Surveillance Technology in Argentina

por los Derechos Civiles

Surveillance Technology in Argentina

December 2021

Team

Written by: Alejo Kiguel, Eduardo Ferreyra, Leandro Ucciferri

Design: El Maizal

Supported by Privacy International

Contents

Executive Summary

Throughout 2020 and 2021, ADC (Association for Civil Rights) participated in a regional study on the purchase and use of surveillance technologies in Latin America, conducted by *Access Now*. ADC dealt with the situation in Argentina; the upshot of this research was published in the paper *Surveillance Technology in Latin America: Made Abroad, Deployed at Home*[1], which also includes the case studies of Brazil and Ecuador.

The present document recaps the findings of that work and updates the state of affairs, including new events such as the introduction of facial recognition in the province of Salta. It also includes recommendations for future regulation of agreements to be made between the public and private sectors, aligned with international principles on business and human rights.

It is clear that the display of surveillance technology continues to grow in Argentina. Biometric data as a means of identification, which began to be applied for public safety purposes, is already being used to verify identities in social security programs, tax or fiscal responsibilities, education, elections, and sports. Meanwhile, more and more government authorities, at national, provincial, and municipal levels, are installing video surveillance cameras in public spaces with facial recognition systems that allow people to be pinpointed by their physical features, thus posing a significant risk to human rights.

Governments generally turn to the private sector when purchasing these types of equipment. The kind of dependence this creates, as companies are responsible for their development, as well as the risks inherent to these solutions, give rise to new questions on who to hold accountable when people's rights are infringed and what should be considered for the procurement processes in each case.

In order to halt the spread of this type of technology throughout the country, it is essential to understand its scope and implications. To this end, we should first be well-informed on how these public-private ventures operate while establishing adequate mechanisms so that both, governments and companies, commit themselves to respect and protect human rights, and secondly, provide efficient mechanisms for redress when those rights are violated.

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

Introduction

The deployment of surveillance equipment is increasing in Argentina. More and more districts are installing it without a proper assessment of its impact on human rights, while others have announced they are planning to follow suit in the short or medium term. Unfortunately, public authorities are resorting to solutions with costs that outweigh the alleged benefits. To stop the trend, we need to be informed on the scope and implications of this type of technology. And here is where the problems begin, since discovering how the different levels of government use these systems is a delicate task.

In addition to being a typically opaque industry, little information is given on it through public channels unless there is a media report or an independent study. And even so, on those occasions when we become aware of its existence, the authorities continue to be reluctant to provide details of the procurement processes in their acquisition.

In Argentina, the introduction of SIBIOS in 2011 was a decisive breakpoint: through Decree 1766/11[2], the national government created the Federal Biometric Identification System for Security (SIBIOS), operated by the Federal Police under the authority of the Argentinian Ministry of Security.

One of the main objectives of SIBIOS was to merge and digitize the independent databases of the Federal Police and the National Registry of Persons (RENAPER). SIBIOS was the outcome of a process started years earlier when the Argentinian Interior Ministry began to gather, process, and store biometric data for the issuance of national ID cards (DNI in Argentina) and passports. Since 2009, RENAPER is entitled to use digital technology to identify citizens, residents, and visitors and has been collecting biometric data, such as fingerprints, palm prints and facial photos of both, citizens and all persons entering the country[3].

SIBIOS is a national system, hence, all twenty-four provinces of the country have signed cooperation agreements with the Argentinian Ministry of Security, including its four federal security forces, and the Argentinian Interior Ministry, which encompasses RENAPER and the National Directorate for Migration. These agreements ensure that local police forces can log into and update the database. In 2017, through Decree 243/17[4], the Government extended access to SIBIOS to any public agency within the Executive or Judicial Branches, at the national and provincial levels, as well

[2] Decree 1766/2011. Argentina.
http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/189382/texact.htm
[3] ADC. “The identity we cannot change.” 2017.
https://adc.org.ar/informes/la-identidad-que-no-podemos-cambiar-biometria-sibios/
[4] Argentinian Ministry of Security. Decree 243/2017.
http://servicios.infoleg.gob.ar/infolegInternet/anexos/270000-274999/273446/norma.htm

as to the City of Buenos Aires. SIBIOS users are not required to obtain a court order or any type of permission before making a query in the biometric database.

For the equipment of SIBIOS, the Ministry of Security turned to a major supplier: the French company Morpho Safran, which, as a result of a merger, became IDEMIA. IDEMIA is responsible for the installation and configuration of the Ministry's Automated Fingerprint Identification System (AFIS). In addition, other products from this company were purchased, such as Morpho Face Investigate Pilot for facial recognition from photo and video files, and Morpho RapID[5] for in-situ identity checks using fingerprints throughout the country.

Another segment of the SIBIOS infrastructure sprang from the close ties between the Interior Ministry of and its Cuban equivalent, particularly between 2011 and 2015: the Ministry then acquired biometric technology from a Cuban state-owned company, DATYS, which developed a product family for biometric identification[6] and verification[7] based on facial, fingerprint, palm print, DNA and voice recognition. In October 2015, the Ministry upgraded it through a USD 1,080,000 contract with DATYS, plus USD 180,000 per year for technical support, during a five-year term. Since the introduction of SIBIOS in 2011, the use of biometric systems has steadily grown throughout the country. In addition to their application for public safety and immigration purposes, biometric data is being applied to verify identity in social security programs (e.g., for access to retirement and pension funds), banking, tax or fiscal responsibilities, education, elections, and sports[8].

In addition to biometric data, the Argentinean government added other surveillance technologies to its inventory. The armed forces, comprising the army, navy, and air force, have developed their own Unmanned Aerial Vehicles (UAVs), beginning in 1996 and furtherly expanding between 2011 and 2014. Meanwhile, the Federal Police turned to a major drone supplier to meet its needs: the Chinese company DJI (Dà-Jiang Innovations Science

---

[5] La Capital. “Identity and police records on the spot during saturation patrol.” June 2016. https://www.lacapitalmdp.com/identidad-y-antecedentes-al-instante-en-los-operativos-de-saturacion/

[6] Facial identification (1:N) is the process of determining whether the biometric traits of a detected face coincide with those of any other one stored in a directory. In this case, the application searches for a match in an identity database.

[7] Facial verification or authentication (1:1) is the process of determining whether the biometric traits of a detected face match a specific one stored beforehand. Here, the application attempts to verify if an individual is the person she really claims to be.

[8] ADC. “Quantifying identities in Latin America.” May 2017. https://adc.org.ar/informes/cuantificando-identidades-en-america-latina/

and Technology Co.). Likewise, in mid-2017, the City of Buenos Aires bought a surveillance balloon, the Skystar 180, made by the Israeli company RT[9].

More recently, national, provincial and municipal authorities[10] have been increasing the use of facial recognition and license plate readers across the country, as part of what appears to be a competition between political leaders in implementing as much technology as possible in pursuit of public safety.

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

[10] The provinces of Santa Fe, Córdoba, Mendoza, Salta, the City of Buenos Aires, and the city of Tigre already have Facial Recognition Systems. Our Surveillance Map is available at https://conmicarano.adc.org.ar/

Regulatory framework

Facial recognition systems, fingerprint scanners, license plate readers, drones, etc., often raise suspicions concerning privacy, defined as the power we exercise over our dignity and autonomy as human beings. Article 19 of the Argentinean National Constitution recognizes that “The private actions of men which in no way offend public order or morality, nor injure a third party, are only reserved to God and are exempted from the authority of judges. No inhabitant of the Nation shall be obliged to perform what the law does not demand nor deprived of what it does not prohibit.” Together with Art. 18, which states that "The domicile shall not be violated, as well as the written correspondence and private papers; and a law shall determine in which cases and for what reasons their search and occupation shall be allowed...," the Supreme Court of the Nation has interpreted the recognition of the right to privacy. Argentina has also ratified international human rights treaties[11] such as the International Covenant on Civil and Political Rights and the American Convention on Human Rights.

Regarding the issue of personal data, Argentina has robust protective legislation, although outdated. Article 43 of the Constitution recognizes the Habeas Data action by stating that ''Any person may file this action to obtain information on the data about herself registered in public records or databases or in private ones intended to supply information, and its purpose; and in case of false data or discrimination, this action may be filed to request the suppression, rectification, confidentiality or updating of the said data. The secrecy of journalistic sources shall not be impaired.'' In turn, National Law No. 25.326 expressly regulates the protection of personal data. At an international level, Argentina has signed Convention 108+[12], and in 2003, the European Commission recognized that Argentina had an adequate level of data protection through Decision 2003/490 EC.[13]

Despite the vigorous legal framework protecting individual privacy, governments resort to the exceptions provided in the norms as a legal basis to deploy surveillance systems for carrying out state functions or public safety. So far, there have been few judicial or administrative actions to safeguard individuals from the massive and continuous collection of biometric data and the emplacement of invasive technologies. This deficiency worsened in October 2020, when the City of Buenos Aires legislature set a dangerous precedent by amending Law No. 5688 to approve the use of facial recognition to identify fugitives mentioned on a

[11] United Nations. Ratification Status for Argentina. https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?CountryID=7&Lang=EN
[12] Council of Europe. Convention 108 and Protocols. https://www.coe.int/es/web/data-protection/convention108-and-protocol
[13] EUR-Lex. Document 32003D0490. 2003. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32003D0490

national watch list.[14] ADC is currently litigating against the City of Buenos Aires through a Declaratory Action of Unconstitutionality to ban the Fugitive Facial Recognition System. In turn, the *Observatorio de Derecho Informático Argentino* (Argentinean IT Law Observatory – O.D.I.A.) filed a collective action to the same end.

[14] Télam. "The legislature approved the use of facial recognition for the arrest of fugitives." October 2020. https://www.telam.com.ar/notas/202010/527676-la-legislatura-aprobo-el-uso-de-reconocimiento-facial-para-la-detencion-de -profugos.html.

Surveillance initiatives in Argentina

There is an observable trend shown by national, provincial, and local governments to increase the use of surveillance technology in Argentina. It is difficult to obtain updated information from each jurisdiction, especially when these systems are used by law enforcement agencies, for which only the most prominent cases will be cited.

It could be established that facial recognition software in cameras is the most widely used type of surveillance technology at all levels of government in Argentina. In April 2019, the City of Buenos Aires announced its adoption of security cameras (CCTV) and monitoring centers. In May, the same year, the town of Tigre, in the Province of Buenos Aires, created the "Tigre Operation Center"[15], using cameras and facial recognition software to search for missing persons and identify people with criminal records. In the same vein, the province of Salta has also deployed facial recognition to combat crime and other provinces such as Mendoza and Santa Fe are seemingly working on similar initiatives.

On October 15, 2019, the government of Cordoba announced, through its social networks, the introduction of a "biometric recognition software" installed in a police van, with four mounted and two fixed cameras[16]. As little information is publicly available, we submitted two Access to Information Requests, on November 7, 2019 and November 11, 2020. The government ignored both, adding to this province's long record of non-compliance with the law on Access to Public Information. According to reports by civil society organizations, such as Red Ciudadana Nuestra Córdoba (Our Córdoba Citizen Network), Fundeps, Foro Ambiental (Environmental Forum), and Córdoba de Todos, the authorities respond to a mere 10% of the requests submitted every year.[17]

In mid-2017, the province of Mendoza began implementing one of the most invasive monitoring programs in Argentina. The province's law enforcement agencies have mobile facial recognition cameras and vehicles equipped with similar technology, as well as fingerprint scanners and license plate readers. [18] Despite our efforts to obtain detailed information, we have only been

---

[15] Ámbito. "Tigre launches a new facial recognition system". May 2019. https://www.ambito.com/municipios/municipios/tigre-lanzo-un-nuevo-sistema-reconocimiento-facial-n5030978

[16] Twitter account of the Government of Córdoba. October 2019. https://twitter.com/gobdecordoba/status/1184116108665729025?s=20

[17] La Voz del Interior. "Responding to requests for information, a pending subject within the Province and the City". November 2019. https://www.lavoz.com.ar/ciudadanos/responder-pedidos-de-informacion-una-cuenta-pendiente-de-provincia-y-municipio

[18] El Sol. "Facial recognition: more than 100 people with arrest warrants found." May 2019. https://www.elsol.com.ar/reconocimiento-facial-hallaron-a-mas-de-100-personas-con-pedido-de-captura

given the names of the suppliers from whom the equipment is purchased (*3M Argentina*, *INTEMA Comunicaciones S.A.*, *Express Software*, and *Hardware S.A.*) and no specifications on the software and hardware. The Ministry of Security of that Province argued that "the requested information affects public safety". In 2018, there was another controversy when the governor, Alfredo Cornejo, held a meeting with Huawei's vice president of sales to procure facial recognition, geolocation and big data systems to fight crime. Human Rights organizations, including *Access Now* and ADC, sent a letter asking to stop such deals.[19] No further information was given on the matter.

Similarly, the Government of San Juan disclosed the "San Juan Accord" to deploy more technology for public safety. This program includes the installation of CCTV cameras and facial recognition, in addition to a "Forensic Video Analysis Laboratory" for the processing of big data which can readily locate people, vehicles, and other items of interest by searching for objects through their particular features.[20]

Unfortunately, not much is informed about the San Juan Accord from publicly available sources. San Juan does not have a law on Access to Information Requests; however, we contacted public officials with a set of inquiries, but as of November 2021, have received no replies yet.

One outstanding feature of the COVID-19 pandemic in 2020 was that local governments turned to technology as a way to curb the spread of the virus. Thermal cameras were installed in buses, subway lines, airports, and public transportation terminals. The national government launched the app "CuidAr", and provinces used mobile software tools to enforce mandatory lockdowns, control crowds, and monitor for symptoms, leading to controversy about the purpose and use of such solutions.[21] As disclosed by ADC's report and technical analysis, several of these apps designed to cope with the health crisis raised serious concerns about people's data privacy and security.[22]

---

[19] "Fundamental rights advocates call on Mendoza government to halt purchase of mass surveillance technology," 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] Official website of San Juan. "San Juan Accord: technology applied to public safety". October 2020. https://sisanjuan.gob.ar/seguridad/2020-10-22/26837-acuerdo-san-juan-tecnologia-aplicada-a-la-seguridad

[21] La Capital. "Cellphone app to control people breaking lockdown rules". March 2020. https://www.lacapital.com.ar/la-ciudad/controlaran-quienes-incumplieron-elaislamiento-una-app-suscelulares-n2572740.html

[22] ADC. "In case of emergency: download an app - Part II". December 2020. https://adc.org.ar/2020/12/22/en-caso-de-emergencia-descargue-una-app-parte-ii/

Supplier companies

AnyVision

AnyVision is an Israeli company that specializes in facial recognition for public safety, as well as applications for healthcare, casinos and banking.[23] We learned through public announcements and press coverage[24] that AnyVision is providing the "biometric recognition software" purchased by the province of Cordoba. AnyVision also appears to be the supplier of the facial recognition software used at Ezeiza International Airport. From official data, we found that the authorities acquired this technology through direct negotiations with a local AnyVision reseller: a company named RC International. The first direct contract between the Airport Security Police (PSA) and RC International dates back to December 2017 and added up to approximately USD 48,000. The contract included the purchase of four AnyVision facial recognition licenses, along with four Internet Protocol (IP) cameras and a server, with the ability to scan and match faces with those of 2.5 million biometric records.[25] A year later, the PSA signed another direct contract with RC International for nearly USD 54,000 to buy five licenses to upgrade the processing infrastructure.[26]

When asked about the installation of AnyVision's facial recognition software on July 17, 2020, RC International's business strategy manager, Pablo Marcovich, confirmed that the PSA had been using it in Ezeiza for two years.[27]

Human Rights Record

A report by NBC in March 2020 affirms that AnyVision's systems are being used in Israel for a secret surveillance scheme to track the movement of Palestinians over the West Bank. According to the report, the project was named "Google Ayosh," implying the software's ability to search for and find

---

[23] For further information, visit AnyVision's website at https://www.anyvision.co/

[24] El Doce YouTube Channel. "Facial recognition system already working in Córdoba". November 2019. https://www.youtube.com/watch?v=x-C2Y_T2KxCo

[25] Procedure Number 279-0032-CDI17 https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhxpHQh1a9rqmrswnHE0fb-4WFyYSFDE6lxSvc3QcWHT4/5pakrCnV2dPCYEG/6/s7e/f0naaJmGFnfhrFxNdKQpW67nH3a2C04dnqj8jmWDuQ==

[26] Procedure number 279-0035-CDI18 https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhzSOD16bvFoRxEndMm7PHzAtBPeqYP9/qDb7KvHTHIh0obV8V5uXVQalfN9iRQ6t0NyEcvs|vrVYCJ5StXEPkNZXp61l5600xzpoafNPUDbtt6dkX1N7sUlXsW/U3fjsZr4FM|ahmgldAmKnOzjXji-P3OSXKNWySBJ/gR9toZ5IZaihRjc3OgmkchygiKgU9i4=

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

people.[28] The project earned the company a defense prize in 2018 for "preventing hundreds of terrorist attacks" through the use of "big data",[29] although it is unclear how such attacks were prevented.

The technology mentioned is one of AnyVision's flagship brands, "Better Tomorrow." The network uses cameras installed with facial recognition and an automated alert system with a watch list to identify the "suspicious persons" in crowds and track and categorize vehicles. It should be noted that, after years of pressure from human rights advocates, Microsoft divested from AnyVision[30]. In 2019, a study[31] by the U.S. National Institute of Standards and Technology (NIST) on racial bias in facial recognition software found that AnyVision's algorithm, like many others tested, performed worse on picking out African or East Asian faces than on those of people from Eastern Europe.

Hikvision and Dahua

Hikvision and Zhejiang Dahua are two of the world's leading surveillance equipment manufacturers. Their presence in Latin America has increased steadily in 2020, as they supply many governments with technological solutions to cope with the COVID-19 pandemic.

According to official sources, the Argentinean Ministry of Transportation allowed the use of Hikvision thermal cameras inside the Retiro train terminal to detect high body temperature in passengers.[32] Similar technology developed by Dahua was deployed at Ezeiza International Airport and in public transportation, including two bus lines.[33]

The presence of Dahua in Argentina is not a novelty: in 2017, Cutral-Có, a major oil town, installed a comprehensive Dahua system, with a

---

[28] 9 Access Now. “Exposed and Exploited: Data Protection In the Middle East and North Africa.” January 2021. https://www.accessnow.org/mena-data-protection-report

[29] NBC News. “Why did Microsoft fund an Israeli firm that surveils West Bank Palestinians?” October 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.” Marchl 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.” December 2019. https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software

[32] Télam. "Two bus lines install thermal cameras to measure the temperature of passengers". May 2020. https://www.telam.com.ar/notas/202005/469479-camaras-termicas-colectivos-pasajeros.html/

[33] Infobae. "Two bus lines install thermal cameras to measure passengers' temperature". May 2020. https://www.infobae.com/sociedad/2020/05/28/two-bus-lines-installed-thermal-cameras-to-measure-passenger-temperature/

professional surveillance system (PSS) at the core, and software simultaneously connected to 256 devices, according to the company's press content.[34] The Cutral-Có project involved the display of 242 video cameras. While there is no official confirmation, Dahua claims that the infrastructure provides the flexibility to expand its scope, for example, by using the recorded video footage with facial recognition and vehicle license plate number identification tools. Independent tests performed on the thermal cameras, particularly Hikvision products, show that this technology is highly inaccurate.[35] A simple fringe on someone's forehead can hide their real body temperature. What is worse, when the Dahua cameras were placed in two bus lines of Buenos Aires City, the fitting of the equipment did not meet industry standards (International Electrotechnical Commission Standards[36]) and their use did not even comply with the company's instructions.

As part of the research done on preparing this report, we submitted two Requests for Access to Information to the National Transportation Ministry and its equivalent of the City of Buenos Aires on November 3, 2020. The requests contained inquiries on the implementation of these technologies and the city's relationship with both companies. As of November 2021, no reply has been given.

Human Rights Record

It is essential that Hikvision and Dahua be transparent for many reasons. As said, these companies have an ample presence in Latin America, where they successfully sell highly controversial technology to national and local governments at low prices. However, as we mentioned before, some of this equipment is deficient in performance[37] or does not even meet the basic standards imposed by the industry or the company itself[38]. All the same, governments of the region are procuring it and exposing the public to an invasive and inaccurate technology as a solution to crime, an argument that is misleading at best.

Both companies are involved in human rights violations, having won contracts worth more than USD 1 billion for government-backed

---

[34] 18 Security Worldmarket. "Cutral-Có transforms into a Safe City in 30 days with Dahua." May 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] International Electrotechnical Commission. "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." June 2020. https://ipvm.com/reports/buenos-aires-bus

surveillance projects in Sinkiang, China[39] since 2016. According to a report by The Wall Street Journal,[40] authorities in Sinkiang are using surveillance systems to persecute the Muslim Uyghur ethnic minority group[41], which has led to criticism and sanctions from the governments of Norway[42], Denmark [43], and the USA[44]. In addition, Dahua has had several cloud vulnerabilities.[45] Independent testing discovered a backdoor in Dahua's systems that allowed unauthorized remote access via the web. Hikvision had a similar flaw in its IP cameras in 2017[46]. Recently, the U.S. Federal Communications Commission added Hikvision and Dahua to a list of communications equipment and services that pose a threat to national security, encouraging domestic companies to avoid using products from these two firms.[47]

Cellebrite

Cellebrite is an Israeli digital intelligence company and a subsidiary of the Japanese Suncorporation Ltd. (listed on the Tokyo Stock Exchange)[48]. Although it is not clear when authorities in Argentina began to use its devices, Cellebrite's presence in the country has grown consistently over the past five years. Its products are purchased through two main local resellers: Security Team Network S.A. and IAFIS Argentina S.A. Argentina rank third in

---

[39] IPVM. "Dahua and Hikvision Win Over $1 Billion In Government-Backed Projects In Xinjiang." April 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." December 2019. https://www.wsj.com/articles/twelve-days-in-xinjiang-how-chinas-surveillance-state-overwhelms-daily-life-1513700355

[41] For further information, see: 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." September 2020 https://www.business-humanrights.org/en/latest-news/norwegian-wealth-funds-ethics-council-recommends-divestment-from-hikvision-based-on-human-rights-concerns-over-co-role-in-mass-surveillance/

[43] Business & Human Rights Resource Centre. "Danish pension fund Akademiker Pension divests from Hikvision for human rights concerns over co. role in mass surveillance." November 2020. https://www.business-humanrights.org/fr/derni%C3%A8res-ctualit%C3%A9s/danish-pension-fund-akademikerpension-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." June 2020. https://www.business-humanrights.org/en/latest-news/usa-eleven-chinese-firms-added-to-economic-blacklist-over-allegatio ns-of-using-forcedlabour-of-ethnic-minorities/

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

[46] IPVM. "Hikvision Backdoor Exploit." September 2017. https://ipvm.com/reports/hik-exploit

[47] Federal Communications Commission. "The Public Safety and Homeland Security Office announces publication of equipment and services covered by the Secure Networks Act Section 2." File No. 18-89. March 2021. https://docs.fcc.gov/public/attachments/DA-21-309A1.pdf

[48] For further information, see Suncorporation's website at: https://www.sun-denshi.co.jp/en

the Americas in the use of licenses for Cellebrite's UFED (Universal Forensic Extraction Device), which is exported to more than 150 jurisdictions.

In the early 2010s, the National Ministry of Justice allocated funds to start developing the Regional Forensic Investigation Laboratories, together with the National Public Prosecutor's Office throughout the country. By 2014, 13 forensic laboratories were using Cellebrite's technology, specifically the UFED line for data extraction[49]. According to an official document from the Ministry of Justice, governments and agencies employing it included: Office of IT Management (OFITEC), Mercedes, Province of Buenos Aires; Forensic Laboratory of Complex Communications, Mar del Plata, Province of Buenos Aires; the City of Buenos Aires and provinces of Entre Rios, Mendoza, San Juan, San Luis, Formosa, Neuquén, Chubut, La Pampa, Corrientes, and Misiones[50]. In La Pampa, the CHINEX[51] complement, developed for the extraction of data from non-standard Chinese telephones, was implemented in addition to the UFED.

Since then, the use of Cellebrite products has expanded to other districts. In 2018, the Public Prosecutor's Office of Salta upgraded its UFED 4PC and TOUCH licenses for a total of USD 23,000, through a direct contract with Security Team Network.[52]

One of the main buyers and users of Cellebrite's technology on a national scale in the country is the National Police Force or Gendarmerie (*Gendaremería Nacional* – GNA). Due to its federal jurisdiction, the GNA deployed Cellebrite products throughout the country to equip forensic laboratories.

In September 2019, a direct contract with signed with Security Team Network S.A. for a total amount of USD 643,900 to acquire a high-end smartphone unlocking workstation. The UFED product is only mentioned once in the technical specification[53]. In November, the Directorate of Criminalistics and Forensic Studies of the GNA purchased four licenses for the "UFED 4PC" software. According to Cellebrite, this product has

---

[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] Ministry of Justice and Human Rights. "Regional Laboratories of Forensic Investigation". August 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." September 2019. https://www.cellebrite.com/en/blog/non-standard-chinese-phones-now-accessible-with-ufed-chinex-kit/

[52] Public Prosecutor's Office, Province of Salta. File No. 130-17.933/17

[53] File No. 37/105-0815-CDI19. https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhwbeNKAPenXR8IR3ih5YSXR79Wk8x7mmrwOCg9J4XRUnx0kCgm3oU8Rx5zyjpByUnJ6t4HsX9ox3IMJ-fHZHcPGbahOwPe58NWP7IaFH5JcDkQ==

"capabilities for extraction, decoding, analysis, reading and management" that can be run on custom hardware.[54]

The licenses were bought through a public bidding process, which finally resulted in a new contract with Security Team Network for a total of ARS 9,587,400 (about USD 159,000 at the time).[55] In June 2020 they were upgraded via another contract with the same company for USD 132,116.[56]

According to a journalistic source, who requested anonymity, the federal security forces (comprising the GNA, the Airport Security Police, the Federal Police, and the Coast Guard) have a total of 35 UFED products. Together with prosecution offices and other public agencies, the licenses used in the country add up to 350.[57] The main user is the GNA, which operates in all provinces and is currently upgrading its digital forensic laboratories, using products such as Cellebrite's UFED Cloud, UFED Pathfinder and UFED Physical Analyzer.[58] The GNA also leases its equipment when collaborating in criminal investigations, for example to the province of Entre Ríos.[59]

In the City of Buenos Aires, the Prosecutor's Office purchased a UFED 4PC license along with Physical Analyzer software[60] in 2019, through a direct contract with Security Team Network for the sum of ARS 440,109 (about USD 10,500 at the time). These products were assigned to the Judicial Investigation Body,[61] which had already renewed a license for another

---

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

[55] Bureau of Criminalistics and Forensic Studies. "Acquisition of software UFED 4PC SOFTWARE for the Criminalistics and Forensic Studies". File No. 37/105-0041-LPU19. July 2018 https://comprar.gob.ar/PLIEGO/PreviewPreviewBidCitizen.aspx?qs?qs=BQoBkoMoEhy5xycgc2RiGO0seBx38Zrkqrf44NYcUHOQXWAZSx|FbiACHf8VyMdhxK5ugYZKg/ha7EWhWl7fjuQEoJmuXixefeg9//er7CV2Q|P|HNndQKKg==

[56] Bureau of Criminalistics and Forensic Studies. "Renewal and update service of forensic software licenses UFEC Touch to UFED 4PC." File No. 37/105-0422-CDI20. March 2020 https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhyrV/4BRRj7a-9qf3aG8azk|h3K/KAn7jb/h6aPDkgsy3caJklV5dh/l98fSQHDGyecUZqnGVTQz3UXLzeKrU0hskSjg8CnHW3bp5dO0tjSzbg==

[57] Clarín. "Phone detectives: secrets of the application that opens cell phones and solves the most complex cases". November 2020. https://web.archive.org/web/20201114090956/ ; https://www.clarin.com/policiales/detectives-telephones-secrets-system-opens-cell-phones-resolves-complex-cases_0_U-0fZd2m.html

[58] Cellebrite. "Argentina's National Police Force is overcoming time and distance barriers with digital intelligence." July 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 Rios. "UFED devices, the new equipment of the Concordia Police and National Gendarmerie in Paraná." February 2019 https://www.elentrerios.com/actualidad/dispositivos-ufed-el-nuevo-equipamiento-con-elque-cuenta-la-polica-de-concordia-y-la-gendarmera-en-paraná.htm

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

[61] City of Buenos Aires. Provision No. 65/UOA/19. July 2019. https://documentosboletinoficial.buenosaires.gob.ar/publico/ck_PJ-DIS-MPF-UOA-65-19-5660.pdf

product, UFED Cloud Analyzer, in 2017, also through a direct contract with the same local provider.[62] In August 2020, the province of Santa Fe's Prosecution Office signed a direct contract with the local company IAFIS Argentina S.A. to renew four UFED Touch 2 licenses for a term of one year, and to acquire three new UFED 4PC licenses, for USD 96,226.[63]

In December 2020, the Airport Security Police engaged in a direct contract with IAFIS to update and upgrade its UFED licenses for ARS 8,057,111 (around USD 90,784), which included the renewal of two UFED 4PC Ultimate and two UFED Touch 2 Ultimate licenses[64] for a two-year period, as well as the hardware swap of two Touch I for two Touch 2 devices.[65]

At the end of 2020, the Ministry of Security began to sign cooperative agreements with more than 15 tech companies, including Cellebrite, which provided for training and information-sharing to improve the capabilities of law enforcement agencies in judicial investigations involving digital evidence.[66]

On November 3, 2020, we filed an Access to Public Information Request with the Ministry to inquire about these deals. The official response, one month later, was that "none the agreements mentioned in the request has been settled, for which there are no documents that can be disclosed to the interested party".

Human Rights Record

Although Cellebrite claims to sell its technology exclusively to governments and law enforcement agencies, the firm has been linked to customers of a shady status.[67] In 2016, the General Directorate of Anti-Corruption and

---

[62] Public Prosecutor's Office of the Province of Buenos Aires. Provision UOA N°45/2017. September 2017. https://mpfciudad.gob.ar/storage/archivos/Disposici%C3%B3n%20UOA%20N%C2%BA%2045-17%20AI%2030-00036938%20Aadjudicacion%20SECURITY%20TEAM%20NETWORK%20S.A.%20-Ufed%20Cloud-.pdf

[63] 8 Public Prosecutor's Office of the Province of Santa Fe. File No. FG-000303-2020. August 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] Airport Security Police. "Renewal of licenses and upgrade of UFED 4PC and UFED TOUCH equipment, by Exclusivity". File No. 279-0027-CDI20. November 2020. https://comprar.gob.ar/PLIEGO/VistaPreviaPliego-Ciudadano.aspx?qs=BQoBkoMoEhy3iTxQqkwwChRpn2XPxXCSk5uijJLSdq2DmF5S3IGnqIsUbG2uGBeZPrbB8BhNUcLFrujs6LrFUaU3GDH8dDYrJv/eOuj/ve1TCc-Z2AXWpaw==

[66] Argentinian Government. "Initiatives for more efficiency in criminal investigations on the digital sphere". October 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." May 2021.

Economic and Electronic Security of Bahrain, together with its Directorate of Criminal Investigations Office reportedly used Cellebrite's UFED to track and prosecute dissidents.[68] A study conducted by Israeli lawyer Eitay Mack found that the company sold forensic technology to the governments of Venezuela, Belarus, Russia, and Indonesia, known for cracking down on political dissent and persecuting members of the LGTBQI+ community.[69]

After internal documents were leaked in 2017, it was revealed that Cellebrite was also closing deals with the Turkish and UAE security forces.[70] Myanmar police also used its technology to arrest two journalists in 2019,[71] and apparently, Hong Kong police as well, to follow up and harass pro-democracy activists in 2020[72]. The Committee to Protect Journalists recently reported that the Botswana government is using Cellebrite equipment to search journalists' devices and determine their sources[73]. Some of them claim to have been victims of torture[74]. Other accounts reveal that Cellebrite tools are being sold to the governments of Nigeria, Bangladesh, Saudi Arabia, and Vietnam[75].

---

https://www.accessnow.org/what-spy-firm-cellebrite-cant-hide-from-investors/

[68] The Intercept. "Phone-Cracking Cellebrite Software Used to Prosecute Tortured Dissident." December 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." November 2020. https://www.haaretz.com/israel-news/technews/.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." April 2019. https://privacyinternational.org/longread/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." May 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." July 2020. https://www.jpost.com/israel-news/hong-kong-democracy-activists-to-israel-stop-exporting-tech-to-police-636918#/

[73] Committee to Protect Journalists, "Equipped by US, Israeli firms, pólice in Botswana search phones for sources." May 2021. Https://cpj.org/2021/05/equipped-us-israeli-firms-botswana-police/; Committee to Protect Journalists, "Botswana police use Israeli Cellebrite tech to search another journalist's phone." July 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." May 2021. https://www.accessnow.org/what-spy-firm-cellebrite-cant-hide-from-investors/; Haaretz. "What Vietnam Is Doing With Israeli Phone-hacking Tech." July 2021. https://www.haaretz.com/israel-news/tech-news/.premium-what-vietnamis-doing-withisrael-s-phone-hacking-tech-1.10003831

Human rights defenders filed a court petition urging the Israeli Ministry of Defense to stop the export of Cellebrite to Hong Kong, Russia, and Belarus[76]
.

In October 2020, the company announced the interruption of its sales to China and Hong Kong[77]. In March 2021, a similar measure was taken for Russia and Belarus[78].

Huawei and ZTE

Both Chinese firms, Huawei Technologies Co. and ZTE Corporation offer a wide range of technological solutions. In addition to cell phones and telecommunications equipment, one of the services they provide is based on technology and systems for building what are known as "smart cities". Both companies interact with local governments in Latin America to provide software devices for public safety.

In July 2020, ZTE began its sales in Argentina through the province of Jujuy. The governor, Gerardo Morales and ZTE vice president, Hua Xin Hai, together with its CEO in Argentina, Dennis Wang, reached an agreement to launch a program called "Jujuy Seguro e Interconectado" (Safe and Interconnected Jujuy), for which the province received a loan from the Hong Kong-based BBVA bank in March 2020, totaling the amount of USD 24,146,142[79]. ZTE settled for a USD 30 million deal to do its part installing cameras, monitoring centers, emergency services, and telecommunications networks[80]. According to Governor Morales, Jujuy will now be "as safe as China". We filed an Access to Information Request for more details on

[76] MIT Technology Review. "Israeli phone hacking company faces court fight over sales to Hong Kong." August 2020. https://www.technologyreview.com/2020/08/25/1007617/israeli-phone-hacking-company-faces-court-fight-oversales-to-hon g-kong/; Haaretz, "Israeli Phone-hacking Firm Cellebrite Halts Sales to Russia, Belarus in Wake of Haaretz Report." March 2021. https://www.haaretz.com/israel-news/.premium-israeli-phone-hacking-firm-cellebrite-halts-sales-to-russia-after-haaretz-report-1.9633312

[77] Cellebrite. "Cellebrite to Stop Selling Its Digital Intelligence Offerings in Hong Kong & China." October 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." March 2021. https://www.cellebrite.com/en/cellebrite-stops-selling-its-digital-intelligence-offerings-in-russian-federation-and-belarus/

[79] Argentinian Government Gazette. Decree 207/2019. March 2019. https://www.boletinoficial.gob.ar/detalleAviso/primera/203703/20190320

[80] Reuters. "'Safe like China': In Argentina, ZTE finds eager buyer for surveillance tech." July 2019. https://www.reuters.com/article/us-argentina-china-zte-insight-idUSKCN1U00ZG

November 11, 2020, but have not received any reply, despite the deadline being exceeded.

In April 2018, Alfredo Cornejo, then the governor of Mendoza, met with Huawei's sales vice president, Tony Sza[81]. The purpose of this meeting, according to media reports, was to discuss the acquisition of facial recognition technology, geolocation, and big data management for public safety. Civil society organizations, including Access Now and ADC, responded by sending a letter to the governor[82] calling to end private negotiations and open a public discussion on the matter. Unfortunately, no further information has been disclosed thereafter.

Human Rights Record

ZTE and Huawei have long been known to have worked with regimes that violate human rights. In 2013, when the advocacy group Bolo Bhi requested both companies to abstain from helping to the development of Pakistan's web censorship firewall, they chose to ignore the human rights impacts of their products and issued vague statements about prioritizing "local" laws over international human rights norms[83]. The same year, Reflets.Info reported that ZTE and Hewlett Packard were collaborating with Telecommunications Infrastructure Co. (TIC), the Iranian government's internet service provider to help limit the type of information to which the Iranian people could access[84]. In 2008, the president of Venezuela, Hugo Chavez, sent representatives from the Ministry of Justice to visit China, where they discovered that ZTE was developing a system that would help Beijing to monitor social, political, and economic behavior through the use of smart cards. Ten years later, the Venezuelan government signed a contract for USD 70 million to deploy a similar program, the "Homeland Card (Carnet de la Patria). This card is being used in campaigns to influence voting decisions[85], provide food subsidies and health care, and manage other social programs that most Venezuelans depend on for their

---

[81] Province of Mendoza website. "The Governor met with representatives of Huawei in Latin America." April 2018. https://www.mendoza.gov.ar/prensa/el-gobernador-se-reunio-con-representantes-de-huawei-en-latinoamerica/

[82] ADC. "Fundamental rights advocates call on Mendoza government to halt purchase of mass surveillance technology." July 2018. https://adc.org.ar/2018/07/13/defensores-de-derechos-fundamentales-piden-algobierno-de-mendoza-que-denga-denga-la-compra-de-tecnologia-de-vigilancia-masiva/

[83] Access Now. "Broken promises: Pakistan announces plans to launch censorship firewall, possibly with Chinese tech." January 2013. https://www.accessnow.org/broken-promises-pakistan-announces-plans-to-launch-censorship-firewall-poss/

[84] Reflets.info. "ZTE and HP team up for a Halal internet in the land of mullahs" (in French). June 2013. https://reflets.info/articles/zte-et-hp-unis-pour-un-halalternet-au-pays-des-mollahs

[85] BBC News. "Venezuela elections: what are red dots and why Henri Falcón accuses Maduro of 'vote buying'." May 2018. https://www.bbc.com/mundo/noticias-america-latina-44192915

subsistence[86]. This system called the attention of citizens and human rights activists and organizations because of the obvious risk it posed of government abuse, invasion of privacy, and community control. After its implementation, the database was hacked[87] and in 2018, the government used the data stored in the cards to identify people who had not voted. It also made the cards mandatory to access the benefits offered by the Government and to purchase fuel at subsidized prices.

Huawei has also been under media scrutiny in recent years. In 2019, an investigation[88] by The Wall Street Journal showed that the company's technical staff had assisted the Ugandan and Zambian governments in spying on their political dissidents in at least two opportunities, which included the interception of their encrypted communications and social media exchanges, plus using cell phone data to track their whereabouts.

In June 2020, a Reuters investigation noted that Huawei sold at least EUR 1.3 million worth of Hewlett-Packard computers seized from the Iranian government and went to great lengths to hide it[89]. In December the same year, IPVM found a "confidential" document available to the public on Huawei's European website, shortly removed afterward. This document explained that Huawei had tested facial recognition software that could send automated "alerts" to Chinese government authorities when their camera systems identified members of the oppressed Uighur minority group[90]. These troubling cases prompted Sweden to ban Huawei and ZTE telecommunications equipment on its 5G network[91]. Other European countries have followed suit or currently contemplate doing so.

NEC

NEC is a major global player in the digital biometric identification industry. With a staff of over 110,000, this 122-year-old Japanese technology giant (listed on the Tokyo Stock Exchange) appears as the immediate choice for

[86] Reuters. "How ZTE is helping Venezuela implement Chinese-style social control." November 2018. https://www.reuters.com/investigates/special-report/venezuela-zte-es/
[87] AlbertoRodNews Twitter account. https://twitter.com/AlbertoRodNews/status/1070733400372326401
[88] The Wall Street Journal. “Huawei Technicians Helped African Governments Spy on Political Opponents.” August 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.” June 2020. https://www.reuters.com/article/us-huawei-iran-probe-exclusive-idUSKBN23A19B
[90] IPVM. “Huawei / Megvii Uyghur Alarms.” December 2020. https://ipvm.com/reports/huawei-megvii-uygur
[91] Reuters. “Sweden bans Huawei, ZTE from upcoming 5G networks.” October 2020. https://www.reuters.com/article/sweden-huawei-int-idUSKBN2750WA

many government agencies around the world[92]. It has been developing biometric technology, such as facial, iris, fingerprint, finger vein, and voice recognition for more than 50 years and has sold to 70 jurisdictions[93]. NEC's equipment forms the backbone of the world's largest biometric system, India's Aadhaar, holding data of 1.3 billion people[94]. In the U.S., more than one-third of law enforcement agencies and state police[95], as well as the facial recognition in airports introduced by U.S. Customs and Border Protection (CBP)[96], are using NEC biometric software since 2019.

The company's products have also made their way into sports stadiums in Colombia[97] and Taiwan[98]. NEC's presence in Latin America is growing as more local governments embrace the "smart city" rhetoric.

NEC started its operations in Argentina in 1978 to conduct business through its local subsidiary in the country and the region. In 2004, the company chose NEC Argentina S.A. as its Regional Software Development Center for the Latin American market[99]. Since 2006, NEC has been the official supplier of biometric systems to the National Interior Ministry and the National Registry of Persons (RNE). Through this technology, RENAPER has expanded the use of its biometric database to other public agencies, such as the Migration Office, the National Recidivism Registry, and the National Ministry of Security, among others, as a consequence of the expansion of the Federal Biometric Identification System for Security (SIBIOS). In 2017, the National Bureau of Migration (DNM) signed a contract with NEC to implement automated passport control, commonly referred to as "eGates," at Argentina's international airports for USD 3,309,318[100]. The official procurement document states that NEC was chosen because the agency

---

[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." November 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." February 2020 https://onezero.medium.com/nec-is-the-most-important-facial-recognition-company-youve-never heardof-12381d530510
[96] EFF. "Skip the Surveillance By Opting Out of Face Recognition At Airports." April 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." October 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." November 2017. https://findbiometrics.com/nec-facial-recognition-sports-stadium-taipei-411022/
[99] NEC. History. https://ar.nec.com/es_AR/about/history/index.html
[100] General Administration Bureau. "Provision of self-service migratory tool." File No. 21-0028-CDI17. September 2017. https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQo-BkoMoEhxKmqLqu e6kMW1chJuEHzB2LvnmYI6tmgdCyJ7Ep7d490YZKW8ptaXbZVpysEhjsnNcElgEeF4JDcgYQh 41LgX8fcn98cZ8e12qM5BlL50fqw==

had already been using its AFIS system[101] and NeoFace[102] products for fingerprint and facial recognition, respectively.

EGates were first implemented and used in 2018 at Ezeiza Airport, and then extended to Jorge Newbery Airport and the seaport, both in the City of Buenos Aires[103]. Border control uses these automated checkpoints to replace human interaction, applying fingerprint and face verification software to match the biometric information of all people moving in or out of the country with the data stored in the RENAPER database. In 2019, the DNM engaged in another contract with NEC for a biometric system to identify people registered on a watch list (e.g., persons with travel restrictions, wanted by INTERPOL, etc.), for a total of ARS 145,189,000 (approximately USD 3 million at the time)[104]. The request specified that the system should be compatible with RENAPER's AFIS to run both identification and verification queries.

Between 2017 and 2020, RENAPER signed multiple contracts with NEC to improve, upgrade and expand its biometric software[105].

In December 2017, RENAPER and what was at the time the Secretariat of Modernization (currently, the Secretariat of Public Innovation, under the National Chief of Cabinet) signed a cooperation agreement to develop a national Digital Identity System (SID)[106], which makes use of facial recognition to validate the identity of individuals when accessing certain state and private services implemented by its Application Programming Interface (API) or Software Development Kit (SDK). The SID was first launched in a pilot phase to test its use in some fintech companies for their

---

[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] Ministry of Interior. "The National Government implements biometric gates at Ezeiza airport". April 2018. http://www.migraciones.gov.ar/accesible/novedad.php?i=4019

[104] General Admistration Bureau. "Tool for Foreigner Identification and Biometric Border Control." File No. 21-0002-LPU19. February 2019. https://comprar.gob.ar/PLIEGO/PreviewPreviewCitizenBid.aspx?qs?qs=BQoBkoMoEhwfHNl0dYheEGyNBwGGvH3GL6jBhnOAiv5hg9nZ3JQi1tBQTuogGzD12zCv6XuNwuBmJTvQzJWApOOrz69pEW2MV9graYTQBzR11CtszG5T6w==

[105] Procurement Department. "Contracting of services, licenses and products related to RENAPER biometric platform". October 2017. File No. 78-0012-CDI17. https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhy7MmMdVUat6QKfRigU80UVxJmyaLvy67Tv2OgtO1qNBgGmFkKWbfpTnnfNopxo|oaRtWe20G7DjI-P49UkgkEP896PfIoNb393/NEPZ2M5G7w==

Procurement Department. "Tool for centralized terminal license management." File No. 78-0022-CDI18. September 2018. https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBko-MoEhzln331uwbedtWpuhJRVlkYFu5E0d6zTuIWgkUVrzCpo|kMsAHgU/dYCpNuyBnX9eXEW4riZstvHDV2ZqhmqPbCKquiSivEogUdA1HkMNIlaA==; Procurement Department. "RENAPER biometric platform expansion and update." File No. 78-0028-CDI18. December 2018.

[106] Ministry of Interior. "SID: Digital Identity System". https://www.argentina.gob.ar/interior/renaper/sid-sistema-de-identidad-digital

bank account onboarding processes[107]. The facial recognition of the SID is NeoFace Watch, purchased with a loan from the World Bank of USD 834,403.

Argentina's Digital Identity System is being expanded to cover multiple use cases, in addition to systems for services and government fintech. In July 2020, the National Interior Ministry signed a cooperation agreement with the National Ministry of Education to implement the system in national universities to have students validate their identities before taking online exams[108]. This expansion is occurring despite concerns about flaws in its facial recognition algorithms[109] and is likely to become the primary way of validating identity, which in turn may lead to discrimination and preventing people who are not registered or correctly identified from accessing public services. The government has minimized this threat, arguing that the facial recognition algorithm is configured under NEC's false positive and false negative rates[110].

Locally, NEC has developed a close relationship with the Government of Tigre, a town in the Province of Buenos Aires. Tigre has been using the company's technology for its entire urban surveillance program since at least 2016, starting with CCTV, automated license plate reading (ALPR), and facial recognition using NeoFace Watch[111]. In 2019, the town remodeled its surveillance infrastructure[112] by launching NeoCenter, developed by NEC to boost its existing capabilities[113]. In addition to the aforementioned features, facial recognition software was upgraded to track people more accurately in public spaces, recording movement paths to locate where someone has been (their travel history) and identify "suspicious behavior" by examining people and vehicles' movements. Tigre further expanded its surveillance technology in 2020 with the installation of a totem cam for facial recognition [114]. When the launch was announced, ADC filed an Access to Public

---

[107] "Fintech" or financial technology refers to new businesses that develop financial services using digital technologies at the core of their products and services.
[108] Ministry of Education. "New system for identity validation of university students." July 2020. https://www.argentina.gob.ar/noticias/nuevo-sistema-para-la-validacion-de-la-identidad-de-estudiantes-universitarios
[109] La Nación. "'I don't like your face": Do apps discriminate?" September 2019. https://www.lanacion.com.ar/tecnologia/no-me-gusta-tu-cara-discriminan-aplicaciones-nid2292711/
[110] ADC. "Your Digital Self: Uncovering Identity and Biometric Narratives in Latin America." April 2019. https://adc.org.ar/informes/tu-yo-digital-descubriendo-las-narrativas-sobre-identidad-y-biometria-en-america-latina/
[111] NEC Corporation YouTube Channel. "The City of Tigre." September 2016. https://www.youtube.com/watch?v=5Lp9PWv0EQ0
[112] City of Tigre. "The Tiger's Eye." https://www.tigre.gob.ar/seguridad/cot
[113] Ámbito. "Tigre launches new facial recognition system". May 2019. https://www.ambito.com/municipios/municipios/tigre-lanzo-un-nuevo-sistema-reconocimiento-facial-n5030978
[114] City of Tigre. New security totem with facial recognition camera in El Talar."

Information Request[115] to inquire on the way this technology was being deployed and its results. The local government delayed the process and in the end, avoided any response, even after several follow-up notices, proving its lack of transparency and accountability.

Tigre's ties with NEC have been so close that the company uses the town as a marketing case study, displaying the solutions it provides, including technology for citizen collaboration in public safety, license plate analysis, facial recognition, behavior detection, crime mapping, and evidence collection, and machine learning technology for data analysis. NEC claims that Tigre is becoming "a model safe city for Latin America. "[116]

IDEMIA

Formerly known as "Morpho Safran" and "Safran Identity and Security ",[117] the French company IDEMIA is one of the world's leading providers of biometric technology.

In the U.S. alone, it furnishes solutions for the FBI[118], INTERPOL[119], the New York Police Department[120], and the U.S. Transportation Security Administration, among others.

In our research for this report, we were unable to find any recent connections between the governments of Argentina, Brazil, or Ecuador and the company under the IDEMIA brand. IDEMIA has an office in Buenos

---

September 2020. http://www.tigre.gov.ar/novedades/detalle/1267

[115] ADC Twitter account. 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." September 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." April 2011. http://web.archive.org/web/20150607084516/http://www.morpho.com/actualites-et-evenements/presse/morphotrak-technology-goes-operational-forthe-fbi?lang=en

[119] Morpho. "Sagem Sécurité to provide Interpol and its 186 member states with latest AFIS, Automated Fingerprint Identification System." February 2008. http://web.archive.org/web/20150607090048/ ; http://www.morpho.com/newsevents-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." November 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." September 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

Aires, Argentina, but focuses on the mobile supplying market. While it is unclear when the Argentinean authorities first procured IDEMIA's equipment, law enforcement began using Morpho products before 2010[121]. The use of this technology spread rapidly with the introduction and growth of SIBIOS, a massive state-run biometric database.

As noted above, the use of Morpho products in Argentina is closely related to SIBIOS. The National Ministry of Security and the Federal Police both employ them. In 2014 and 2015, the Ministry allocated more than USD 7 million to contracts with Morpho S.A. to

purchase biometric technology[122]. The Federal Police makes use of Morpho RapID devices to carry out fingerprint identification[123], as well as Morpho Face Detective for facial recognition to identify people in crowds[124].

Since the Federal Police has nationwide jurisdiction, the use of Morpho has extended throughout the country, in cities such as Campana[125], Luján[126], Balcarce[127], Córdoba[128], Chaco[129], and a number of towns in the Province of

---

[121] Zona Norte. "The Morpho Touch security system is already applied in Tigre." August 2008. https://www.zonanortediario.com.ar/05/08/2008/el-sistema-deseguridad-morpho-touch-ya-se-aplica-en-tigre/

[122] Argentinian Federal Police, Administration Superintendence, Procurement Department, Direct Contract N° 25/2014, File N°581-01-000726-14: Argentinian Federal Police, Administration Superintendence, Procurement Department, Direct Contract N° 25/2014, File N°26/2014, File N° 581-01-000640-14. https://www.boletinoficial.gob.ar/detalleAviso/tercera/2134792/20150119 File Nº550-01-001003-2014y 563-01-001091-2014 https://www.boletinoficial.gob.ar/detalleAviso/tercera/2125517/20141024 File Nº581-01-000726/2014 and 563-01-001090/2014. https://www.boletinoficial.gob.ar/detalleAviso/tercera/2125518/20141024

[123] The Ministry's official Twitter account publicized its use in 2018. https://web.archive.org/web/20201230202624/https://twitter.com/MinSeg/status/1038127257401810944?s=20; https://web.archive.org/web/20201230202648/https://twitter.com/minseg/status/1033045304638156803; and https://www.argentina.gob.ar/noticias/gdetuvimos-en-retiro-un-hombre-que-ten%C3%ADa-pedido-de-captura

[124] Federal Police Official Twitter account, showing the use of Morpho Face Detective at Retiro train station. January 2019: https://web.archive.org/web/20201230203110/https://twitter.com/PFAOficial/status/1090673247161597952?s=20

[125] La Auténtica Defensa. "The Morpho Rapid system is already applied in Campana." March 2009. www.laautenticadefensa.net/62085

[126] El Civismo. "Modern equipo for personal identification". September 2010. https://www.elcivismo.com.ar/notas/7191/

[127] La Vanguardia. "Breaking News: Federal Police operation in Balcarce". February 2019. http://www.diariolavanguardia.com/noticias/21448--cobramos-porlo-que-trabajamos--no-le-robamos-la-plata-a-nadie-/

[128] La Voz. "'Cañete', Cordoba's most wanted fugitive, is recaptured." May 2017. https://www.lavoz.com.ar/sucesos/recapturaron-canete-el-profugo-cordobes-mas-buscado

[129] Chaco Police Department. "The police train and test a new identification system." March 2013. https://web.archive.org/web/20201230210055/ and http://policia.chaco.gov.ar/index.php/ecmPagesView/view/id/101

Buenos Aires[130]. Government agencies deal with a major retailer of IDEMIA equipment, known as IAFIS Argentina S.A., which happens to be the same firm selling Cellebrite's products. AFIS mentions multiple police forces in several Argentine provinces as its clients[131], as well as public prosecutors' offices and other public institutions, although it does not specify which products are supplied to them.

The City of Buenos Aires acquired Morpho Face Investigate software from IAFIS Argentina S.A. in 2011 for ARS 33,198,500 (more than USD 6 million at the time) and began testing its operation in subways to identify pickpockets [132]. According to official procurement and public bidding documents, the City uses Morpho's fingerprint and facial recognition technology in judicial investigations. IAFIS has been providing them with technical support since at least 2015, with different contracts that add up to over USD 6.5 million[133].

Human Rights Record

In 2017, Morpho (which later became IDEMIA) was denounced for flaws in the registration and biometric authentication kits used in Kenya's general elections, which led to the National Assembly canceling its public contracts and banning new ones. The resolution was challenged and overturned by the High Court of Kenya[134]. The opposition coalition accused the firm of complicity in electoral fraud, but the company denied these charges. Safran, IDEMIA's forerunner before the merge, was also fined by the French court for paying bribes to secure business in Nigeria[135].

---

[130] Primera Plana. "Federal Police enters the interior of Buenos Aires with control and prevention operations." May 2019.
http://primeraplana.com.ar/policia-federal-desembarca-en-el-interior-bonaerense-conoperativos-de-control-y-prevencion/

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

[132] Infobae. "Facial identification software evaluated to spot pickpockets in subway." January 2013.
https://www.infobae.com/2013/01/13/691102-evaluan-un-software-identificacion-facial-ubicar-pungas-el-subte/

[133] Buenos Aires Purchases. Purchase process number: 2900-1047-CDI15
https://www.buenosairescompras.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhzAdZmPYqqZ4su3ScBBrBvMPHSPHPxZ74bjkpi4POk3iZKynCGKbKt|RDsvNlcW1mJISgBUffWWWFY1vgdwt/W5yzl3PnouupiCeVWiQuysmvw==
Purchase process number: 2900-0858-CDI17.
https://www.buenosairescompras.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhzjp0DPq1u2nl3iH|4rzqLn9Phu5zQ6mkLN3u849mLkhWIq/6PJyo37gtSRaUyG3uJLK1ZE-2CoQE3RKSJHwBng31I/q82/vv9su9cJDc2PG2g==

[134] Biometric Update. "Biometrics in Africa this week: Idemia suspension in Kenya overturned, local solutions sought for cybercrime." April 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." September 2012.
https://www.bbc.com/news/business-19498916

In September 2020, Amnesty International discovered that three European companies, IDEMIA among them, sold surveillance technology to the Chinese government[136]. Specifically, IDEMIA was given a contract to provide facial recognition software directly to the Shanghai Public Security Bureau in 2015. Due to the risk that Chinese authorities would use the equipment for mass surveillance and other human rights abuses, Amnesty International, Access Now, and other organizations, as well as European countries, called on the European Union to strengthen human rights safeguards in surveillance and ensure that all relevant companies carry out human rights impact assessments[137]. France, where IDEMIA's headquarters are located, opposed this request[138].

Other Firms

As mentioned above, the companies listed in this section are those on which most information could be obtained and who have the closest ties with government agencies. However, others deserve a mention, due to their participation in different initiatives where surveillance technologies were purchased and deployed.

BGH Tech Partner

Boris Garfunkel and Sons, or BGH, is an Argentinean company that markets a wide variety of products but over the last decade has specialized in the development of technological solutions. The company is responsible for the equipment of San Juan province's Laboratory of Forensic Video Analysis[139].

BGH claims to provide only encrypted communications and location mapping services to law enforcement agencies, but according to media reports[140] the lab will soon be equipped with facial recognition software for identifying people and detecting and classifying objects, attributes, and

---

[136] Amnesty International. "EU companies selling surveillance tools to China's human rights abusers." September 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." November 2020. https://www.accessnow.org/urgentcall-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." October 2018. https://netzpolitik.org/2018/surveillance-exports-how-eu-member-states-are-compromising-new-human-rights-standards/

[139] BGH. "San Juan implements state-of-the-art communications technology for provincial police." September 2020. https://www.bghtechpartner.com/2020/09/11/san-juan-implementa-tecnologia-de-comunicacionesde-ultima-generacion-para-la-policia-provincial/

[140] San Juan Government Information Service. "San Juan Accord: technology applied to safety". October 2020. https://sisanjuan.gob.ar/seguridad/2020-10-22/26837-acuerdo-san-juan-tecnologia-aplicada-a-la-seguridad

behaviors, as well as vehicle license plate reading. We have sought further information on BGH's products, both from the government and from the company itself, but have so far been unsuccessful. It seems plausible that its technology is provided by Hikvision, given that BGH began retailing this company's products in 2018[141]. The solutions now offered by BGH include thermal, in-vehicle, wearable, and facial recognition cameras, as well as drones and robots[142].

Danaide S.A. and NTechLab

According to independent reports[143], the Argentinean company Danaide, hired by the City of Buenos Aires to install facial recognition in public spaces [144], may be using Find Face[145] software developed by Russian company NTechLab. Despite our numerous attempts to get more information through filing Access to Information Requests, the government only confirms that Danaide won the contract bid, refusing to reply whether the company itself had developed the facial recognition algorithm.

On the Russian version of the NTechLab's website[146], Danaide's UltraIP software[147], sold in Argentina, is listed in the section referring to partners. In response to ADC's Access to Information Request[148] in June 2019, authorities of the City of Buenos Aires confirmed that UltraIP is the name of the software being licensed.

In October 2020, Human Rights Watch alerted on flaws in NTechLab's system and its misuse by the government to identify and target children for criminal prosecution, which is a clear violation of human rights[149]. In Moscow, NTechLab provides the software for a surveillance program that

---

[141] BGH. "BGH Tech Partner adds Hikvision to its portfolio." February 2018. https://www.bghtechpartner.com/2018/02/02/bgh-tech-partner-suma-hikvision-su-portfolio/
[142] AR Channel. "BGH boosts its video surveillance portfolio with Hikvision." January 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." March 2020. https://onezero.medium.com/the-u-s-fears-live-facial-recognition-in-buenos-aires-its-a-fact-of-life-52019eff454d
[144] ADC. "#ConMiCaraNo (Not-With-My-Face): Facial recognition in the City of Buenos Aires." May 2019. https://adc.org.ar/2019/05/23/con-mi-cara-no-reconocimiento-facial-en-la-ciudad-de-buenos-aires/
[145] NTechLab. Find Face official website. https://findface.pro/en/
[146] NTechLab. Partners (in Russian). https://web.archive.org/web/20200511205745/ ; https:/findface.pro/partners/
[147] Danaide. Software developments. https://danaide.com.ar/desarrollos/desarrollossoftware.html
[148] ADC. Request for access to information No.2019-21065074-GCABA-DGAYCSE. July 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." October 2020. https://www.hrw.org/news/2020/10/09/argentina-child-suspects-private-data-published-online

the government has abused, according to human rights organizations, by spying on people during the COVID-19 pandemic to enforce confinement[150].

IBM

In December 2016, the National Ministry of Security signed a contract with local company Unitech S.A., described as the acquisition of "advanced software for criminal investigations," for the amount of USD 3,515,518.77[151]. In the procurement documents, the technical specifications indicate that the products and services included: nine IBM i2 Enterprise Insight Analysis licenses[152], an IBM i2 Collaborate add-on, IBM i2 Text chart, and multiple technical support services.

There is a history of IBM technology being used in the Philippines during the violent "war on drugs". According to a 2009 investigation led by Human Rights Watch[153], there is evidence that government authorities and police were in collusion with death squads murdering street children, drug dealers, and petty criminals during Rodrigo Duterte's term as mayor of Davao. In 2012, IBM agreed with Sara Duterte, daughter of Rodrigo and mayor of the city at the time, to upgrade the Davao police command center and "improve public safety operations in the city" as violence on the streets continued. According to a report by The Intercept[154], IBM refused to answer queries about its human rights record in Davao City.

IBM spokesperson Edward Barbini briefly noted that the company "no longer provides technology to the Davao Intelligence Operations Center, and has not done so since 2012," without mention to whether technical support on the existing equipment continued. The company's public records state it as an ongoing program after that date.

---

[150] Reuters. “Russia’s lockdown surveillance measures need regulating, rights groups say.” April 2020. https://uk.reuters.com/article/uk-health-coronavirus-russia-facial-reco-idUKKCN2253CG

[151] General Administration Bureau. "Acquisition of advanced software licenses for criminal anlaysis with firm Unitech S.A.” File Nº347-0066-CDI16. December 2016. https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhxZRJeGCUUs0CDTFEc5IK6J-8mooLYATqqyEzFwVde9PPWAMiJ0jPJGKn6pHkBSQAUfnO3onZZEr5bCGawx17Ios-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.” April 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.” March 2019. https://theintercept.com/2019/03/20/rodrigo-duterte-ibm-surveillance/

Nubicom and Datandhome Supplier SA

In 2018 and 2019, the government of Salta agreed to install facial recognition devices[155] as part of the update of their plan called "Salta Inteligente" (Intelligent Salta), which consisted of deploying over 1400 cameras throughout the provincial territory, some of them with facial recognition capabilities. Although the initiative was to be launched in 2018, there have been claims against the providing companies for not complying with the agreement[156].

Until 2019, the company Datandhome Supplier SA dealt with Salta's video surveillance equipment and software, allegedly with facial recognition, while Nubicom SRL was in charge of the system connectivity service. In 2019, the province terminated the agreement with Datandhome for "serious non-compliances"[157] and signed a direct contract with Nubicom, who thus became responsible for both, the maintenance and technical support of the cameras and software, as well as the connectivity[158].

Nubicom is a tech solutions company from Salta and one of the main telecommunications companies in that province, as well as in Catamarca and Jujuy. In addition to connectivity and software for its video surveillance system, it is also the main Internet service provider in Salta and has a section dedicated to government services, including video surveillance with facial recognition, among others[159]. Although no official information could be obtained on the subject, journalistic sources claim that the company earns nearly U$D 400.000 from these types of contracts[160].

As part of our investigation, we filed an Access to Information Request to the province of Salta, including questions about the implementation of these technologies, its suppliers, and the procurement processes. As of November 2021, no response has been given yet.

---

[155] Salta advances in the development of Smart Government with state-of-the-art citizen security.
[156] Law cases and irregularities: the story of the company that installed cameras in Salta. March 2020 https://www.quepasasalta.com.ar/nota/231354-juicios-e-irregularidades-el-historial-de-la-empresa-que-instalo-las-camaras-en-salta/
[157] Why DatandHome's contract was terminated and who is Nubicom. March 2020 https://informatesalta.com.ar/contenido/225500/el-porque-de-la-rescision-del-contrato-a-datandhome-y-quien-es-nubicom
[158] Ibidem
[159] Nubicom official website. https://www.nubicom.com.ar/servicios/nubigob/
[160] The camera system costs more than 400 thousand dollars per month. https://www.eltribuno.com/salta/nota/2021-5-9-1-45-0-el-sistema-de-camaras-cuesta-mas-de-440-mil-dolares-por-mes

Conclusion and recommendations for improving business and human rights standards and practices

The research done for this study is a first approach to the surveillance initiatives that are being implemented in Argentina, and how the public and private sectors link to one another in their deployment. The fact that governments are compelled to rely on companies for their development, as well as the inherent risks posed by these technologies, should lead us to reformulate the appropriate procurement processes and the terms of the agreements, to avoid abuses and human rights violations. Shared efforts should be made in the search for more transparent procedures, respectful of people's fundamental rights.

To this end, the mechanisms provided by the global business and human rights framework are a starting point to be considered for the design of safeguards for the industry. Namely, the 'Guiding Principles on Business and Human Rights (UNGPs)[161] adopted by the UN in 2011, the Guidelines for Multinational Enterprises (LDEM) of the OECD (Organization for Economic Co-operation and Development)[162], and the Tripartite Declaration of Principles Concerning Multinational Enterprises and Social Policy (MNE Declaration) of the International Labor Organization (ILO)[163] are the main instruments that should guide governments and companies in their behavior.

The UNGPs establish three fundamental pillars: the duty of governments to protect human rights, of companies to respect them, and a joint commitment to remedy any harm they may cause.

Below, we mention some of the guidelines to be considered when drawing up an adequate regulation of public-private agreements:

- **Transparency**

Transparency is crucial for the adequate protection of human rights. In government contracting, and more specifically, public-private partnerships for the deployment of surveillance equipment, the requirement should be even greater.

Indeed, it is the opposite: the procurement processes are characterized by a considerable lack of transparency. Companies have an interest in preserving the secrecy of their systems' development and algorithms, while governments make little effort to look into and provide the details of the

[161] Guiding Principles on Business and Human Rights, UN, 2011. https://. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf
[162] Available at http://mneguidelines.oecd.org/guidelines/
[163] Available at https://www.ilo.org/empent/Publications/WCMS_094386/lang--en/index.htm

contracts. Thus, it is key that contracts be made public, both at the bidding stage and on their signature and subsequent execution.

In Argentina, despite the various regulations aimed at transparency[164], it was arduous to obtain information on the contracts under scrutiny for this report and the supplier companies, to say the least. Our investigation has proven that publicly available information is scarce, and the use of Access to Public Information Requests has been of little help. Governments exploit the exceptions provided by the laws as an excuse for not giving details of these transactions, or may even choose not to respond at all. In short, companies and governments are generally reluctant to explain the scope of these technologies and how they were developed.

Adequate control requires that information on government procurement be public and easily accessible to any interested party. Exceptions to this for reasons of security or trade secrets should be extremely occasional and based on explicitly stated grounds. In this regard, the Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights has stated that ''on applying a restriction to the right of access to public information, not only the requirements of legality and a legitimate end must be present, but also those of necessity and proportionality. The necessity of the measure is met when the limitation is not only conducive to achieving the desired goal but also compelling''[165], i.e., the alternative that least restricts the right to access information must be chosen. Even in such exceptional cases, consideration should be given to the possibility that the information be disclosed in a safeguarded environment, such as before a judge, to determine whether secrecy is justified.

- **Due Diligence**

The development of surveillance technologies, as well as their use by governments, presents inherent risks to human rights. Companies must therefore act with human rights due diligence.

Due diligence should be understood as ''an ongoing process of management that a sound and prudent company should undertake, considering circumstances such as the field and context in which it operates, as well as its size and other factors, so as to address its

[164] In Argentina, the right of access to public information is stated by Law 27,275, enacted by the National Congress in 2016. Available at https://www.boletinoficial.gob.ar/#!DetalleNorma/151503/20160929

[165] ''Right to Information and National Security''. Office of the Special Rapporteur for Freedom of Expression, 2020. Available at https://www.oas.org/es/cidh/expresion/informes/DerechoInformacionSeguridadNacional.pdf

responsibility to respect human rights."[166] In turn, the UNGPs establish that both, companies and governments must conduct human rights due diligence to identify, prevent, mitigate and account for possible negative impacts, while also tackling them should they occur. Even in cases where these harmful effects cannot be avoided, due diligence should enable companies to "mitigate, prevent recurrence and, where appropriate, remediate" as set out in the OECD Due Diligence Guidance for Responsible Business Conduct[167]. In addition, companies need to expressly state their commitment to respect human rights and how they will do so through publicly available instruments.

In public-private partnerships for the deployment of technologies that may have effects on human rights, the development, procurement, and execution processes should conduct due diligence to envisage, avoid and/or mitigate any disadvantageous effect of their use. Specifically, possible repercussions on the right to privacy should be evaluated, since "in addition to its direct connection with the tech industry as a result of the increasing use of personal data, privacy is a right that eases the exercise of other human rights"[168]. To this end, they should ensure that adequate impact assessments have been conducted. By requiring companies to adhere to human rights due diligence principles, governments can also ensure that surveillance equipment is properly assessed in its design and development and not solely in its installation. This is particularly true in the case of public-private partnerships for in the display of such technologies, considering that their development pertains exclusively to the companies while governments perform only as a leaser with no oversight on the previous stages.

Thus, it is vital that due diligence be applied from the beginning of the process.

• Accountability and redress

Accountability and remedial or reparation mechanisms are also part of due diligence and a key ingredient of the human rights protection system, as they allow authorities to answer for their actions and victims to receive adequate reparation. Here it should be borne in mind that remedial mechanisms can be both judicial and non-judicial. The appropriate means of redress will depend on the particularities of each case, but as to the legal mechanism, corporations must collaborate with courts' actions. In

---

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

[167] Available at http://mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf

[168] How to implement human rights due diligence in technology development. ADC 2020

Argentina, so far, there have been very few judicial or administrative resolutions on personal data protection or privacy that safeguard individuals from the massive and continuous collection of biometric data and the deployment of invasive surveillance technologies.

In public-private partnerships, the traditional avenues for complaints are often ineffective, whether administrative or judicial, and even more burdensome when transnational companies are involved[169]. Government liability does not exclude that of the provider company, who should also be held accountable when the technology developed has an impact on human rights.

- **Legality**

The principle of legality states that any restriction on a fundamental right must be established by law. The Inter-American Court of Human Rights, in interpreting what should be understood as a law, explains that "the protection of human rights requires that government acts fundamentally affecting them should not be left to the discretion of public authorities, but furnished by a set of guarantees aimed at ensuring that the inviolable attributes of the individual are not affected. The most important of these guarantees must be that the restrictions to be established by law be approved by the Legislative Branches''.

Thus understood, the use of surveillance in public spaces should always be regulated by norms established by Congress, and a mere administrative resolution would not suffice, as is some of the cases scrutinized[170].

Nonetheless, the principle of legality is a necessary but not sufficient condition. In addition to being regulated by law, the use of this type of technology should be proportional and necessary. Hence, in public-private partnerships, not only is it key to comply with the principle of legality, but also to thoroughly explain the necessity and proportionality of the technologies used. To this end, a human rights impact analysis is essential to identify the situations in which these rights may be infringed.

[169] OHCHR Accountability and Redress Mechanisms Project (ARP I) OHCHR: Enhancing the effectiveness of judicial mechanisms in cases of corporate human rights abuses.
[170] See case of Facial Recognition in the City of Buenos Aires at https://www.lanacion.com.ar/tecnologia/es-inconstitucional-reconocimiento-facial-porteno-nid2307648/

adc.org.ar