accessnow.org

Surveillance Tech in Latin America

Made Abroad, Deployed at Home

Access Now defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions, and convenings such as RightsCon, we fight for human rights in the digital age.

This paper was last updated on August 10, 2021

This paper is an Access Now publication. It is written by Gaspar Pisanu and Verónica Arroyo from Access Now, Leandro Ucciferri and Eduardo Ferreyra from Asociación por los Derechos Civiles (Argentina), Thiago Moraes, José Renato Laranjeira, Eduarda Costa Almeida, Fernando Fellows Dourado, Carolina Reis, and Felipe Rocha da Silva from Laboratório de Políticas Públicas e Internet (Brazil), and Jonathan Finlay and Anais Córdova-Páez from LaLibre.net (Ecuador). We would like to thank the Access Now team members who provided support, including Ángela Alarcón, Hinako Sugiyama, Isedua Oribhabor, Juliana Castro, Sage Cheng, Marwa Fatafta, Daniel Leufer, Estelle Massé, Peter Micek, Natalia Krapiva, Javier Pallero, Gustaf Bjorksten, Raman Jit Singh Chima, Leanna Garfield, and Donna Wentworth. We would also like to thank all the journalists, researchers and activists that helped us provide key insight and information for this publication. We look forward to receiving feedback and further inputs from experts in digital rights, surveillance, and privacy.

Access Now (https://www.accessnow.org) defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions, and convenings such as RightsCon, we fight for human rights in the digital age.

August 2021

For more information you may contact:
Gaspar Pisanu
(gaspar@accessnow.org)
Verónica Arroyo
(veronica@accessnow.org)
Ángela Alarcón
(angela@accessnow.org)

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Swipe left, swipe right, like, share, repeat. We are increasingly aware of the impact digital technology has on our rights. Lawmakers around the world are turning their attention to companies like Google, Facebook, Amazon, Microsoft, and Apple, and in many cases they are developing new laws and policies to regulate these gatekeepers of fundamental rights. But other companies are flying under the radar, selling surveillance technology that is deployed across Latin America without sufficient transparency or public scrutiny. This is eroding democratic processes, stripping us of privacy, and undermining freedom of speech and other basic human rights.

We often hear public officials frame the acquisition and use of surveillance tools like facial recognition as a technological advancement and a positive measure to "fight crime." Yet tools to identify, single out, and track us everywhere we go are **inherently incompatible with our human rights and civil liberties**. In addition, research shows that systems for facial recognition and other ways to identify people remotely by their physical characteristics — or "biometrics" — are often deeply flawed, racially biased, and discriminatory. That is why there is a growing movement around the world to ban use of AI for mass biometric surveillance.[1]

Unfortunately, many Latin American governments are moving in the opposite direction, eagerly purchasing this technology and ramping up the implementation of mass biometric surveillance.[2] Notably, as we reveal in this report, most of the surveillance technology deployed in Latin America is acquired from Asia (Israel, China, and Japan), Europe (U.K. and France), and the U.S., either directly or indirectly through a network of dealers. These suppliers include **AnyVision, Hikvision, Dahua, Cellebrite, Huawei, ZTE, NEC, IDEMIA,** and **VERINT**, among others.

Consider the growing biometric surveillance infrastructure in **Argentina**, **Brazil**, and **Ecuador**, the countries we highlight in this report.

In 2011, **Argentina** introduced a massive biometric database called **SIBIOS**. Over the past decade, it has become the infrastructure for many other surveillance technologies, deployed both at national and local level, from surveillance balloons in the autonomous city of Buenos Aires to facial recognition cameras in the province of Córdoba to thermal cameras in the main airports.

In **Brazil**, both the public and private sectors are using surveillance technologies, citing reasons like public safety, fraud detection, and tracking school attendance. States in the Northeast and Southeast regions, two of the most populous regions in the country, have heavily promoted use of facial recognition technologies as a measure to increase public security, without providing evidence to back these claims. The more concerning cases from a security standpoint are the surveillance technologies

[1] Access Now. "Ban Biometric Surveillance." June 2021. https://www.accessnow.org/ban-biometric-surveillance/

[2] Access Now. "Instead of banning facial recognition, some governments in Latin America want to make it official." December 2020. https://www.accessnow.org/facial-recognition-latin-america/

"donated" by private companies to local governments, sometimes used on the public as a test population.

In 2010, **Ecuador** implemented the "Integrated Security Service **ECU911**," developing a nationwide law enforcement surveillance infrastructure that currently has more than 6,600 cameras, some of which integrate facial recognition technology. In 2019, we learned the government has used this same infrastructure to spy on political adversaries and citizens the authorities intended to coerce.

Why is surveillance technology being adopted so quickly despite the threat to people's fundamental rights? The public relies on the media to be a watchdog, raising awareness when there are risks to our rights and democratic freedoms. Unfortunately, in Latin America, when the press reports and politicians address the very real and sensitive issue of violence and crime in the streets, in many cases they uncritically portray these tools as the solution to the problem. Governments face pressure from the public to find "solutions," and technology companies capitalize on this dynamic to make a profit, despite their duty to ensure their products are not used to violate human rights.

When neither government officials nor the public understands how these technologies actually work, and no one has built in or enforced the transparency and accountability necessary to protect people, **we have the perfect recipe for the continued expansion and pervasive use of these technologies.**

This report is an effort to **expose the companies behind these dangerous products and the government purchasing and deployment policies and practices that are undermining people's rights**. In many Latin American countries, the process by which authorities enter into agreements for the acquisition of surveillance technology is under-handed and opaque. Governments make deals with little or no public debate or oversight, and often with little regard for transparency laws and the duty to communicate with the public. The countries that allow the export of these surveillance products to Latin America are also culpable. Companies that fail to conduct due diligence and facilitate human rights abuse must be held accountable.

To that end, we worked with our partners at **Asociación por los Derechos Civiles (ADC)**, the **Laboratório de Políticas Públicas e Internet (LAPIN)**, and **LaLibre.net (Tecnologías Comunitarias)** to **investigate the companies supplying the technology**, examining their records on human rights. We **analyzed the impact of the technology** on the rights of people in **Argentina**, **Brazil**, and **Ecuador**, providing case examples for each country. Finally, we **prepared recommendations** for **lawmakers**, **governments**, **companies**, the **media,** and the **general public**, encouraging all stakeholders to take action.

Latin American countries have a long history of persecuting dissidents and people in marginalized communities, and authorities continue to abuse public power. The COVID-19 pandemic has now given governments a new excuse to deploy dangerous surveillance tools in the name of public safety, even as they fail to protect human rights. We hope this report spurs civil society organizations, media outlets, and citizens to **ask questions, investigate companies, and demand that their governments protect and promote human rights**. As our case studies demonstrate, the stakes could not be higher.

I. INTRODUCTION:
A COLLABORATION TO EXPOSE THE SUPPLIERS

Access Now, the Asociación por los Derechos Civiles (ADC), the Laboratório de Políticas Públicas e Internet (LAPIN), and LaLibre.net collaborated on the research for this report, which represents the final result of a comprehensive investigation done in Argentina, Brazil, and Ecuador in the last quarter of 2020.

It is well known that the national and local governments in each of these countries are increasingly implementing mass surveillance technologies. However, there is often little or no readily available information about who is providing this technology, what type of technology is being purchased, and under what conditions it is being deployed. This opacity frustrates civil society's opportunity to understand what is happening and respond appropriately. So our organizations decided to map the vendors and technologies being sold, and uncover the relationships between governments and companies. This report aims to shed light on these transactions, expose the harm to human rights, and put the companies irresponsibly selling surveillance tech in Latin America under public scrutiny.

In order to get as much information as possible, we sent freedom of information requests, reviewed news reports, and reached out to company representatives to gather information and conduct interviews. We discovered that many surveillance tech companies with poor human rights records have found in Latin American countries the perfect "techno-solutionist" clients to whom they can sell rights-harming technology without major obstacles. We also identified patterns in the relationships between governments and these companies, showing a disregard for compliance with fundamental transparency and accountability standards.[3] These and other findings allow us to conclude that in Argentina, Brazil, and Ecuador, the threat to human rights is expanding along with the growing arsenal of technologies purchased in the dark and deployed by governments with little respect for human rights. For that reason, we conclude this report with a warning that the current situation must change, and offer urgent recommendations to governments and companies.

Our research methodology comprises three stages:

1) **Investigation**: Each organization gathered information from public purchase/budget sites, official communications, news articles, responses to our freedom of information requests of specific public offices and interviews with companies representatives, journalists, and researchers.
2) **Local reports:** We prepared an explanation and analysis of the legal and political context and current state of surveillance deployment in each country.
3) **Cross analysis**: We examined the behavior and business models of each supplier selling surveillance technology (directly or through local representatives) and assessed their global human rights records.

[3] United Nations Office of the High Commissioner for Human Rights, "Guiding Principles on Business and Human Rights" June 2011. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

II. THE COMPANIES: WHO PROFITS FROM HUMAN RIGHTS VIOLATIONS?

We begin this report by focusing on the companies that supply the surveillance technologies governments are deploying in Argentina, Brazil, and Ecuador. We highlight the companies that have a significant market share in these countries or sell technology that is particularly dangerous for human rights. We provide background information on their history, the technologies they sell, and their position in these Latin American countries' markets. Finally, we review their human rights records, as a key element for understanding the dangers their products pose in Latin America. After providing detailed information on the companies, we proceed to the case studies that demonstrate the damage that is already being done to people's fundamental rights.

We obtained most of the information on the companies from official statements by public authorities and company representatives, media reports, social media, and direct interviews. In the vast majority of cases, we were not able to establish direct communication with the companies.

It is especially challenging to get information about how the technologies are being used when they were acquired through local suppliers and not directly from the manufacturers. This is another way for surveillance companies to remain in the dark and avoid public scrutiny, in addition to ignoring inquiries and failing to be communicative and transparent.

⇛ AnyVision

Company Name	**AnyVision Interactive Technologies Ltd**
Headquarters	Holon, Israel
Countries of Operation	Israel, United Kingdom, United States
Countries where its surveillance technologies are deployed among Argentina, Brazil, and Ecuador	Argentina
Founded	2015
Public / Private	Private
Major Shareholder(s)	DFJ Growth, OG Technology Partners, LightSpeed Venture Partners, Qualcomm Ventures, Bosch Building Technologies SVP [in 2020]
Number of Employees	240 in 2020
Annual Revenue	Not available

AnyVision is an Israeli company that specializes in facial recognition technology for public security, as well as applications for healthcare, casinos, and banking.[4] Only through public announcements and media coverage[5] were we able to discover that AnyVision is the company supplying the "biometric recognition software" acquired by the Province of Córdoba in **Argentina.**

AnyVision also seems to be the supplier of the software used in Ezeiza International Airport, in the Province of Buenos Aires, Argentina. From official records, we found that authorities acquired a facial recognition system through direct negotiations with a local AnyVision reseller in the country, the company **RC International**. The first direct contract between the Airport Security Police (PSA) and RC International dates to December 2017, and it was worth approximately $48,000 USD. The contract entailed the acquisition of four facial recognition licenses from AnyVision, together with four Internet Protocol (IP) cameras and one server, with the capacity to scan and compare faces against 2.5 million face records.[6] A year later, PSA signed another direct contract with RC International for around $54,000 USD, to acquire five licenses and improve the processing infrastructure.[7]

On July 17, 2020, when asked about the implementation of AnyVision's technology, RC International's Business & Strategy manager, Pablo Marcovich, confirmed[8] that the PSA had been using AnyVision's facial recognition technology in Ezeiza for two years.

AnyVision's human rights record

According to an investigation published by NBC in March 2020, Israeli authorities used AnyVision's technology in a secret surveillance scheme to monitor the movement of Palestinians in the West Bank, a project named "Google Ayosh" in reference to the technology's ability to search and find people.[9] The project won the company a top defense industry award in 2018 for "preventing hundreds of terror attacks" with the use of "large amounts of data,"[10] although it is not clear how exactly the project prevented such attacks. In addition to uncovering the classified project, NBC says[11] it has evidence that Isreali police are using AnyVision's technology to track Palestinians' movement throughout East Jerusalem.

[4] For more information, see AnyVision's website at https://www.anyvision.co/

[5] El Doce YouTube account. "The facial recognition system is already working in Córdoba" (in Spanish) November 2019. https://www.youtube.com/watch?v=xC2Y_T2KxCo

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

[7] Process number 279-0035-CDI18 https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhzSOD16bvFoRxEndMm7PHzAtBPeqYP9/qDb7KvHTHIh0obV8V5uXVQalfN9iRQ6t0NyEcvs|vrVYCJ5StXEPkNZXp61l5600xzpoafNPUDbtt6dkX1N7sUlXsW/U3fjsZr4FM|ahmgldAmKnOzjXjiP3OSXKNWySBJ/gR9toZ5IZaihRjc3OgmkchygiKgU9i4=

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

[9] Access Now. "Exposed And Exploited: Data Protection In The Middle East And North Africa." January 2021. https://www.accessnow.org/mena-data-protection-report

[10] 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

[11] 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

The technology in question is one of AnyVision's core products, "Better Tomorrow." The system uses installed facial recognition cameras and an automated watchlist alerting system to identify the faces of "suspects" in crowds, and track and categorize vehicles. AnyVision also provides facial recognition technology used at 27 Israeli military checkpoints in the West Bank to authenticate the identity of Palestinians crossing into Israel.

Notably, after years of pressure from human rights advocates, **Microsoft** divested from AnyVision.[12] In 2019, a U.S. National Institute of Standards and Technology (NIST) study[13] on racial bias in facial recognition software found that AnyVision's algorithm, like many of the other algorithms tested, performed worse on African or East Asian faces than on Eastern European faces.

⇛ Hikvision and Dahua

Company Name	**Hangzhou Hikvision Digital Technology Co Ltd**
Headquarters	Hangzhou, the People's Republic of China
Countries of Operation	Worldwide
Countries where its surveillance technologies are deployed among Argentina, Brazil, and Ecuador	Argentina, Brazil, Ecuador
Founded	2001
Public / Private	Listed on Shenzhen Stock Exchange
Major Shareholder(s)	China Electronics Technology Group Corporation (a Chinese government-owned company) (38.88%), Gong Hongjia, a director of Hikvision and venture capital investor (13.43%) [in 2019]
Number of Employees	40,403 in 2019
Annual Revenue	RMB 57.66 billion (USD $8.8 billion) in 2019

[12] The Verge. "Microsoft to end investments in facial recognition firms after AnyVision controversy." March 2020. https://www.theverge.com/2020/3/27/21197577/microsoft-facial-recognition-investing-divest-anyvision-controversy

[13] NIST. "NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software." December 2019. https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software

Company Name	**Zhejiang Dahua Technology Co., Ltd.**
Headquarters	Hangzhou, the People's Republic of China
Countries of Operation	Worldwide
Countries where its surveillance technologies are deployed among Argentina, Brazil, and Ecuador	Argentina, Brazil
Founded	2001
Public / Private	Listed on Shenzhen Stock Exchange
Major Shareholder(s)	Fu Liquan (35.97%) in 2019
Number of Employees	10,197 in 2019
Annual Revenue	RMB 26.15 billion (USD $4 billion) in 2019

Hikvision and **Zhejiang Dahua** are two of the largest surveillance equipment manufacturers. Their presence in Latin America has grown exponentially in 2020, as the companies provide various governments with technological solutions to address the COVID-19 pandemic.

According to official sources, the Ministry of Transportation of **Argentina** authorized the testing of thermal cameras from Hikvision inside the Retiro train terminal, to identify passengers with fever.[14] Authorities used the same technology, this time developed by Dahua, in Ezeiza International Airport and in public transportation, including two bus lines,[15] as well as two **Brazilian** airports: the airport at Guarulhos, in São Paulo[16] (the largest airport in South America), and the Galeão Airport in Rio de Janeiro.[17]

Dahua's presence in Argentina is not new. In 2017, Cutral-Có, an important oil producing city, deployed a comprehensive Dahua system, including a Professional Surveillance System (PSS) as the project's core, and software connected simultaneously to 256 devices, according to Dahua's press materials.[18] Our search of publicly available sources, including media coverage of the initiative, did not yield any additional details.

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

[15] Infobae. "Two bus lines installed thermal cameras to measure the temperature of the passengers" (in Spanish) May 2020.https://www.infobae.com/sociedad/2020/05/28/dos-lineas-de-colectivos-instalaron-camaras-termicas-para-medir-la-temperatura-de-los-pasajeros/

[16] Guarulhos Online. "Guarulhos Airport installs thermal cameras to measure the temperature of passengers" (in Portuguese). June 2020. https://guarulhosonline.com.br/cidade/aeroporto-de-guarulhos-instala-cameras-termicas-para-medir-a-temperatura-dos-passageiros/

[17] Vinicius Novaes. "RIOgaleão reinforces preventive measures with thermal cameras" (in Portuguese). December 2020. https://www.panrotas.com.br/aviacao/aeroportos/2020/12/riogaleao-reforca-medidas-de-prevencao-com-cameras-termicas_178330.html

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

The project in Cutral-Có entailed the deployment of 242 video cameras. Although there's no official confirmation, Dahua itself states that the implemented infrastructure provides flexibility to expand its use, for example, by using the recorded video footage with facial recognition software and tools to identify license plate numbers.

Independent tests of thermal cameras, particularly Hikvision products, show this technology to be highly inaccurate.[19] Even having your hair cover your forehead might hide your real body temperature. What's worse, when Dahua's cameras were deployed in two bus lines in Buenos Aires, the installation failed to follow industry standards (International Electrotechnical Commission standards[20]) and the use did not comply with the company's own instructions.[21]

As part of the research for this report, we submitted two freedom of information requests before the National Ministry of Transportation and its counterpart in the City of Buenos Aires, on November 3, 2020. These requests included questions about the implementation of these technologies and the city's relationship with both companies. As of August 2021, our questions were not answered.

Moreover, we made several attempts to reach out to Dahua through various channels, including via email and LinkedIn messages, to interview representatives working in the region or at their global headquarters. Once again, as of August 2021, we were still awaiting an official response from a Dahua representative. Hikvision, meanwhile, treated our request for an interview as a technical support ticket, and the request became a dead end.

The preference for these companies seems to be related to their competitive price, as some Brazilian representatives of public authorities interviewed have stated. According to an IPVM report, HikVison or Dahua products can cost up to 10 times less than some of their competitors.[22]

In Mogi Das Cruzes in Brazil, Dahua went beyond providing surveillance technology at a lower cost — **it provided it for free**. The company donated equipment in order to test its technology in the streets during the *Festa do Divino* (Feast of the Divine), deploying facial recognition cameras and monitoring equipment for vehicles, including recorders, microphones, touch screens, and even drones.[23] In São Paulo, Governor João Doria received at least R$ 8.5 million (around $1.5 million USD) as "gifts" for the City Cameras program. Donations came from several Chinese companies: **Huawei, Hikvision, Dahua,**

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

[20] International Electrotechnical Commission. "Standards development." https://www.iec.ch/standards-development

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

[22] While Axis (Sweden) cameras cost on average $372 USD, Hikvision (China) cameras cost around $37 USD. For more information, see: IPVM. "Brazil Assembly Powers Hikvision Local Expansion." July 2020. https://ipvm.com/reports/hik-brazil?code=allow

[23] Security Department. "Security for Divino's party will have face-recognition cameras" (in Portuguese) May 2019. http://www.mogidascruzes.sp.gov.br/noticia/seguranca-para-a-festa-do-divino-tera-cameras-com-reconhecimento-facial#:~:text=A%20quermesse%20da%20Festa%20do,custos%20para%20a%20administra%C3%A7%C3%A3o%20municipal

and ZTE. Through these donations, officials deployed at least 4,000 surveillance cameras. It is not clear whether they integrate facial recognition technology.[24]

The penetration of these companies in the Brazilian market has been especially notable. Hikvision is currently the only foreign video surveillance manufacturer with assembly operation in the Manaus free trade zone.[25] Moreover, according to an interview conducted with a local authority, in 2020 Hikvision supplanted the British company **Facewatch** for implementation of facial recognition technology in Campina Grande (Paraíba, Brazil).

In addition, some Brazilian companies which provide surveillance equipment have these companies as their manufacturer. A good example is the company **Intelbras**, which is a leader in Brazil for video surveillance technologies. Since 2018, it has had an agreement with Dahua, under which the latter has priority in the provision of CCTV equipment.[26]

Something similar is happening in **Ecuador**. **Full Tecnologia FullTec CIA. LTDA.** is a local company that made more than $1 million USD by selling Hikvision products to the national government and municipalities. Hikvision's sales are focused on large cities, such as Guayaquil and Quito, and surrounding municipalities, such as Nayón, Pedro Moncayo, and Daule. We also found that it sells to other cities in Ecuador, such as Quevedo, Ambato, Pelileo, Guano, Salcedo, Santa Elena, and Rumiñahui, all belonging to the decentralized circuit.[27] [28] [29] [30]

In 2019, the company **ANDEANTRADE S.A** provided the historical center for the Metropolitan District of Quito with Hikvision's video surveillance cameras with facial recognition, for more than $602,976,00 USD.[31]

Hikvision and Dahua's human rights record

[24] Bruno Ribeiro. "Chinese donations to Dória add up to R$8.5 million" (in Portuguese). July 2017. https://sao-paulo.estadao.com.br/noticias/geral,doacoes-de-chineses-a-sp-somam-r-8-5-mi,70001912058

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

[26] Intelbras social contract also states that Dahua currently owns 10% of the Brazilian company 's assets. For more information, see: Intelbras. "Draft of the Preliminary Prospect of the Public Offering of Primary and Secondary Distribution of Common Shares issued by Intelbras" (in Portuguese). 2020. https://ww69.itau.com.br/fileserver/relatorios/intelbras-sa-ind-telecom-eletro-bra-prospecto-pre.pdf

[27] Official Public Procurement System. SIE-GADMPM-020-2018. December 2018. https://www.compraspublicas.gob.ec/ProcesoContratacion/compras/PC/informacionProcesoContratacion2.cpe?idSoliCompra=BRlmsq33mpYSQbPbDK9oJTzqZSQXsCmgrOSChp_ddnA,

[28] Official Public Procurement System. SIE-GADMA-118-2018. November 2018. https://www.compraspublicas.gob.ec/ProcesoContratacion/compras/PC/informacionProcesoContratacion2.cpe?idSoliCompra=iL00ryPdwU_lpDLbghrZNhbEP-6oyJtDtUbINhNnX98,

[29] Official Public Procurement System. SIE-GADPN-02-2019N. December 2019. https://www.compraspublicas.gob.ec/ProcesoContratacion/compras/PC/informacionProcesoContratacion2.cpe?idSoliCompra=SSGg5qeThJ2cPtAXO6hZeeB7BB8WojteF3tmWYZYM2s,

[30] Official Public Procurement System. SIE-GADMQ-006-2019. December 2019. https://www.compraspublicas.gob.ec/ProcesoContratacion/compras/PC/informacionProcesoContratacion2.cpe?idSoliCompra=bCDa1cd5ztLy9wcH_d5PXToQ4JsCMfZg_iiQ1xdj-zQ,

[31] Official Public Procurement System. SIE-EMS-003-2019. August 2019. https://www.compraspublicas.gob.ec/ProcesoContratacion/compras/PC/informacionProcesoContratacion2.cpe?idSoliCompra=FcPNLZ70povlg7KbsiZ-AnBh7MrENuiMXThS2d0Y4fI,

It is essential for Hikvision and Dahua to be transparent for many reasons. As we have discussed, these companies have an extensive presence in the Latin American region, successfully selling highly controversial technology to national and local governments at low prices. As noted above, some of this technology may not perform well[32] nor comply with either the companies' or basic industry standards.[33] Yet **governments in Latin America are buying from them anyway, presenting invasive and inaccurate technology to the general public as a solution to crime, an argument that is at best misleading.**

Hikvison and Dahua have also gained a competitive edge in the region by offering products and services for free, taking advantage of the fragile economy in many Latin American countries to test their surveillance systems on citizens. While our goal in this report is not to analyze unfair competition practices, the issue merits attention given the recent scandals associated with the monopolistic and exploitative behavior of Big Tech companies.

Both companies are implicated in human rights violations. They have each won contracts for over $1 million USD for government-backed surveillance projects in Xinjiang, China[34] since 2016. According to an investigation by *The Wall Street Journal*,[35] authorities in Xinjiang are using surveillance technology to persecute the Muslim Uyghur minority ethnic group,[36] which has led to sanctions and criticism by the governments of Norway,[37] Denmark,[38] and the U.S.[39]

In addition, Dahua has had a series of vulnerabilities in its cloud system.[40] An independent researcher discovered a backdoor to Dahua systems that allowed remote unauthorized access via the web. Hikvision had a similar vulnerability in 2017 in its IP cameras.[41] The U.S. Federal Communications

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

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

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

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

[36] For more information, see: https://campaignforuyghurs.org/

[37] Business & Human Rights Resource Centre. "Norwegian wealth fund's ethics council recommended divestment from Hikvision for human rights concerns over co. role in mass surveillance." 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/

[38] Business & Human Rights Resource Centre. "Danish pension fund AkademikerPension divests from Hikvision for human rights concerns over co. role in mass surveillance." November 2020 https://www.business-humanrights.org/fr/derni%C3%A8res-actualit%C3%A9s/danish-pension-fund-akademikerpension-divests-from-chinese-surveillance-equipment-maker-over-human-rights-concerns/

[39] Business & Human Rights Resource Centre. "USA: Eleven Chinese firms added to economic blacklist over allegations of using forced labour of ethnic minorities." July 2020 https://www.business-humanrights.org/en/latest-news/usa-eleven-chinese-firms-added-to-economic-blacklist-over-allegations-of-using-forced-labour-of-ethnic-minorities/

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

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

Commission recently added Hikvision and Dahua to a list of companies that pose a threat to U.S. national security, encouraging U.S. companies to avoid using products by these companies.[42]

⇛ Cellebrite

Company Name	**Cellebrite DI Ltd.**
Headquarters	Petah Tikva, Israel
Countries of Operation	Worldwide
Countries where its surveillance technologies are deployed among Argentina, Brazil, and Ecuador	Argentina
Founded	1999
Public / Private	Private
Major Shareholder(s)	Suncorporation Ltd. (71.5%) Israel Growth Partners (24.41%)
Number of Employees	452 in 2019
Annual Revenue	USD $71.1 million in 2019

Cellebrite is an Israeli digital intelligence company and a subsidiary of Suncorporation Ltd., a Japanese company (Tokyo Stock Exchange listed).[43] Although it's tricky to pinpoint a specific date when authorities in **Argentina** began using the company's technology, Cellebrite's presence in the country has grown steadily over the last five years. Its products are obtained in Argentina through two main local resellers: **Security Team Network S.A.** and **IAFIS Argentina S.A.** Argentina ranks third in the Americas as a market for the use of Cellebrite's Universal Forensic Extraction Device (UFED) licenses, which are exported to more than 150 jurisdictions.

During the early 2010s, the Ministry of Justice allocated funds to kickstart the development of a network of Regional Forensic Investigation Laboratories, in collaboration with Public Prosecutor's Offices throughout the country. In 2014, there were already 13 forensic labs using Cellebrite's technology, specifically the UFED[44] product line for data extraction. According to an official document by the Ministry of Justice, the jurisdictions using this technology included: Oficina de Gestión de Información Tecnológica (OFITEC), Mercedes, Provincia de Buenos Aires; Laboratorio Forense de

[42] Federal Communications Commission. “PUBLIC SAFETY AND HOMELAND SECURITY BUREAU ANNOUNCES PUBLICATION OF THE LIST OF EQUIPMENT AND SERVICES COVERED BY SECTION 2 OF THE SECURE NETWORKS ACT.” WC Docket No. 18-89. March 2021 https://docs.fcc.gov/public/attachments/DA-21-309A1.pdf

[43] For more information, see Suncorporation’s website at https://www.sun-denshi.co.jp/eng/

[44] Cellebrite. UFED: “The industry standard for accessing digital device data.” https://cf-media.cellebrite.com/wp-content/uploads/2020/06/ProductOverview_Cellebrite_UFED_A4.pdf

Comunicaciones Complejas, Mar del Plata, Provincia de Buenos Aires; Ciudad Autónoma de Buenos Aires; Entre Ríos; Mendoza; San Juan; San Luis; Formosa; Neuquén; Chubut; La Pampa; Corrientes; and Misiones.[45] In the case of La Pampa, on top of UFED, they had implemented the CHINEX add-on,[46] developed to carry out data extraction from non-standard Chinese phones.

The use of Cellebrite's products has since expanded to other provinces. In 2018, the Public Prosecutor's Office in Salta updated its UFED 4PC and Touch licenses for a total of $23.000 USD, under a direct contract with Security Team Network.[47]

One of the main users of Cellebrite's technology at the national level in Argentina is the National Gendarmerie (GNA). Given its federal jurisdiction, GNA deployed Cellebrite's products throughout the country to equip forensic labs.

In September 2019, the GNA closed a direct contract with Security Team Network S.A. for a total of $643.900 USD, to acquire a workstation for unlocking high-end smartphones. The UFED product is only mentioned once in the technical specifications breakdown.[48] In November, the Gendarmerie's Directorate of Criminalistics and Forensic Studies acquired four licenses for the "UFED 4PC" software. According to Cellebrite, this product is used for "extraction, decoding, analysis, reader, and management capabilities" that can run on user-customizable hardware.[49] The Gendarmerie acquired these licenses through a public tender, ultimately contracting again with Security Team Network for a total of 9.587.400 pesos (around $159.000 USD at the time).[50]

More recently, the Gendarmerie updated these licenses in June 2020, under a contract with Security Team Network for a total of $132.116 USD.[51]

According to a journalist who wished to remain anonymous, the federal security forces (comprising the National Gendarmerie, the Airport Security Police, the Federal Police, and the Coast Guard) have a total of 35 UFED products, and, when counting in all the Public Prosecutor's Offices and other Law

[45] Justice and Human Rights Ministry. "Regional Research Laboratories Forensic" (in Spanish). August 2014 http://www.saij.gob.ar/docs-f/ediciones/libros/Laboratorios_Regionales_de_Invest._Forense.pdf

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

[47] Public Ministry, Province of Salta. File Nº 130-17.933/17

[48] File Nº 37/105-0815-CDI19. https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhwbeNKAPenXR8IR3ih5YSXR79Wk8x7mmrwOCg9|4XRUnx0kCgm3oU8Rx5zyjpByUn|6t4HsX9ox3IM|fHZHcPGbahOwPe58NWP7IaFH5JcDkQ==

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

[50] Directorate of Criminalistics and Forensic Studies. "ACQUISITION OF SOFTWARE UFED 4PC FOR THE DIRECTORATE OF CRIMINALISTICS AND FORENSIC STUDIES." File Nº 37/105-0041-LPU19. July 2018 https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhy5xycgc2RiGO0seBx38Zrkqrf44NYcUHOQXWAZSx|FbiACHf8VyMdhxK5ugYZKg/ha7EWhWl7fjuQEoJmuXixefeg9/er7CV2Q|P|HNndQKg==

[51] Directorate of Criminalistics and Forensic Studies. "UFEC TOUCH I FORENSIC SOFTWARE LICENSE RENEWAL AND UPDATE SERVICE TO UFED 4PC." File Nº 37/105-0422-CDI20. March 2020 https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhyrV/4BRRj7a9qf3aG8azk|h3K/KAn7jb/h6aPDkgsy3caJklV5dh/l98fSQHDGyecUZqnGVTQz3UXLzeKrU0hskSjg8CnHW3bp5dO0tjSzbg==

Enforcement Agencies (LEAs), there are 350 licenses being used in the country.[52] The primary user is the Gendarmerie, which works across provinces and is currently improving its digital forensic labs, using products such as Cellebrite's UFED Cloud, UFED Pathfinder, and UFED Physical Analyzer.[53] The GNA also lends its equipment when collaborating in criminal investigations, for example, in the case of the province of Entre Ríos.[54]

In Buenos Aires, the Public Prosecutor's Office acquired one UFED 4PC license together with the Physical Analyzer[55] software in 2019, through a direct contract with Security Team Network, for the sum of 440.109 pesos (around $10,500 USD at the time). These products were allocated to the Judicial Investigations Center.[56] This center had already renewed a license for another product, the UFED Cloud Analyzer, in 2017, also under a direct contract with the same local company.[57]

In August 2020, the Public Prosecutor's Office, in the province of Santa Fe, signed a direct contract with the local company IAFIS Argentina S.A., to renew four UFED Touch 2 licenses for a year, and acquire three new licenses for UFED 4PC, for a total of $96,226 USD.[58]

In December 2020, the Airport Security Police signed a direct contract with IAFIS Argentina S.A., to update and upgrade its UFED licenses, for a total of 8.057.111 pesos (around $90,784 USD). The contract included the renewal of two UFED 4PC Ultimate and two UFED Touch 2 Ultimate[59] licenses for two years, as well as a hardware trade-in of two Touch I devices for two UFED Touch 2.[60]

The Ministry of Security began signing cooperation agreements with more than 15 technology companies, including Cellebrite, in late 2020. These agreements include trainings and information

[52] Clarín. “Telephone detectives: secrets of the system that opens cell phones and solves the most complex causes” (in Spanish). November 2020. https://web.archive.org/web/20201114090956/https://www.clarin.com/policiales/detectives-telefonos-secretos-sistema-abre-celulares-resuelve-causas-complejas_0_U-d0fZd2m.html

[53] Cellebrite. “The National Gendarmerie of Argentina is overcoming barriers of time and distance with digital intelligence” (in Spanish). July 2020 https://www.cellebrite.com/es/blog-es/la-gendarmeria-nacional-de-argentina-esta-superando-las-barreras-de-tiempo-y-distancia-con-inteligencia-digital/

[54] El Entre Ríos. “UFED devices, the new equipment available to the Concordia police and the Gendarmerie in Paraná” (in Spanish). February 2019 https://www.elentrerios.com/actualidad/dispositivos-ufed-el-nuevo-equipamiento-con-el-que-cuenta-la-polica-de-concordia-y-la-gendarmera-en-paran.htm

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

[56] Government of the Autonomous 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

[57] Ministry of the Attorney General of Buenos Aires Province. Provision UOA Nº 45/2017. September 2017. https://mpfciudad.gob.ar/storage/archivos/Disposici%C3%B3n%20UOA%20N%C2%BA%2045-17%20AI%2030-00036938%20Adjudicacion%20SECURITY%20TEAM%20NETWORK%20S.A.%20-Ufed%20Cloud-.pdf

[58] Ministry of the Attorney General of Santa Fe Province. File Nº FG-000303-2020. August 2020 https://www.mpa.santafe.gov.ar/regulations_files/5f328fd04126a_Resoluci%C3%B3n%20N%C2%B0%20274.pdf

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

[60] Airport Security Police. “Renewal of licenses and improvement of UFED 4PC and UFED TOUCH equipment, for Exclusivity.” File Nº 279-0027-CDI20. November 2020 https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhy3iTxQqkwwChRpn2XPxXCSk5uij|LSdq2DmF5S3lGnqlsUbG2uGBeZPrbB8BhNUcLFrujs6LrFUaU3GDH8dDYrJv/eOuj/ve1TCcZ2AXWpaw==

sharing to improve LEAs' capacity in judicial investigations that involve digital evidence.[61] On November 3, 2020, we submitted a freedom of information request before the Ministry to inquire about these agreements. The official reply the Ministry gave in December 2020 states that "no subscription of any of the agreements referred to in the request for public information under examination has been concluded, which is why there are no documents about them that can be made known to the interested party."

Cellebrite's human rights record

Cellebrite claims to sell its technology exclusively to governments and law enforcement agencies and has reportedly marketed to government authorities interrogating asylum seekers.[62][63]

In 2016, the Bahraini General Directorate of Anti-Corruption and Economic and Electronic Security and the Criminal Investigations Directorate reportedly used Cellebrite's UFED to investigate and prosecute dissidents.[64] According to an investigation conducted by attorney Eitay Mack in Israel, the company has sold forensic technology to the governments of Venezuela, Belarus, Russia, as well as Indonesia, which are known for cracking down on political dissent and persecuting the LGTBQI community.[65]

After internal documents were leaked in 2017, it was revealed that Cellebrite was also in talks with LEAs in Turkey and the United Arab Emirates.[66] Moreover, Myanmar police used the same technology to arrest two journalists in 2019[67] and Hong Kong's police allegedly used it to harass and investigate pro-democracy protesters in 2020.[68] The Committee to Protect Journalists has recently revealed that Botswana's government is using Cellebrtie's technology to search devices of journalists for sources.[69]

[61] Government of Argentina. "Acciones para mayor eficiencia en la investigación criminal en el ámbito digital." October 2020. https://www.argentina.gob.ar/noticias/acciones-para-mayor-eficiencia-en-la-investigacion-criminal-en-el-ambito-digital

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

[63] Access Now. "What spy firm Cellebrite can't hide from investors." May 2021. https://www.accessnow.org/what-spy-firm-cellebrite-cant-hide-from-investors/

[64] The Intercept. "Phone-Cracking Cellebrite Software Used to Prosecute Tortured Dissident." December 2016. https://theintercept.com/2016/12/08/phone-cracking-cellebrite-software-used-to-prosecute-tortured-dissident/

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

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

[67] The Washington Post. "Security-tech companies once flocked to Myanmar. One firm's tools were used against two journalists." May 2019. https://www.washingtonpost.com/world/asia_pacific/security-tech-companies-once-flocked-to-myanmar-one-firms-tools-were-used-against-two-journalists-/2019/05/04/d4e9f7f0-5b5d-11e9-b8e3-b03311fbbbfe_story.html

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

[69] Committee to Protect Journalists, "Equipped by US, Israeli firms, police 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/

Some of the journalists claim to have been tortured.[70] More reports reveal Cellebrite's tools being sold to Nigeria, Bangladesh, India, Saudi Arabia, and Vietnam.[71]

Human rights advocates filed a court petition to urge Israel's Ministry of Defense to halt Cellebrite's export to Hong Kong, Russia, and Belarus.[72] In October 2020, Cellebrite announced it will stop selling its technology to China and Hong Kong.[73] In March 2021, Cellebrite also announced it will also stop sales to Russia and Belarus.[74]

⇛ Huawei and ZTE

Company Name	**Huawei Technologies Co., Ltd.**
Headquarters	Shenzhen, the People's Republic of China
Countries of Operation	Worldwide
Countries where its surveillance technologies are deployed among Argentina, Brazil, and Ecuador	Argentina, Brazil
Founded	1987
Public / Private	Private
Major Shareholder(s)	Wholly owned by its employees
Number of Employees	194,000 employees
Annual Revenue	RMB 858.8 billion (USD $132 billion) in 2019

[70] Id.

[71] 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-vietnam-is-doing-with-israel-s-phone-hacking-tech-1.10003831

[72] 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-over-sales-to-hong-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

[73] 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/

[74] 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/

Company Name	**ZTE Corporation**
Headquarters	Shenzhen, the People's Republic of China
Countries of Operation	Worldwide
Countries where its surveillance technologies are deployed among Argentina, Brazil, and Ecuador	Argentina, Brazil
Founded	1985
Public / Private	Listed on both the Hong Kong and Shenzhen Stock Exchanges
Major Shareholder(s)	ZTE Holdings (21.85%), Hong Kong Securities Clearing Company Limited (16.31%)
Number of Employees	70,066 employees on a group basis (60,514 employees on a company basis) in 2019
Annual Revenue	RMB 90.737 billion (USD $13.94 billion) in 2019

Both Chinese companies, **Huawei Technologies Co**. and **ZTE Corporation,** offer a broad range of technological solutions. One of the services they offer is technology and systems for building what's known as "smart cities." They are each actively engaging primarily with local governments across Latin America to provide tools for public security.

In July 2020, ZTE landed in the province of Jujuy, **Argentina**. The governor, Gerardo Morales, received the vice president of ZTE Corporation and the general manager of ZTE Argentina, Hua Xinhai and Dennis Wang. They reached an agreement to deploy a program called "Jujuy Seguro e Interconectado" (Safe and interconnected Jujuy), for which the province received a loan in March 2020 from the Hong Kong-based BBVA bank for USD $24,146.142.[75] ZTE closed the deal for USD $30 million to fill part of this agenda by providing the installation of cameras, monitoring centers, emergency services, and telecommunications infrastructure.[76] According to governor Morales, now Jujuy "will be as safe as China." We sent a freedom of information request asking for more details on November 11, 2020, but we did not receive a reply despite having met the legal deadline.

In April 2018, Alfredo Cornejo, the governor of the province of Mendoza, Argentina, met with the vice president of sales at Huawei, Tony Sze.[77] The purpose of the meeting, according to media reports, was

[75] Official Gazette. Decree 207/2019. March 2019 https://www.boletinoficial.gob.ar/detalleAviso/primera/203703/20190320

[76] 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

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

to discuss the acquisition of technology for facial recognition, geolocation, and big data management for public security. Civil society organizations including Access Now and ADC responded with a letter to the governor,[78] asking for an end to the private negotiations and a public discussion of the issue. Unfortunately, the governor released no further information.

Huawei is also present in the region through a network of dealers and resellers. One example is in Bahia in **Brazil**, where authorities chose the Brazilian branch of the Spanish chain **El Corte Ingles** for an "additional contractual provision" for the "Safe Bahia Consortium 2014" to supply Huawei's facial recognition hardware (cameras) and software. The Brazilian telecommunication provider **"Oi"** has also signed a contract with Huawei to sell facial recognition technology in Brazil.[79] Authorities tested this technology on the public during the carnivals in Rio de Janeiro in 2019. The system captured approximately three million face images, but only 10 arrests were made based on use of the system, according to the Rio de Janeiro Military Police spokesman, Colonel Mauro Fliess.[80]

To accelerate buy-in for its technology and test out its capabilities, Huawei also donated to Campinas, in the state of São Paulo, the necessary equipment for a "smart city" project. Campinas is now known for its "open laboratory," which includes privacy-invading facial recognition technology, leading to its designation as the "smartest city" in Brazil.[81]

ZTE and Huawei's human rights record

ZTE and Huawei have long been known to work with regimes that violate human rights. In 2013, when the advocacy group Bolo Bhi asked both companies not to participate in building an internet censorship firewall for the government in **Pakistan**, they chose to ignore the human rights impacts of their products and issue cursory statements about prioritizing "local" laws over international human rights law and norms.[82] That same year, Reflets.Info reported that ZTE alongside Hewlett Packard were collaborating with Telecommunications Infrastructure Co. (TCI), Iran's state-owned internet service provider, to help limit the kind of information Iranians can access online.[83]

In 2008, then-Venezuelan President Hugo Chávez sent officials from the Justice Ministry to visit ZTE. They learned how China, through the use of smart cards, was developing a system that would help

[78] ADC. "Fundamental rights defenders ask the Mendoza government to stop the purchase of mass surveillance technology" (in Spanish). 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/

[79] Folha de S.Paulo. "Chinese Huawei Partners with Oi for Facial Recognition Cameras" (in Portugese). October 2018. https://www1.folha.uol.com.br/tec/2018/10/chinesa-huawei-faz-parceria-com-oi-para-cameras-de-reconhecimento-facial.shtml

[80] Defesanet. "Facial Recognition - At Carnival in Rio identified 8 thousand people of interest" (in Portuguese). May 2019. https://www.defesanet.com.br/tecdi/noticia/32851/Reconhecimento-Facial---No-Carnaval-do-Rio-identificou-8-mil-pessoas-de-interesse/

[81] The Rio TImes. "Campinas is "Smartest" and Most Connected City in Brazil, per Unofficial Ranking." September 2019. https://riotimesonline.com/brazil-news/brazil/life-brazil/campinas-is-the-smartest-and-most-connected-city-in-brazil/

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

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

Beijing monitor individuals' social, political, and economic behavior. After 10 years, the **Venezuelan government** hired ZTE for $70 million USD to deploy a similar program, the "carnet de la patria," or homeland license. The cards are being used in campaigns to influence voting decisions,[84] give out food subsidies, provide healthcare, and administer other social programs on which the majority of Venezuelans depend for survival.[85] This smart card system raised the alarm of citizens and human rights activists and organizations due to the clear risk of government abuse, privacy invasion, and community control. After its implementation, the "carnet de la patria" database was hacked,[86] and in 2018, the government used the homeland cards and the data behind them to identify people who didn't vote. It also made the cards mandatory to obtain government benefits and to buy fuel at subsidized prices.

Huawei has also been under a lot of media scrutiny in recent years. In 2019, a *Wall Street Journal* investigation[87] showed that technicians from the company have, in at least two cases, personally helped the governments of **Uganda** and **Zambia** spy on their political opponents, including intercepting their encrypted communications and social media, and using cell phone data to track their whereabouts.

In June 2020, an investigation conducted by *Reuters* showed that Huawei sold at least 1.3 million euros worth of embargoed Hewlett-Packard computer equipment to the Iranian government and took a lot of efforts to hide it.[88] In December of the same year, IPVM found a "confidential" document hosted publicly on Huawei's own European website that was shortly afterward deleted. This document showed how Huawei has tested a facial recognition software that could send automated "Uighur alarms" to **Chinese government** authorities when its camera systems identify members of the oppressed minority group.[89]

This and other worrisome cases led **Sweden** to ban telecoms equipment from Huawei and ZTE in its 5G network,[90] and other European nations have either taken or are considering taking similar actions.

[84] BBC News. "Elections in Venezuela: what are the red dots and why does Henri Falcón accuse Maduro of "buying votes" (in Spanish). May 2018. https://www.bbc.com/mundo/noticias-america-latina-44192915

[85] Reuters. "How ZTE helps Venezuela implement Chinese-style social control" (in Spanish). November 2018. https://www.reuters.com/investigates/special-report/venezuela-zte-es/

[86] AlbertoRodNews Twitter account. https://twitter.com/AlbertoRodNews/status/1070733400372326401

[87] 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

[88] 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

[89] IPVM. "Huawei / Megvii Uyghur Alarms." December 2020. https://ipvm.com/reports/huawei-megvii-uygur

[90] Reuters. "Sweden bans Huawei, ZTE from upcoming 5G networks." October 2020. https://www.reuters.com/article/sweden-huawei-int-idUSKBN2750WA

⇛ NEC

Company Name	**NEC Corporation**
Headquarters	Tokyo, Japan
Countries of Operation	Worldwide
Countries where its surveillance technologies are deployed among Argentina, Brazil, and Ecuador	Argentina, Brazil
Founded	1899
Public / Private	Listed on Tokyo Stock Exchange
Major Shareholder(s)	N/A
Number of Employees	Approximately 110,000 in 2020
Annual Revenue	JPY 3,095.2 billon (USD $28.35 billion) in 2020

NEC is a major player in the digital biometric identification industry at the global level. It is a 122 year-old-old company and has over 110,000 employees. The Japanese tech giant (listed on the Tokyo Stock Exchange) presents itself[91] as the go-to choice for multiple government agencies throughout the world. It has been developing biometric technology, such as facial, iris, fingerprint, finger vein, and voice recognition technology, for over 50 years, selling to 70 jurisdictions.[92] NEC's technologies form the backbone for the world's biggest biometric system, **India**'s Aadhaar, which has enrolled 1.3 billion people.[93] In the **U.S.**, over one third of state police and law enforcement agencies use NEC's biometric systems as of 2019.[94] U.S. Customs and Border Protection (CBP) uses NEC's facial recognition software at airports,[95] and the technology has also made its way to sport stadiums in **Colombia**[96] and **Taiwan**.[97] NEC's presence in Latin America is growing as more local governments adopt "smart city" rhetoric.

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

NEC established its operations in **Argentina** in 1978, to carry out business in the country and the region through its own local subsidiary. **In 2004, the company chose NEC Argentina S.A. as the Regional Software Development Center for the company's Latin American market**.[98] Since 2006, NEC has been the official supplier of biometric technology for the national Ministry of Interior and the National Citizens Registry (RENAPER). Thanks to this technology, RENAPER has expanded the use of its biometric database for verification and identification to other public bodies, such as the Migration Office, the National Directorate of Recidivism, and the Ministry of Security, among others, which was also a result of the Federal Biometric Identification System for Security's (SIBIOS) expansion.

In 2017, the National Migration Office (DNM) signed a contract with NEC to implement automated passport control gates, commonly referred to as "eGates," in Argentina's international airports, for a total of $3.309.318 USD.[99] The official procurement documents state that NEC was chosen given that the National Migration Office was already using the company's AFIS[100] and NeoFace[101] products, for fingerprint and facial recognition respectively.

The eGates were first implemented and used by the public in 2018 at Ezeiza airport, but were later on expanded to Aeroparque airport and the sea port, both in the City of Buenos Aires.[102] Border control uses these eGates checkpoints to replace some human interactions, using fingerprint and facial verification software to compare a scan against the biometric data gathered from anyone entering or leaving the country. The enrollment data for eGates is held by RENAPER.

In 2019, the DNM signed another contract with NEC for a biometric system to identify people from a watchlist (for example, people with travel restrictions, those wanted by INTERPOL, etc.), for a total of 145.189.000 pesos (about $3 million USD at the time).[103] The request specified 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, update, and further expand their biometric systems.[104]

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

[99] Directorate General of Administration. "PROVISION OF SOLUTION OF SELF-ASSISTED IMMIGRATION PROCESS." File Nº 21-0028-CDI17. September 2017. https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhxKmqLque6kMW1chJuEHzB2LvnmYI6tmgdCyJ7Ep7d490YZKW8ptaXbZVpysEhjsnNcElgEeF4JDcgYQh41LgX8fcn98cZ8e12qM5BlL50fqw==

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

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

[102] Home Office. "The National Government launched the biometric gates at the Ezeiza airport" (in Spanish). April 2018. http://www.migraciones.gov.ar/accesible/novedad.php?i=4019

[103] Directorate General of Administration. "INTEGRAL SOLUTION FOR IDENTIFICATION OF FOREIGNERS AND BIOMETRIC CONTROL OF RESTRICTIONS." File Nº 21-0002-LPU19. February 2019. https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhwfHN|0dYheEGyNBwGGvH3GL6jBhnOAiv5hg9nZ3JQi1tBQTuogGzD12zCv6XuNwuBmJTvQzJWApOOrz69pEW2MV9graYTQBzR11CtszG5T6w==

[104] Purchasing Division. "Contracting of services, licenses and products related to the RENAPER biometric platform." October 2017. File Nº 78-0012-CDI17. https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhy7MmMdVUat6QKfRigU80UVxJmyaLvy67Tv2OgtO1qNBgGmFkKWbfpTnnfNopxo|oaRtWe20G7DjIP49UkgkEP896PfIoNb393/NEPZ2M5G7w==
Purchasing Division. "Comprehensive centralized terminal management solution for managing licenses." File Nº78-0022-CDI18. September 2018. https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhzl

In December 2017, RENAPER and the former Modernization Secretariat (currently the Public Innovation Secretariat, under the Office of the Chief of Staff) signed a cooperation agreement to develop a national Digital Identity System (SID).[105] The system uses facial recognition to validate people's identity when they access certain state and private services that implement its Application Programming Interface (API) and/or software development kit (SDK). The SID was first launched in a pilot phase, to test its use by some fintech companies for the onboarding process to create a bank account.[106] The facial recognition element of SID's software is NeoFace Watch, acquired with a loan from the **World Bank** for $834.403,90 USD.

Argentina's Digital Identity System is being expanded to cover multiple use cases, on top of the systems for state-run services and fintechs. In July 2020, the Ministry of Interior signed a cooperation agreement with the Ministry of Education to implement the system in national universities, to require students to validate their identities before taking online exams.[107] This expansion is happening despite concerns about the flaws in its facial recognition algorithms.[108] As this system becomes more widespread, it may become the primary way to validate one's identity, threatening discrimination and exclusion of people who are not in the system, or are misidentified, from accesing public services. The government has minimized this threat, arguing the facial recognition algorithm is set up under NEC's default false positive and false negative rates.[109]

At the local level, NEC has developed a close relationship with the government of Tigre, a city in Buenos Aires. The municipality has been using NEC's technology for its entire urban surveillance program since at least 2016, starting with CCTV, automated license plate recognition (ALPR), and facial recognition using NeoFace Watch.[110]

n331uwbedtWpuhJRVlkYFu5E0d6zTuIWgkUVrzCpo|kMsAHgU/dYCpNuyBnX9eXEW4riZstvHDV2ZqhmqPbCKquiSivEogUdA1HkMNIlaA==
Purchasing Division. "EXPANSION AND UPDATE OF THE EXISTING BIOMETRIC PLATFORM OF RENAPER." File Nº 78-0028-CDI18. December 2018. https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhzNiQxEvvRD1M4Hrw70Q0R4HTin1WArUVSpJfI4xYYgmiT77fvnNNo8g|PlFmMreDTagF|N6f4dFxdRnoYveFKYmjFSg8zlglzEUYmrvWH5MQ==
Purchasing Division. "MAINTENANCE SERVICE, SUPPORT AND TECHNICAL ASSISTANCE FOR THE ABIS SYSTEM." File Nº 78-0029-CDI18. December 2018.
https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhyGzxXg3NEnQt|kEbGqFjvyvkPpcD27XbPjrB79ynaMSOETGHQanjODkHz9Nz64Gib/l6s/AI|E2d1ogkSzvDmTJdhqutPSEbqYs|rd|4j|BA==
Purchasing Division. "INTEGRAL SERVICE FOR MIGRATION AND GRAL MAINTENANCE. OF ALL THE EXISTING AFIS PLATFORM." File Nº 78-0001-CDI20. April 2020. https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhxz8ZzajHoNTGv6h2avQkrsmYw2yzxlp7rrnVp3vvETTUXRKICLVaNVdpDAhqicxls3LP/xxu4zp9sqDVtRdJGZ6ZJhpzdesliW7C8vB7JEGg==

[105] Home Office. "SID - Digital ID System" (in Spanish)
https://www.argentina.gob.ar/interior/renaper/sid-sistema-de-identidad-digital

[106] "Fintech" or financial technology, is a term used to refer to new businesses that develop financial services using digital technologies at the core of their products or services.

[107] Ministry of Education. "New system for validating the identity of university students" (in Spanish). July 2020.
https://www.argentina.gob.ar/noticias/nuevo-sistema-para-la-validacion-de-la-identidad-de-estudiantes-universitarios

[108] La Nación. ""I don't like your face": do applications discriminate?" (in Spanish). September 2019.
https://www.lanacion.com.ar/tecnologia/no-me-gusta-tu-cara-discriminan-aplicaciones-nid2292711/

[109] ADC. "Your digital self: Discovering the narratives about identity and biometrics in Latin America" (in Spanish). April 2019.https://adc.org.ar/informes/tu-yo-digital-descubriendo-las-narrativas-sobre-identidad-y-biometria-en-america-latina/

[110] NEC Corporation YouTube channel. "The city of Tigre" (in Spanish). September 2016.
https://www.youtube.com/watch?v=5Lp9PWv0EQ0

In 2019, Tigre revamped its surveillance[111] infrastructure by launching NeoCenter, developed by NEC to further the city's existing capabilities.[112] On top of the features mentioned above, facial recognition software has been updated to track people more precisely in public spaces, recording movement paths to pinpoint where someone was (their travel history), and identifying "suspicious behaviors," through analysis of the movement of both people and vehicles. Tigre further expanded its surveillance technology in 2020, with the installation of a totem with cameras for facial recognition.[113]

When Tigre announced the launch, ADC filed[114] a freedom of information request to learn more about how the technology is being used and the legal frameworks for its use. The local government delayed the process and failed to respond, even after multiple follow-ups, indicating a lack of transparency and accountability.

Tigre has been such a close partner of NEC that the company uses the city as a marketing case study, showcasing the solutions they provide the city, including technology for citizen collaboration in public security, license plate analysis, facial recognition, behavior detection, building a crime map and gathering evidence, and machine learning technologies for analyzing data. NEC claims that Tigre is becoming "a model of safe city in Latin America."[115]

NEC has also been involved in deploying surveillance equipment at airports in **Brazil**. The Federal Customs Service of Brazil (*Receita Federal*), for instance, has acquired NEC facial recognition technology to identify passengers suspected of evading import taxes.[116] The system has already been in operation in 14 Brazilian airports since 2016.[117]

NEC's human rights record

In December 2020, **Justice for Myanmar**, a group of activists, conducted an investigation[118] into the Myanmar military's corruption and influence in the information and communications sector. The group uncovered evidence of the military's theft of public assets, exposed new military procurement networks, and revealed the global network of businesses that are enabling the military to continue to commit war crimes and crimes against humanity.

[111] Municipality of Tigre. "Tigre's Eyes" (in Spanish). https://www.tigre.gob.ar/seguridad/cot

[112] Ámbito. "Tigre launched a new facial recognition system" (in Spanish). May 2019. https://www.ambito.com/municipios/municipios/tigre-lanzo-un-nuevo-sistema-reconocimiento-facial-n5030978

[113] Municipality of Tigre. "New security totem with facial recognition camera in El Talar" (in Spanish). September 2020. http://www.tigre.gov.ar/novedades/detalle/1267

[114] ADC Twitter account. https://twitter.com/adcderechos/status/1131556333466116096?s=20

[115] NEC. "Tigre City Integrated Urban Safety Solutions." https://www.nec.com/en/case/tigre/index.html
NEC brochure for Tigre case study:
https://web.archive.org/web/20170321095617/http://www.nec.com/en/case/tigre/pdf/brochure.pdf

[116] NEC. "Federal Revenue Service will use NEC's facial identification technology at 14 international airports in the country" (in Portuguese). 2016. https://br.nec.com/pt_BR/press/PR/20160409060302_11186.html

[117] Ministry of Economy. "Internal Revenue Service Launches Face Recognition System" (in Portuguese). 2016. https://receita.economia.gov.br/noticias/ascom/2016/agosto/receita-federal-apresentou-hoje-1-8-em-coletiva-de-imprensa-detalhes-sobre-o-novo-sistema-de-reconhecimento-facial-1

[118] Justice for Myanmar. "Nodes of Corruption, Lines of Abuse." December 2020. https://www.justiceformyanmar.org/stories/nodes-of-corruption-lines-of-abuse-how-mytel-viettel-and-a-global-network-of-businesses-support-the-international-crimes-of-the-myanmar-military

According to the investigation, **NEC** provided microwave transmission equipment to Myanmar's military forces through **Vittel** (Vietnam telecommunications Company) and **Mytel** (Myanmar's newest mobile operator). In doing this, NEC and other companies that are supplying technology through Mytel and Viettel risk contributing to the grave human rights violations in Myanmar.

Business & Human Rights Resource Centre (BHRRC) invited NEC and another 20 of the companies mentioned in the report to respond to the accusations. In its answer, NEC said it would "refrain from commenting on individual cases."[119] The company previously failed to reply when BHRRC asked whether or not it was asked by Japanese authorities to develop drones for military use with the Israeli government.[120]

In 2019, it was widely reported that NEC's facial recognition system was used in the first known wrongful arrest case due to algorithmic bias.[121] NEC responded by stating that "a match using facial recognition alone is not a means for positive identification" and failed to clarify how the company will prevent similar cases from happening in the future.

This course of action directly conflicts with NEC's stated commitment to respect human rights and privacy in its Group Code of Conduct,[122] and represents failure to provide transparency as contemplated in its own "NEC Group AI and Human Rights Principles."[123]

⇛ IDEMIA

Company Name	Idemia France SAS
Headquarters	Courbevoie, France
Countries of Operation	Worldwide
Countries where its surveillance technologies are deployed among Argentina, Brazil, and Ecuador	Argentina
Founded	2008
Public / Private	Private

[119] Business & Human Rights Resource Centre. "NEC's response." January 2021. https://www.business-humanrights.org/en/latest-news/necs-response/

[120] Business & Human Rights Resource Centre. "Japan: Reported joint drone development with Israel." October 2016. https://www.business-humanrights.org/es/%C3%BAltimas-noticias/japan-reported-joint-drone-development-with-israel/

[121] New York Times. "Wrongfully Accused by an Algorithm." June 2020. https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

[122] NEC. "Group Code of Conduct." Updated in January 2019. https://www.nec-enterprise.com/documents?id=1432&hash=7c546360141e92ca5009db242402001dd7e393ef5198076b4f5e5a9f1c869f29

[123] NEC. "NEC Unveils "NEC Group AI and Human Rights Principles." April 2019. https://www.nec.com/en/press/201904/global_20190402_01.html

Major Shareholder(s)	Advent International (a majority shareholder)
Number of Employees	Approximately 15,000 in 2019
Annual Revenue	€2.3 billion ($2.7 billion USD) in 2019

Previously known as "Morpho Safran" and "Safran Identity and Security,"[124] the French company **IDEMIA** is one of the leading suppliers of biometric technology in the world. In the U.S. alone, the company provides solutions to the Federal Bureau of Investigation (FBI),[125] INTERPOL,[126] the New York Police Department,[127] and the U.S. Transportation Security Administration, among others.

In our research for this report, we were not able to find any recent connections between the Argentinian, Ecuadorian, or Brazilian governments and the company under the IDEMIA brand. IDEMIA has an office in Buenos Aires, Argentina, but it is focused on the mobile carrier market. While it is not clear when Argentinian authorities first purchased IDEMIA's technology, Law Enforcement Agencies (LEAs) began using Morpho products before 2010.[128] Use of the technology then took off with the introduction, and consequent expansion, of **SIBIOS**, a state owned massive biometric database.

As we will highlight in our case study on Argentina in this report, the use of Morpho products is intimately related to SIBIOS. These products are used by the National Ministry of Security and the Federal Police. In 2014 and 2015, the Ministry spent over $7 million USD in contracts with Morpho S.A. for biometric technology.[129] The Federal Police employs Morpho RapID devices in the field, to carry out

[124] IDEMIA, "OT-Morpho becomes IDEMIA, the global leader in trusted identities." Septmeber 2017. https://www.idemia.com/press-release/ot-morpho-becomes-idemia-global-leader-trusted-identities-2017-09-28.

[125] Morpho. "MorphoTrak Technology Goes Operational for the FBI." April 2011. http://web.archive.org/web/20150607084516/http://www.morpho.com/actualites-et-evenements/presse/morphotrak-technology-goes-operational-for-the-fbi?lang=en

[126] Morpho. "Sagem Sécurité to provide Interpol and its 186 member states with latest AFIS, Automated FingerprintIdentification System." February 2008. http://web.archive.org/web/20150607090048/http://www.morpho.com/news-events-348/press/sagem-securite-to-provide-interpol-and-its-186-member-states-with-latest-afis-automated-fingerprint-identification-system?lang=en
Morpho. "Safran Identity & Security is the exclusive partner of INTERPOL for facial recognition." November 2016: http://www.morpho.com/en/media/safran-identity-security-exclusive-partner-interpol-facial-recognition-20161123

[127] Morpho. "Morpho Trak Deploys Morpho Biometric Identification System at NYPD." 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

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

[129] Argentine Federal Police Superintendency of Administration, Procurement Division, Direct Hire N° 25/2014, File N° 581-01-000726-14: https://www.boletinoficial.gob.ar/detalleAviso/tercera/2134795/20150119
Argentine Federal Police Superintendency of Administration, Procurement Division, Direct Hire N° 26/2014, File N° 581-01-000640-14: https://www.boletinoficial.gob.ar/detalleAviso/tercera/2134792/20150119
File N° 550-01-001003-2014 y 563-01-001091-2014
https://www.boletinoficial.gob.ar/detalleAviso/tercera/2125517/20141024
File N° 581-01-000726/2014 y 563-01-001090/2014
https://www.boletinoficial.gob.ar/detalleAviso/tercera/2125518/20141024

fingerprint identification of individuals,[130] as well as "Morpho Face Detective" for facial recognition to identify people in crowds.[131]

Given that the Federal Police have nationwide jurisdiction, the use of Morpho's technology has expanded throughout the country, such as in the cities of Campana,[132] Luján,[133] Balcarce,[134] Córdoba,[135] Chaco,[136] and multiple towns in the Province of Buenos Aires.[137]

State agencies rely on one main reseller of IDEMIA's technology, **IAFIS Argentina S.A.**, the same company that sells Cellebrite's products. This reseller names multiple police forces from various provinces in Argentina as their clients,[138] as well as Public Prosecutor's Offices and other public institutions, although it doesn't specify which products it is supplying.

The City of Buenos Aires acquired the Morpho Face Investigate software from IAFIS Argentina S.A. in 2011 for 33.198.500 pesos (more than $6 million USD at the time), and started testing its use in the subway to identify pickpockets.[139]

According to official procurement and public tender documents, the Metropolitan Police in the City of Buenos Aires uses both fingerprint and facial recognition technology from Morpho for judicial investigations. IAFIS Argentina S.A. has provided technical support to them since at least 2015, with several contracts for more than $6.5 million USD in total.[140]

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

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

[132] La Auténtica Defensa. "The Morpho Rapid system is applied in Campana" (in Spanish). March 2009.
www.laautenticadefensa.net/62085

[133] El Civismo. "Modern equipment to identify people" (in Spanish). September 2010.
https://www.elcivismo.com.ar/notas/7191/

[134] "La Vanguardia. “Advancement: Federal Police operation in Balcarce” (in Spanish). February 2019.
http://www.diariolavanguardia.com/noticias/21448--cobramos-por-lo-que-trabajamos--no-le-robamos-la-plata-a-nadie-/

[135] La Voz. "They recaptured "Cañete", the "most wanted" fugitive from Córdoba" (in Spanish). May 2017.
https://www.lavoz.com.ar/sucesos/recapturaron-canete-el-profugo-cordobes-mas-buscado

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

[137] Primera Plana. "Federal Police disembark in the interior of Buenos Aires with control and prevention operations" (in Spanish). May 2019. http://primeraplana.com.ar/policia-federal-desembarca-en-el-interior-bonaerense-con-operativos-de-control-y-prevencion/

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

[139] Infobae. "Evaluation of a facial identification software to locate "pungas" in the subway” (in Spanish). January 2013.
https://www.infobae.com/2013/01/13/691102-evaluan-un-software-identificacion-facial-ubicar-pungas-el-subte/

[140] Purchasing Department of Buenos Aires. Number of purchase processes: 2900-1047-CDI15
https://www.buenosairescompras.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhzAdZmPYqqZ4su3ScBBrBvMPHSPHPxZ74bjkpi4POk3iZKynCGKbKt|RDsvNlcW1mJISgBUffWWFY1vgdwt/W5yzl3PnouupiCeVWiQuysmvw==
Number of purchase processes: 2900-0858-CDI17.
https://www.buenosairescompras.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhzjp0DPq1u2nI3iH|4rzqLn9Phu5zQ6mkLN3u849mLkhWIq/6PJyo37gtSRaUyG3uJLK1ZE2CoQE3RKSJHwBng31I/q82/vv9su9cJDc2PG2g==

IDEMIA's human rights record

In 2017, Morpho (which later became **IDEMIA)** was blamed for problems with its biometric registration and authentication kits used in the 2017 general election in Kenya, resulting in the National Assembly cancelling its public contracts and blocking any new ones. That decision was challenged and overturned by Kenya's High Court.[141] Kenya's opposition coalition accused the French firm of complicity in electoral fraud, but the company has denied these charges. **Safran (previous entity prior to the IDEMIA merger) was also fined by a French court for having paid bribes to secure business in Nigeria[142]**

In September 2020, **Amnesty International** found that three European companies, one of which was IDEMIA, sold surveillance technology to the Chinese government.[143] Specifically, IDEMIA was awarded a contract to supply facial recognition equipment directly to the Shanghai Public Security Bureau in 2015. Due to the risk of Chinese authorities using this equipment for mass surveillance and other human rights abuses, Amnesty International, Access Now, and other organizations, as well as some European countries, have been asking the European Union to strengthen human rights safeguards in its surveillance export decisions and ensure all relevant companies conduct a human rights impact assessment.[144] France, where IDEMIA is headquartered, has been resisting this call.[145]

⇛ Verint

Company Name	**Verint Systems Inc.**
Headquarters	New York, the U.S.
Countries of Operation	Worldwide
Countries where its surveillance technologies are deployed among Argentina, Brazil, and Ecuador	Ecuador
Founded	2002
Public / Private	Listed on Nasdaq

[141] 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

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

[143] 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/

[144] 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/urgent-call-to-council-of-the-eu-human-rights-must-come-first-in-dual-use-final-draft/

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

Major Shareholder(s)	N/A
Number of Employees	Approximately 6,500 in 2019
Annual Revenue	€2.3 billion ($2.7 billion USD) in 2019

VERINT is one of the few U.S.-based companies to have made its way into the Latin American market. Approximately half of its employees are located in Israel.

In **Ecuador**, the city of **Guayaquil** acquired VERINT's surveillance technologies from the distributor **Union Electrica S.A.,** a company that has won contracts worth millions from the **Corporation for Citizen Security**, a private non-profit entity created to manage vídeo surveillance and other security services for Guayaquil.[146] The purpose was to integrate 100 surveillance cameras with facial recognition for security in educational institutions. This integration cost $2,569,906.41 USD and included products like cameras with facial capture capability, systems for facial recognition, data storage solutions, licenses for cameras and monitoring, and peripheral megaphone equipment, services, and infrastructure. In 2020, these cameras and products were integrated into the **ECU911** mass surveillance program of Ecuador.

VERINT's human rights record

In 2014, an investigation conducted by Privacy International[147] detailed how **VERINT** provided monitoring centers capable of mass interception of telephone, mobile, and IP networks to **Kazakhstan** and **Uzbekistan**. Kazakhstan has been condemned for laws restricting free speech and assembly, flawed trials, internat shutdowns, and torture,[148] while in Uzbekistan there are testimonies of lawyers, journalists, and bloggers whose communications were intercepted, and who were then persecuted for politically motivated reasons.[149] Both countries have been long known for extensive digital surveillance of their citizens.[150]

Privacy International also published a special report about the state of surveillance in **Colombia**, in 2015.[151] According to the report, Colombia's government uses a system called Unique Monitoring and Analysis Platform or **PUMA** (after its initials in Spanish). PUMA has the potential capacity to intercept and store all communications transmitted over the backbone infrastructure upon which all Colombians

[146] Corporation for Citizen Security of Guayaquil. https://cscg.gob.ec/

[147] Privacy International. "Private Interests: Monitoring Central Asia." November 2014. https://privacyinternational.org/report/837/private-interests-monitoring-central-asia

[148] Human Rights Watch. "Kazakhstan." https://www.hrw.org/europe/central-asia/kazakhstan; Access Now, "Civil society reports internet shutdowns in two cities in Kazakhstan during February 28 protests." March 2021. https://www.accessnow.org/internet-shutdowns-kazakhstan-feb-28-protests/

[149] Human Rights Watch. "Uzbekistan." https://www.hrw.org/europe/central-asia/uzbekistan

[150] Access Now, "Commonwealth of surveillance states: On the export and resale of Russian surveillance technology to post-Soviet Central Asia." June 2013. https://www.accessnow.org/cms/assets/uploads/archive/docs/Commonwealth_of_Surveillance_States_ENG_1.pdf

[151] Privacy International. "A shadow state: surveillance and public order in Colombia" (in Spanish). August 2015. https://www.privacyinternational.org/sites/default/files/2017-12/ShadowState_Espanol.pdf

depend to talk and send messages to one another. PUMA is powered by proprietary technology from VERINT, primarily using its RELIANT monitoring center platform.

VERINT technicians reportedly placed 16 “IP-PROBER” probes[152] on the trunk networks to intercept data and forward it to PUMA's monitoring centers. The Administrative Department of Security (DAS) used them to carry out communications network surveillance, and the agency was later investigated for illegal activities and then dissolved due to its espionage and harassment of politicians, journalists, activists, and Supreme Court judges who opposed Álvaro Uribe’s government.

In 2012, the Business & Human Rights Resource Centre invited companies including VERINT to respond to accusations of providing surveillance technology to oppressive regimes in the Middle East.[153] VERINT did not respond.

Other companies supplying surveillance tech in Latin America

As we mentioned in the introduction to this report, we have focused on companies with the most publicly available information about their businesses in Latin America, pose a particular human rights threat, and are pervasive due to their relationships with government bodies. However, there are multiple companies worth mentioning that are keeping a lower profile and merit further investigation.

BGH Tech Partner

Company Name	**BGH Tech Partner S.A.**
Headquarters	Buenos Aires, Argentina
Countries of Operation	[Not Available]
Countries where its surveillance technologies are deployed among Argentina, Brazil, and Ecuador	Argentina
Founded	1913
Public / Private	Private
Major Shareholder(s)	[Not Available]
Number of Employees	[Not Available]
Annual Revenue	[Not Available]

[152] Directorate of Administration and Finance, Colombia National Police. File N°06-7-10124- 10. September 2010. http://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=10-12-351033

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

Boris Garfunkel e Hijos, or **BGH**, is an **Argentinian** company that began by selling a broad range of products but over the last decade has focused in part on the development of technological solutions. The company is responsible for technology deployment for the "Laboratory of Forensic Video Analysis" in the province of **San Juan**.[154] While the company claims it is only providing law enforcement with solutions for encrypted communications and location mapping services, according to media reports,[155] this laboratory will soon be equipped with facial recognition software for identifying people and detecting and classifying objects, attributes, and behaviors, as well as recognizing vehicle license plates.

We tried to obtain information about BGH technology deployment, both from the government and the company itself, but with no success. It is possible that the technology comes from **Hikvision**, given that in 2018, BGH started selling Hikvision products.[156] The solutions BGH now offers include thermal, vehicular, portable, and facial recognition cameras, as well as technologies such as drones and robots.[157]

Danaide S.A. and NTechLab

Company Name	**Danaide S.A.**
Headquarters	Buenos Aires, Argentina
Countries of Operation	Argentina
Countries where its surveillance technologies are deployed among Argentina, Brazil, and Ecuador	Argentina
Founded	1999
Public / Private	Private
Major Shareholder(s)	[Not Available]
Number of Employees	[Not Available]
Annual Revenue	[Not Available]

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

[155] Information Service Government of San Juan. "San Juan Agreement: technology applied to security" (in Spanish). October 2020. https://sisanjuan.gob.ar/seguridad/2020-10-22/26837-acuerdo-san-juan-tecnologia-aplicada-a-la-seguridad

[156] BGH. ""BGH Tech Partner suma Hikvision a su portfolio." February 2018. https://www.bghtechpartner.com/2018/02/02/bgh-tech-partner-suma-hikvision-su-portfolio/

[157] Canal AR. "BGH boosts its video surveillance portfolio with Hikvision" (in Spanish). January 2018. https://canal-ar.com.ar/25431-BGH-impulsa-su-porfolio-de-videovigilancia-con-Hikvision.html

Company Name	**N-Tech.Lab Ltd.**
Headquarters	Nicosia, Cyprus
Countries of Operation	Russia
Countries where its surveillance technologies are deployed among Argentina, Brazil, and Ecuador	Argentina
Founded	2015
Public / Private	Private
Major Shareholder(s)	[Not available] Among minority shareholders, the Russian Direct Investment Fund and leading sovereign wealth funds of the Middle Eastern countries made a capital investment of RUB 1 billion (USD $13 million) in 2020.
Number of Employees	[Not Available]
Annual Revenue	[Not Available]

According to some independent reporting,[158] the local **Argentinian** company **Danaide,** hired by Buenos Aires to implement its facial recognition system,[159] may be using Find Face[160] software developed by the Russian company **NTechLab**. Despite our multiple attempts to get more details through freedom of information requests, the government would confirm only that Danaide won a contract bid, declining to clarify whether it developed the facial recognition algorithm itself.

In the Russian version of the NTechLab website,[161] Danaide's **UltraIP**[162] software, which is sold in Argentina, appears in the partners section. In response to ADC's freedom of information request in June 2019,[163] Buenos Aires officials confirmed UltraIP is the name of the software it licensed.

In October 2020, Human Rights Watch alerted the public to flaws in the NTechLab system and its misuse by the government to identify and target children for criminal prosecution in violation of human rights.[164] In **Moscow,** NTechLab provides the software for a surveillance program which rights groups

[158] 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

[159] ADC. "#ConMiCaraNo: Facial recognition in the City of Buenos Aires" (in Spanish). May 2019. https://adc.org.ar/2019/05/23/con-mi-cara-no-reconocimiento-facial-en-la-ciudad-de-buenos-aires/

[160] NTechLab. Find Face official website. https://findface.pro/en/

[161] NTechLab. Partners (in Russian). https://web.archive.org/web/20200511205745/https:/findface.pro/partners/

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

[163] ADC. FOIA request NO-2019-21065074-GCABA-DGAYCSE. July 2019. https://adc.org.ar/wp-content/uploads/2019/07/Respuesta-PAIP-reconocimiento-facial-GCBA-V2.pdf

[164] Human Rights Watch. "Argentina: Child Suspects' Private Data Published Online." October 2020. https://www.hrw.org/news/2020/10/09/argentina-child-suspects-private-data-published-online

say the government has abused by surveilling people during the COVID-19 pandemic to enforce a lockdown.[165]

IBM

Company Name	International Business Machines Corporation
Headquarters	New York, U.S.
Countries of Operation	Worldwide
Countries where its surveillance technologies are deployed among Argentina, Brazil, and Ecuador	Argentina
Founded	1911
Public / Private	Listed on New York Stock Exchange
Major Shareholder(s)	N/A
Number of Employees	Approximately 350,000 in 2020 (on group basis)
Annual Revenue	USD $45 billion in 2020

In December 2016, the National Ministry of Security of Argentina signed a contract with the local company **Unitech S.A**., described as the acquisition of "advanced software for criminal investigations," for a total of $3.515.518,77 USD.[166] Within the procurement documents, the technical specifications state that the products and services in the contract included: nine licenses for IBM i2 Enterprise Insight Analysis,[167] an IBM i2 Collaborate add-on and IBM i2 Text chart, and multiple tech support services.

There are precedents of IBM technology used in the Philippines during the violent "war on drugs." According to a 2009 investigation lead by Human Rights Watch[168] there's evidence that government officials and the police were complicit with death squads that assassinated street children, drug dealers, and petty criminals during Rodrigo Durarte's mandate as Mayor in Davao's City. In 2012, IBM made an agreement with Sara Duterte, Rodrigo Duterte's daughter and mayor of the city at that time, to upgrade Davao's police command center in order to "further enhance public safety operations in the city" while the violence in the streets continued. According to a The Intercept's report,[169] IBM declined

[165] 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

[166] Directorate General of Administration. "ADQ. OF ADVANCED SOFTWARE LICENSES FOR CRIMINAL ANALYSIS WITH THE UNITECH S.A. FIRM." File Nº 347-0066-CDI16. December 2016. https://comprar.gob.ar/PLIEGO/VistaPreviaPliegoCiudadano.aspx?qs=BQoBkoMoEhxZR|eGCUUs0CDTFEc5IK6|8mooLYATqyEzFwVde9PPWAMi|0jPJGKn6pHkBSQAUfnO3onZZEr5bCGawx17losLJTLKoi9VrlOdxyH6GqsNTw==

[167] IBM. i2 Enterprise Insight Analysis 2.3.0. https://www.ibm.com/support/knowledgecenter/SSXVXZ_2.3.0/com.ibm.i2.landing.doc/eia_welcome.html

[168] Human Rights Watch. "You Can Die Any Time." April 2009. https://www.hrw.org/sites/default/files/reports/philippines0409webwcover_0.pdf

[169] The Intercept. "Inside the Video Surveillance Program IBM Built for Philippine Strongman Rodrigo Duterte." March 2019. https://theintercept.com/2019/03/20/rodrigo-duterte-ibm-surveillance/

to respond to queries about its human rights record in Davao City. IBM spokesperson Edward Barbini briefly noted that the company “no longer supplies technology to the Intelligent Operations Center in Davao, and has not done so since 2012,” though he declined to clarify whether IBM serviced the technology after that point, and IBM’s public filings mention the program as ongoing after that date.

Johnson Controls

Company Name	**Johnson Controls International PLC**
Headquarters	Cork, Ireland
Countries of Operation	Worldwide
Countries where its surveillance technologies are deployed among Argentina, Brazil, and Ecuador	Brazil
Founded	1885
Public / Private	Listed on New York Stock Exchange
Major Shareholder(s)	Dodge & Cox Stock Fund (11.3%) in 2020
Number of Employees	Approximately 97,000 in 2020 (on group basis)
Annual Revenue	USD $22,317 million in 2020

In São Paulo, the facial recognition technology installed in the subway was provided by Johnson Controls, a company headquartered in Ireland. This is another case where authorities did not use the traditional procurement system.[170] Instead they acquired the facial recognition technology via an international public procurement, which grants foreign competitors more opportunity to make their offers.

[170] IDEC. “Action questions lack of transparency in SP Subway bidding” (in Portuguese). February 2020. https://idec.org.br/noticia/acao-questiona-falta-de-transparencia-e-solicita-informacoes-sobre-licitacao-do-metro-de-sp

III. CASE STUDIES: HOW THE TECHNOLOGY IS DEPLOYED

CASE STUDY: Argentina

By Asociación por los Derechos Civiles (ADC)

Since 2015, the use of surveillance technologies in Argentina has grown gradually but steadily, opening major risks to the right to privacy throughout the country. In every instance, the private sector has played a key role in deploying technologies, nurturing close relationships with government bodies at local, provincial, and national levels.

We are now facing the peak of a trend that began more than a decade ago in 2008, when local governments started using technologies such as video surveillance cameras (or CCTV) to support their political campaigns,[171] promoting an image of progress toward increased public safety.

According to a study conducted by the Faculty of Psychology of the University of Buenos Aires,[172] a high percentage of the population considers the public safety and security situation in Argentina "very serious” or “extremely serious," and nine out of 10 people think they are "quite or very likely" to suffer a crime in the short term. Because of these fears, public safety has been at the forefront of public officials' narrative to justify the *means* to an *end*. These officials have at the same time cited public safety as a reason to avoid sharing details about their agreements with technology companies, how people’s personal information is processed, and any specifications for the equipment acquired.

Although Argentina has both strong Constitutional protections for human rights, including the right to privacy, and a comprehensive data protection framework, the acquisition and implementation of surveillance technologies is usually carried out with little to no oversight or transparency.[173]

Deployed technology

Uncovering the extent of surveillance mechanisms and systems used by various levels of government is no easy feat, as the information is not readily available through public channels unless the media reports on it, or independent research is carried out.

In addition to CCTV, authorities have slowly introduced more invasive technologies into society over the past decade. **A particular turning point was marked by the introduction of SIBIOS in 2011.** Through Executive Decree 1766/11,[174] the national government created the Federal Biometric Identification

[171] Natalia Zuazo, Revista Anfibia. “Other people's lives” (in Spanish).
http://revistaanfibia.com/cronica/la-vida-de-los-otros/

[172] Faculty of Psychology, University of Buenos Aires. “Insecurity Monitor” (in Spanish). December 2020.
http://www.psi.uba.ar/opsa/informes/monitor_inseguridad_pais_2.pdf

[173] For more information on the broader state of privacy in Argentina, visit:
https://privacyinternational.org/state-privacy/57/state-privacy-argentina

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

System for Security (**SIBIOS**), managed by the Federal Police under the authority of the Ministry of Security.

One of the main goals of SIBIOS was to merge and digitize the independent databases held by the Federal Police and the National Citizens Registry (**RENAPER**, in Spanish). SIBIOS represented the culmination of work that began a few years prior to its launch, when the Ministry of Interior started collecting, processing, and storing biometric data for the issuance of identity cards (DNI) and passports. Since 2009, RENAPER has been allowed to use digital technologies to identify citizens, residents, and visitors. From that point forward, they have been collecting biometric data from every citizen, including fingerprints, palm prints, and face photos, as well as from everyone entering the country.[175]

SIBIOS is a nationwide system, so all provinces in the country have signed cooperation agreements with the national government, together with the Ministry of Security (including its four federal security forces) and the Ministry of Interior (including RENAPER and the National Migration Office). These agreements guarantee that their local police forces can update and access the database. In 2017, through Executive Decree 243/17,[176] the government expanded access to SIBIOS to any public body within the Executive or Judiciary branches at the national and provincial levels, as well as granting access in the Autonomous City of Buenos Aires (Argentina's capital city). Users of SIBIOS are not obliged to obtain a warrant or judicial authorization before running queries on the biometric database.

The Ministry of Security relied on one major vendor for their infrastructure connected to SIBIOS, the French company Morpho Safran, which as a result of a merger became **IDEMIA**. IDEMIA is responsible for the installation and set-up of the Ministry's Automated Fingerprint Identification System (AFIS). The Ministry has acquired and used other products from the company, including Morpho Face Investigate Pilot, for facial recognition from photo and video files, and Morpho RapID,[177] for on-the-ground fingerprint identification checks throughout the country.

Another part of the SIBIOS infrastructure was built by the Ministry of Interior, which nurtured a close relationship with its counterpart in Cuba, particularly between 2011 and 2015. The Ministry acquired its biometric technology from the state-owned Cuban company **DATYS**, which has developed a suite of products for biometric identification[178] and verification,[179] based on facial recognition, fingerprints, palm prints, DNA, and voice. In October 2015, the Ministry updated its biometric technology through a $1.080.000 USD contract with DATYS, plus $180.000 USD per-year for technical support, for a five-year term.

[175] ADC. "The Identity We Can't Change: How biometrics undermine our human rights." 2017. https://adc.org.ar/wp-content/uploads/2019/11/0027-B-The-identity-we-can%C2%B4t-change-12-2017.pdf

[176] Argentine Ministry of Security. Decree 243/2017. http://servicios.infoleg.gob.ar/infolegInternet/anexos/270000-274999/273446/norma.htm

[177] La Capital. "Instantly identity and background in saturation operations" (in Spanish). June 2016. https://www.lacapitalmdp.com/identidad-y-antecedentes-al-instante-en-los-operativos-de-saturacion/

[178] Facial identification,(1:n) is the process to analyze if a detected face image matches one of the face images stored in a database. Here the system is trying to match people against a database of identities.

[179] Facial verification or authentication: (1:1) is the process to analyze if a detected face image matches with a specific face image already stored. Usually, the system attempts to answer the question "is the person in this image the person they claim to be?"

Since the introduction of SIBIOS in 2011, the use of biometric technologies has grown exponentially throughout the country. **In addition to its use for public safety and immigration, biometrics are used for verifying identity in contexts such as social security programs (for example, for access to retirement and pension funds), banking, taxes and fiscal duties, education, elections, and sports**.[180]

Besides biometrics, the Argentinian government has added other surveillance technologies to its repertoire. Military forces at the national level — including the Army, the Navy, and the Air Force — have carried out projects to develop their own Unmanned Aerial Vehicles (UAVs), starting as early as 1996, with further development between 2011 and 2014. Federal police forces have meanwhile relied on one major vendor of commercial drones to fulfil their needs, the Chinese company **DJI** (Dà-Jiang Innovations Science and Technology Co.). In addition, in mid-2017, the Autonomous City of Buenos Aires acquired a surveillance balloon, the Skystar 180, produced by the Israeli company **RT**.[181]

More recently, authorities have increasingly made use of facial recognition and automated license plate readers throughout the country, as part of what seems to be a race among public officials to implement as much technology as possible for the purposes of public safety.

Legal framework

As we note above, Argentina has extensive privacy protections. The national Constitution enshrines this fundamental right in Articles 18 and 19, and Argentina has ratified international human rights treaties[182] such as the International Covenant on Civil and Political Rights and the American Convention on Human Rights.

Moreover, Argentina boasts a robust — although outdated — data protection regime, through Article 43 of the Constitution and National Law Nº 25.326 on the protection of personal data. It is also a signatory to Convention 108+[183] and the European Commission recognized Argentina as having an adequate level of data protection in 2003, through decision 2003/490 EC.[184]

Unfortunately, these laws have proven to be insufficient to protect citizens from state surveillance. **Governments use the exceptions in these laws as legal bases for the deployment of surveillance programs for the normal exercise of state functions, service improvement, and public safety.** To date, there have been very few privacy or data protection-related court challenges and judicial or

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

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

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

[183] Council of Europe. Convention 108 and Protocols. https://www.coe.int/es/web/data-protection/convention108-and-protocol

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

administrative decisions to shield people from the ongoing massive gathering of biometric data and deployment of invasive surveillance technologies.

This deficiency in legal decisions to safeguard people's rights worsened in October 2020, when the legislative power of the Autonomous City of Buenos Aires set a dangerous precedent by passing an amendment to the Law N° 5688 approving the use of facial recognition to identify fugitives from a national watchlist.[185]

Local cases

The trend of increasing deployment of pervasive technologies, which began with CCTVs and SIBIOS, is even more prevalent at the local and provincial levels in Argentina. It's tricky to get updated information from every jurisdiction in the country, particularly when the users of these technologies are local Law Enforcement Agencies (LEAs), so we will focus on the most far-reaching cases and those for which, as part of this project, we did further research to get more detailed information.

We identify surveillance cameras with facial recognition capabilities and software as the most widely used technology at every level of government in Argentina. In April 2019, the Government of the Autonomous City of Buenos Aires announced the implementation of facial recognition software for the security cameras (CCTV) and monitoring centers in the city. In May of the same year, the City of Tigre in the province of Buenos Aires set up the Tigre Operations Center[186] to use cameras and facial recognition software to search for missing persons and identify people with criminal records.

On October 15, 2019, the provincial government in Córdoba announced, through social media, the introduction of "biometric recognition software" deployed in a police SUV, with four mounted cameras and two fixed cameras.[187] Due to the lack of more detailed publicly available information, we sent two freedom of information requests, on November 7, 2019, and November 11, 2020. In both cases, the government didn't provide a response. This adds to the province's long record of non-compliance with the local access to public information law, where it is estimated according to data provided by civil society organization like Red Ciudadana Nuestra Córdoba, Fundeps, Foro Ambiental and Córdoba de Todos, that authorities answer only 10% of the requests they receive per year.[188]

In mid 2017, the province of Mendoza started implementing one of the most invasive surveillance programs in Argentina. Law enforcement agencies in the province have mobile facial recognition cameras and cars equipped with the same technology, as well as fingerprint scanners and license plate

[185] Telam. "The Legislature approved the use of facial recognition for the arrest of fugitives" (in Spanish). October 2020. https://www.telam.com.ar/notas/202010/527676-la-legislatura-aprobo-el-uso-de-reconocimiento-facial-para-la-detencion-de-profugos.html

[186] Ámbito. "Tigre launched a new facial recognition system" (in Spanish). May 2019. https://www.ambito.com/municipios/municipios/tigre-lanzo-un-nuevo-sistema-reconocimiento-facial-n5030978

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

[188] La Voz del Interior. "Respond to requests for information, a pending account from the Province and the municipality" (in Spanish). November 2019. https://www.lavoz.com.ar/ciudadanos/responder-pedidos-de-informacion-una-cuenta-pendiente-de-provincia-y-municipio

readers.[189] Despite our efforts to obtain detailed information from the government, they would provide only the names of the vendors from whom they acquired the equipment (3M Argentina, INTEMA Comunicaciones S.A, Express Software, and Hardware S.A.), not the specifications for the software and hardware. The province's Ministry of Security argued this is because “the required information affects public safety.”

Following this trend, the government of the Province of San Juan announced the “Acuerdo San Juan,” an agreement to implement more technology for public security. This program includes the deployment of CCTV cameras and facial recognition technology, plus a “laboratory of forensic video analysis” for big data processing, to instantly locate people, vehicles, and other items of interest, by searching for objects with particular attributes.[190]

Unfortunately, we could not find much information about the San Juan agreement using publicly available sources. San Juan does not have a law on requests to access public information, but we reached out anyway to public officials with our questions. As of August 2021, they had not replied to any of our inquiries.

Notably, during the COVID-19 pandemic in 2020, local governments started to see technology as a way to mitigate the spread of the virus. Authorities installed thermal cameras in bus and metro lines, airports, and public transport stations. The national government introduced the app “CuidAr,”[191] and provinces used mobile apps to enforce mandatory quarantines, control crowds, and monitor symptoms, stirring controversy over the purpose and uses of these apps.[192] As ADC’s technical analysis and report showed, apps in several provinces, deployed to respond to the public health emergency, present serious concerns for people’s information security and privacy.[193]

CASE STUDY: Brasil

By Laboratório de Políticas Públicas e Internet (LAPIN)

In Brazil, both the public and private sector are using surveillance technologies for a variety of reasons, including public safety and security, fraud detection, and student attendance management at schools. Among the surveillance technologies available, public authorities have a growing interest in facial recognition technologies.

[189] El Sol. “Facial recognition: they found more than 100 people with an arrest warrant” (in Spanish). May 2019. https://www.elsol.com.ar/reconocimiento-facial-hallaron-a-mas-de-100-personas-con-pedido-de-captura

[190] San Juan official website. “San Juan Agreement: technology applied to security” (in Spanish). October 2020. https://sisanjuan.gob.ar/seguridad/2020-10-22/26837-acuerdo-san-juan-tecnologia-aplicada-a-la-seguridad

[191] Council of Europe. “”Digital Solutions to Fight COVID-19.” October 2020. https://rm.coe.int/report-dp-2020-en/16809fe49c

[192] La Capital. “They will control those who breached the isolation with an App on their cell phones” (in Spanish). March 2020. https://www.lacapital.com.ar/la-ciudad/controlaran-quienes-incumplieron-elaislamiento-una-app-sus-celulares-n2572740.html

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

The use of this technology is not much of a novelty in Brazil. A 2019 report from Instituto Igarapé shows that it has been implemented since at least 2011.[194] Since that time, there has been an increase in use cases, and lawmakers have proposed bills to regulate the technology that have been advancing in both federal and state chambers.

Among the myriad public sector uses of facial recognition, we highlight the use that is the most prominent in Brazil: facial recognition for **public security**. Authorities that deploy the technology under this rationale are implementing it in several public spaces, including public events and festivities. A key factor cited to justify its implementation is the concerning figures for violence and crime in the country. For example,

- ➔ in 2018, the number of homicides was 57,956, a rate of 27.8 murders for 100 thousand inhabitants;[195]
- ➔ that same year, Brazil had a prison population of more than 720,000 individuals;[196] and
- ➔ today it remains one of the major transit countries for international drug trafficking.[197]

The technology is also being used for purposes such as **fraud detection in accessing public services, including free public transportation allowances and other social benefits.** In the State of Alagoas, the technology is used in 102 municipalities to verify the identity of social program beneficiaries, like pregnant women and the families of malnourished children.[198] São Paulo city uses a similar mechanism in the urban transportation system to verify the identity of people who use the free entry card. However, the technology deployed captures screenshots of every individual boarding a bus, not just the cardholders, and more than 1.5 million people use buses on a given day in São Paulo.[199] Lastly, in the capital city, Brasília, approximately 2,000 buses are equipped with facial recognition cameras. The company that supplies the technology, **PRODATA**, claims that their solution is developed entirely in house. However, according to information we obtained through a private interview with a representative, several components are imported, such as technology from **Anders** (U.S.) and **Compulab** (Israel).

The same technology is being implemented for **school attendance management** at some public institutions. On the pretext of improving resource management, educational institutions are using facial recognition technology to enable parents to track students, to automatically monitor and control

[194] Igarapé Institute. "Facial Recognition in Brazil" (in Portuguese). 2019. https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/

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

[196] Bueno, S., & Lima, R. S. de. "Brazilian Yearbook of Public Security 2019. Forum Brazilian Public Security" (in Portuguese). 2019. https://www.forumseguranca.org.br/wp-content/uploads/2019/10/Anuario-2019-FINAL_21.10.19.pdf

[197] United Nations Office on Drugs and Crime. "World Drug Report 2020." June 2020. https://wdr.unodc.org/wdr2020/field/WDR20_BOOKLET_1.pdf

[198] Renata Bello. "Facial recognition technology will bring more security to the Food and Nutritional Complementation Program" (in Portuguese). March 2018. http://reconhecimentofacial.com.br/2018/03/11/alagoas-tecnologia-de-reconhecimento-facial-trara-mais-seguranca-ao-programa-de-complementacao-alimentar-e-nutricional/

[199] Diário Do Transporte. "Passenger demand on São Paulo buses has exceeded 1.5 million people per business day since July 7th" (in Portuguese). July 2020. https://diariodotransporte.com.br/2020/07/27/demanda-de-passageiros-nos-onibus-de-sao-paulo-tem-ultrapassado-a-15-milhao-de-pessoas-por-dia-util-desde-07-de-julho/

attendance, and to give out school meals.[200] The use of facial recognition in schools is widespread throughout Brazil, with examples from north to south, including municipal schools,[201] elite private schools,[202] and even at the largest Brazilian university, the University of São Paulo.[203] Although most pilot programs for this technology started between 2018 and 2020, there have been initiatives since before 2014.[204]

For this report, we submitted 33 freedom of information requests to several local administrations, which included state public security secretaries, police forces, city halls, and public transport services. At the federal level, we asked SERPRO, a public company responsible for government data processing, and Receita Federal, the federal revenue service agency, questions regarding the facial recognition services they provide in the context of their activities. We got answers to most of these requests, but they lacked detail and were generic.[205] Accordingly, in some situations we presented administrative appeals.[206]

Deployed technology

It's worth noting that we were not able to identify any case where authorities used the traditional procurement system, open competition. **The most concerning cases were those where local government authorities deployed surveillance technologies that were "donated" to test on the population**. We gave several examples of such scenarios when we addressed each company.

Unfortunately, when reached with freedom of information requests, public authorities seldom provided information on the technical specifications for these technologies. The main reasons they cited were claims of intellectual property/trade secrets protection and lack of knowledge. The few times we obtained information on technical specifics, the information was very superficial.

For example, when we asked about the accuracy of a facial recognition system, Bahia's Public Security Secretaries (Secretarias da Segurança Pública, or SSPS), responded by noting that the system alerts

[200] Revista de Segurança Eletrônica. "Schools use face recognition to control attendance and wasted lunches" (in Portuguese). April 2018. https://revistasegurancaeletronica.com.br/escolas-usam-reconhecimento-facial-para-controlar-frequencia-e-desperdicio-de-merenda/

[201] Diário do Aço. "Facial Recognition System is already working in schools in Ipatinga" (in Portuguese). February 2020. https://www.diariodoaco.com.br/noticia/0075842-sistema-de-reconhecimento-facial-ja-funciona-nas-escolas-de-ipatinga

[202] Reconhecimento Facial. "Maple Bear Porto Alegre School starts using 2BFACE!" (in Portuguese). Jun 2017. http://reconhecimentofacial.com.br/2017/06/07/escola-maple-bear-porto-alegre-passa-utilizar-o-2bface/

[203] Estadão. "Poli-USP tests face monitoring camera" (in Portuguese). July 2017. https://sao-paulo.estadao.com.br/noticias/geral,poli-usp-testa-novo-sistema-de-seguranca-com-cameras-de-monitoramento-facial,70001900605

[204] Baguete. "Ruá launches facial recognition system" (in Portuguese). December 2015. https://www.baguete.com.br/noticias/09/12/2015/rua-lanca-sistema-de-reconhecimento-facial

[205] By the time this report was completed, only five institutions had not answered the freedom of information requests: the Public Security Secretary from the State of Ceará, the Public Secretary from the State of Piauí, and the city halls of Anapolis, Pilar, and Arapiraca.

[206] A case which deserves highlighting is the one from SERPRO. After we presented all possible administrative appeals, the company refused to share important information about facial recognition equipment providers or the level of accuracy for the system, claiming trade secrets. As this publication was completed, LAPIN was considering strategic litigation to address this case at the Judiciary.

police forces when a suspect's identification reaches a 90% likelihood rate. In its turn, the government of Campina Grande informed us that the system has an accuracy above 85% and the camera has a zoom reach of 2 km. However, they did not provide the number of false positives or negatives. Nor did they address the accuracy of the system under different light conditions or on people with different skin colors.

Our questions about the system's efficiency in identifying criminals were also unanswered. Media reports on cases provide reason to doubt the system's efficacy. In Bahia, police arrested more than 200 people based on the use of facial recognition technologies from December 2018 to August 2020,[207] but it is not clear how many of those arrests were false positives. There was a news report on one false positive case, in which the police approached a 25-year-old boy with special needs, mistaking him for a man wanted for assault.[208]

In Rio de Janeiro, the police force claimed that by using technology around the Maracanã Stadium area, it was possible to serve 63 arrest warrants during the America Cup in 2019. News media reported two false positives at the time. One suspect was confused with an individual who was already in jail.[209] The other was a man who was put in prison for several days before police discovered their error.[210]

Even more concerning than lack of accuracy is the fact that facial recognition systems may disproportionately target people of color, as revealed by a study from a Brazilian research institute, "Redes de Observatórios de Segurança."[211] This raises concern about these technologies misidentifying people who already face discrimination in Brazil.

Legal framework

Like Argentina, Brazil has a legal framework to protect privacy. The federal Constitution of Brazil enshrines this fundamental right in Article 5º, X, and XII, and Brazil recognizes international human rights treaties such as the International Covenant on Civil and Political Rights and the American Convention on Human Rights. Moreover, Brazil has unique broad legislation on internet issues, the "Marco Civil da Internet," which establishes specific rules for protecting the right to privacy in the online context through Articles 3º, 8º, and 11. Finally, the country has set a precedent with its adoption of the

[207] G1 Bahia. "Man arrested in Salvador after being identified by the facial recognition system" (in Portuguese). March 2021. https://g1.globo.com/ba/bahia/noticia/2021/03/14/homem-e-preso-em-salvador-apos-ser-identificado-pelo-sistema-de-reconhecimento-facial.ghtml.

[208] Redação 4P. "Salvador's facial recognition system confuses men with special needs with burglar" (in Portuguese). January 2020. https://midia4p.cartacapital.com.br/sistema-de-reconhecimento-facial-de-salvador-confunde-homem-com-necessidades-especiais-com-assaltante/

[209] O Globo Rio. "Facial recognition fails on the second day, and an innocent woman is mistaken for a criminal already arrested" (in Portuguese). July 2019. https://oglobo.globo.com/rio/reconhecimento-facial-falha-em-segundo-dia-mulher-inocente-confundida-com-criminosa-ja-presa-23798913

[210]Band News. "Man is arrested by mistake in Copacabana" (in Portuguese). July 2019. https://bandnewsfmrio.com.br/editorias-detalhes/homem-e-preso-por-engano-em-copacabana

[211] In the study, 151 cases of facial recognition technology use were identified among four federal states. In 42 of these cases, there was data on racial identity. From these 42, 38 of the tracked individuals were Black people. For more information, see: Rede de Observatórios da Segurança. "Portraits of Violence" (in Portuguese). 2019. https://www.ucamcesec.com.br/wp-content/uploads/2019/11/Rede-de-Observatorios_primeiro-relatorio_20_11_19.pdf

federal Data Protection Law (Lei Geral de Proteção de Dados , or LGPD), which was passed after years of multi-stakeholder engagement and enshrines modern legal standards for data protection.

State surveillance-related legislation is also on the rise. According to Instituto Igarapé and the association Data Privacy Brasil,[212] as of June 2020, **at least four state laws address facial recognition technologies at some level**; three of these, Law nº 16.873/2019, from **Ceará**, Law nº 21.737/2015, from **Minas Gerais**, and Law nº 8.113/2019, from **Alagoas**, regulate its use at stadiums. In turn, Law nº 7.123/2015, in **Rio de Janeiro**, focuses on the deployment of the technology in the inter-municipal transportation system. Unfortunately, all of the aforementioned laws provide little or no legal safeguards when deploying the technology. More recently, in November 2020, the **Federal District** approved Law nº 6.712/2020, which regulates the use of the technology for public security purposes at public spaces in the Brazilian capital.[213] Law nº 6.712 follows some good practices, such as making it mandatory to have a human review when the system identifies a person before any decision is taken. However, the law neither determines cybersecurity measures, nor procedures, for the exercise of data subject's rights. Furthermore, it allows the use of the technology for criminal offense investigations. Despite the law already being in force, there is no register of the technology that is used for public security purposes in the Federal District so far.

Several legislative initiatives have been proposed in the states over the last two years. Some examples are Bill nº 391/2019 - **Minas Gerais**;[214] Bill nº 318/2019 - **Rio de Janeiro**;[215] Bill nº 148/2019 - **Paraná**;[216] and Bill nº 865/2019 - **São Paulo**.[217] Another one worth mentioning is Bill nº 42/2020 - **Ceará**.[218] Although it doesn't focus on facial recognition, the law allows police to collect data from private cameras in public areas, expanding the prying eyes of the state. Finally, there are also proposals at the **federal level**, such as Bill nº 4.612/2019 and Bill nº 4.858/2020. Although there is no forecast for these proposals to be included in the National Congress' agenda, the number of bills regarding the deployment of surveillance technologies in the last years reveals the growing interest in the topic.

In December 2019, the Brazilian Ministry of Justice and Public Security published Ordinance nº 793/2019.[219] Among other provisions, it promotes the implementation of "video monitoring systems with facial recognition solutions, Optical Character Recognition, the use of artificial intelligence, or others."

[212] Igarapé Institute and Data Privacy Research. "Regulation of facial recognition in the public sector: assessment of international experiences" (in Portuguese). June 2020. https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf

[213] Official Gazette. Law Nº 6.712. November 2020. https://www.tjdft.jus.br/institucional/relacoes-institucionais/arquivos/lei-no-6-712-de-10-de-novembro-de-2020.pdf

[214] Legislative Assembly of Minas Gerais. Bill Nº 391/2019. 2019. https://www.almg.gov.br/atividade_parlamentar/tramitacao_projetos/interna.html?a=2019&n=391&t=PL

[215] Legislative Assembly of Rio de Janeiro. Bill Nº 218/2019. 2019. http://alerjln1.alerj.rj.gov.br/scpro1923.nsf/0c5bf5cde95601f903256caa0023131b/d9e71e222a9c8e1c832583d0006d6f05?OpenDocument&Highlight=0,318%2F2019

[216] Legislative Assembly of Paraná. Bill Nº 148/2019. 2019. http://portal.assembleia.pr.leg.br/modules/mod_legislativo_arquivo/mod_legislativo_arquivo.php?leiCod=82332&tipo=I

[217] Legislative Assembly of São Paulo. Bill Nº 865/2019, 2019. https://www.al.sp.gov.br/propositura/?id=1000278098

[218] Legislative Assembly of Ceará. Bill Nº 42/2019, 2019. https://www2.al.ce.gov.br/legislativo/tramit2020/8531.htm

[219] Official Diary of the Union. Ordinance Nº 793. October 2019. https://www.in.gov.br/en/web/dou/-/portaria-n-793-de-24-de-outubro-de-2019-223853575

Although the **Brazilian data protection act, Lei Geral de Proteção de Dados, or LGPD, has recently come into force, it does not apply in public safety and security contexts.** This fact undermines LGPD's effectiveness in addressing the use of facial recognition technology in several current cases in Brazil.[220] A team of experts recently proposed a draft for a "Criminal LGPD" Bill which addresses data protection principles and obligations for the processing of personal data by law enforcement authorities,[221] but we do not know whether or when it will be enacted.

Local cases

We'll highlight two regions where facial recognition technologies are heavily promoted for public security: the **Northeast** (NE) and the **Southeast** (SE), two most populous regions of the country.[222] This fact by itself raises some eyebrows as it showcases how **populous areas can become perfect laboratories for the testing of facial recognition technologies**. Many of the cases were implemented by state or city-level Public Security Secretaries. However, police forces (civil and military) have also directly implemented the technology.

Starting with the **Northeast region**, three states should be addressed. In the state of **Bahia**, facial recognition technologies are strategically and widely used in public places such as airports, subways, stadiums, streets, and squares. The technology has also been deployed at significant public events, such as the 2020 carnivals. In Salvador, cameras captured 4.3 million facial records and the police detained 42 people.[223] In Feira de Santana, 1.3 million people had their faces captured, with 33 detained.[224]

The state of **Ceará** takes a different approach and doesn't embed the technology in street cameras, but in police force smartphones which capture faces when authorities approach suspects. When police take a photo, they can compare it with facial images in a Public Security Secretaries database.[225]

[220] While it does not apply in the context of public security, in article 4, paragraph 1, the LGPD states that the future legislation to address the topic shall provide for proportional and strictly necessary measures to serve the public interest, and must observe due legal process, as well as the LGPD's principles of data protection and data subject rights.

[221] Chamber of Deputies. LGPD Criminal Bill. 2020. https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf

[222] According to the Brazilian Institute of Geography and Statistics, IBGE, the population estimate of these two regions in 2020 sum up to more than 146 million people, 69% of the country's population. For more information, see: https://ftp.ibge.gov.br/Estimativas_de_Populacao/Estimativas_2020/POP2020_20201030.pdf

[223] Bahia. "Facial Recognition System has registered more than 4.3 million images" (in Portuguese). February 2019. http://www.bahia.ba.gov.br/2020/02/noticias/carnaval/sistema-de-reconhecimento-facial-ja-registrou-mais-de-43-milhoes-de-imagens/

[224] G1 BA. "Feira de Santana registers 33 arrests for facial recognition during micareta" (in Portuguese). April 2019. https://g1.globo.com/ba/bahia/noticia/2019/04/29/feira-de-santana-registra-33-prisoes-por-reconhecimento-facial-durante-micareta.ghtml

[225] Daniel Praciano. "Security Department analyzes partnership with Chinese technology company to implement new solutions" (in Portuguese). August 2019. http://blogs.diariodonordeste.com.br/narede/seguranca/secretaria-de-seguranca-analisa-parceria-com-empresa-chinesa-de-tecnologia-para-implantar-novas-solucoes/12531

The third example in NE is the state of **Paraíba**. According to the Paraíba Public Security Secretaries, the technology is still in its initial implementation phase, with a contract signed in 2020. Therefore it is still not clear where facial recognition technology will be installed. However, the municipality of Campina Grande used the technology during the traditional festivities of *São João*, which 1.8 million people attended, coming from several regions of the country.[226]

In the **Southeast region**, we call attention to its two biggest state capitals, as well as two other large cities in the region.

In **Rio de Janeiro**, police tested the technology in two public events. In the 2019 Carnival, they spread cameras throughout the Copacabana region, where 1.6 million people were estimated to be present.[227] Also, during the 2019 Copa America, a soccer event that took place between July 6th and October 19th, there were facial recognition cameras in the vicinity of Maracanã stadium. In interviews with public authorities, it was revealed that there are plans to permanently install these cameras on public spaces.

In **São Paulo** city, facial recognition technologies were also used during the 2020 Carnival, using live cameras installed in areas where carnival events took place.[228] Furthermore, there is an ongoing project by the civil police to use the technology for real-time personal identification registration.[229] At the same time, authorities will carry out criminal investigations using screen capture obtained from several cameras installed in both public and private spaces. They will also implement facial recognition technology in the metro stations, where about 3.5 million people use the transport system daily.

Another city from the state of São Paulo, **Campinas**, is known for its "open laboratory" on the use of several "smart city" technologies, including facial recognition technology. There, 30 cameras have already been installed in several public transport stations and vicinities.[230] For this sort of initiative, Campinas was awarded the "smartest" city in Brazil in 2019.[231]

Finally, we highlight the case of **Mogi das Cruzes,** another city in the state of São Paulo, which is known for implementing facial recognition technology for security purposes. There were six live cameras

[226] Viva Campina. "Overall balance of the 2019 Greatest São João in the World has the best results of the last editions" (in Portuguese). July 2019. https://www.vivacampina.com.br/noticia/balanco-geral-do-maior-sao-joao-do-mundo-2019-conta-com-os-melhores-resultados-das-ultimas-edicoes

[227] Jornal do Brasil. "Carnival brings 1.6 million tourists and R$3.5 billion in revenue to Rio" (in Portuguese). March 2019. https://www.jb.com.br/rio/carnaval_2019__rio/2019/03/987757-carnaval-traz-1-6-milhao-de-turistas-e-receita-de-r--3-5-bilhoes-para-o-rio.html

[228] Tilt. Helton Simões Gomes. "For the 1st time, SP has real-time facial monitoring at Carnival; understand" (in Portuguese) February 2020. https://www.uol.com.br/tilt/noticias/redacao/2020/02/19/folia-vigiada-sp-tera-reconhecimento-facial-ao-vivo-no-carnaval-entenda.htm

[229] Tilt. Helton Simões Gomes. "Urban Big Brother? What will the SP police face recognition be like" (in Portuguese). November 2019. https://www.uol.com.br/tilt/noticias/redacao/2019/11/15/big-brother-urbano-como-vai-funcionar-o-reconhecimento-facial-em-sao-paulo.htm

[230] Correio. "Spy cameras start testing phase" (in Portuguese). December 2019. https://correio.rac.com.br/_conteudo/2019/12/campinas_e_rmc/888175-cameras-espias-iniciam-fase-de-testes.html

[231] Prefeitura de Campinas. "Campinas is the smartest and most connected city in Brazil" (in Portuguese). September 2019. http://www.campinas.sp.gov.br/noticias-integra.php?id=37205

operating during the "Festa do Divino Espírito Santo."[232] The police created a database of people they are searching for, such as wanted criminals and lost children, using images scraped from social media network profile pictures.[233] The system operates as part of a partnership between the municipality and **Dahua Technology**, where the technology was given to authorities for free, and according to the city, it can be used in other public spaces since its mainframe was installed on vehicles.[234]

CASE STUDY: Ecuador

By LaLibre.net

The use of video surveillance systems in public spaces in Ecuador dates back to 2002, a year in which the mayors of Quito and Guayaquil, the two most populated cities in the country, launched the first pilot programs for the "Sistema Ojos de Águila" (Eagle Eyes System). This project was initially carried out within the two municipalities and was touted as a tool to reduce crime[235] and improve the population's perception of safety. At that time, authorities installed eight[236] **PELCO** brand video surveillance cameras in Quito and 20[237] in Guayaquil, in the central areas of each city.

Other municipalities quickly followed the example of these two large cities, despite the fact that **there are no conclusive studies to demonstrate the effectiveness of this type of surveillance on citizen security, reduction of crime, or prevention of violent deaths**.[238] However, national and local media outlets used images taken from the cameras to show what they consider to be public safety "achievements."

Between 2010 and 2014, the government of Rafael Correa set new policies to "reduce crime and build a peaceful social coexistence." This consisted of creating a decentralized model for the National Police, with a new zoning and management model. The policies were designed and implemented mainly by the Ministry of Justice, the Ministry of Security Coordination, and the Ministry of Interior, with direction by its minister José Serrano. There is research to suggest the changes may have given the appearance of reducing crime, but did not have significant impact. According to the researchers Castro, Jácome, and Mancero (2015), officials did want to improve crime indicators, and they did show reduced rates in

[232] "Festa do Divino Espírito Santo" is a religious festival in Mogi das Cruzes celebrated annually, where people gather in public spaces to watch processions and concerts, among other things. Last year, it hosted around 200,000 attendees during the seven days of the festival. For more information, see: http://www.festadodivino.org.br/

[233] Diário TV 1ª Edição. "Facial recognition system reinforces security at the Festa do Divino festivity in Mogi das Cruzes" (in Portuguese). June 2019. https://g1.globo.com/sp/mogi-das-cruzes-suzano/festa-do-divino/2019/noticia/2019/06/07/sistema-de-reconhecimento-facial-reforca-seguranca-na-quermesse-da-festa-do-divino-em-mogi-das-cruzes.ghtml

[234] City Hall of Mogi das Cruzes. "Security for the Festa do Divino will have face recognition cameras" (in Portuguese). May 2019. https://www.mogidascruzes.sp.gov.br/noticia/seguranca-para-a-festa-do-divino-tera-cameras-com-reconhecimento-facial

[235] Castro, D., Jácome, J.C., Mancero, J. "Citizen Security in Ecuador: Ministerial Policy and Impact Assessment, Years 2010-2014" (in Spanish). Nova Criminis 9. Pp.111-148. 2015

[236] El Universo. "Eight cameras for the Eagle Eyes plan" (in Spanish). April 2002. https://www.eluniverso.com/2002/04/22/0001/10/2388C8238A14459AB2ADE998D58D7FFB.html

[237] El Universo. "Controversy over the use and management of the 'Ojos de Águila' system" (in Spanish). December 2007. https://www.eluniverso.com/2007/12/16/0001/10/B3296480B7784A66AA773C39D74E9B3A.html

[238] Ethnodata. "An exploration of the relationship between the gain in security infrastructure and the rate of violent deaths in Ecuador" (in Spanish). 2020. https://www.ethnodata.org/es-es/muertes-violentas/upc/

2014, the same year in which the price of oil declined, and the economic boom slowed.[239] But the reduction in crime may not have been the result of using facial recognition equipment, but instead a reflection of categorizing crime in a new way, as part of modifications under the new Comprehensive Organic Criminal Code and meticulous statistical work.[240] In 2010, the new administration officials created the national service called **"Integrated Security Service ECU911."**.

The ECU911 service is administered by a public body, reporting to the President, that directs all emergency calls (police, fire departments, ambulances, etc.) to a single number -911- that implies the deployment of several monitoring and video surveillance centers nationwide which are interconnected and gather information from different territories. The implementation of this "Integrated Service" has not been exempt from criticism. In 2019, the former President of Ecuador, Lenin Moreno, revealed that it had been used for espionage. He said the institution's work was "diversified to another perverse task: spying on political adversaries and citizens that they (the government) intended to coerce."[241] There were also reports about corruption in the deployment and implementation process.[242] Despite these facts, the Integrated Service has continued to develop and expand without challenges.

In 2012, the Planning and Development Secretariat established a new division for administrative planning units: national, zone, districts, and circuits. These represent a unit of surveillance under "sub-circuits" for monitoring and control. Before this, the mechanisms for control had never been so centralized. For the next seven years, authorities prioritized improving National Police equipment, and based on the new order of units, it had better representation in the territory. In 2017, when Rafael Correa ended his term, the government invested $781 million USD in infrastructure and equipment for the National Police.[243]

At the end of this research, the former Ecuadorian government was one of the least popular in Latin America,[244] perhaps due to its aggressive police and security forces and dismal record of human rights violations.[245] The Ministry of Government (Interior and Police) was managed by a Police Commander General, the Ministry of Defense by an Army Division Major-General, and the Director of the Integrated Security Service ECU911 is a Lieutenant Colonel of the General Staff Police. All of them were directly appointed by the executive, without competition or opposition.

[239] El Universo. "$ 77,530 million Ecuador received in 7 years for oil exports" (in Spanish). January 2015. https://www.eluniverso.com/noticias/2015/01/05/nota/4399061/77530-millones-recibio-pais-7-anos-exportacion-petrolera

[240] Ethnodata. "An exploration of the relationship between the gain in security infrastructure and the rate of violent deaths in Ecuador." 2020. https://www.ethnodata.org/es-es/muertes-violentas/upc/

[241] El Comercio. "Lenín Moreno says that ECU 911 was used in a 'perverse' way for espionage" (in Spanish). April 2019. https://www.elcomercio.com/actualidad/lenin-moreno-ecu-911-espionaje.html

[242] Vistazo. "ECU-911: Contracts that panic" (in Spanish). May 2019, https://www.vistazo.com/seccion/pais/ecu-911-contratos-que-dan-panico

[243] Presidential Report Notice. "781 million dollars is the government investment in infrastructure and equipment for the police" (in Spanish). Accessed January 2020. https://www.presidencia.gob.ec/781-millones-de-dolares-es-la-inversion-del-gobierno-en-infraestructura-y-equipamiento-para-la-policia/

[244] Mitofsky. "Approval of leaders America and the world" (in Spanish). March 2021. http://www.consulta.mx/index.php/encuestas-e-investigaciones/el-mundo/item/download/1209_7300384f47710f38dd84cec8765dd463

[245] OEA. "IACHR Presents Observations on its Visit to Ecuador" (in Spanish). January 2020. https://www.oas.org/es/cidh/prensa/comunicados/2020/008.asp

In order to obtain information for the current report, we filed several formal requests based on the right of access to public information established in the Organic Law of Transparency and Access to Public Information, Art. 1 and Art. 18 (numeral 1 and 2) and Art. 66 of the Constitution of the Republic of Ecuador. We presented the requests to various institutions but obtained very few responses.

When we asked about the vídeo surveillance technology officials have implemented, the use of facial recognition technologies, and the legal framework for implementation, the National Assembly responded to only some of our questions. We learned that the debate over the current data protection bill was still in progress and there is no legal framework for the use of video surveillance and biometric recognition technologies.[246] In some cases, authorities requested more time to provide additional information to complement the initial response.

We also sent a request to the ECU911 in the hope of obtaining information regarding how people's data are processed, who can access that data, the existence of security protocols, whether they conducted a human rights impact assessment, and the names of the products and devices deployed, among other questions. Unfortunately, the institution excused itself from providing information, claiming it is a state secret. **ECU911 did say they do not have cameras with facial recognition capabilities, but multiple official announcements indicate otherwise.**[247]

As we completed this report in August 2021, we had not received answers from other relevant institutions, including the Ministry of Government, the Ministry of Telecommunications and Society of Information, and the National Direction of Public Data Registry (DINARDAP).

Deployed technologies

In April 2019, the *New York Times* published an investigation on Ecuador's use of video surveillance technology developed by Chinese companies.[248] It revealed the operation of 4,300 cameras used for intelligence tasks without regulation. In this report, we took into account the video surveillance infrastructure controlled directly by the ECU911, but there are hundreds of video surveillance devices that function autonomously in the municipalities of Quito and Guayaquil. In 2020, these cities were connected with the Integrated Security Service ECU911 to increase its capabilities.

To obtain the real number of "Eagle Eyes'' installed in the country, we asked the Director of the Integrated Security Service ECU911, Juan Zapata, to provide information in this regard. While he refused to respond, his earlier statements indicate that in October 2019 (before the integration with the municipal systems of Quito and Guayaquil), the Service had 4,638 active devices for video

[246] National Assembly response. December 2020. https://nube.cyberzen.ec/s/qjto9dZwmmW9GRT

[247] Integrated Security Service ECU911. "ECU 911 presented a report related to international cooperation mechanisms and tools" (in Spanish). October 2019. https://www.ecu911.gob.ec/ecu-911-presento-informe-relacionado-con-mecanismos-y-herramientas-de-cooperacion-internacional/

[248] New York Times. "Made in China and exported to Ecuador: the state surveillance apparatus" (in Spanish). April 2020. https://www.nytimes.com/es/2019/04/24/espanol/america-latina/ecuador-vigilancia-seguridad-china.html

surveillance.[249] There were 890[250] cameras in the Municipality of Quito that were integrated in January 2020 and 1,100 cameras of the Municipality of Guayaquil in September. Based on this information, **there are more than 6,600[251] cameras controlled by the ECU911.**

The COVID-19 pandemic has resulted in increased control and surveillance, which a large part of the public sees as positive and accepts. While such surveillance is seen as justifiable due to the fear that a health and humanitarian crisis generates, these tools have not been used solely to measure social distancing or provide security to citizens. According to President Lenin Moreno, these instruments are also used for espionage and political harassment, establishing the possibility of recurrence.[252]

It's worth mentioning that in July 2020 the **Inter-American Development Bank** contributed to the Ecuadorian government's development of software called "**Distancia2**" for use with the video surveillance cameras already deployed on the streets. The software, which authorities and the media have widely promoted, uses artificial intelligence to measure the physical distance between people, alerting monitoring agencies when COVID-19 distancing rules are not being followed.[253]

The surveillance technologies implemented in Ecuador are provided primarily by the following companies: **Axis** (Sweden), **Hikvision** (China), and **VERINT** (Israel and U.S.). However, there is small-scale deployment using products from **Intelligent Security Systems** (Russia), **Pelco Corporations** (U.S.), and **Tiandy** and **ZKTeco** (China). Most of them interoperate by means of protocols and standards developed by **OVNIF**,[254]an organization dedicated to the development of standards for the interoperability of security devices.

Legal framework

Ecuador has some provisions in the law regarding privacy on a constitutional and international level. The Constitution of Ecuador enshrines the fundamental right to privacy in Article 66, and Ecuador recognizes the international human rights treaties such as the International Covenant on Civil and Political Rights and the American Convention on Human Rights. **However, in contrast to Brazil and Argentina, Ecuador lacked a specific regulation on data protection and privacy until 2021.** After the leak of personal data of 20 million Ecuadorians in 2019,[255] the President and several institutions

[249] Integrated Security Service ECU911. "At Smart City 2019, the ECU 911 video surveillance system modernization plan was announced" (in Spanish). October 2019. https://www.ecu911.gob.ec/en-smart-city-2019-se-anuncio-el-plan-de-modernizacion-del-sistema-de-videovigilancia-del-ecu-911/

[250] Integrated Security Service ECU911. "1,518 cameras of the ECU 911 and the Municipality interconnected for the security of Quito" (in Spanish). January 2020. https://www.ecu911.gob.ec/1-518-camaras-del-ecu-911-y-del-municipio-interconectadas-para-la-seguridad-de-quito/

[251] Integrated Security Service ECU911. "ECU 911 cameras register indiscipline and non-compliance with citizens in several cities of the country" (in Spanish).May 2020. https://www.ecu911.gob.ec/camaras-del-ecu-911-registran-indisciplina-e-incumplimiento-ciudadanos-en-varias-urbes-del-pais/

[252] El Comercio. "Lenín Moreno says that ECU 911 was used in a 'perverse' way for espionage" (in Spanish). April 2019. https://www.elcomercio.com/actualidad/lenin-moreno-ecu-911-espionaje.html

[253] El Comercio. "Security cameras will monitor physical distancing in Ecuador" (in Spanish). June 2020. https://www.elcomercio.com/actualidad/camaras-vigilaran-distanciamiento-fisico-covid19.html

[254] For more information, see: https://www.onvif.org/

[255] BBC News. "Data breach in Ecuador: the "serious computer failure" that exposed the personal information of almost the entire population of the South American country" (in Spanish). September 2019. https://www.bbc.com/mundo/noticias-america-latina-49721456

committed to the development of a data protection law in the short term to respond to public concerns.[256] In May 2021, the National Assembly approved a modern data protection law.[257] It is yet to be determined whether this law will be enough to protect citizens from intrusive surveillance technologies since there's no specific regulation planned in this regard.

Local cases

In 2019, the mayors of Quito and Guayaquil undertook parallel projects with the similar goal of acquiring cameras and video analytics licenses for artificial intelligence-powered facial recognition.

In January 2020, authorities signed an inter-institutional agreement for the integration of the surveillance infrastructure for the monitoring centers of Quito with those of the ECU911, increasing the total surveillance capacity to 1,518[258] video surveillance devices for the city. The 628 cameras of the Integrated Service ECU911 and the 890 cameras of the Municipality of Quito, as well as any new cameras, are now accessible to both institutions.

Later in 2020, Guayaquil's video surveillance devices were integrated with the ECU911, just as Quito’s system and that of other regions had been in the previous months. The government built a new operational center of ECU911 in the city for approximately $13 million USD, including $1 million USD for the acquisition of software for video analytics and several cameras for integration into the national video surveillance system. There are, accordingly, more than 2,000 devices that monitor this city.

Based on press releases and public procurements, we conclude that the integrated surveillance system is mainly used in Guayaquil and Quito, but the technology is installed nationwide even in small municipalities, such as Shushufindi[259] [260] and Quevedo.[261]

[256] El Universo. "The Bill on Protection of Personal Data in Ecuador" (in Spanish). August 2020. https://www.eluniverso.com/larevista/2020/08/24/nota/7953820/datos-personales-ley-ecuador

[257] Official Registry. Fifth Supplement Nº 459. https://www.registroficial.gob.ec/index.php/registro-oficial-web/publicaciones/suplementos/item/14857-quinto-suplemento-al-registro-oficial-no-459

[258] Integrated Security Service ECU911. "1,518 cameras of the ECU 911 and the Municipality interconnected for the security of Quito" (in Spanish). January 2020. https://www.ecu911.gob.ec/1-518-camaras-del-ecu-911-y-del-municipio-interconectadas-para-la-seguridad-de-quito/

[259] Official Public Procurement System. SIE-GADMSFD-012-2016. August 2016. https://www.compraspublicas.gob.ec/ProcesoContratacion/compras/PC/informacionProcesoContratacion2.cpe?idSoliCompra=lIWn6R6_KAorcEHiMtHkUdaqUHKgoWj2Xc9ws8xEKOY,

[260] Official Public Procurement System. SIE-GADMSFD-2018-059. December 2018. https://www.compraspublicas.gob.ec/ProcesoContratacion/compras/PC/informacionProcesoContratacion2.cpe?idSoliCompra=6N1fWVKkcDQjCErudz79IPThdQYl2SDKXJgMZHkNfh0,

[261] Official Public Procurement System. SIE-GADMQ-006-2019. December 2019. https://www.compraspublicas.gob.ec/ProcesoContratacion/compras/PC/informacionProcesoContratacion2.cpe?idSoliCompra=bCDa1cd5ztLy9wcH_d5PXToQ4JsCMfZg_iiQ1xdj-zQ,

IV. CONCLUSION AND RECOMMENDATIONS

The technologies discussed in this report pose a growing threat to our human rights: they give authorities the capacity to identify, follow, single out, and track people everywhere they go, undermining our rights to privacy and data protection, the right to free assembly and association (leading to the criminalization of protest and inducing a chilling effect), and the rights to equality and non-discrimination. Civil society groups across the world have been raising the alarm about the use of facial recognition and other biometric surveillance technologies, and there are movements and campaigns to ban applications of these technologies in the European Union,[262] the United States,[263] India,[264] Russia,[265] and many other places.

The goal of this report is not just to show that these technologies threaten our rights, but to expose the lack of transparency and accountability for the companies that make deals with governments for implementation. In some cases, these companies provide this dangerous technology for free in order to test it on the population, disregarding the impact on people's fundamental rights. While we hope that this report motivates rights organizations, journalists, and activists to keep asking questions and investigating companies and governments, the burden of preventing harm should not fall only on civil society. Governments have a duty to protect citizens' fundamental rights, and companies must respect those rights. We need **lawmakers** to take **bold and concrete action to stop the spread of this technology**, **banning technology that enables mass surveillance**, and putting in place safeguards to protect people, such as remedies for those whose privacy is violated, and robust measures to **increase accountability and transparency — both for the companies that develop the technology and the authorities that deploy it**. Allowing broad exceptions for use of the technology for "public safety" reasons opens the door to abuse of these systems. Public safety is also not a legitimate excuse for keeping citizens, journalists, and others in civil society in the dark.

When using any sort of technology, and even more so in cases where fundamental rights are at stake, **governments** should conduct human rights impact assessments before making a decision or deploying the system, and decline to purchase or use technology from companies with a poor human rights record. Public agencies should improve their transparency by communicating and sharing the documents related to meetings and agreements for the acquisition of surveillance technology, and consult with civil society about the potential for harmful impact.

Meanwhile, **companies** must commit to comply with standards of transparency, accountability, and respect for human rights. In order to do that, they have to improve their communication when asked for information about products and services with implications for human rights, implement robust human

[262] For more information, visit https://reclaimyourface.eu/

[263] For more information, visit https://banthescan.amnesty.org/

[264] Internet Freedom Foundation. "FF proposes a three year moratorium on the use of Facial Recognition Technology in India #ProjectPanoptic." March 2020. https://internetfreedom.in/we-have-written-to-the-government-seeking-a-3-year-moratorium-on-government-use-of-facial-recognition-technology-in-india-projectpanoptic/

[265] For more information, visit https://bancam.ru/en

rights due diligence procedures, produce transparency reports, proactively and continuously seek information to understand and become aware of the human rights impact of their technologies, and provide adequate remedies to victims of abuses they facilitate.[266]

Public and traditional media have a fundamental role in creating awareness and debate by changing the narrative about surveillance tech from magical solutions to tools that require a broad public discussion and a commitment to comply with human rights laws and principles.

[266] United Nations Office of the High Commissioner for Human Rights, "Guiding Principles on Business and Human Rights" June 2011. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf