las cámaras de seguridad (CCTV) y los centros de monitoreo de la ciudad. En mayo de ese mismo año, la ciudad de Tigre, provincia de Buenos Aires, creó el Centro de Operaciones de Tigre[186] para usar cámaras y software de reconocimiento facial para buscar a personas desaparecidas e identificar a aquellas con antecedentes penales.

El 15 de octubre del 2019, el gobierno provincial de Córdoba anunció, a través de sus redes sociales, la introducción de un "software de reconocimiento biométrico" desplegado en una camioneta de la policía, con cuatro cámaras montadas y dos cámaras fijas.[187] Debido a la falta de mayor información disponible al público, presentamos dos pedidos de acceso a la información, uno el 7 de noviembre del 2019 y el otro el 11 de noviembre del 2020. El gobierno no respondió ninguno de los pedidos. Esto se suma al largo historial de la provincia de incumplimiento de la ley de acceso a la información pública. Se estima, según los datos provistos por organizaciones de la sociedad civil, como Red Ciudadana Nuestra Córdoba, Fundeps, Foro Ambiental y Córdoba de Todos, que las autoridades responden a apenas el 10 % de los pedidos que reciben cada año.[188]

[185] Télam. "La legislatura aprobó el uso de reconocimiento facial para la detención de prófugos". Octubre del 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 lanzó un nuevo sistema de reconocimiento facial". Mayo del 2019. https://www.ambito.com/municipios/municipios/tigre-lanzo-un-nuevo-sistema-reconocimiento-facial-n5030978

[187] Cuenta de Twitter del Gobierno de Córdoba. Octubre del 2019. https://twitter.com/gobdecordoba/status/1184116108665729025?s=20

[188] La Voz del Interior. "Responder pedidos de información, una cuenta pendiente de la Provincia y el municipio". Noviembre del 2019. https://www.lavoz.com.ar/ciudadanos/responder-pedidos-de-informacion-una-cuenta-pendiente-de-provincia-y-municipio

A mediados del 2017, la provincia de Mendoza empezó a implementar uno de los programas de vigilancia más invasivos de la Argentina. Las agencias de aplicación de la ley de la provincia cuentan con cámaras móviles de reconocimiento facial y con vehículos equipados con la misma tecnología, así como también escáneres de huellas dactilares y lectores de matrículas de vehículos.[189] A pesar de nuestros esfuerzos por obtener información detallada del gobierno, solo nos han dado los nombres de los proveedores a quienes compran los equipos (3M Argentina, INTEMA Comunicaciones S.A., Express Software, y Hardware S.A.), y ninguna especificación sobre el software y el hardware. El Ministerio de Seguridad de la provincia argumentó que esto se debe a que "la información requerida afecta a la seguridad pública".

Siguiendo esta tendencia, el gobierno de la provincia de San Juan anunció el "Acuerdo San Juan", un convenio para implementar más tecnología para la seguridad pública. Este programa incluye el despliegue de cámaras de CCTV y tecnología de reconocimiento facial, además de un "Laboratorio de Análisis Forense de Videos" para el procesamiento del *big data*, con el fin de localizar inmediatamente a personas, vehículos y otros elementos de interés mediante la búsqueda de objetos con atributos particulares.[190]

Lamentablemente, no fuimos capaces de encontrar mucha información acerca del Acuerdo San Juan recurriendo a fuentes disponibles al público. San Juan no cuenta con una ley sobre pedidos de acceso a la información pública, pero, de todas maneras, nos comunicamos con representantes públicos para hacerles preguntas. A agosto del 2021, aún no han respondido a ninguna de nuestras consultas.

Es notable que, durante la pandemia de COVID-19 en el 2020, los gobiernos locales comenzaron a ver la tecnología como una manera de mitigar la propagación del virus. Las autoridades instalaron cámaras térmicas en autobuses y líneas de metro, aeropuertos y estaciones de transporte público. El gobierno nacional lanzó la aplicación "CuidAr"[191], y las provincias usaron aplicaciones móviles para hacer cumplir las cuarentenas obligatorias, controlar multitudes y monitorear síntomas, lo que provocó controversias acerca del propósito y el uso de tales aplicaciones.[192] Como se expuso en el informe y análisis técnico de ADC, las aplicaciones de varias provincias, desplegadas para hacer frente a la emergencia sanitaria, suscitaron graves preocupaciones acerca de la privacidad y la seguridad de la información de las personas.[193]

[189] El Sol. "Reconocimiento facial: hallaron a más de 100 personas con pedido de captura". Mayo del 2019. https://www.elsol.com.ar/reconocimiento-facial-hallaron-a-mas-de-100-personas-con-pedido-de-captura
[190] Sitio web oficial de San Juan. "Acuerdo San Juan: tecnología aplicada a la seguridad". Octubre del 2020. https://sisanjuan.gob.ar/seguridad/2020-10-22/26837-acuerdo-san-juan-tecnologia-aplicada-a-la-seguridad
[191] Consejo de Europa. "Digital Solutions to Fight COVID-19." Octubre del 2020. https://rm.coe.int/report-dp-2020-en/16809fe49c
[192] La Capital. "Controlarán a quienes incumplieron el aislamiento con una app en sus celulares". Marzo del 2020. https://www.lacapital.com.ar/la-ciudad/controlaran-quienes-incumplieron-elaislamiento-una-app-sus-celulares-n2572740.html
[193] ADC. "En caso de emergencia: descargue una app – Parte II". Diciembre del 2020. https://adc.org.ar/2020/12/22/en-caso-de-emergencia-descargue-una-app-parte-ii/

CASO DE ESTUDIO: Brasil

Por Laboratório de Políticas Públicas e Internet (LAPIN)

En Brasil, tanto el sector público como el privado están usando tecnologías de vigilancia por varias razones, que incluyen la seguridad pública, la detección de fraude y la asistencia escolar de estudiantes. Entre las tecnologías de vigilancia disponibles, las autoridades públicas tienen un creciente interés en las tecnologías de reconocimiento facial.

El uso de esta tecnología no es novedad en Brasil. Un informe del 2019 del Instituto Igarapé demuestra que se implementa desde, al menos, el 2011.[194] Desde entonces, ha habido un aumento en los casos de uso, y quienes formulan las leyes han propuesto proyectos de ley para regular la tecnología que han avanzado tanto en las cámaras federales como en las estatales.

Entre los varios usos del reconocimiento facial en el sector público, destacamos el uso que es más prominente en Brasil: el reconocimiento facial para la **seguridad pública**. Las autoridades que despliegan la tecnología por este propósito lo hacen en distintos espacios públicos, incluidos los eventos y festividades públicos. Un factor clave mencionado para justificar su implementación son las preocupantes tasas de violencia y delitos en el país. Por ejemplo,

- ➔ en el 2018, la cantidad de homicidios fue 57 956, una tasa de 27,8 asesinatos cada 100 habitantes;[195]
- ➔ ese mismo año, Brasil tuvo una población presidiaria de más de 720 000 personas;[196] y
- ➔ actualmente, sigue siendo uno de los países con mayor tráfico internacional de drogas.[197]

La tecnología también se utiliza con propósitos como la **detección de fraude en el acceso a servicios públicos, incluidas las asignaciones para el transporte público gratuito y otros beneficios sociales.** En el estado de Alagoas, la tecnología se usa en 102 municipios para verificar la identidad de personas que se benefician de programas sociales, como embarazadas y familias de niños y niñas con desnutrición.[198] La ciudad de São Paulo utiliza un mecanismo similar en el sistema de transporte urbano para verificar la identidad de las personas que cuentan con la tarjeta de uso gratuito. Sin embargo, la tecnología desplegada hace capturas de cada persona que sube al autobús, no solo de quienes tengan la tarjeta, y más de 1,5 millones de personas usan el autobús todos los días en São Paulo.[199] Por último, en la ciudad capital, Brasilia, aproximadamente 2 000 autobuses cuentan con

[194] Instituto Igarapé. “Reconocimiento facial en Brasil” (en portugués). 2019. https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/

[195] Instituto de Pesquisa Econômica Aplicada. “Atlas de violencia” (en portugués). 2020. https://www.ipea.gov.br/atlasviolencia/download/24/atlas-da-violencia-2020

[196] Bueno, S., & Lima, R. S. de. “Anuario brasilero de la seguridad pública del 2019. Foro brasilero de la seguridad pública” (en portugués). 2019. https://www.forumseguranca.org.br/wp-content/uploads/2019/10/Anuario-2019-FINAL_21.10.19.pdf

[197] Oficina de las Naciones Unidas contra la Droga y el Delito. “World Drug Report 2020.” Junio del 2020. https://wdr.unodc.org/wdr2020/field/WDR20_BOOKLET_1.pdf

[198] Renata Bello. “La tecnología de reconocimiento facial aportará más seguridad al Programa de Complementación Alimenticia y Nutricional” (en portugués). Marzo del 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. “La demanda de pasajeros en los autobuses de São Paulo excedió los 1,5 millones de personas por día hábil desde el 7 de julio” (en portugués). Julio del 2020.

cámaras de reconocimiento facial. La empresa que provee la tecnología, **PRODATA**, alega que su solución está completamente desarrollada de manera interna. No obstante, según la información que obtuvimos a través de entrevistas privadas con una persona representante de la empresa, muchos componentes son importados, como tecnología de **Anders** (EE. UU.) y **Compulab** (Israel).

La misma tecnología se está implementando para la **gestión de la asistencia escolar** en algunas instituciones públicas. Con el pretexto de mejorar la gestión de recursos, las instituciones educativas están usando tecnología de reconocimiento facial para habilitar a padres y madres a hacer un seguimiento de los y las estudiantes para monitorear y controlar automáticamente la asistencia y entregar las comidas escolares.[200] El uso del reconocimiento facial en las escuelas está generalizado en todo Brasil, con ejemplos de norte a sur, incluidas escuelas municipales,[201] escuelas privadas de élite,[202] e incluso la universidad brasileña más importante: la Universidad de São Paulo.[203] Aunque la mayoría de los programas piloto de esta tecnología comenzaron entre el 2018 y el 2020, ha habido iniciativas desde antes del 2014.[204]

Para este informe, presentamos 33 pedidos de acceso a la información ante distintas administraciones locales, las cuales incluyeron secretarías estatales de seguridad pública, fuerzas policiales, municipios y servicios de transporte público. A escala federal, les hicimos preguntas a SERPRO, una empresa pública responsable del procesamiento de datos, y a *Receita Federal*, la agencia de servicios de ingresos federales, acerca de los servicios de reconocimiento facial que brindan en el contexto de sus actividades. Obtuvimos respuestas a la mayoría de estos pedidos, pero carecieron de detalles y fueron genéricas.[205] Consecuentemente, en algunas situaciones presentamos apelaciones administrativas.[206]

Tecnología desplegada

Cabe mencionar que no pudimos identificar ningún caso en que las autoridades usaran el sistema de contratación tradicional, de competencia abierta. **Los casos más preocupantes fueron aquellos en los que las autoridades gubernamentales locales desplegaron tecnologías de vigilancia**

https://diariodotransporte.com.br/2020/07/27/demanda-de-passageiros-nos-onibus-de-sao-paulo-tem-ultrapassado-a-15-milhao-de-pessoas-por-dia-util-desde-07-de-julho/

[200] Revista de Segurança Eletrônica. “Las escuelas usan reconocimiento facial para controlar la asistencia y los almuerzos desperdiciados” (en portugués). Abril del 2018. https://revistasegurancaeletronica.com.br/escolas-usam-reconhecimento-facial-para-controlar-frequencia-e-desperdicio-de-merenda/

[201] Diário do Aço. “El Sistema de Reconocimiento Facial ya funciona en escuelas de Ipatinga” (en portugués). Febrero del 2020. https://www.diariodoaco.com.br/noticia/0075842-sistema-de-reconhecimento-facial-ja-funciona-nas-escolas-de-ipatinga

[202] Reconhecimento Facial. “Escuela Maple Bear Porto Alegre empieza a usar 2BFACE” (en portugués). Junio del 2017. http://reconhecimentofacial.com.br/2017/06/07/escola-maple-bear-porto-alegre-passa-utilizar-o-2bface/

[203] Estadão. “Poli-USP prueba la cámara de monitoreo facial” (en portugués). Julio del 2017. https://sao-paulo.estadao.com.br/noticias/geral,poli-usp-testa-novo-sistema-de-seguranca-com-cameras-de-monitoramento-facial,70001900605

[204] Baguete. “Ruá lanza sistema de reconocimiento facial” (en portugués). Diciembre del 2015. https://www.baguete.com.br/noticias/09/12/2015/rua-lanca-sistema-de-reconhecimento-facial

[205] Al momento en que se completó este informe, solo cinco instituciones no respondieron los pedidos de acceso a la información: la Secretaría de Seguridad Pública del estado de Ceará, la Secretaría Pública del estado de Piauí, y los municipios de Anapolis, Pilar y Arapiraca.

[206] Un caso que amerita destacarse es el de SERPRO. Tras presentar todas las apelaciones administrativas posibles, la empresa se rehusó a compartir información importante sobre los proveedores de equipos de reconocimiento facial o el nivel de precisión del sistema, haciendo alusión al secreto comercial. Al momento de publicación de este informe, LAPIN estaba considerando la litigación estratégica para abordar este caso ante el Poder Judicial.

“donadas” para probarlas en la población. Varios ejemplos de estos casos fueron mencionados en la sección que aborda cada empresa.

Desafortunadamente, ante la recepción de pedidos de acceso a la información, las autoridades públicas casi no han brindado información sobre las especificaciones técnicas de estas tecnologías. Los motivos a los que recurren principalmente tienen que ver con la protección de la propiedad intelectual, el secreto comercial y una falta de conocimiento. Las pocas veces en que obtuvimos información acerca de especificaciones técnicas, tal información era muy superficial.

Por ejemplo, cuando preguntamos sobre la precisión del sistema de reconocimiento facial, las Secretarías de Seguridad Pública de Bahía (*Secretarias da Segurança Pública*, o SSPS), respondieron que el sistema alerta a las fuerzas policiales cuando la identificación de un sospechoso llega a una tasa de probabilidad del 90 %. A su vez, el gobierno de Campina Grande nos informó que el sistema tiene una precisión mayor al 85 % y que el zoom de la cámara tiene un alcance de 2 km. Sin embargo, no nos informaron las cifras de falsos negativos ni falsos positivos. Tampoco mencionaron la precisión del sistema ante diferentes condiciones de luz o en personas de diferentes colores de piel.

Nuestras preguntas sobre la eficiencia del sistema en la identificación de delincuentes tampoco obtuvieron respuesta. Informes mediáticos sobre estos casos nos dan motivos para dudar de la eficiencia del sistema. En Bahía, la policía arrestó a más de 200 personas mediante el uso de las tecnologías de reconocimiento facial desde diciembre del 2018 hasta agosto del 2020,[207] pero no está claro cuántos de esos arrestos fueron falsos positivos. Un artículo de noticias informó el caso de un falso positivo, en el que la policía abordó a un muchacho de 25 años con necesidades especiales, confundiéndolo con un hombre buscado por asalto.[208]

En Río de Janeiro, las fuerzas policiales afirmaron que, mediante el uso de tecnología en los alrededores de la zona del Estadio Maracanã, pudieron entregar 63 órdenes de arresto durante la Copa América del 2019. Los medios informaron dos falsos positivos en ese momento. En el primer caso, se confundió a una sospechosa con una delincuente que ya estaba en prisión.[209] El segundo caso fue un hombre al que encarcelaron durante varios días antes de que la policía descubriera que había cometido un error.[210]

Aún más preocupante que la falta de precisión es el hecho de que los sistemas de reconocimiento facial pueden enfocarse desproporcionadamente en personas de color, como lo reveló un estudio del

[207] G1 Bahia. “Hombre arrestado en Salvador tras ser identificado por el sistema de reconocimiento facial” (en portugués). Marzo del 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. “El sistema de reconocimiento facial de Salvador confunde a hombre de necesidades especiales con asaltante” (en portugués). Enero del 2020. https://midia4p.cartacapital.com.br/sistema-de-reconhecimento-facial-de-salvador-confunde-homem-com-necessidades-especiais-com-assaltante/

[209] O Globo Rio. “El reconocimiento facial falló en el segundo día, y una mujer inocente fue confundida con una delincuente que ya había sido arrestada” (en portugués). Julio del 2019. https://oglobo.globo.com/rio/reconhecimento-facial-falha-em-segundo-dia-mulher-inocente-confundida-com-criminosa-ja-presa-23798913

[210] Band News. “Hombre arrestado por equivocación en Copacabana” (en portugués). Julio del 2019. https://bandnewsfmrio.com.br/editorias-detalhes/homem-e-preso-por-engano-em-copacabana

instituto brasileño de investigación Rede de Observatórios de Segurança.[211] Esto suscita la preocupación de que estas tecnologías pueden identificar incorrectamente a personas que ya se enfrentan a la discriminación en Brasil.

Marco legal

Al igual que Argentina, Brasil cuenta con un marco legal para la protección de la privacidad. La Constitución Federal de Brasil recoge este derecho fundamental en el Artículo 5, X y XII, y el país reconoce tratados internacionales de derechos humanos, como el Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana de Derechos Humanos. Además, Brasil cuenta con una legislación única y amplia sobre cuestiones de internet, el *Marco Civil da Internet*, que establece normas específicas para la protección del derecho a la privacidad en el contexto en línea a través de los artículos 3, 8 y 11. Finalmente, el país ha establecido un precedente con la adopción de la Ley Federal de Protección de Datos (*Lei Geral de Proteção de Dados*, o LGPD), que fue aprobada tras años de participación de múltiples partes interesadas y recoge estándares legales modernos para la protección de datos.

También está en alza la legislación en materia de vigilancia estatal. Según el Instituto Igarapé y la asociación Data Privacy Brasil,[212] a junio del 2020, **al menos cuatro leyes estatales abordan, en cierto punto, las tecnologías de reconocimiento facial**; tres de ellas, la Ley N° 16.873/2019, de **Ceará**, la Ley N° 21.737/2015, de **Minas Gerais**, y la Ley N° 8.113/2019, de **Alagoas**, regulan su uso en estadios. Por su parte, la Ley N° 7.123/2015 de **Río de Janeiro** se centra en el despliegue de esta tecnología en el sistema de transporte intermunicipal. Lamentablemente, todas las leyes mencionadas anteriormente brindan pocas o nulas salvaguardas al momento de desplegar la tecnología. Más recientemente, en noviembre del 2020, el **Distrito Federal** aprobó la Ley N° 6.712/2020, que regula el uso de la tecnología para propósitos de seguridad pública en espacios públicos de la capital brasilera.[213] La Ley N° 6.712 sigue algunas buenas prácticas, como establecer la obligatoriedad de llevar adelante una revisión humana cuando el sistema identifique a una persona antes de que se tome una decisión. Sin embargo, la ley tampoco determina medidas ni procedimientos de ciberseguridad para el ejercicio de los derechos del sujeto. Además, permite el uso de la tecnología para investigaciones de delitos penales. A pesar de que la ley ya está vigente, no hay registro de que la tecnología se haya usado aún para propósitos de seguridad pública en el Distrito Federal.

Se han propuesto distintas iniciativas legislativas en los estados durante los últimos dos años. Algunos ejemplos son el proyecto de ley N° 391/2019, de **Minas Gerais**;[214] el proyecto N° 318/2019, de **Río de**

[211] En el estudio, se identificaron 151 casos de uso de tecnología de reconocimiento facial en cuatro estados federales. En 42 de estos casos, había datos sobre identidad racial. De estos 42, 38 de las personas rastreadas eran negras. Para obtener más información, consulte: Rede de Observatórios da Segurança. “Retratos de violencia” (en portugués). 2019. https://www.ucamcesec.com.br/wp-content/uploads/2019/11/Rede-de-Observatorios_primeiro-relatorio_20_11_19.pdf

[212] Instituto de Investigación de Privacidad de datos Igarapé. “Regulación de reconocimiento facial en el sector público: evaluación de experiencias internacionales” (en portugués). Junio del 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] Boletín Oficial. Ley N° 6.712. Noviembre del 2020. https://www.tjdft.jus.br/institucional/relacoes-institucionais/arquivos/lei-no-6-712-de-10-de-novembro-de-2020.pdf

[214] Asamblea Legislativa de Minas Gerais. Proyecto N° 391/2019. 2019. https://www.almg.gov.br/atividade_parlamentar/tramitacao_projetos/interna.html?a=2019&n=391&t=PL

Janeiro;[215] el proyecto N° 148/2019, de **Paraná**;[216] y el proyecto N° 865/2019, de **São Paulo**.[217] Otro proyecto que vale la pena mencionar es el N° 42/2020, de **Ceará**.[218] Aunque no se centra en el reconocimiento facial, la ley permite a la policía recopilar datos de cámaras privadas en zonas públicas, ampliando la visión entrometida del estado. Finalmente, también existen propuestas a **escala federal**, como el proyecto N° 4.612/2019 y el N° 4.858/2020. Si bien no hay predicciones sobre que estas propuestas se incluyan en la agenda del Congreso Nacional, la cantidad de proyectos en relación con el despliegue de las tecnologías de vigilancia en los últimos años revela el creciente interés en el tema.

En diciembre del 2019, el Ministerio de Justicia y Seguridad Pública de Brasil publicó la Ordenanza N° 793/2019.[219] Entre otras disposiciones, promueve la implementación de "sistemas de monitoreo por video con soluciones de reconocimiento facial, reconocimiento óptico de caracteres, el uso de inteligencia artificial u otros".

Aunque la **ley de protección de datos personales de Brasil, *Lei Geral de Proteção de Dados*, o LGPD, ha entrado en vigencia hace poco, no se aplica a contextos de seguridad pública.** Este hecho socava la efectividad de la LGPD en el abordaje del uso de la tecnología de reconocimiento facial en varios casos actuales de Brasil.[220] Un equipo de especialistas propuso recientemente un borrador para un proyecto de ley de una "LGPD Penal" que aborde principios de protección de datos personales y obligaciones para el procesamiento de datos personales impuestas a las autoridades de aplicación de la ley,[221] pero no sabemos si se promulgará ni cuándo.

Casos locales

Destacaremos dos regiones en las que las tecnologías de reconocimiento facial se promocionan fuertemente para la seguridad pública: la **noreste** (NE) y la **sudeste** (SE), dos de las más pobladas del país.[222] Este hecho en sí mismo llama la atención, ya que muestra que **zonas densamente pobladas pueden convertirse en laboratorios perfectos para el testeo de tecnologías de reconocimiento facial**. Muchos de los casos se implementaron por el estado o por Secretarías de Seguridad Pública a

[215] Asamblea Legislativa de Río de Janeiro. Proyecto N° 218/2019. 2019. http://alerjln1.alerj.rj.gov.br/scpro1923.nsf/0c5bf5cde95601f903256caa0023131b/d9e71e222a9c8e1c832583d0006d6f05?OpenDocument&Highlight=0,318%2F2019

[216] Asamblea Legislativa de Paraná. Proyecto N° 148/2019. 2019. http://portal.assembleia.pr.leg.br/modules/mod_legislativo_arquivo/mod_legislativo_arquivo.php?leiCod=82332&tipo=I

[217] Asamblea Legislativa de São Paulo. Proyecto de Ley N° 865/2019, 2019. https://www.al.sp.gov.br/propositura/?id=1000278098

[218] Asamblea Legislativa de Ceará. Proyecto de Ley N° 42/2019, 2019. https://www2.al.ce.gov.br/legislativo/tramit2020/8531.htm

[219] Diario Oficial de la Unión. Ordenanza N° 793. Octubre del 2019. https://www.in.gov.br/en/web/dou/-/portaria-n-793-de-24-de-outubro-de-2019-223853575

[220] Aunque no se aplica en el contexto de la seguridad pública, en el Artículo 4, Párrafo 1, la LGPD señala que la legislación futura que aborde el tema contemplará medidas proporcionales y estrictamente necesarias para el interés público, y deberá cumplir los debidos procesos jurídicos, así como también los principios de la LGPD sobre la protección de datos personales y los derechos de los dueños de los datos.

[221] Cámara de Diputados. Proyecto de Ley de LGPD Penal. 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] Según el Instituto Brasileño de Geografía y Estadística, IBGE, la estimación poblacional de estas dos regiones en el 2020 asciende a más de 146 millones de personas, que representan el 69 % de la población del país. Para obtener más información, consulte: https://ftp.ibge.gov.br/Estimativas_de_Populacao/Estimativas_2020/POP2020_20201030.pdf

nivel ciudad. Sin embargo, las fuerzas policiales (civiles y militares) también implementaron la tecnología directamente.

Comenzando por la **región noreste**, se deben tener en cuenta tres estados. En el estado de **Bahía**, las tecnologías de reconocimiento facial se usan estratégica y ampliamente en espacios públicos, como aeropuertos, subterráneos, estadios, calles y plazas. La tecnología también se ha desplegado en eventos públicos significativos, como los carnavales del 2020. En Salvador, las cámaras capturaron 4,3 millones de registros faciales y la policía detuvo a 42 personas.[223] En Feira de Santana, se capturaron los rostros de 1,3 millones de personas y se detuvo a 33 de ellas.[224]

El estado de **Ceará** toma un enfoque distinto y no integra la tecnología en cámaras ubicadas en las calles, sino en los teléfonos inteligentes de las fuerzas policiales que capturan rostros cuando las autoridades se acercan a personas sospechosas. Cuando la policía toma una fotografía, puede compararla con imágenes faciales que se encuentran en la base de datos de las Secretarías de Seguridad Pública.[225]

El tercer ejemplo en el NE es el estado de **Paraíba**. Según las Secretarías de Seguridad Pública de Paraíba, la tecnología aún está en fase de implementación inicial, con un contrato que se firmó en el 2020. Por lo tanto, aún no está claro dónde se instalará la tecnología de reconocimiento facial. Sin embargo, la municipalidad de Campina Grande usó la tecnología durante las festividades tradicionales de São João, a las que asistieron 1,8 millones de personas, provenientes de varias regiones del país.[226]

En la **región sudeste**, destacamos a sus dos capitales estatales más grandes y también a dos grandes ciudades de la región.

En **Río de Janeiro**, la policía probó la tecnología en dos eventos públicos. En el carnaval del 2019, colocaron cámaras a lo largo de la región de Copacabana, donde se estima que hubo presentes 1,6 millones de personas.[227] Además, durante la Copa América del 2019, un evento futbolístico que tuvo lugar entre el 6 de julio y el 19 de octubre, se colocaron cámaras de reconocimiento facial en los

[223] Bahía. “El sistema de reconocimiento facial ha registrado más de 4,3 millones de imágenes” (en portugués). Febrero del 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 arrestos mediante reconocimiento facial durante el micareta” (en portugués). Abril del 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. “El Departamento de Seguridad analiza sociedad con empresa de tecnología china para implementar nuevas soluciones” (en portugués). Agosto del 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. “El balance general del Mejor São João del mundo del 2019 cuenta con mejores resultados en las últimas ediciones” (en portugués). Julio del 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. “El Carnaval atrae a 1,6 millones de turistas y recauda ingresos de BRL 3 500 millones para Río” (en portugués). Marzo del 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

alrededores del Estadio Maracanã. En entrevistas con autoridades públicas, se reveló que se planifica instalar permanentemente estas cámaras en espacios públicos.

En la ciudad de **São Paulo**, también se utilizaron tecnologías de reconocimiento facial durante el carnaval del 2020, empleando cámaras en vivo instaladas en zonas en las que se llevaba a cabo el evento.[228] Además, existe un proyecto actual de la policía civil para usar esta tecnología para el registro de identificación personal en tiempo real.[229] Al mismo tiempo, las autoridades llevarán a cabo investigaciones penales utilizando capturas de pantalla obtenidas de distintas cámaras instaladas tanto en espacios públicos como privados. También implementarán tecnología de reconocimiento facial en las estaciones de metro, donde cerca de 3,5 millones de personas usan el sistema de transporte a diario.

Otra ciudad del estado de São Paulo, **Campinas**, es conocida por su "laboratorio abierto" sobre el uso de distintas tecnologías de "ciudades inteligentes", que incluyen la tecnología de reconocimiento facial. Allí, ya se instalaron 30 cámaras en distintas estaciones de transporte público y cercanías.[230] Para este tipo de iniciativa, Campinas recibió reconocimiento como la ciudad "más inteligente" de Brasil del 2019.[231]

Finalmente, destacamos el caso de **Mogi das Cruzes,** otra ciudad del estado de São Paulo, conocida por implementar tecnología de reconocimiento facial con propósitos de seguridad. Había seis cámaras en vivo operativas durante la "*Festa do Divino Espírito Santo*".[232] La policía creó una base de datos de personas a las que están buscando, como delincuentes y niños(as) desaparecidos(as), usando imágenes extraídas de fotos de perfil de redes sociales.[233] El sistema opera como parte de una sociedad entre el municipio y **Dahua Technology**. La tecnología fue provista a las autoridades de manera gratuita, según la ciudad, y puede ser usada en otros espacios públicos, dado que su central se instaló en vehículos.[234]

---

[228] Tilt. Helton Simões Gomes. "Por primera vez, SP cuenta con monitoreo en tiempo real en el Carnaval; entienda" (en portugués). Febrero del 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. "¿Gran Hermano urbano? Cómo será el reconocimiento facial de la policía de SP" (en portugués). Noviembre del 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. "Las cámaras de espionaje inician su fase de testeo" (en portugués). Diciembre del 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 es la ciudad más inteligente y más conectada de Brasil" (en portugués). Septiembre del 2019. http://www.campinas.sp.gov.br/noticias-integra.php?id=37205

[232] "*Festa do Divino Espírito Santo*" es un festival religioso en Mogi das Cruzes que se celebra anualmente, en el que las personas se reúnen en espacios públicos para ver procesiones y conciertos, entre otras cosas. El año pasado, recibió a aproximadamente 200 000 personas durante los siete días del evento. Para obtener más información, consulte: http://www.festadodivino.org.br/

[233] Diário TV 1ª Edição. "Sistema de reconocimiento facial refuerza la seguridad en la Festa do Divino en Mogi das Cruzes" (en portugués). Junio del 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] Municipalidad de Mogi das Cruzes. "La seguridad para la Festa do Divino contará con cámaras de reconocimiento facial" (en portugués). Mayo del 2019. https://www.mogidascruzes.sp.gov.br/noticia/seguranca-para-a-festa-do-divino-tera-cameras-com-reconhecimento-facial

CASO DE ESTUDIO: Ecuador

Por LaLibre.net

El uso de sistemas de vigilancia por video en espacios públicos en Ecuador data del 2002, año en el que los alcaldes de Quito y Guayaquil, las dos ciudades más pobladas del país, lanzaron los primeros programas piloto del "Sistema Ojos de Águila". Inicialmente, este proyecto se llevó adelante entre los dos municipios y fue promocionado como una herramienta para reducir el crimen[235] y mejorar la percepción de la seguridad por parte de la población. En ese momento, las autoridades instalaron ocho[236] cámaras de videovigilancia de la marca **PELCO** en Quito y 20[237] en Guayaquil, en las zonas centrales de cada ciudad.

Rápidamente, otras municipalidades siguieron el ejemplo de estas dos grandes ciudades, a pesar del hecho de que **no existen estudios concluyentes para demostrar la efectividad de este tipo de vigilancia en la seguridad ciudadana, la reducción del crimen o la prevención de muertes violentas**.[238] Sin embargo, los medios locales y nacionales utilizaron imágenes extraídas de las cámaras para demostrar lo que ellos consideran como "logros" de la seguridad pública.

Entre el 2010 y el 2014, el gobierno de Rafael Correa estableció nuevas políticas para "reducir el crimen y crear una coexistencia social pacífica". Esto consistía en crear un modelo descentralizado para la Policía Nacional, con un nuevo modelo de zonas y administración. Estas políticas fueron diseñadas e implementadas principalmente por el Ministerio de Justicia, el Ministerio de Coordinación de Seguridad, y el Ministerio del Interior, bajo la dirección de su ministro: José Serrano. Existen investigaciones que sugieren que los cambios pueden haber dado una apariencia de reducción del crimen, pero que no han tenido un impacto significativo. Según los investigadores Castro, Jácome, y Mancero (2015), las autoridades sí tenían la intención de mejorar los indicadores de delincuencia, y también demostraron tasas menores en el 2014, año en el que bajó el precio del petróleo y se ralentizó el crecimiento económico.[239] Sin embargo, la reducción de la delincuencia puede no haber sido resultado del uso de equipos de reconocimiento facial, sino el reflejo de categorizar el crimen de manera distinta, como parte de modificaciones en virtud del nuevo Código Orgánico Integral Penal y meticuloso trabajo estadístico.[240] En el 2010, las nuevas autoridades administrativas crearon un servicio nacional llamado **"Servicio Integrado de Seguridad ECU911"**.

El servicio ECU911 está administrado por un organismo público, dependiente del presidente, que dirige todas las llamadas de emergencia (policía, departamento de bomberos, ambulancias, etc.) a un único

[235] Castro, D., Jácome, J.C., Mancero, J. "Seguridad ciudadana en Ecuador: Policía ministerial y evaluación de impactos, años 2010-2014". Nova Criminis 9. Pp.111-148. 2015
[236] El Universo. "Ocho cámaras para plan Ojos de Águila". Abril del 2002. https://www.eluniverso.com/2002/04/22/0001/10/2388C8238A14459AB2ADE998D58D7FFB.html
[237] El Universo. "Polémica por el uso y dirección del sistema de 'Ojos de Águila'". Diciembre del 2007. https://www.eluniverso.com/2007/12/16/0001/10/B3296480B7784A66AA773C39D74E9B3A.html
[238] Ethnodata. "Una exploración de la relación entre el incremento de infraestructura en seguridad y la tasa de muertes violentas en el Ecuador". 2020. https://www.ethnodata.org/es-es/muertes-violentas/upc/
[239] El Universo. "$77.530 millones recibió Ecuador en 7 años por exportación petrolera". Enero del 2015. https://www.eluniverso.com/noticias/2015/01/05/nota/4399061/77530-millones-recibio-pais-7-anos-exportacion-petrolera
[240] Ethnodata. "Una exploración de la relación entre el incremento de infraestructura en seguridad y la tasa de muertes violentas en el Ecuador". 2020. https://www.ethnodata.org/es-es/muertes-violentas/upc/

número, el 911, lo que implica el despliegue de distintos centros de videovigilancia y monitoreo a nivel nacional, que están interconectados entre sí y recopilan información de distintos territorios. La implementación de este "Servicio Integrado" no ha estado exenta de críticas. En el 2019, el expresidente de Ecuador Lenín Moreno reveló que se había utilizado para espionaje. Expresó que el trabajo de la institución "se diversificó a otra tarea perversa: espiar rivales políticos y a ciudadanía que ellos (el gobierno) intentaban coaccionar".[241] También existieron informes sobre corrupción en el proceso de despliegue e implementación.[242] A pesar de ello, el Servicio Integrado se ha seguido desarrollando y expandiendo sin dificultades.

En el 2012, la Secretaría Nacional de Planificación y Desarrollo estableció una nueva división para unidades de planificación administrativa: nacionales, zonales, distritales y de circuito. Representan una unidad de vigilancia bajo "subcircuitos" para el monitoreo y control. Antes de esto, los mecanismos de control nunca habían estado tan centralizados. Durante los siguientes siete años, las autoridades dieron prioridad a la mejora de los equipos de la Policía Nacional y, con el nuevo orden de unidades, tuvo mejor representación en el territorio. En el 2017, al finalizar el mandato de Rafael Correa, el gobierno invirtió USD 781 millones en infraestructura y equipos para la Policía Nacional.[243]

Al momento en que se finalizó esta investigación, el anterior gobierno ecuatoriano es uno de los menos populares de América Latina,[244] quizás debido a la agresividad de la policía y las fuerzas de seguridad y los pésimos antecedentes en materia de violaciones de derechos humanos.[245] El Ministerio de Gobierno (Interior y Policía) estaba bajo el cargo del Comandante General de la Policía, el Ministerio de Defensa estaba en manos de un General Mayor de la División Militar, y el director del Servicio Integrado de Seguridad ECU911 es un teniente coronel de la Policía General. Todos ellos fueron designados directamente por el Poder Ejecutivo, sin competencia ni oposición.

Con el objetivo de obtener información para elaborar este documento, presentamos varios pedidos formales en base al derecho al acceso a la información pública establecido en la Ley Orgánica de Transparencia y Acceso a la Información Pública, Artículos 1 y 18 (números 1 y 2) y el Artículo 66 de la Constitución de la República del Ecuador. Presentamos los pedidos ante varias instituciones, pero obtuvimos muy pocas respuestas.

Cuando consultamos sobre la tecnología de videovigilancia que las autoridades han implementado, el uso de las tecnologías de reconocimiento facial y el marco legal que respaldaba la implementación, la Asamblea Nacional respondió solo algunas de nuestras preguntas. Se nos informó que el debate sobre el actual proyecto de ley de protección de datos personales aún estaba en curso y que no había marco

[241] El Comercio. "Lenín Moreno dice que el ECU911 se usó de manera 'perversa' para espionaje". Abril del 2019. https://www.elcomercio.com/actualidad/lenin-moreno-ecu-911-espionaje.html

[242] Vistazo. "ECU-911: Contratos que dan pánico". Mayo del 2019. https://www.vistazo.com/seccion/pais/ecu-911-contratos-que-dan-panico

[243] Aviso oficial presidencial. "781 millones de dólares es la inversión del gobierno en infraestructura y equipamiento para la policía". Consultado en enero del 2020. https://www.presidencia.gob.ec/781-millones-de-dolares-es-la-inversion-del-gobierno-en-infraestructura-y-equipamiento-para-la-policia/

[244] Mitofsky. "Aprobación de mandatarios América y el mundo". Marzo del 2021. http://www.consulta.mx/index.php/encuestas-e-investigaciones/el-mundo/item/download/1209_7300384f47710f38dd84cec8765dd463

[245] OEA. "CIDH presenta observaciones de su visita a Ecuador". Enero del 2020. https://www.oas.org/es/cidh/prensa/comunicados/2020/008.asp

legal para el uso de tecnologías de videovigilancia y de reconocimiento biométrico.[246] En algunos casos, las autoridades solicitaron más tiempo para brindar información adicional que complementara la respuesta inicial.

También enviamos una solicitud al ECU911 con la esperanza de obtener información sobre el procesamiento de los datos de las personas, quién puede acceder a ellos, la existencia de protocolos de seguridad, la realización de evaluaciones de impacto en los derechos humanos, y los nombres de los productos y servicios desplegados, entre otras consultas. Lamentablemente, la institución se excusó de brindar información, alegando que se trataba de un secreto de Estado. **ECU911 sí expresó que no contaban con cámaras con capacidades de reconocimiento facial, pero múltiples anuncios oficiales indican lo contrario.**[247]

Al momento de la finalización de este informe en agosto del 2021, no hemos recibido respuestas de varias otras instituciones relevantes, incluidos el Ministerio de Gobierno, el Ministerio de Telecomunicaciones y Sociedad de la Información, y la Dirección Nacional de Registro de Datos Públicos (DINARDAP).

Tecnología desplegada

En abril del 2019, el *New York Times* publicó una investigación sobre el uso de la tecnología de videovigilancia desarrollada por empresas chinas.[248] Reveló la operación de 4 300 cámaras usadas para tareas de inteligencia sin regulación. En este informe, tuvimos en cuenta la infraestructura de videovigilancia controlada directamente por el ECU911, pero existen cientos de dispositivos de videovigilancia que funcionan de manera autónoma en los municipios de Quito y Guayaquil. En el 2020, estas ciudades se conectaron al Servicio Integrado de Seguridad ECU911 para aumentar sus capacidades.

Para obtener la cantidad real de "Ojos de Águila" instalados en el país, le solicitamos al director del Servicio Integrado de Seguridad ECU911, Juan Zapata, que nos brindara información sobre este aspecto. Si bien se rehusó a responder, sus declaraciones anteriores indican que, en octubre del 2019 (antes de la integración con los sistemas municipales de Quito y Guayaquil), el Servicio tenía 4 638 dispositivos activos de videovigilancia.[249] En enero del 2020, se integraron 890[250] cámaras en el

[246] Respuesta de la Asamblea Nacional. Diciembre del 2020. https://nube.cyberzen.ec/s/qjto9dZwmmW9GRT
[247] Servicio Integrado de Seguridad ECU911. "ECU911 presentó informe relacionado con mecanismos y herramientas de cooperación internacional". Octubre del 2019. https://www.ecu911.gob.ec/ecu-911-presento-informe-relacionado-con-mecanismos-y-herramientas-de-cooperacion-internacional/
[248] New York Times. "Hecho en China y exportado a Ecuador: el aparato de vigilancia estatal". Abril del 2020. https://www.nytimes.com/es/2019/04/24/espanol/america-latina/ecuador-vigilancia-seguridad-china.html
[249] Servicio Integrado de Seguridad ECU911. "En Smart City 2019, se anunció el plan de modernización del sistema de videovigilancia del ECU911". Octubre del 2019. https://www.ecu911.gob.ec/en-smart-city-2019-se-anuncio-el-plan-de-modernizacion-del-sistema-de-videovigilancia-del-ecu-911/
[250] Servicio Integrado de Seguridad ECU911. "1.518 cámaras del ECU911 y del municipio interconectadas para la seguridad de Quito". Enero del 2020. https://www.ecu911.gob.ec/1-518-camaras-del-ecu-911-y-del-municipio-interconectadas-para-la-seguridad-de-quito/

municipio de Quito y, en septiembre, 1 100 cámaras en el municipio de Guayaquil. En base a esta información, **hay más de 6 600[251] cámaras bajo el control del ECU911.**

La pandemia de COVID-19 provocó un mayor control y vigilancia, lo cual gran parte del público acepta y considera positivo. Si bien tal vigilancia se considera justificada debido al miedo que causa la crisis sanitaria y humanitaria, estas herramientas no se han utilizado solamente para medir la distancia social o brindar seguridad a la ciudadanía. Según el presidente Lenín Moreno, estos instrumentos también se utilizan para el espionaje y el acoso político, lo que establece la posibilidad de recurrencia.[252]

Cabe mencionar que, en julio del 2020, el **Banco Interamericano de Desarrollo** contribuyó al desarrollo de un software del gobierno ecuatoriano llamado **Distancia2** para el uso de cámaras de videovigilancia ya desplegadas en las calles. El software, ampliamente promocionado por las autoridades y los medios, usa inteligencia artificial para medir la distancia física entre las personas, alertando a las agencias de monitoreo cuando las normas de distanciamiento por COVID-19 no se están cumpliendo.[253]

Las tecnologías de vigilancia implementadas en Ecuador son provistas principalmente por las siguientes empresas: **Axis** (Suecia), **Hikvision** (China), y **VERINT** (Israel y EE. UU.). Sin embargo, hay un despliegue a pequeña escala utilizando productos de **Intelligent Security Systems** (Rusia), **Pelco Corporations** (EE. UU.), y **Tiandy** y **ZKTeco** (China). La mayoría interopera por medio de protocolos y estándares desarrollados por **OVNIF**,[254] una organización dedicada al desarrollo de estándares para la interoperabilidad de dispositivos de seguridad.

Marco legal

Ecuador cuenta con algunas disposiciones en la ley en materia de privacidad a nivel constitucional e internacional. La Constitución de Ecuador recoge el derecho fundamental a la privacidad en el Artículo 66, y el país reconoce tratados internacionales de derechos humanos, como el Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana de Derechos Humanos. **Sin embargo, a diferencia de Brasil y Argentina, Ecuador careció de una regulación específica sobre la protección de datos personales y la privacidad hasta 2021.** Tras la filtración de los datos personales de 20 millones de personas ecuatorianas en el 2019,[255] el presidente y varias instituciones se comprometieron a desarrollar una ley de protección de datos personales a corto plazo para responder a preocupaciones públicas.[256] En mayo del 2021, la Asamblea Nacional aprobó una ley de protección de datos personales

[251] Servicio Integrado de Seguridad ECU911. "Cámaras del ECU911 registran indisciplina e incumplimiento ciudadanos en varias urbes del país". Mayo del 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 dice que el ECU 911 se usó de manera 'perversa' para espionaje". Abril del 2019. https://www.elcomercio.com/actualidad/lenin-moreno-ecu-911-espionaje.html

[253] El Comercio. "Cámaras de seguridad vigilarán el distanciamiento físico en el Ecuador". Junio del 2020. https://www.elcomercio.com/actualidad/camaras-vigilaran-distanciamiento-fisico-covid19.html

[254] Para obtener más información, consulte: https://www.onvif.org/

[255] BBC News. "Filtración de datos en Ecuador: la 'grave falla informática' que expuso la información personal de casi toda la población del país sudamericano". Septiembre del 2019. https://www.bbc.com/mundo/noticias-america-latina-49721456

[256] El Universo. "El proyecto de Ley de Protección de Datos Personales en Ecuador". Agosto del 2020. https://www.eluniverso.com/larevista/2020/08/24/nota/7953820/datos-personales-ley-ecuador

moderna.[257] Aún falta determinar si la ley será suficiente para proteger a la ciudadanía contra tecnologías de vigilancia intrusivas, ya que no hay planes de formular una regulación específica para el asunto.

Casos locales

En el 2019, los alcaldes de Quito y Guayaquil emprendieron proyectos paralelos con la meta similar de adquirir cámaras y licencias de análisis de videos para el reconocimiento facial basado en inteligencia artificial.

En enero del 2020, las autoridades firmaron un acuerdo interinstitucional para la integración de infraestructura de vigilancia para los centros de monitoreo de Quito con aquellos del ECU911, aumentando la capacidad de vigilancia total a 1 518[258] dispositivos de videovigilancia para la ciudad. Ambas instituciones ahora pueden acceder a las 628 cámaras del Servicio Integrado ECU911 y las 890 del municipio de Quito, así como también a cualquier cámara nueva.

Más adentrado el año 2020, los dispositivos de videovigilancia de Guayaquil se integraron con el ECU911, tal como lo habían hecho el sistema de Quito y el de otras regiones durante meses anteriores. El gobierno creó un nuevo centro operativo del ECU911 en la ciudad por un monto de aproximadamente USD 13 millones, que incluyó USD 1 millón por la adquisición de software para el análisis de videos y varias cámaras para la integración al sistema nacional de videovigilancia. Existen, en consecuencia, más de 2 000 dispositivos que monitorean la ciudad.

En base a los comunicados de prensa y las contrataciones públicas, concluimos que el sistema de vigilancia integrado se usa mayoritariamente en Guayaquil y Quito, pero la tecnología está instalada en todo el país en pequeños municipios, como Shushufindi[259] [260] y Quevedo.[261]

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

[258] Servicio Integrado de Seguridad ECU911. "1.518 cámaras del ECU911 y del municipio interconectadas para la seguridad de Quito". Enero del 2020.
https://www.ecu911.gob.ec/1-518-camaras-del-ecu-911-y-del-municipio-interconectadas-para-la-seguridad-de-quito/

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

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

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

IV. CONCLUSIÓN Y RECOMENDACIONES

Las tecnologías analizadas en este informe representan una creciente amenaza para nuestros derechos humanos: les dan a las autoridades la capacidad de identificar, seguir, individualizar y rastrear a personas adonde sea que vayan, socavando los derechos a la privacidad y a la protección de los datos personales, el derecho a la libertad de reunión pacífica y de asociación (lo que resulta en la penalización de protestas y un efecto inhibidor inducido) y los derechos a la igualdad y no discriminación. Grupos de la sociedad civil en todo el mundo han dado la voz de alarma sobre el uso de tecnologías de reconocimiento facial y otras tecnologías de vigilancia biométrica, y existen movimientos y campañas para prohibir aplicaciones de estas tecnologías en la Unión Europea,[262] los Estados Unidos,[263] la India,[264] Rusia,[265] y muchos otros lugares.

El objetivo del presente informe no es únicamente demostrar que estas tecnologías amenazan nuestros derechos, sino también exponer la falta de transparencia y rendición de cuentas de las empresas que hacen acuerdos con gobiernos para la implementación. En algunos casos, las empresas proporcionan esta tecnología peligrosa de manera gratuita para probarla en la población, pasando por alto el impacto en los derechos fundamentales de las personas. Si bien esperamos que este informe motive a organizaciones de derechos, periodistas y activistas a seguir haciendo preguntas e investigando a las empresas y los gobiernos, la carga de prevenir daños no debería recaer solamente en la sociedad civil. Los gobiernos tienen la responsabilidad de proteger los derechos fundamentales de sus ciudadanos y ciudadanas, y las empresas deben respetar tales derechos. Necesitamos que **quienes formulen las leyes** tomen **acciones concretas para detener la propagación de esta tecnología**, **prohibiendo tecnología que permita la vigilancia masiva** y estableciendo salvaguardas para proteger a las personas, como recursos para quienes hayan sufrido una violación a su privacidad, y medidas robustas para **aumentar la rendición de cuentas y la transparencia**, **tanto de las empresas que desarrollan la tecnología como de las autoridades que la despliegan**. Permitir amplias excepciones para el uso de la tecnología en pos de la "seguridad pública" da paso a abusar de estos sistemas. La seguridad pública tampoco es excusa legítima para mantener en la oscuridad a la ciudadanía, periodistas y otras personas de la sociedad civil.

Al usar cualquier tipo de tecnología, e incluso más en casos en que los derechos fundamentales están en riesgo, los **gobiernos** deberían llevar a cabo evaluaciones de impacto de derechos humanos antes de tomar una decisión o desplegar un sistema, y negarse a adquirir o usar tecnología de empresas con malos antecedentes de derechos humanos. Las agencias públicas deberían mejorar su transparencia comunicando y compartiendo los documentos relacionados con las reuniones y los acuerdos de adquisición de tecnología de vigilancia, y consultar con la sociedad civil sobre potenciales impactos dañinos.

[262] Para obtener más información, visite https://reclaimyourface.eu/
[263] Para obtener más información, visite https://banthescan.amnesty.org/
[264] Internet Freedom Foundation. "FF proposes a three year moratorium on the use of Facial Recognition Technology in India #ProjectPanoptic." Marzo del 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 obtener más información, visite https://bancam.ru/en

A su vez, las **empresas** deben comprometerse a cumplir los estándares de transparencia, rendición de cuentas y observancia de los derechos humanos. Para lograrlo, deben mejorar su comunicación cuando se les solicita información sobre productos y servicios con consecuencias para los derechos humanos, implementar procedimientos sólidos de debida diligencia en materia de derechos humanos, elaborar informes de transparencia, buscar información de manera proactiva y continua para entender y concientizarse sobre el impacto de sus tecnologías en los derechos humanos, y brindar reparaciones adecuadas a víctimas de los abusos que ellas facilitan.[266]

Los **medios públicos y tradicionales** cumplen un papel fundamental de sensibilización y creación de debate. Deben cambiar la narrativa sobre la tecnología de vigilancia: de soluciones mágicas a herramientas que exigen un extenso debate público y un compromiso con el cumplimiento de los principios y las leyes de derechos humanos.

[266] Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. “Principios Rectores sobre las Empresas y los Derechos Humanos”. Junio del 2011.
https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_sp.pdf