Tecnologías de Vigilancia en Argentina

APC
por los Derechos Civiles

Diciembre 2021

Equipo
Redacción: Alejo Kiguel, Eduardo Ferreyra, Leandro Ucciferri
Diseño y diagramación de informes: El Maizal
Con el apoyo de Privacy International

Contenido

Resumen Ejecutivo

Durante 2020 y 2021, la Asociación por los Derechos Civiles (ADC) formó parte de una investigación regional coordinada por la organización Access Now sobre la adquisición y utilización de tecnologías de vigilancia en América Latina. La ADC fue la encargada de investigar la situación en Argentina y el producto de dicha colaboración fue publicado en el informe "Tecnología de Vigilancia en América Latina: Hecha en el exterior, utilizada en casa."[1], el cual incluye además investigaciones de Brasil y Ecuador.

Este reporte reproduce los hallazgos encontrados en dicha colaboración y constituye una actualización del estado de situación a través de la inclusión de nuevas iniciativas relevadas, como el caso del sistema de reconocimiento facial de la provincia de Salta. Además introduce recomendaciones para una futura regulación de los acuerdos entre sectores públicos y privados que se encuentre alineada con los principios internacionales sobre empresas y derechos humanos.

A partir del mismo descubrimos que el despliegue de tecnologías de vigilancia continúa creciendo en Argentina. La utilización de nuestros datos biométricos como mecanismo de identificación -que comenzó a ser aplicada con fines de seguridad pública- ya se está efectuando para verificar identidades en programas de seguridad social, responsabilidades impositivas o fiscales, educación, elecciones y deportes. Por su parte, cada vez son más las autoridades gubernamentales -tanto a nivel nacional, provincial y local- que despliegan cámaras de videovigilancia en espacios públicos con sistemas de reconocimiento facial que permiten identificar a las personas por los rasgos de su rostro, generando así importantes riesgos para los derechos de las personas.

Los Estados suelen recurrir al sector privado para adquirir estas tecnologías. La dependencia de los gobiernos en las empresas, al delegar el desarrollo, así como los riesgos intrínsecos que tienen las tecnologías analizadas, genera nuevos desafíos respecto a quién debe responder cuando estas tecnologías vulneran derechos de las personas, y cómo deben ser los procesos de contratación en estas iniciativas.

Para evitar que estas tecnologías sigan propagándose en nuestro país, es clave estar informados sobre sus alcances. Para ello, es necesario en primer lugar conocer en detalle cómo funcionan estas alianzas público-privadas y, al mismo tiempo, establecer mecanismos adecuados para que tanto Estados como empresas se comprometan a respetar y proteger los derechos humanos, a la vez que existan mecanismos de reparación eficientes cuando se vulneren derechos.

Introducción

El despliegue de tecnología de vigilancia se extiende en Argentina. Cada vez más lugares implementan estos sistemas sin haber realizado evaluaciones de impacto en derechos humanos. A su vez, otras localidades anuncian que adoptarán estas herramientas en el corto o mediano plazo. Desafortunadamente, las autoridades públicas recurren cada vez más a herramientas cuyos costos superan de forma amplia a sus presuntos beneficios. Para evitar que sigan propagándose estas tecnologías en nuestro país, es necesario estar informados sobre sus alcances. Sin embargo, es allí en donde empiezan los problemas.

Descubrir cómo los distintos niveles de gobierno utilizan los mecanismos y sistemas de vigilancia no es una tarea sencilla. Además de tratarse de una industria tradicionalmente opaca, la información no suele publicarse a través de canales públicos a menos que los medios informen sobre el tema o que se lleve a cabo una investigación independiente. Aún así, en los casos donde tomamos conocimiento sobre su utilización, las autoridades continúan siendo muy reticentes a brindar detalles de las contrataciones.

En Argentina, la introducción de SIBIOS en el 2011 marcó un momento particularmente decisivo. Mediante el Decreto 1766/11[2], 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 de la Nación.

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 de la Nación 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 y ciudadanas como de todas las personas que ingresan al país[3].

SIBIOS es un sistema nacional, así que todas las provincias del país firmaron acuerdos de cooperación con el Ministerio de Seguridad de la Nación (incluidas sus cuatro fuerzas federales de seguridad) y el Ministerio del Interior de la Nación (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 243/17[4], 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. Quienes usan SIBIOS no tienen la obligación de obtener una orden o autorización judicial antes de hacer consultas en la base de datos biométricos.

Para la infraestructura conectada a SIBIOS, el Ministerio de Seguridad recurrió a un proveedor importante: la empresa francesa Morpho Safran, que, como resultado de una fusión, se convirtió en IDEMIA. Ésta es responsable de la instalación y configuración del Sistema Automatizado de Identificación de Huella Dactilar (AFIS) del Ministerio. Además, 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[5] para verificaciones de identidad in situ mediante huellas dactilares en todo el país.

Otra porción de la infraestructura de SIBIOS estuvo a cargo del Ministerio del Interior, a partir de una estrecha relación con su equivalente cubano, particularmente entre el 2011 y el 2015. El Ministerio adquirió la tecnología biométrica de una empresa propiedad del Estado cubano, DATYS, que desarrolló una familia de productos para la identificación[6] y la verificación[7] biométrica, basados en 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 creció exponencialmente en todo el país. Además de su uso para la seguridad pública y la inmigración, los datos biométricos comenzaron a utilizarse 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[8].

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[9].

Más recientemente, las autoridades nacionales, provinciales y locales[10] 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 normativo

Las tecnologías de reconocimiento facial, scanners de huellas digitales, lectores de patentes, drones y otros, suelen generar sospechas debido a posibles afectaciones a la privacidad, entendida esta como el poder que ejercemos sobre nuestra dignidad y autonomía como seres humanos. En la Constitución Nacional Argentina, el artículo 19 reconoce que "Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe." En conjunto con el art. 18 que expresa que "El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación.", la Corte Suprema de la Nación ha interpretado el reconocimiento del derecho a la privacidad. A su vez, Argentina ha ratificado tratados internacionales de derechos humanos[11], como el Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana de Derechos Humanos.

En cuanto a la protección de datos personales, Argentina cuenta con un régimen de protección de datos robusto, aunque desactualizado. En el texto constitucional, el Artículo 43 reconoce la acción de Habeas Data al expresar que "Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística." A su vez, la Ley Nacional Nº 25.326 regula de forma expresa la

protección de datos personales. En el plazo internacional, firmó el Convenio 108+[12] y la Comisión Europea reconoció en 2003 que Argentina tenía un nivel de protección de datos adecuado mediante la decisión 2003/490 CE[13].

A pesar del robusto marco normativo que protege la privacidad de las personas, 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, han habido muy pocas acciones 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 falta de mecanismos judiciales o extrajudiciales para proteger 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[14]. En la actualidad, ADC se encuentra litigando contra el Gobierno de la Ciudad de Buenos Aires a través de una Acción Declarativa de Inconstitucionalidad para que prohíba el Sistema de Reconocimiento Facial de Prófugos. Por su parte, el Observatorio de Derecho Informático Argentino (O.D.I.A) inició un amparo colectivo con el mismo objetivo.

Iniciativas de vigilancia en Argentina

Existe una marcada tendencia por parte de los gobiernos nacionales, provinciales y locales de aumentar el despliegue de tecnologías de vigilancia 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.

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, el municipio de Tigre, Provincia de Buenos Aires, creó el Centro de Operaciones de Tigre[15] para usar cámaras y software de reconocimiento facial para buscar a personas desaparecidas e identificar a aquellas con antecedentes penales. En el mismo sentido, la provincia de Salta también ha desplegado cámaras con tecnología de reconocimiento facial para combatir el delito y otras provincias como Mendoza y Santa Fe ya estarían trabajando en la implementación de iniciativas similares.

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[16]. Debido a la falta de 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 a 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[17].

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[18]. 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". En 2018 volvió a verse envuelto en una controversia cuando el gobernador, Alfredo Cornejo, mantuvo una reunión con el vicepresidente de ventas de la empresa tecnológica Huawei para contratar tecnologías de reconocimiento facial, geolocalización y big data para combatir la inseguridad. Organizaciones de Derechos Humanos, incluidas Access Now y ADC, enviaron una carta al gobernador pidiéndole que detenga las negociaciones[19]. No hubo más información al respecto.

En el mismo sentido, 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 de big data, con el fin de localizar inmediatamente a personas, vehículos y otros elementos de interés mediante la búsqueda de objetos con atributos particulares[20].

Lamentablemente, no encontramos 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 noviembre del 2021, aún no han respondido a ninguna de nuestras consultas.

Es notable que, durante la pandemia del 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 subte, aeropuertos y estaciones de transporte público. El Gobierno nacional lanzó la aplicación "CuidAr", 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[21]. Como se expuso en el informe y análisis técnico de ADC, las aplicaciones de varias provincias, implementadas para hacer frente a la emergencia sanitaria, suscitaron graves preocupaciones acerca de la privacidad y la seguridad de la información de las personas[22].

Empresas proveedoras

AnyVision

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[23]. Gracias a anuncios públicos y a la cobertura de la prensa[24], pudimos identificar que AnyVision es la empresa que proporciona el "software de reconocimiento biométrico" adquirido por la provincia de Córdoba.

AnyVision también parece ser el proveedor del software de reconocimiento facial que se utiliza en el Aeropuerto Internacional de Ezeiza. 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 incluyó 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[25]. Un año después, la PSA firmó otro contrato directo con RC International por un monto de aproximadamente USD 54.000 para adquirir cinco licencias para mejorar la infraestructura de procesamiento[26].

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[27] que desde hace dos años que la PSA usaba la tecnología de reconocimiento facial de AnyVision en Ezeiza.

Antecedentes de Derechos Humanos

Según una investigación publicada por NBC en marzo del 2020, la tecnología de AnyVision sería utilizada en Israel en un esquema de vigilancia secreta para monitorear el movimiento de personas palestinas sobre Cisjordania. Según la misma fuente, el proyecto sería denominado "Google Ayosh", en alusión a la capacidad de la tecnología de buscar y encontrar personas[28]. 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"[29], aunque no queda claro cómo el proyecto evitó tales ataques.

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

Cabe notar que, tras años de presión por parte de defensores y defensoras de derechos humanos, Microsoft se desligó de AnyVision[30]. En el 2019, un estudio[31] 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

Hikvision y Zhejiang Dahua son dos de los fabricantes de equipos de vigilancia más importantes del mundo. 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 la Nación de Argentina autorizó el testeo de cámaras térmicas de Hikvision dentro de la terminal de trenes de Retiro para identificar pasajeros y pasajeras que tuvieran fiebre[32]. 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[33].

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[34].

El proyecto de Cutral-Có implicó el despliegue de 242 cámaras de video. Si bien no hay confirmación oficial, lDahua 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[35]. 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 la Ciudad Autónoma de Buenos Aires, la instalación no cumplió los estándares de la industria (estándares de la Comisión Electrotécnica Internacional[36]) y su uso no cumplió las instrucciones de la propia empresa.

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 Autónoma 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 noviembre del 2021, aún no hemos obtenido respuesta.

Antecedentes de Derechos Humanos

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 anteriormente, algunas de estas tecnologías pueden no tener un buen desempeño[37] o no cumplir los estándares básicos que la propia industria o empresa imponen[38]. Aun así, los gobiernos latinoamericanos les están comprando, exponiendo al público una tecnología invasiva e imprecisa como solución a la delincuencia, argumento que, en el mejor de los casos, es engañoso.

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[39], desde 2016. Según una investigación de The Wall Street Journal[40], las autoridades de Sinkiang están usando

tecnología de vigilancia para perseguir al grupo étnico minoritario musulmán uigur[41], que ha resultado en sanciones y críticas por parte de los gobiernos de Noruega[42], Dinamarca[43], y EE. UU[44]. Además, Dahua ha tenido una serie de vulnerabilidades en su sistema en la nube[45]. 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[46]. 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[47].

Cellebrite

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)[48]. 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 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 de la Nación asignó fondos para iniciar el desarrollo de Laboratorios Regionales de Investigación Forense, en colaboración con el Ministerio Público Fiscal de la Nación en todo el país. En el 2014,

ya había 13 laboratorios forenses que usaban la tecnología de Cellebrite, específicamente la línea de productos UFED[49] 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 Misiones[50]. En el caso de La Pampa, además del UFED, habían implementado el complemento CHINEX[51], 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[52].

Uno de los principales compradores y 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[53]. 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[54].

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)[55]. Más recientemente, Gendarmería actualizó esas licencias en junio del 2020, en un contrato con Security Team Network por un total de USD 132.116[56].

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[57]. 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 Physical Analyzer de Cellebrite[58]. La GNA también presta su equipo cuando colabora en investigaciones penales, por ejemplo en el caso de la provincia de Entre Ríos[59].

En la Ciudad Autónoma de Buenos Aires, la Fiscalía adquirió una licencia de UFED 4PC junto con software Physical Analyzer[60] 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[61]. 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[62].

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[63].

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[64] por una duración de dos años, y también la permuta de hardware de dos dispositivos Touch I por dos UFED Touch 2[65].

El Ministerio de Seguridad comenzó a celebrar contratos de cooperación con más de 15 empresas de tecnología, incluida Cellebrite, a finales 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[66]. 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 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".

Antecedentes de Derechos Humanos

Aunque Cellebrite asegura vender su tecnología exclusivamente a gobiernos y agencias del orden público, la compañía estuvo vinculada con clientes de dudosa legitimidad[67].

En el 2016, la Dirección General Anticorrupción y Seguridad Económica y Electrónica y la Dirección de Investigaciones Penales de Bahréin usaron el UFED de Cellebrite, según se informa, para investigar y perseguir a disidentes[68]. 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+[69].

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[70]. Además, la policía de Myanmar usó la misma tecnología para arrestar a dos periodistas en el 2019[71] y la policía de Hong Kong la usó aparentemente para acosar e investigar a manifestantes prodemocráticos en el 2020[72]. 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[73]. Algunos/as periodistas afirman haber sido objeto de torturas[74]. Informes adicionales revelan que se venden herramientas de Cellebrite a Nigeria, Bangladesh, Arabia Saudí y Vietnam[75].

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[76].

En octubre del 2020, Cellebrite anunció que dejaría de vender su tecnología a China y Hong Kong[77]. En marzo del 2021, agregó que pondrá fin a las ventas a Rusia y Bielorrusia[78]

Huawei y ZTE

Ambas empresas chinas, Huawei Technologies Co. y ZTE Corporation, ofrecen una amplia gama de soluciones tecnológicas. Además de teléfonos celulares y equipos de telecomunicaciones,

uno de los servicios que prestan se basa en tecnología y sistemas para la construcción de lo que se conoce como "ciudades inteligentes". Ambas compañías interactúan con gobiernos locales de América Latina para brindar herramientas para la seguridad pública.

En julio del 2020, ZTE llegó a Argentina a través de la provincia de Jujuy. El gobernador, Gerardo Morales, recibió al vicepresidente de ZTE Corporation y al gerente general de ZTE Argentina, Hua Xinhai y Dennis Wang, respectivamente. 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[79]. 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[80]. 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 entonces gobernador de la provincia de Mendoza se reunió con el vicepresidente de ventas de Huawei, Tony Sza[81]. 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[82], 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.

Antecedentes de Derechos Humanos

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[83]. 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[84].

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[85], dar subsidios para alimentos, brindar atención a la salud y administrar otros programas sociales de los que depende la mayor parte del pueblo venezolano para sobrevivir[86]. 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[87] 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[88] 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[89]. 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" automatizadas a autoridades del gobierno chino cuando sus sistemas de cámaras identificaran miembros del grupo minoritario oprimido de la etnia uigur[90].

Estos preocupantes casos provocaron que Suecia prohibiera los equipos de telecomunicaciones de Huawei y ZTE en su red 5G[91], y otras naciones europeas han tomado medidas similares o están pensando hacerlo.

NEC

En la industria de la identificación biométrica digital, NEC es un actor principal a nivel mundial. NEC 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[92] como la elección inmediata para muchas agencias gubernamentales en todo el mundo. Ha desarrollado 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 la ha vendido a 70 jurisdicciones[93]. 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[94]. 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[95]. Aduanas y Protección Fronteriza (CBP) de EE. UU. usa el software de reconocimiento facial en los aeropuertos[96], y la tecnología también se abrió paso a los estadios deportivos en Colombia[97] y Taiwán[98]. 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[99]. Desde el 2006 NEC es el proveedor oficial de tecnología biométrica del Ministerio del Interior de la Nación y del Registro 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 de la Nación, 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[100]. El documento de contratación oficial expone que se eligió a NEC porque la Dirección Nacional de Migraciones ya estaba utilizando los productos AFIS[101] y NeoFace[102] 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 aeroparque Jorge Newbery y al puerto marítimo, ambos en la Ciudad Autónoma de Buenos Aires[103]. 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 contrastar la información biométrica de todas las personas que ingresan o dejan el país con los datos que existen en la base de datos del RENAPER.

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)[104]. 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[105].

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 de la Nación) firmó un acuerdo de cooperación para desarrollar un Sistema de Identidad Digital (SID) nacional106. 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[107]. 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 de la Nación firmó un acuerdo de cooperación con el Ministerio de Educación de la Nación para implementar el sistema en las universidades nacionales con el objetivo de que los y las estudiantes validen sus identidades antes de rendir exámenes en línea[108]. Esta ampliación está ocurriendo a pesar de las preocupaciones acerca de las fallas en sus algoritmos de reconocimiento facial[109]. 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[110].

A escala local, NEC ha estrechado una relación cercana con el Gobierno de Tigre, municipio de la Provincia de Buenos Aires. Éste 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[111].

En el 2019, Tigre remodeló su infraestructura de vigilancia[112] lanzando NeoCenter, desarrollado por NEC para incrementar las capacidades existentes en el municipio[113]. 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 vehículos. Asimismo, Tigre amplió aún más su tecnología de vigilancia en el 2020 con la instalación de un tótem de cámaras para el reconocimiento facia[114].

Cuando Tigre anunció el lanzamiento, ADC presentó[115] 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 al municipio como un caso de estudio de marketing, exhibiendo las soluciones que le brinda, 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"[116].

IDEMIA

Anteriormente conocida como “Morpho Safran” y “Safran Identity and Security”[117], la empresa francesa IDEMIA es uno de los proveedores líderes de tecnología biométrica en todo el mundo. Solo en EE. UU., brinda soluciones para el FBI[118], la INTERPOL[119], el Departamento de Policía de Nueva York[120], 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. Ésta cuenta con una oficina en la Ciudad Autónoma de 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[121]. 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 destacamos anteriormente, en Argentina el uso de productos de Morpho está estrechamente relacionado con SIBIOS. Tanto el Ministerio de Seguridad de la Nación 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[122]. La Policía Federal hace uso de dispositivos Morpho RapID para llevar a cabo la identificación dactilar de individuos[123], al igual que de Morpho Face Detective de reconocimiento facial para identificar personas en multitudes[124].

Dado que la Policía Federal tiene jurisdicción en todo el territorio nacional, el uso de la tecnología de Morpho se expandió por todo el país, en ciudades como Campana[125], Luján[126], Balcarce[127], Córdoba[128], Chaco[129], y múltiples municipios de la Provincia de Buenos Aires[130].

Las agencias estatales recurren a un revendedor principal de la tecnología de IDEMIA, conocido como IAFIS Argentina S.A., que resulta ser la misma empresa que vende productos de Cellebrite. Este revendedor nombra como clientes a múltiples fuerzas policiales de varias provincias argentinas[131], así como también Fiscalías y otras instituciones públicas, aunque no especifica qué productos les provee.

La Ciudad Autónoma 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 subte de la ciudad para identificar a carteristas[132].

Según documentos oficiales de contratación y licitación pública, la Policía Metropolitana de la Ciudad Autónoma de Buenos Aires usa tecnología de reconocimiento dactilar y facial de Morpho en investigaciones 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[133].

Antecedentes de Derechos Humanos

En el 2017, Morpho (que más adelante se convirtió en IDEMIA) fue denunciada por irregularidades con sus kits de registro y autenticación biométricos que fueron usados en las elecciones generales de Kenia del 2017, lo que causó que la Asamblea Nacional de ese país cancelara sus contratos públicos y prohibiera nuevos contratos. Tal resolución fue impugnada y revocada por el Tribunal Superior de Kenia[134]. La coalición opositora 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[135].

En septiembre del 2020, Amnistía Internacional descubrió que tres empresas europeas, una de las cuales era IDEMIA, vendían tecnología de vigilancia al gobierno chino[136]. 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[137]. Francia, donde se encuentra la sede central de IDEMIA, se ha resistido a esta petición[138].

Otras Empresas

Como fue mencionado anteriormente, las empresas detalladas en este capítulo son aquellas sobre las cuales se pudo obtener mayor información y las cuales ostentan una mayor relación con los órganos gubernamentales. Sin embargo, existen también otras empresas que merecen ser mencionadas por su participación en distintas iniciativas de compra y utilización de tecnologías de vigilancia.

BGH Tech Partner

Boris Garfunkel e Hijos, o BGH, es una empresa argentina que comercializa una gran variedad de productos pero que, en la última década, se especializó 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[139]. 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[140] 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[141]. Las soluciones que ahora ofrece BGH incluyen cámaras térmicas, vehiculares, portátiles y de reconocimiento facial, así como tecnologías como drones y robots[142].

Danaide S.A. y NTechLab

Según algunos informes independientes[143], la empresa argentina local Danaide, contratada por la Ciudad Autónoma de Buenos Aires para implementar su sistema de reconocimiento facial en espacios públicos[144], puede que esté usando el software Find Face[145] 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, rehusandose a aclarar si la propia empresa había sido la desarrolladora del algoritmo de reconocimiento facial.

En la versión rusa del sitio web de NTechLab[146], el software UltraIP[147] 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[148], autoridades de la Ciudad

Autónoma 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 y niñas por persecución penal en violación de derechos humanos[149]. 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[150].

IBM

En diciembre del 2016, el Ministerio de Seguridad de la Nación 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[151]. 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[152] de IBM, un complemento i2 Collaborate de IBM, i2 Text chart de IBM y múltiples servicios de soporte técnico.

Existen antecedentes de que la tecnología de IBM fue utilizada en Filipinas durante la violenta "guerra contra las drogas". Según una investigación del 2009 liderada por Human Rights Watch[153], 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[154], 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.

Nubicom y Datandhome Supplier SA

En 2018 y 2019 el Gobierno de Salta instaló cámaras con software de reconocimiento facial[155] como parte de la actualización del plan “Salta Inteligente”. El proyecto contempló el despliegue de más de 1400 cámaras en todo el territorio provincial, algunas de ellas con la capacidad para detectar rostros.

Si bien la iniciativa estaría activa desde 2018, desde entonces hubieron reclamos hacia las empresas prestadoras del servicio de videovigilancia por incumplimiento en los contratos de instalación de las cámaras[156].

Hasta el año 2019, la empresa Datandhome Supplier SA era la proveedora de los dispositivos de videovigilancia y software, los cuales presuntamente incluían el sistema de reconocimiento facial mientras que la empresa Nubicom SRL proveía el servicio de conectividad del sistema.

En 2019, Salta rescindió el contrato con Datandhome por "incumplimientos graves" en la instalación de las cámaras comprometidas[157]. Luego de rescindir el contrato, se suscribió una contratación directa con Nubicom que de esta forma quedó a cargo del mantenimiento de las cámaras y el software. Así, tanto la conectividad como el mantenimiento y soporte técnico del sistema quedaron a cargo de Nubicom[158].

Nubicom es una empresa salteña dedicada a proveer soluciones de tecnología. Es una de las principales prestadoras de servicio de telecomunicaciones en Salta, Catamarca y Jujuy. Además de brindar el servicio de conectividad y software para el sistema de videovigilancia, también es la principal proveedora de servicio de internet en Salta y tienen un área dedicada a servicios para gobiernos, entre los cuales se encuentra el servicio de videovigilancia con reconocimiento facial, entre otros[159].

Si bien no se pudo obtener información oficial al respecto, fuentes periodísticas informaron que la firma Nubicom factura cerca de U$D 400.000 en contratos de videovigilancia[160].

Como parte de la investigación para elaborar este informe, presentamos un pedido de acceso a la información ante la provincia de Salta. El pedido incluía preguntas sobre el proceso de implementación de estas tecnologías y sobre los proveedores y procesos de contratación. A noviembre del 2021, aún no hemos obtenido respuesta.

Conclusión y recomendaciones para mejorar las normas y prácticas en relación con las empresas y los derechos humanos

Las investigaciones realizadas para este informe constituyen un primer paso para entender cuales son las iniciativas de vigilancia que se están implementando en Argentina y cómo funcionan las relaciones entre el sector público y privado en el desarrollo y despliegue de ellas. La dependencia de los gobiernos en las empresas al delegar el desarrollo, así como los riesgos intrínsecos que tienen las tecnologías analizadas, nos obligan a repensar cómo deben ser los procesos de contratación y convenios entre el sector público y privado para evitar abusos y vulneraciones a los derechos humanos.

La búsqueda de un modelo transparente y respetuoso de los derechos fundamentales de las personas requiere esfuerzos compartidos de todas las partes afectadas. Para ello, los instrumentos internacionales que establecen el marco internacional sobre empresas y derechos humanos constituyen uno de los puntos de partida a tener en cuenta para el diseño de salvaguardas para la industria. A saber, los 'Principios Rectores sobre las Empresas y los Derechos Humanos' (PRNU)[161] aprobados por la ONU en 2011, las Líneas Directrices para Empresas Multinacionales (LDEM) de la Organización para la Cooperación y el Desarrollo Económico (OCDE)[162], y la Declaración Tripartita de Principios sobre las Empresas Multinacionales y la Política Sociales (Declaración EMN) de la Organización Internacional del Trabajo (OIT)[163] son los principales instrumentos que enmarcan cómo deberían comportarse Estados y empresas.

Los PRNU establecen tres pilares fundamentales: la obligación de los Estados de proteger los derechos humanos, el deber de las empresas de respetarlos y el compromiso conjunto de remediar los daños que puedan ocasionar.

A continuación mencionamos algunos de los lineamientos que deberían ser tenidos en cuenta al pensar en una regulación adecuada de los acuerdos entre sector público y privado:

- **Transparencia**

La transparencia es un requisito indispensable para una adecuada protección de los derechos humanos. En el ámbito de las contrataciones del Estado, y específicamente en las alianzas público-privadas para la utilización de tecnologías de vigilancia, la exigencia es aún mayor.

A pesar de esto, las contrataciones, en materia de tecnologías de vigilancia suelen estar caracterizadas por una considerable falta de transparencia. Las empresas tienen intereses en preservar la confidencialidad sobre cómo desarrollan y funcionan sus sistemas y algoritmos, y los Estados no hacen mayores esfuerzos para conocer y brindar los detalles de las contrataciones. Por ello resulta fundamental que los contratos sean públicos, tanto desde la etapa de licitación pública, como en su contratación y posterior ejecución.

En Argentina, a pesar de las distintas normativas que apuntan a la transparencia[164], en, conseguir los detalles sobre las contrataciones que estuvieron bajo investigación para este informe y las las empresas proveedoras fue al menos dificultoso. La experiencia en la investigación indica que la información disponible públicamente es escasa y que recurrir a los Pedidos de Acceso a la Información Pública tampoco suele ser una vía idónea. Los gobiernos recurren a las excepciones contenidas en las leyes como base legal para

no brindar detalles de las contrataciones o en algunos casos directamente eligen no responder. Particularmente, las empresas y el Estado suelen ser reacios a brindar detalles sobre cómo funcionan las tecnologías y cómo fueron los procesos en la etapa de desarrollo de las empresas.

Para un adecuado control es necesario que la información sobre las contrataciones del Estado sea pública y de fácil acceso para cualquier parte interesada. Las excepciones al acceso a la información pública por razones de seguridad o secretos comerciales deben ser de carácter sumamente excepcional, con explicaciones concretas que la justifiquen. Al respecto, la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos ha manifestado que "al aplicar una restricción al derecho de acceso a la información pública, no solo los requisitos de legalidad y protección de un fin legítimo deben cumplirse, sino también el requisito de necesidad y proporcionalidad. La necesidad de la medida se cumplirá cuando la limitación no solo sea conducente para alcanzar el logro deseado, sino que además resulte imperiosa"[165], es decir que debe elegirse la alternativa que menos restrinja el derecho a acceder a la información. Aún en esos casos excepcionales, debería considerarse la posibilidad de que la información sea revelada en un ámbito seguro como podría ser ante un juez para que este determine si el secreto está justificado.

- **Debida Diligencia**

El desarrollo de tecnologías de vigilancia, así como su utilización por parte de los Estados constituyen una actividad intrínsecamente riesgosa para los derechos humanos. Por ello las empresas deben actuar con debida diligencia en derechos humanos.

La debida diligencia debe ser entendida como "un proceso continuo de gestión que una empresa prudente y razonable debe llevar a cabo, a la luz de sus circunstancias –como el sector en el que opera, el contexto en que realiza su actividad, su tamaño y otros factores– para hacer frente a su responsabilidad de respetar los derechos humanos"[166] . A su vez, los PRNU establecen que tanto empresas como Estados deben proceder con diligencia debida en materia de derechos humanos para identificar, prevenir, mitigar y rendir cuentas de los impactos adversos, al tiempo que deben hacer frente a las consecuencias negativas cuando tienen lugar. Aún en los casos donde no sea posible evitar los impactos negativos, la debida diligencia debe permitir a las empresas "mitigarlos, prevenir su recurrencia y, cuando corresponda, repararlos'[167], tal como establece la guía de debida diligencia de la OCDE para una conducta empresarial responsable. Además, es necesario que las empresas manifiesten de forma expresa y a través de instrumentos disponibles al público su compromiso de respetar los derechos humanos y cómo lo harán.

En el contexto de las asociaciones público-privadas para el despliegue de tecnologías que puedan tener algún impacto en los derechos humanos, los procesos de desarrollo, contratación y despliegue deberían realizar una adecuada debida diligencia para considerar, evitar y/o mitigar los efectos adversos de su utilización. Específicamente, debe evaluarse la posible afectación al derecho a la privacidad ya que, "además de su conexión directa con la industria tecnológica a raíz del creciente uso de datos personales, es un derecho que facilita el ejercicio de otros derechos humanos"[168]. Para ello, deberían garantizar que se han realizado evaluaciones de impacto adecuadas. Al exigir a las empresas que se adhieran a las obligaciones de diligencia debida en materia de derechos humanos, los Estados también pueden garantizar que una tecnología sea evaluada adecuadamente en sus fases de diseño y desarrollo, y no sólo en la fase de despliegue. En el caso

de las alianzas público - privadas para tecnologías de vigilancia esto es especialmente relevante, teniendo en cuenta que por las características propias de este tipo de relaciones, el desarrollo suele ser exclusivo del sector privado y el Estado recién aparece para la contratación y utilización, pero sin supervisar las etapas previas. Por ello, es necesario que sea aplicada en todo el proceso, tanto en su desarrollo, como en la contratación y posterior despliegue.

- **Rendición de cuentas y reparación**

La rendición de cuentas y los mecanismos de remediación o reparación también forman parte de la debida diligencia y constituyen un elemento fundamental del sistema de protección de derechos humanos ya que permiten que las autoridades respondan por sus actos y que las víctimas tengan acceso a una reparación adecuada. Aquí debe ser tenido en cuenta que los mecanismos de reparación pueden ser tanto judiciales como no judiciales. La vía idónea de reparación dependerá de cada caso, pero en caso de que sea un mecanismo judicial, la empresa debe colaborar con el proceso judicial. En Argentina, hasta el momento, han habido muy pocas acciones 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.

En el contexto de las alianzas público-privadas las vías tradicionales para reclamar, ya sea judiciales o extrajudiciales, suelen ser poco efectivas y cuando se trata de empresas transnacionales el reclamo es aún más dificultoso[169]. Aunque las responsabilidades y obligaciones puedan ser distintas, la responsabilidad que tiene el Estado no debe ser excluyente de que la empresa proveedora de la tecnología también deba rendir cuentas cuando la tecnología que han desarrollado permita una afectación en los derechos humanos.

Legalidad

El principio de legalidad exige que cualquier restricción a un derecho fundamental sea establecida por una ley. La Corte Interamericana de Derechos Humanos al interpretar que es lo que debe entenderse como una ley, explica que"la protección de los derechos humanos requiere que los actos estatales que los afecten de manera fundamental no queden al arbitrio del poder público, sino que estén rodeados de un conjunto de garantías enderezadas a asegurar que no se vulneren los atributos inviolables de la persona, dentro de las cuales, acaso la más relevante tenga que ser que las limitaciones se establezcan por una ley adoptada por el Poder Legislativo".

Así entendido, la utilización de tecnologías de vigilancia en espacios públicos debería estar siempre regulada por una ley emanada del Congreso, y no bastaría con una mera resolución administrativa, como sucede en algunos de los casos analizados[170].

Sin embargo, el principio de legalidad es una condición necesaria pero no suficiente. Además de estar regulada por una ley, la utilización de este tipo de tecnologías debería ser proporcional y necesaria. En el contexto de las alianzas público privadas resulta particularmente relevante que se cumpla con el principio de legalidad, pero también que la necesidad y proporcionalidad de las tecnologías utilizadas sea minuciosamente evaluada y explicada. Para ello, el análisis de impacto en derechos humanos es indispensable para comprender la manera en que se pueden estar vulnerando estos derechos.

Notas

[1] https://www.accessnow.org/cms/assets/uploads/2021/09/vigilancia-latam-espa.pdf

[2] Decreto 1766/2011. Argentina. http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/189382/texact.htm

[3] ADC. "La identidad que no podemos cambiar" 2017. https://adc.org.ar/informes/la-identidad-que-no-podemos-cambiar-biometria-sibios/

[4] Ministerio de Seguridad de Argentina. Decreto 243/2017. http://servicios.infoleg.gob.ar/infolegInternet/anexos/270000-274999/273446/norma.htm

[5] 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/

[6] 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.

[7] 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?"

[8] ADC. "Cuantificando identidades en América Latina". Mayo del 2017. https://adc.org.ar/informes/cuantificando-identidades-en-america-latina/

[9] RT. "SKYSTAR 180" https://www.rt.co.il/skystar-180

[10] Las provincias de Santa Fe, Córdoba, Mendoza, Salta, la Ciudad de Buenos Aires, y la localidad de Tigre ya cuentan con Sistemas de Reconocimiento Facial. Mapa de Vigilancia dispnible en https://conmicarano.adc.org.ar/

[11] Naciones Unidas. Ratification Status for Argentina. https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?CountryID=7&Lang=EN

[12] Consejo de Europa. Convenio 108 y Protocolos. https://www.coe.int/es/web/data-protection/convention108-and-protocol

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

[14] 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

[15] 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

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

[17] 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

[18] 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

[19] "Defensores de derechos fundamentales piden al gobierno de Mendoza que detenga la compra de tecnología de vigilancia masiva", ADC, July 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/

[20] 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

[21] 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-suscelulares-n2572740.html

[22] 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/

[23] Para obtener más información, visite el sitio web de AnyVision en https://www.anyvision.co/

[24] Canal de YouTube de El Doce. "Ya funciona el sistema de reconocimiento facial en Córdoba". Noviembre del 2019. https://www.youtube.com/watch?v=x-C2Y_T2KxCo

[25] Número de procedimiento 279-0032-CDI17 https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhxpHQh1a9rqmrswnHE0fbV4WFyYSFDE6lxSvc3QcWHT4/5pakrCnV2dPCYEG/6/s7e/f0naaJmGFnfhrFxNdKQpW67nH3a2C04dnq|8jmWDuQ==

[26] Número de procedimiento 279-0035-CDI18 https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhzSOD16bvFoRxEndMm7PHzAtBPeqYP9/qDb7KvHTHIh0obV8V5uXVQalfN9iRQ6t0NyEcvs|vrVYCJ5StXEPkNZXp61l5600xzpoafNPUDbtt6dkX1N7sUlXsW/U3fjsZr4FM|ahmgldAmKnOzjXjiP3OSXKNWySBJ/gR9toZ5IZaihRjc3OgmkchygiKgU9i4=

[27] https://digital.practia.global/cuando-tu-foto-se-convierte-en-tu-huella-digital/

[28] 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

[29] 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

[30] 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

[31] 3 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

[32] 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

[33] 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-tempera tura-de-los-pasajeros/

[34] 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

[35] 9 IPVM. “Hikvision Temperature Screening Tested.” Mayo del 2020. https://ipvm.com/reports/hikvision-temperature-test

[36] Comisión Electrotécnica Internacional. “Standards development.” https://www.iec.ch/standards-development

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

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

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

[40] 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

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

[42] 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-fro m-hikvision-based-on-human-rights-concerns-over-co-role-in-mass-surveillance/

[43] 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-akademiker-pension-dive sts-from-chinese-surveillance-equipment-maker-over-human-rights-concerns/

[44] 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-allegatio ns-of-using-forced-labour-of-ethnic-minorities/

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

[46] IPVM. “Hikvision Backdoor Exploit.” Septiembre del 2017. https://ipvm.com/reports/hik-exploit

[47] 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

[48] Para obtener más información, visite el sitio web de Suncorportation en https://www.sun-denshi.co.jp/en

[49] 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

[50] 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

[51] 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/

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

[53] Expediente Nº 37/105-0815-CDI19. https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhwbeNKAPenXR8IR3i-h5YSXR79Wk8x7mmr wOCg9|4XRUnx0kCgm3oU8Rx5zyjpByUn|6t4HsX9ox3IM|-fHZHcPGbahOwPe58NWP7IaFH5JcDkQ==

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

[55] Dirección de Criminalística y Estudios Forenses. "ADQUISICIÓN DE SOFTWARE UFED 4PC PARA LA DIRECCIÓN DE CRIMINALÍSTICA Y ESTUDIOS FORENSES". Expediente Nº 37/105-0041-LPU19. Julio del 2018 https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhy5xycgc2RiGO0seBx38Zrkqr-f44NYcUHOQX WAZSx|FbiACHf8VyMdhxK5ugYZKg/ha7EWhWl7fjuQEoJmuXixe-feg9/er7CV2Q|P|HNndQKg==

[56] Dirección de Criminalística y Estudios Forenses. "SERVICIO DE RENOVACIÓN Y ACTUALIZACIÓN DE LICENCIAS DE SOFTWARE FORENSE UFEC TOUCH I HACIA UFED 4PC". Expediente Nº 37/105-0422-CDI20. Marzo del 2020 https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhyrV/4BRRj7a-9qf3aG8azk|h3K/KAn7jb/h6aP Dkgsy3caJklV5dh/l98fSQHDGyecUZqnGVTQz3UXL-zeKrU0hskSjg8CnHW3bp5dO0tjSzbg==

[57] 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

[58] 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-argentinaesta-superando-las-barreras-de-tiempo-y-distancia-con-inteligencia-digital/

[59] 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

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

[61] 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

[62] 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%20A djudicacion%20SECURITY%20TEAM%20NETWORK%20S.A.%20-Ufed%20Cloud-.pdf

[63] 8 Ministerio Público de la Acusación de la Provincia de Santa Fe. Expediente Nº FG-000303-2020. Agosto del 2020 https://www.mpa.santafe.gov.ar/regulations_files/5f328fd04126a_Resoluci%C3%B3n%20N%C2%B0%20274.pdf

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

[65] Policía de Seguridad Aeroportuaria. “Renovación de licencias y mejoramiento de equipos UFED 4PC y UFED TOUCH, por Exclusividad”. Expediente Nº 279-0027-CDI20. Noviembre del 2020 https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhy3iTxQqkwwChRpn2XPxXCSk5uij|LSdq2DmF5S3lGnqlsUbG2uGBeZPrbB8BhNUcLFrujs6LrFUaU3GDH8dDYrJv/eOuj/ve1TCcZ2AXWpaw==

[66] 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

[67] 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/

[68] 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/

[69] 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

[70] 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

[71] 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-tomyanmar-one-firms-tools-were-used-against-two-journalists-/2019/05/04/d4e9f7f0-5b5d-11e9-b8e3-b03311fbbbfe_story.html

[72] 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#/

[73] 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/

[74] id.

[75] 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-withisrael-s-phone-hacking-tech-1.10003831

[76] 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-hon g-kong/; Haaretz, “Israeli Phone-hacking Firm Cellebrite Halts Sales to Russia, Belarus in Wake of Haaretz Report.” Marzo del 2021. https://www.haaretz.com/israel-news/.premium-israeli-phone-hacking-firm-cellebrite-halts-sales-to-russia-after-haaretz-repo rt-1.9633312

[77] 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/

[78] 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/

[79] Boletín Oficial. Decreto 207/2019. Marzo del 2019. https://www.boletinoficial.gob.ar/detalleAviso/primera/203703/20190320

[80] 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

[81] 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/

[82] 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-algobierno-de-mendoza-que-detenga-la-compra-de-tecnologia-de-vigilancia-masiva/

[83] 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/

[84] 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

[85] 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

[86] 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/

[87] Cuenta de Twitter AlbertoRodNews. https://twitter.com/AlbertoRodNews/status/1070733400372326401

[88] 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

[89] 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

[90] IPVM. “Huawei / Megvii Uyghur Alarms.” Diciembre del 2020. https://ipvm.com/reports/huawei-megvii-uygur

[91] 0Reuters. “Sweden bans Huawei, ZTE from upcoming 5G networks.” Octubre del 2020. https://www.reuters.com/article/sweden-huawei-int-idUSKBN2750WA

[92] NEC. Integrated Report 2020. https://www.nec.com/en/global/ir/pdf/annual/2020/ar2020-e_two.pdf

[93] NEC. Biometric Authentication. https://www.nec.com/en/global/solutions/biometrics/index.html

[94] NEC. “Biometric Identification for Over 1 Billion People.” Noviembre del 2018. https://www.nec.com/en/case/uidai/index.html

[95] 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-neverheard-of-12381d530510

[96] 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

[97] NEC. “NEC contributes to football stadium safety in Colombia.” Octubre del 2016. https://www.nec.com/en/press/201610/global_20161012_03.html

[98] 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/

[99] NEC. Historia. https://ar.nec.com/es_AR/about/history/index.html

[100] 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=BQoBkoMoEhxKmqLque6kMW1chJuEHzB2LvnmYI6tmg dCyJ7Ep7d490YZKW8ptaXbZVpysEhjsnNcElgEeF4JDcgYQh41LgX8fcn98cZ8e12qM5BlL50fqw==

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

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

[103] 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

[104] 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|0dYheEGyNBwGGvH3GL6jBhnOAiv5 hg9nZ3JQi1tBQTuogGzD12zCv6XuNwuBmJTvQzJWApOOrz69pEW2MV9graYTQBzR11CtszG5T6w==

[105] 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=BQoBkoMoEhy7MmMdVUat6QKfRigU80UVxJmyaLvy67T v2OgtO1qNBgGmFkKWbfpTnnfNopxo|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=BQoBkoMoEhzl n331uwbedtWpuhJRVlkYFu5E0d6zTuIWgkUVrzCpo|kMsAHgU/dYCpNuyBnX9eXEW4riZstvHDV2ZqhmqPbCKquiSivEogUdA1Hk MNIlaA==

División Compras. “AMPLIACIÓN Y ACTUALIZACIÓN DE LA PLATAFORMA BIOMÉTRICA EXISTENTE DEL RENAPER”. Expediente Nº 78-0028-CDI18. Diciembre del 2018.

[106] Ministerio del Interior. “SID: Sistema de Identidad Digital”. https://www.argentina.gob.ar/interior/renaper/sid-sistema-de-identidad-digital

[107] “Fintech” o tecnología financiera hace referencia a nuevos negocios que desarrollan servicios financieros utilizando tecnologías digitales como centro de sus productos y servicios.

[108] 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

[109] 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/

[110] 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/

[111] Canal de YouTube de NEC Corporation. “La ciudad de Tigre”. Septiembre del 2016. https://www.youtube.com/watch?v=5Lp9PWv0EQ0

[112] Municipalidad de Tigre. “Ojos de Tigre”. https://www.tigre.gob.ar/seguridad/cot

[113] 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

[114] 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

[115] Cuenta de Twitter de ADC. https://twitter.com/adcderechos/status/1131556333466116096?s=20

[116] 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

[117] 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

[118] 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-technol ogy-goes-operational-for-the-fbi?lang=en

[119] 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 -Estados-miembros-con-el-último-sistema-automático-de-identificación-de-huellas-dactilares-afis-afis? lang = es "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

[120] 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

[121] 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/

[122] 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 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

[123] 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

[124] 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

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

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

[127] 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-/

[128] 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

[129] 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

[130] 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-conoperativos-de-control-y-prevencion/

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

[132] 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/

[133] Buenos Aires Compras. Número del proceso de compra: 2900-1047-CDI15 https://www.buenosairescompras.gob.ar/PLIEGO /VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhzAdZmPYqqZ4su3ScBBrBvMPHSPHPxZ74bjkpi4POk3iZKynCGKbKt|RDsvNl cW1mJISgBUffWWFY1vgdwt/W5yzl3PnouupiCeVWiQuysmvw== Número del proceso de compra: 2900-0858-CDI17. https://www.buenosairescompras.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhzjp0DPq1u2nI3iH|4rzqLn 9Phu5zQ6mkLN3u849mLkhWIq/6PJyo37gtSRaUyG3uJLK1ZE2CoQE3RKSJHwBng31I/q82/vv9su9cJDc2PG2g==

[134] 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

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

[136] 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/

[137] 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/

[138] 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/

[139] 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-comunicacionesde-ultima-generacion-para-la-policia-provincial/

[140] 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

[141] 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/

[142] 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

[143] 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

[144] 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/

[145] NTechLab. Sitio web oficial de Find Face. https://findface.pro/en/

[146] NTechLab. Socios (en ruso). https://web.archive.org/web/20200511205745/https:/findface.pro/partners/

[147] Danaide. Software developments. https://danaide.com.ar/desarrollos/desarrollossoftware.html

[148] ADC. Solicitud de acceso a la información NO-2019-21065074-GCABA-DGAYC-SE. Julio del 2019. https://adc.org.ar/wp-content/uploads/2019/07/Respuesta-PAIP-reconocimiento-facial-GCBA-V2.pdf

[149] 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

[150] 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

[151] Dirección General de Administración. “ADQ. DE LICENCIAS DE SOFTWARE AVANZADO PARA EL ANÁLISIS CRIMINAL CON LA FIRMA UNITECH S.A.”. Expediente Nº 347-0066-CDI16. Diciembre del 2016. https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhxZR|eGCUUs0CDTFEc5IK6|-8mooLYATqyEzF wVde9PPWAMi|0jPJGKn6pHkBSQAUfnO3onZZEr5bCGawx17los-LJTLKoi9VrlOdxyH6GqsNTw==

[152] 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

[153] Human Rights Watch. “You Can Die Any Time.” Abril del 2009. https://www.hrw.org/sites/default/files/reports/philippines0409webwcover_0.pdf

[154] 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/

[155] Salta avanza en el desarrollo de un Estado Inteligente con seguridad ciudadana de última generación

[156] Juicios e irregularidades: el historial de la empresa que instaló las camaras en Salta Marzo 2020 https://www.quepasasalta.com.ar/nota/231354-juicios-e-irregularidades-el-historial-de-la-empresa-que-instalo-las-camaras-en-salta/

[157] El porque de la rescisión del contrato a DatandHome y quien es Nubicom Marzo 2020 https://informatesalta.com.ar/contenido/225500/el-porque-de-la-rescision-del-contrato-a-datandhome-y-quien-es-nubicom

[158] Ibidem

[159] Página oficial de Nubicom https://www.nubicom.com.ar/servicios/nubigob/

[160] El sistema de cámaras cuesta más de 400 mil dolares por mes https://www.eltribuno.com/salta/nota/2021-5-9-1-45-0-el-sistema-de-camaras-cuesta-mas-de-440-mil-dolares-por-mes

[161] Principios Rectores sobre Empresas y Derechos Humanos, ONU, 2011https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_sp.pdf

[162] Disponible en https://www.oecd.org/daf/inv/mne/MNEguidelinesESPANOL.pdf

[163] Disponible en https://www.ilo.org/empent/Publications/WCMS_124924/lang--es/index.htm

[164] En Argentina, el derecho de acceso a la información pública se encuentra regulado por la ley 27.275 Sancionada por el Congreso de la Nación en el año 2016, Disponible en https://www.boletinoficial.gob.ar/#!DetalleNorma/151503/20160929

[165] "Derecho a la Información y Seguridad Nacional". Relatoría Especial para la Libertad de Expresión, 2020, disponible en https://www.oas.org/es/cidh/expresion/informes/DerechoInformacionSeguridadNacional.pdf

[166] Disponible en https://adc.org.ar/wp-content/uploads/2020/10/Guia-Debida-Diligencia-DDHH-Analisis-de-Impacto-en-Privacidad.pdf

[167] Disponible en https://mneguidelines.oecd.org/Guia-de-la-OCDE-de-debida-diligencia-para-una-conducta-empresarial-responsable.pdf

[168] ¿Cómo implementar la debida diligencia en derechos humanos en el desarrollo de tecnología?, ADC 2020

[169] Proyecto sobre rendición de cuentas y mecanismos de reparación (ARP I) del ACNUDH: Aumentar la eficacia de los mecanismos judiciales en casos en que las empresas incurren en vulneraciones de derechos humanos

[170] Ver caso de Reconocimiento Facial de la Ciudad Autónoma de Buenos Aires. Ver https://www.lanacion.com.ar/tecnologia/es-inconstitucional-reconocimiento-facial-porteno-nid2307648/

adc.org.ar