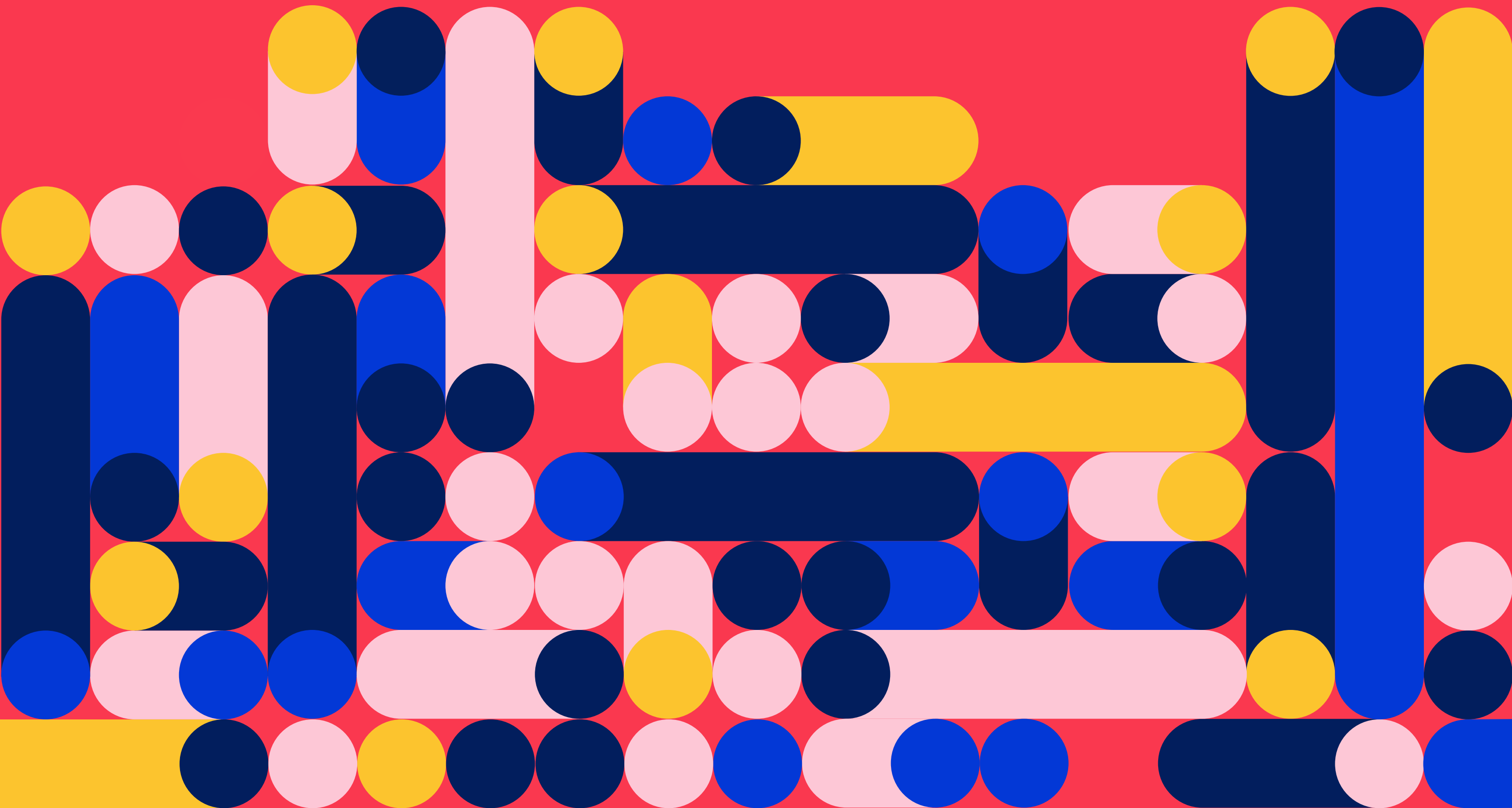
Facial recognition in Latin America

Trends in the implementation of a perverse technology

AlSur



Facial recognition in Latin America: trends in the implementation of a perverse technology

Text: Jamila Venturini y Vladimir Garay (Derechos Digitales)
Review: María Paz Canales (Derechos Digitales), Juan Diego Castañeda (Fundación Karisma) y Cristin León (Al Sur).
Translation to Portuguese: Dafne Melo.
Translation to English: Pedro Nogueira.
Layout: Rocío Rubio.
Graphs: Data Sketch.

Data collection: Abdías Zambrano (Ipandetec), Alejo Kiguel (ADC), Bárbara Simão (Internet Lab), Dilmar Villena (Hiperderecho), Joana Varon y Vanessa Koetz (Coding Rights), Juliana Valdés, Juan Diego Castañeda y Joan López (Fundación Karisma), Luã Cruz (IDEC), Maricarmen Sequera (TEDIC), Michele Bordachar (Derechos Digitales), Santiago Narváez (R3D).

with the support of

AlSur

NED | NATIONAL ENDOWMENT FOR DEMOCRACY
SUPPORTING FREEDOM AROUND THE WORLD

By way of introduction

Facial recognition is a biometric identification technology that, by analyzing certain characteristic features of the face, seeks to establish a person's identity. Although it is less accurate than other forms of biometric identification, such as fingerprint or iris reading, it does not require physical contact. This allows its deployment, for example, in public spaces for large-scale surveillance purposes and without those who are being subjected to its scrutiny necessarily being aware of it.

Although its introduction dates back to the 1960s, several recent technical advances have been key to its application in recent years. The development of new technologies for image capture and processing, advances in the field of "big data" -associated with the collection, storage and processing of large volumes of data- as well as advances in "deep learning" techniques in the "training" of algorithms, have facilitated the increasing adoption of facial recognition systems in different fields. Today, facial recognition has varied applications ranging from unlocking mobile devices to attempts to "read" intentions and emotions, a use that links it to the phrenological techniques and theories developed in the 19th century.

While facial recognition systems can be diverse, they all require at least three elements to work: a way to capture images, software tasked with analyzing the images, and a database of faces for comparison. The accuracy of the system will depend on access to a database that allows the identification of the images with previously cataloged subjects, that the images meet certain minimum quality standards required by the software for its analysis (size, brightness, that the image capture the analysis points used by the system, etc.), the way the algorithms have been "trained" to make the associations between the captured data and those in the database that allow the comparison, as well as the design of the software itself, which will indicate the precise parameters according to which the comparisons will be made to produce the identification. Problems at any of these levels can prevent the system from correctly performing the function for which it has been implemented, which can result in failed recognition, arbitrary discrimination and false positives, all situations - unfortunately - commonly associated with the use of facial recognition systems, especially when used to monitor public space and to safeguard access to social rights.

This problem increases dramatically when the people subject to this technology belong to historically vulnerable groups such as women, dark-skinned people or trans people. Thus, the implementation of facial recognition systems entails the technical reproduction of social exclusion biases and, when used for surveillance purposes, threatens the right to dignity, due process and the presumption of innocence, among others.

Because it is a biometric identification technology, that is, it processes information related to our bodies, facial recognition is a highly intrusive technique that forces the collection and storage of highly intimate data, taking away our control over our face and potentially endorsing its use against our own interests and benefits.

When used for the surveillance of public space and combat common crime, facial recognition erodes the autonomy of people in favor of a system that aims at absolute control through the technical management of identities, reproducing the inequalities and exclusions that historically have put non-hegemonic communities at a disadvantage.

The objective of this research is to foster public debate about the way in which facial recognition systems have advanced in Latin America, on the basis of state initiative. These developments have been marked by excessive opacity and little commitment on the part of the authorities to ensure minimum conditions in their deployment in order to mitigate the impact on the exercise of fundamental rights.

What are the facial recognition technologies present in the region? What are they used for? Who provides them? How are they regulated? How are they audited? These are some of the questions that this research attempts to answer.

The report begins with an explanation of the methodology used to collect information on the initiatives, followed by an overview of the trends observed in the region and a more in-depth analysis of the companies that provide facial recognition technology. We conclude with some considerations about the observed impact of the identified initiatives.

Mapping facial recognition in Latin America

This report presents a qualitative analysis based on findings from the information collected on the deployment of facial recognition systems in nine Latin American countries; it was conducted between April and May 2021. The research was developed by the organizations that are part of Consorcio Al Sur, based on a methodology proposed by the following organizations: Coding Rights, IPANDETEC, InternetLab, R3D, Derechos Digitales, TEDIC and Fundación Karisma.

The objective of the research was to map in detail the existing initiatives in the region, with special emphasis on identifying the companies providing the dominant biometric technologies and their countries of origin, the type of relationship established with the states, the areas in which their presence predominates and their potential social, economic and political consequences. For this reason, the analysis focuses on initiatives implemented at the initiative of the state, although it recognizes the existence of a number of applications of facial recognition systems driven by the private sector with great potential for affecting fundamental rights. Furthermore, this research is considered the first step in a broader effort to map biometric identification technology in Latin America.

This report is complemented by the website https://estudio.reconocimientofacial.info/, which has more details on each of the initiatives, technology providers and more information on regional trends in the implementation of facial recognition systems in the region. Also, at reconocimientofacial.info it is possible to find news and updates on actions to resist the implementation of these systems, models for requesting access to information, among other information.

Methodology

The exercise of identifying and characterizing the facial recognition systems present in the region and the entities responsible for providing and implementing such technology was carried out through the preparation of standardized data sheets, which provide relevant information, including area of application, current status of the initiative's operation, country of origin of the suppliers and sector to which they belong, features of the contract, existence of previous impact studies and audits subsequent to the implementation of the system, and more. The objective was to be able to typify the information in order to make it comparable and facilitate the identification of regional trends.

Facial recognition systems developed within the framework of public policies were considered, especially those systems implemented to assist public space surveillance and identity authentication, particularly as a measure of access to rights and social benefits. Systems deployed in private spaces such as stores, shopping malls or private banks were not included, nor were systems implemented in areas such as electronic commerce or access to digital devices or applications where they do not condition access to a public service.

The information compiled in the data sheets includes the following aspects:

- Country
- Name of the initiative
- Description of the system
- Area of application
- Type of use
- Date of implementation
- Current status of the initiative
- Technology providers involved
    - Name
    - Country
    - Sector (government, private, academic, civil society)
    - Website
    - Type of contract (direct, tender, donation)
    - Contracting details
- Is there any legal or regulatory basis for implementation?
- Was there a public participation process prior to implementation?
- Did the implementation process consider conducting an impact study on privacy and/or human rights?
- Is there a planned external audit of the implementation?
- Are there any records of security incidents, discriminatory use, or other types of abuse related to the initiative since its implementation?
- Organization that filled out the data sheet.

The information was compiled from the following sources:

- Information access requests.
- Semi-structured interviews with key actors: companies, public agents, etc.
- Keyword search in search mechanisms: various internet search engines, media, transparency portals, government websites, etc.
- Consultation with human rights organizations, social movements, journalists and activists in each country.

What, how, where? Regional trends on the implementation of facial recognition in Latin America

Within the framework of this research, 38 initiatives for the use of facial recognition have been mapped, spread over nine Latin American countries and implemented under different public policies. Although this is not an exhaustive list of the totality of existing systems in the region, the numbers serve to provide a general idea of the Latin American panorama regarding the advancement of this technology and its development.

Most of the facial recognition systems documented in the research date back to the last three years, with only seven of them implemented prior to 2018. Of the 38 systems listed, 22 are currently active, five have been deactivated , three are in the pilot stage and eight are in the process of implementation.

Regarding the five systems that have been deactivated, in two cases it was due to a court order that prevented their continued operation and use, both in Brazil ("ViaQuatro"[1] and "Edital de Licitação do Metrô de São Paulo" [São Paulo Subway Tender Notice]).[2] In two other cases the systems were never implemented (the "Sistema Integrado de Videovigilancia Inteligente para Transmilenio" ["Integrated Intelligent Video Surveillance System for Transmilenio"] in Colombia"[3] and the "Fórmula anti evasión Transantiago y Metro de Valparaíso" ["Anti-evasion formula Transantiago and Valparaíso Metro"] in Chile) and one was canceled due to failures, interruptions and lack of security measures ("Aplicación móvil de reconocimiento facial para entregar la Clave Única" ["Mobile facial recognition application to deliver the Unique Key"] in Chile).[4]

Regarding the areas of application of the systems, by far the most recurrent use is "public security" (30 systems listed) and "surveillance of public spaces" (31 systems listed). This is followed by transportation (7 systems listed), social assistance and migration (3 systems, respectively). Within the framework of this research, it was not possible to document facial recognition systems implemented in the field of education or in electoral processes, despite the fact that these are areas in which, anecdotally - and especially in the context of a pandemic - their implementation has increased. Also, it should be noted that 10 initiatives are used to control access to economic, social and cultural rights, such as social benefits granted by the state, while the use of six of them is related to the control of access to civil and political rights, as access to identification by citizens.

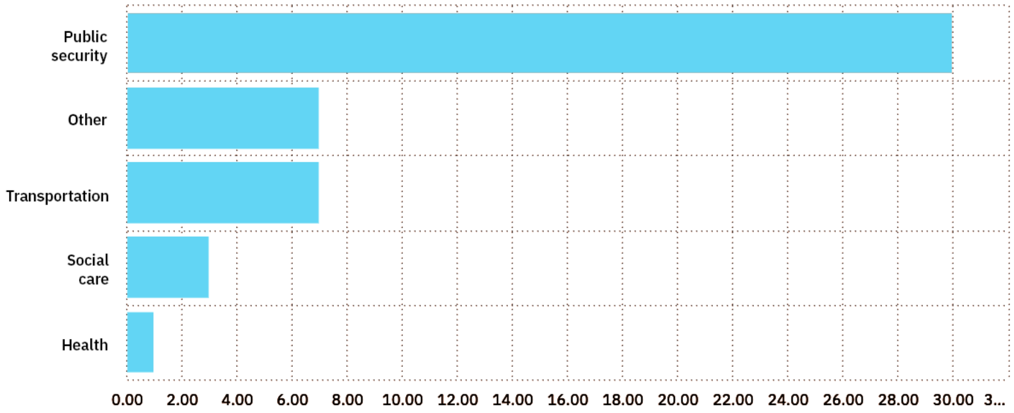
[1] See https://reconocimientofacial.info/reconhecimento-facial-a-banalizacao-de-uma-tecnologia-controversa/

[2] See https://reconocimientofacial.info/justicia-brasilena-condena-empresa-de-metro-por-uso-de-reconocimiento-facial-sin-consentimiento-en-sao-paulo/

[3] See https://digitalid.karisma.org.co/2021/07/01/SIVIT-reconocimiento-facial/

[4] See https://www.biobiochile.cl/noticias/nacional/chile/2020/03/29/registro-civil-anuncio-que-bajo-la-app-para-obtener-clave-unica-hubo-denuncia-sobre-su-seguridad.shtml

Area of application of the initiatives



Regarding the normative bases that regulate the implementation of facial recognition technology, it is important to mention that in more than 60% of the cases there is no specific legal basis to support the implementation. Only 14 of the 38 documented cases indicate the existence of regulations that would support the deployment of this type of technology. However, it is noteworthy that in most of the cases the regulations cited are not specifically for the use of facial recognition or biometric data, but are a broad interpretation of regulations referring to the use of other types of technologies (for example, the operation of video surveillance cameras), that are analogized to facial recognition with dubious arguments or specific powers that could be fulfilled through the use of facial recognition ("to oversee compliance with provisions on evasion in public transport", "immigration verification functions, foreigners and immigration control", etc.)

Few are the cases in which specific regulations are indicated that refer to facial recognition or other biometric identification technologies. Examples of this would be Portaria No. 1,515 of December 18, 2018 of the National Traffic Department - DENATRAN in Brazil, which enables the implementation of biometric data collection and storage for the granting of driver's licenses,[5] the regulations governing the "Sistema Público Integral de Video Vigilancia" [Comprehensive Public Video Surveillance System] created by the law of the City of Buenos Aires N. 5688 in Argentina[6] and bill 234 in Colombia[7] which establishes that the "Registraduría Nacional del Estado Civil" [National Civil Registry] will be able to identify and authenticate nationals in digital media in Colombia through "all types of biometrics" and which is being reviewed by the Constitutional Court. Even at the level of personal data protection, in those countries where general rules exist, references to the specific regulation of the use of biometric data are scarce. In the opinion of the various local experts, none of the regulations used to justify the implementation of facial recognition systems offers adequate treatment from a human rights point of view.

This deficient regulatory context aggravates the risks that this type of technology poses to the exercise of fundamental rights. It should also be mentioned that most attempts to regulate biometric identification technologies seem to be more concerned with validating their implementation than with balancing their purpose with respect for the rights of citizens. Therefore, while it is true that specific regulation can be beneficial when it seeks to remedy deficiencies in the general regulations on personal data protection, this will only be possible when its formula-

[5] See https://www.legisweb.com.br/legislacao/?id=372479

[6] See http://www2.cedom.gob.ar/es/legislacion/normas/leyes/ley5688.html

[7] See http://leyes.senado.gov.co/proyectos/index.php/textos-radicados-senado/p-ley-2020-2021/2021-proyecto-de-ley-234-de-2020

tion considers a focus on preventing impact risks on the exercise of fundamental rights, including notably privacy and non-discrimination.

In the vast majority of cases, the facial recognition systems identified within the framework of this study were implemented without any kind of public consultation or participation, with the exception of a surveillance system in Chile, an initiative whose discussion involved the participation of regional councilors, popularly elected representatives who are part of the country's decentralized regional government structure. During the discussion of the law governing the "Sistema de Reconocimiento Facial de Prófugos"[Facial Recognition System for Fugitives] in Buenos Aires, various organizations were able to present letters expressing their concerns,[8] but there was no discussion in the "Comisión de Derechos Humanos de la Legislatura de la Ciudad de Buenos Aires" [Human Rights Commission of the Legislature of the City of Buenos Aires] as initially foreseen, which generated an important demand from civil society.[9] In the rest of the initiatives there was no open consultation or any instance of public participation regarding the design and implementation of facial recognition systems.

There were not either any privacy or human rights impact studies, the former being understood as assessments that look at the risks of the use of personal data by a system for the informational self-determination and privacy of its holders, while the latter can be defined as a process to identify, understand, evaluate and address the adverse effects of a public activity or policy on the enjoyment of the human rights of the holders of the affected rights.

The only exception is the Facial Recognition System for Fugitives in Buenos Aires, which -in response to a request for access to public information made by the Asociación de Derechos Civiles- states to have conducted "corresponding tests in order to reduce to the greatest extent possible the error rate, together with other restrictions imposed on the configuration of the data registry and control measures for personnel with access to the system", and thus minimize the "negative impacts in terms of human rights".

Generally, the development of external audits of the functioning of implemented systems is not a common practice either. External audits of the operation of technical systems that impact the exercise of rights are a good practice that allows to obtain information independently of the operation of the system and the potential risks that its design or implementation may pose for the exercise of the rights of users or persons impacted by a specific technology. Its absence prevents iterative improvement processes in which the vision of the system operators is complemented by external visions that contribute to its improvement and avoid negative impacts of the implementation of a system.

Only three of the 38 mapped initiatives report some kind of audit, two in Colombia and one in Argentina. Regarding Colombian systems, there is an announcement by the Mayor of Bogotá regarding the eventual conduction of external audits to Ágata, the Data Analytics Agency;[10] in the case of the "Sistema Integrado de Videovigilancia Inteligente para Transmilenio" [Comprehensive Intelligent Video Surveillance System for Transmilenio] -now deactivated- there was an audit by the Universidad Francisco José de Caldas-IDEXUD of the installation and operation of the biometric equipment.[11]

[8] See https://adc.org.ar/2020/09/18/avanza-la-regulacion-del-reconocimiento-facial-en-la-legislatura-portena

[9] See https://www.telam.com.ar/notas/202010/527676-la-legislatura-aprobo-el-uso-de-reconocimiento-facial-para-la-detencion-de-profugos.html

[10] See http://www.sdp.gov.co/noticias/agata-la-nueva-agencia-analitica-de-datos-hara-de-bogota-lider-global-transparencia-e-inteligencia

[11] See https://www.yumpu.com/es/document/read/55729155/informe20de20gestic3b3n202015

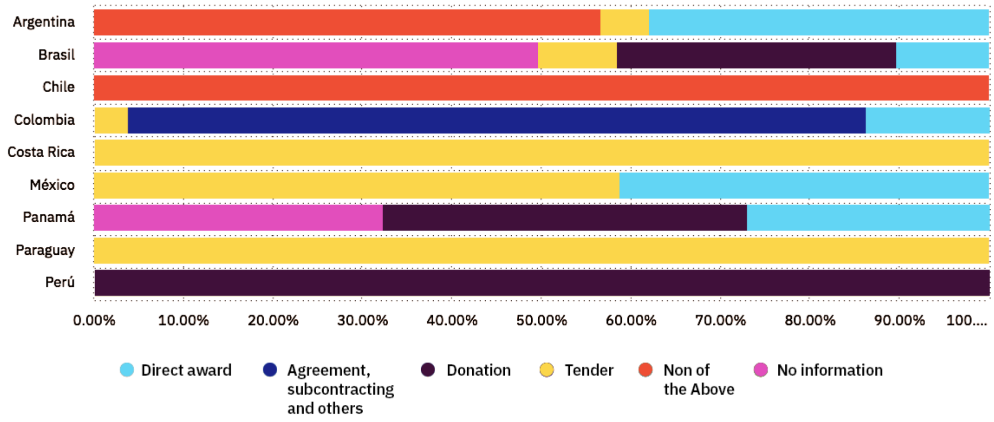
In Argentina, the law regulating the operation of the Facial Recognition System for Fugitives in Buenos Aires considers the creation of a Special Commission for Monitoring Video Surveillance Systems, composed of the Presidents of the Justice and Security Commissions, and three deputies appointed by the First Vice-Presidency of the body, allowing for the possibility of summoning specialists and civil society organizations to analyze and make proposals.[12]

Providers

A variety of companies are involved in providing services for the implementation of initiatives that use facial recognition systems technology in our region. These companies play different roles, ranging from the deployment of the necessary infrastructure for the operation of these systems to providing biometric analysis technology. While the participation of local companies is relevant, it should be noted that they are generally not responsible for software development. In some cases, they specialize in selling systems developed abroad.

It is important to note the presence of companies questioned internationally for their alleged involvement in human rights violations. Particularly illustrative is the case of Chinese companies Dahua and Hikvision, banned from operating in the United States, while having contracts worth millions in Mexico. France's IDEMIA (ex-Morpho Safran), present in at least four countries of the region, and UK's FaceWatch, whose software is used in one of the initiatives identified in Brazil, have also been the subject of concerns by international organizations.

Type of contract by country of implementation



Local companies are often large providers of services to the state and, in several cases, have some connection with political figures or corruption scandals.

Argentina

In Argentina, four initiatives for the use of active facial recognition systems were identified. All of them involve the participation of Argentine companies or foreign multinationals, in some cases through their local representatives.

[12] See http://www2.cedom.gov.ar/es/legislacion/normas/leyes/ley6339.html

- DANAIDE SA, contracted for 1,511,300 USD to provide the comprehensive video analysis service in the Facial Recognition System for Fugitives (SRFP) implemented in the Autonomous City of Buenos Aires, active since 2019;
- NEC Argentina SA - part of the global group NEC CORPORATION of Japanese origin , contracted for 44,906,400 ARS (462,702 USD approximately)[13] through a tender process to provide hardware, software and maintenance services in the "Sistema de Reconocimiento Facial de Tigre NeoCenter" [Tigre NeoCenter Facial Recognition System], in the town of Tigre, province of Buenos Aires, also active since 2019;
- Nubicom, contracted to implement the "Reconocimiento Facial Salta" [Salta Facial Recognition] system in the city of Salta, capital of the province, and active since 2018;
- France's Morpho Safran (currently IDEMIA), and Cuba's DATYS, contracted to provide the technology behind the "Sistema Federal SIBIOS de Identificación Biométrica para la Seguridad" [Federal System of Biometric Identification for Security, SIBIOS], active since 2011.

In addition to the companies identified, the facial recognition software used in the SRFP and called UltraIP was developed by the Russian company NtechLab. According to journalistic sources, the system was used in more than 3,000 video surveillance cameras in Russia.[14]

The contracting modality of the companies, in the cases where data were available, was direct contracting in the City of Buenos Aires and Salta. According to the local press, the contracting of DANAIDE SA had been denounced by the current Argentina's Vice President Cristina Fernandez de Kirchner for espionage in 2018.[15]

In the case of Salta, the company initially contracted to provide the video surveillance devices and software for the Salta Facial Recognition system was DATANDHOME SUPPLIER SA. Nubicom was the connectivity service provider. However, the contract with the former was rescinded in 2019 due to "serious non-compliance" in the installation of the committed cameras. Therefore, a direct contract was signed with Nubicom, which also became in charge of the connectivity and maintenance of the cameras and software.

According to press reports, the contracting of Nubicom has been marked by a number of defects, including an abbreviated procedure for emergency reasons that were not made explicit. The monthly cost charged by the company for the provision of services reached 440,000 dollars, according to the same source. DATANDHOME filed a lawsuit for 6 million dollars against the province of Salta for non-payment.[16]

In the case of the municipality of Tigre, the company NEC Argentina SA was awarded a public tender to provide an "Comprehensive Security Platform" in 2018 and again in 2019, this time under the concept of "Acquisition of Intelligent Security Totems". In 2020, the company was awarded a new public tender for "maintenance service of sixty (60) units of Intelligent Security Totems (TSI)". In Argentina, the Japanese group NEC Corporation has been established since 1978 and has since obtained multiple contracts with the state.

[13] The conversion of local currency values to U.S. dollars is an estimate for reference purposes. It was made based on consultation at https://www.xe.com in August 2021 and does not correspond to the equivalent amount at the time of contracting.

[14] See https://onezero.medium.com/the-u-s-fears-live-facial-recognition-in-buenos-aires-its-a-fact-of-life-52019eff454d and https://www.hrw.org/es/news/2020/10/09/argentina-publica-en-linea-datos-personales-de-ninos-y-ninas-acusados-de-cometer

[15] See https://realpolitik.com.ar/nota/37024/larreta-le-dio-el-control-del-reconocimiento-facial-a-una-empresa-denunciada-por-espiar-a-cfk/

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

Morpho Safran, now called IDEMIA, and DATYS are the providers of the Federal System of Biometric Identification for Security, SIBIOS. The former is a French multinational company dedicated to technology development, mainly focused on the sale of facial recognition products. The company has been criticized by Amnesty International for exporting digital surveillance technology to China, due to the human rights risk involved.[17] IDEMIA was blamed for problems with the general election in Kenya in 2017, which resulted in the National Assembly canceling its existing contracts and banning it from entering into new ones. The decision was repealed by the country's Supreme Court.[18]

DATYS is a Cuban company founded in 2005. According to information obtained by the Asociación por los Derechos Civiles (ADC), the DATYS contracted tool allows the automatic identification of people by comparing fingerprints and, as a secondary method, faces.[19]

Brasil

In Brazil, six initiatives for the use of facial recognition systems were identified with the following technology providers involved:

- Admobilize, from the United States, contracted for the development of technologies in a facial and emotion recognition system installed in the ViaQuatro consortium's subway stations in the city of São Paulo, active between March and September 2018.
- Staff of Security Technologies do Brasil Software Ltda, a Brazilian company that imported Facewatch software from the United Kingdom to implement a facial identification system in the 2019 edition of the traditional San Juan festival, which occurs annually in the city of Campina Grande, state of Paraíba.
- Brisanet Telecomunicações, a Brazilian company that provided infrastructure for the system implemented at the San Juan festival in Campina Grande in 2019.
- Tecway, a Brazilian company awarded in a tender process the development of biometric technologies for the Integrated Monitoring Camera Center of Itacoatiara, state of Amazonas, currently in the process of implementation.
- Engie Brasil Soluções Integradas Ltda., a Brazilian company member of the Engie Ineo Johnson consortium, awarded the implementation of a facial recognition system in the São Paulo city subway in 2019.
- Ineo Infracom, a French company member of the Engie Ineo Jonhson consortium awarded the implementation of a facial recognition system in the São Paulo city subway in 2019.
- Johnson Controls BE do Brasil Ltda, a U.S. company member of the Engie Ineo Jonhson consortium awarded the implementation of a facial recognition system in the São Paulo city subway in 2019.

In the case of Campina Grande, the technology was obtained through a donation from the providers to the company Medow Entertainment, responsible for the organization of the San Juan festival in 2019. The company Staff of Security Technologies do Brasil Software Ltda, responsible

[17] Amnesty International, "Out of control: failling EU laws for digital surveillance export" (2020). See https://www.amnesty.org/en/documents/eur01/2556/2020/en/

[18] See https://www.biometricupdate.com/202101/criticism-sparked-by-delay-of-biometric-election-systems-unveiling-in-uganda-procurement-in-kenya

[19] Asociación por los Derechos Civiles, "La identidad que no podemos cambiar: cómo la biometría afecta nuestros derechos humanos" (2017), see https://adc.org.ar/wp-content/uploads/2019/06/027-A-la-identidad-que-no-podemos-cambiar-04-2017.pdf. And "Tu yo digital – Descubriendo las narrativas sobre identidad y biometría en América Latina: los casos de Argentina, Brasil,nColombia y México" (2019), see https://adc.org.ar/wp-content/uploads/2020/06/050-tu-yo-digital-04-2019.pdf

for importing the Facewatch software has ties to a political figure involved in several corruption scandals at the national level.[20]

Based on information from Privacy International, the Facewatch company has local distributors in Brazil and Argentina. In the United Kingdom, their systems have been adopted by different types of businesses in order to identify people considered undesirable in such a business (due to antisocial behavior, attempted theft, etc.) and their blacklisting. When passing by a camera to enter the business or event, the system identifies whether or not the person is on the list and, if so, sends an alert. The system has generated controversy in the country regarding the legality of its use and privacy implications, as reported by the BBC.[21]

According to Privacy International, in 2019 the Facewatch system was used in at least three shopping centers in Brazil. Regarding an investigation into a possible collaboration between the company and London police for the exchange of data, the organization warns of the announced intention of the governor of Rio de Janeiro to allow the local police to exchange their own list of people suspected of committing crimes with facial recognition companies.[22]

Meanwhile, the Brazilian company Tecway, contracted to develop the Itacoatiara Integrated Monitoring Camera Center, has as part of its record an investigation by the Public Prosecutor's Office of the state of Amazonas due to possible wrongdoing in a public tender and an appointment by the commission installed in the Brazilian Senate to investigate irregularities during the management of the pandemic Covid-19.[23] One of the company's partners is a relative of a national congressperson and tried to run for local office in Manaus, capital of Amazonas.[24]

Two initiatives have the services of the public technology provider: the "Servicio Federal de Processamento de Datos" (SERPRO) [Federal Data Processing Service], which offers the base and storage of biometric data. SERPRO is involved in the implementation of the validation of the national driver's license by means of biometric data and "proof of life", a mandatory annual requirement so that there is no interruption in the payment of pensions by the Brazilian social security system. In this case, the objective is to replace the in-person process with an app, where the beneficiary sends a "selfie" that is compared with the photo registered in the system's databases.

SERPRO is a public company linked to the Ministry of the Economy and its purpose is to execute information and data processing services, including teleprocessing and communication of data, voice and image activities as required, in a limited and specialized manner.

Two recent initiatives in the Judiciary question the misuse of data stored by SERPRO. The first requests the suspension of data exchange with the Brazilian Intelligence Agency (ABIN).[25] The second questions the legality of using the driver's license database to offer facial recognition services to the public and private sector.[26]

[20] See https://agenciasportlight.com.br/index.php/2019/06/11/o-governador-witzel-e-as-caras-ocultas-no-milionario-negocio-de-reconhecimento-facial/.

[21] See https://www.bbc.com/news/technology-55259179

[22] See https://privacyinternational.org/long-read/4216/facewatch-reality-behind-marketing-discourse

[23] See https://amazonasatual.com.br/promotora-chama-de-esdruxula-forma-como-ssp-am-iniciou-negocio-de-r-427-milhoes-para-aluguel-de-viaturas-2/ and https://www.metropoles.com/colunas/igor-gadelha/cpi-pede-quebra-de-sigilo-de-empresa-de-parente-do-lider-do-mdb

[24] See https://simenao.com.br/simenao/autor-de-post-que-viralizou-teve-candidatura-indeferida-pela-ficha-limpa

[25] See https://theintercept.com/2020/06/06/abin-carteira-motorista-serpro-vigilancia/ and https://www.jota.info/stf/do-supremo/psb-aciona-stf-contra-compartilhamento-de-dados-da-cnh-entre-serpro-e-abin-16062020

[26] See https://computerworld.com.br/plataformas/ministerio-publico-acusa-serpro-de-oferecer-servico-ilegal/

Chile

In Chile, while ten initiatives for the use of facial recognition systems in the public sector were identified, six of which are active, it was not possible to identify the providers involved in their implementation, generally due to the slow response of public bodies to requests for access to information submitted for this research.

Only in the case of the municipality of San Joaquín was it possible to identify the companies Enel Distribucion Chile SA and Sistema de Seguridad y Tecnologías SpA as awarded in a public tender published in 2019 the improvement of the municipality's telesurveillance system.[27] The amount offered for the contracted work was 789,888,183 Chilean pesos (CLP), the equivalent today to about 1,023,965 dollars.

Enel Distribución Chile SA was contracted for the service of providing "power control or surveillance systems". The company is part of the Enel Group, a multinational of Italian origin, responsible for the distribution of electricity in several locations in the country, but has entered the security camera business in 2018.

Colombia

Five initiatives for the use of facial recognition systems were identified in Colombia with the following suppliers involved:

- The Colombian mixed public services company EMTEL, contracted through an inter-administrative agreement by the Mayor's Office of Bogotá for 11,758,251,357 COP (approximately 3,100,000 USD) signed in 2015, to gather the necessary efforts for the implementation of the Comprehensive Intelligent Video Surveillance System for Transmilenio (SIVIT), deactivated in 2021.
- Inversiones Tecnológicas de América, also Colombian, was subcontracted by EMTEL to supply equipment for the operation of SIVIT: cameras, lighting, switches and screens, and more.
- Compañía Internacional de Integración S.A. and TecniDidácticos IND S.A.S (Unión Temporal Tecnocom), Colombian, contracted for 11,298,307,350.00 COP (approximately 2,865,268 USD) to lead the implementation of the ABIS Multibiometric System for the national police and the Ministry of the Interior, active since 2017.
- IDEMIA, a French company, subcontracted by the former for the development of the system's fingerprint records and the migration of the system previously used by the police to ABIS. The amount of the contract was 1,000,000,000 COP (approximately 253,603 USD). The same company is involved in the implementation of the "Cédula de identidad digital" ["Digital Identity Card"], specifically the multibiometric engine Morpho Biometric Search Service.[28]
- HERTA Security, Spanish, also subcontracted by Unión Temporal Tecnocom to migrate photographs to the digital database and install their applications in the ABIS system (Biodata, BioFinder and Biogenerator).
- Empresa de Telecomunicaciones de Bogotá, Colombian public company responsible for developing implementation tests in facial recognition cameras of the Data Analytics Agency (Ágata) of Bogotá, active since 2020.

[27] See https://www.mercadopublico.cl/Procurement/Modules/RFB/DetailsAcquisition.aspx?qs=/qaUKJpnZ48L4Wtkl40xyg==

[28] See https://www.idemia.com/mbss

- BYTTE SAS, Colombian, awarded a public tender worth 13,994,000,000 COP (approximately 3,549,058 USD) to lead the deployment of the Integrated Multibiometric Information System currently in the process of implementation.

The inability to activate the biometric recognition cameras provided for in the SIVIT and contracted with EMTEL led to an investigation of two assistant managers of the city's Surveillance and Security Fund by Bogotá's ombudsman.[29] Although the investigation was closed in 2021,[30] charges were brought against the former assistant managers for negligence in contracting, since they did not take into consideration the warnings that such a system could only operate if it had a photographic database that did not exist.

In 2019, the mayor of Popayán and the former secretary of Municipal Transit were investigated for possible acts of corruption, like the irregular delivery of transit services to a firm called Quipux through Emtel.[31]

Unión Temporal Tecnocom faced four trials in 2017 for alleged breaches in the development of the contract that was established with the National Police for the development of the ABIS system. The decisions were favorable to the company. Both TecniDidácticos and Compañía Internacional de Integración S.A. have entered into several contracts with the Colombian state. The French company IDEMIA is the company that the National Civil Registry has been contracting for more than 10 years. And TecniDidácticos has been under investigation since 2020 for alleged irregularities in a contract with the Mayor's Office of Medellín for the supply of N95 masks during the Covid-19 pandemic.[32]

In the case of Ágata, there are several investors and facilitators of the initiative, including Bogotá Aqueduct and Sewage company, Bogotá Energy Group, the Special Administrative Unit of the District Cadastre, the District Planning Secretariat, Transmilenio S.A. and the Bogotá Metro Company. However, Empresa de Telecomunicaciones de Bogotá (ETB) has a 51% majority stake in the Agency. In addition, it led its formation process together with entities of the Mayor's Office of Bogota.[33] The company has several contracts with various public institutions in the city of Bogotá.

ETB was sanctioned for violating the right to free choice of its users for failing to comply with the termination of contracts within the established deadlines and was involved in some irregularities related to breaches in the execution of contracts.[34]

Finally, Bytte S.A.S. has had contracts with both public and private entities for the adaptation of access control software and support for ID issuance systems. Clients include Civil Aeronautics and

[29] See https://www.personeriabogota.gov.co/sala-de-prensa/notas-de-prensa/item/578-inhabilitado-exsubgerente-de-fondo-de-vigilancia-y-seguridad

[30] Secretariat of Security, Coexistence and Justice, "Cierre de investigación disciplinaria del proceso 015-2019". January, 2021. Available at: https://scj.gov.co/sites/default/files/notificaciones_control_interno_disciplinario/ESTADO%20001%20Firmado%7D.pdf

[31] See https://caracol.com.co/emisora/2019/01/29/popayan/1548787323_962726.html

[32] See https://www.kienyke.com/crimen-y-corrupcion/denuncias-corrupcion-contratos-coronavirus-alcaldia-medellin

[33] See https://www.valoraanalitik.com/2020/12/14/bogot-lanza-gara-nueva-agencia-de-anal-tica-de-datos/ https://bogota.gov.co/mi-ciudad/administracion-distrital/que-es-la-agencia-analitica-de-datos-de-la-alcaldia-de-bogota and https://gestor.etb.net.co/mp4/ABECE.pdf

[34] See https://www.eltiempo.com/bogota/sancion-superintendencia-de-industria-y-comercio-impone-millonaria-sancion-a-la-etb-522846

the Universidad Pedagógica y Tecnológica de Colombia, Tunja. In 2010 the company developed a partnership with Safran Morpho, today IDEMIA.[35]

Costa Rica

Three initiatives involving the use of facial recognition systems have been identified in Costa Rica. The French company IDEMIA - which has a factory in Costa Rica - was contracted together with a consortium through a tender process in the amount of 3,674,203 USD for the development of the software used in the Automated Biometric Identification System (ABIS), which includes different biometric identification elements, including facial recognition.[36]The system was implemented at the end of 2020, with particular emphasis on issuing identity cards and identity cards to minors (12 to 18 years old).

IAFIS, a company created in Argentina for the sale of Morpho systems (now IDEMIA) in Latin America, is also part of the consortium.[37] Componentes El Orbe S.A., a Costa Rican company with operations in several Central American countries, is involved in ABIS and is a member of the consortium. All of the companies involved in the contract have worked on other projects with the State of Costa Rica. In the case of IAFIS, it is responsible for the Automated Fingerprint Identification System of the Supreme Electoral Tribunal.

In the case of the Biometric Identification Migration System, in the process of being implemented, in February 2020 the period for receiving offers was closed within the framework of the open tender for contracting. The estimated budget is 3,317,389,479.96 CRC (equivalent to around 5,344,276.41 USD). According to the public procurement system, the award is still under evaluation. However, according to the General Directorate of Migration and Foreigners, the project was awarded to the GSI-Dinámica-Veridos-Sertracen consortium. Both Grupo de Soluciones Informáticas SA (GSI) and Sertracen are companies with a significant presence in Central America.

The consortium was also benefited with the contract for the implementation of the Biometric Passport for the Bicentennial, which plans to integrate facial recognition as an authentication mechanism until March 2022. In that case, the contract amount was 5,501,308.159 USD. The consortium includes Dinámica Consultores Internacional S.A., also from Costa Rica, and Veridos from Germany.

México

In Mexico, three initiatives were identified for the implementation of facial recognition systems for the surveillance of public spaces. The providers involved are the following:

- Dahua, a company of Chinese origin, contracted through a direct award in the amount of 600 million MXN (approximately 29,494,148 USD) for the implementation and maintenance of the Video-Intelligence System of the State of Coahuila. Currently in pilot stage,

  the initiative involves the installation of 300 surveillance cameras with facial recognition capabilities in 11 cities in the state.

[35] See https://repository.urosario.edu.co/bitstream/handle/10336/13091/PedrozoBoada-MullerJose-2017.pdf?sequence=1&isAllowed=y

[36] The contract can be found at https://www.sicop.go.cr/moduloPcont/pcont/ctract/es/CE_COJ_COQ038_O.jsp?contract_no=CE201905000256&contract_mod_seq=00&typeExp=Y

[37] See https://www.linkedin.com/company/iafisgroup/about/

- The Mexican company Teléfonos de México S.A.B. de C.V. was awarded in a national public tender the total amount of 197,564,863.80 MXN (about 9,702,029 USD) for the implementation of the C2 Command and Control Center of Mexico City's Central de Abastos.

- Also contracted in the same tender were Hanwa, from South Korea, for the development of biometric technologies; and the U.S. engineering company Intelligent Security Systems, also dedicated to the development of biometric technology.
- Compañía SYM Servicios Integrales, S.A. de C.V. from Mexico, was contracted for a total amount of 728,010,176 MXN (approximately 36,118,859 USD) for the implementation and maintenance of the "Centro de Comando, Control, Comunicación, Cómputo y Coordinación "C5 SITEC" [Command, Control, Communication, Computing and Coordination Center "C5 SITEC'] - active since May 2021. The initiative includes the installation of 40 cameras with facial recognition capability, installed at 20 points in the municipality of Aguascalientes in the state of the same name.

Regarding the Coahuila Video Intelligence System, Dahua has stated to the press that the algorithms provided have been "tropicalized" to identify the "Mexican phenotype," suggesting that the company had some access to data on Mexican individuals to train their facial recognition systems. The initiative was presented to the public shortly after a visit by the governor of Coahuila to China, where he met with the company. Its CEO, Zhijie Li, was present at the launch of the system.

The company, one of the most important in the global video surveillance market, was sanctioned by the United States in 2019 for human rights violations due to its participation in harassment campaigns against an Islamic minority.[38] The company has contracts for surveillance projects in Xinjiang, where the Chinese government is accused of genocide against the Uighur population. According to information published by the U.S. press in early 2021, its facial recognition software was able to identify people of such ethnicity.[39]

Hikvision, one of those awarded in the "Proyecto de Videovigilancia Urbana Integral con Tecnología Analítica" [Comprehensive Urban Video Surveillance Project with Analytical Technology], was sanctioned by the United States in 2019 and by Norway in 2020 for human rights abuses.[40] Their surveillance technologies would also be used by the Chinese government to crack down on Muslim minorities.

Mexico's Telefónica de México has been in charge of the vast majority of projects related to the installation of surveillance cameras in Mexico City. This company is owned by Carlos Slim who has won projects worth millions, and has had an important participation in infrastructure projects in the last three administrations of Mexico City. In one of the projects with the participation of the company, several irregularities have been found such as unjustified payments, lack of verification of expenses, lost invoices, and more.[41]

In the case of Aguascalientes, the way of contracting by direct award could be in violation of the provisions of the "Ley De Adquisiciones, Arrendamientos y Servicios del Estado de Aguascalientes" [Procurement, Leasing and Services Law of the State of Aguascalientes]. The contract states that it is based on Sections I and VII of Article 63 of said Law, which establish that a direct award may be made if there are no substitute or equivalent services or goods to those offered

[38] See https://www.icij.org/investigations/china-cables/us-blacklists-chinese-companies-linked-to-uighur-abuses/

[39] See https://www.latimes.com/business/technology/story/2021-02-09/dahua-facial-recognition-china-surveillance-uighur

[40] See https://www.dw.com/en/us-blacklists-28-chinese-companies-over-xinjiang-rights-abuses/a-50732014

[41] See https://poderlatam.org/2020/01/el-negocio-de-slim-en-el-centro-historico-de-la-cdmx/

by the company or if another type of contracting procedure could compromise confidential and/or reserved information. However, equivalent initiatives have been contracted through public tenders, which supports the fact of the possible violation of the provisions of the aforementioned law.

The contracted company, SYM Servicios Integrales, has a long history in government provisioning in the area of security systems and equipment, between video surveillance systems in the public space and surveillance systems.[42] According to emails leaked by Wikileaks, the company has sold surveillance systems manufactured by the Hacking Team company to local governments in Mexico (including those of Tamaulipas, Campeche, Puebla and Jalisco). SYM Servicios Integrales S.A. de C.V. is one of the subsidiaries of Grupo Kabat, which also markets Hacking Team systems to governments of other states in Mexico. According to the New York Times, these systems were used by the government of Puebla to spy on political opponents in the electoral context.[43]

Panama

In Panama, three initiatives for the use of facial recognition were mapped in which two foreign companies are involved. One of them is Huawei Technologies, contracted for the development of biometric technologies for the "Centro de Operaciones de Seguridad y Emergencias C2" [C2 Security and Emergency Operations Center], an initiative that has been active since 2018. The amount of the contract, US$9.3 million, was paid through a non-refundable loan from China, meaning that the services were donated by the Chinese government to the country. It should be noted that Huawei Technologies maintains a corporation that represents its interests in Panama, all the people on its Board of Directors are Chinese citizens and do not live in Panama.

The other company involved in the provision of biometric technologies in Panama is Canada's General Dynamics Mission Systems, contracted for the "Proyecto de Reconocimiento Facial Biométrico del Aeropuerto de Tocumen" [Biometric Facial Recognition Project at Tocumen Airport" and "Paso Centro de Operaciones Nacionales" [Paso National Operations Center], both active since 2019. The contracts reached the amount of 4,786,388 and 27.5 million USD, respectively. The company holds different contracts with the Panamanian government in the framework of the country's cooperation with the Canadian Chamber of Commerce.

Paraguay

Three facial recognition initiatives were identified in Paraguay. All involve two national suppliers responsible for the implementation and maintenance of the systems. The first is Tecnología, Seguridad y Vigilancia del Paraguay S.R.L., contracted through a USD 3 million tender as part of the facial recognition project in urban public spaces currently being implemented in Asunción, Encarnación, San Ignacio, Caaguazú, Coronel Oviedo and Ciudad del Este. The company has been providing services for Paraguay's police since at least 2011, according to the local press, which has also raised doubts regarding the effective functioning of the facial recognition technologies deployed.[44]

[42] See https://www.quienesquien.wiki/es/empresas/sym-servicios-integrales-sa-de-cv?collection=all&name=SYM+SERVICIOS+INTEGRALES+SA+DE+CV&tipo-entidad=&pais=&estado=&ciudad=&fuente=&size=&sort-all=#summary-supplier_contract

[43] See https://r3d.mx/2017/01/05/nyt-documenta-uso-de-malware-para-espionaje-politico-en-puebla/

[44] See https://www.abc.com.py/edicion-impresa/economia/2019/11/11/tsv-srl-es-la-eterna-proveedora-tecnologica-del-911-de-la-policia/

Also from Paraguay, Asunción Comunicaciones S.A. was awarded the tender for the "Ampliación de Capacidades, Garantías y Facial del Sistema AFIS (Automated Fingerprint Identification System)" [Expansion of Capabilities, Guarantees and Facial of the AFIS System]. The contract has resulted in 1,676,303 USD in revenue in 2017 and 1,813,215 USD in 2019. As part of the service, the company has provided biometric mobile software licenses, biometric mobile central middleware licenses, criminal AFIS registered license, facial central software upgrade license and facial software workstation upgrade license.

Asunción Comunicaciones S.A. has also been awarded a public tender for the implementation of the AFIS System in a sporting event, as part of a joint action with the Paraguayan Football Association and the National Police, led by the Ministry of the Interior. The pilot action carried out in 2019 resulted in an investment of approximately 1,642,093 USD.

Peru

In Peru, a single initiative to implement facial recognition systems was identified in Gamarra, one of the country's most important shopping malls, located in the metropolitan region of Lima. The system has been in the process of implementation since 2019. The initiative involved the participation of the Peruvian company Desarrollos Terrestres, responsible for installing the cameras.

The contracting mechanism in this case is particular: the company Desarrollos Terrestres has been entering into agreements with different district municipalities in Lima. According to these agreements, the company was obliged to install the cameras and provide the municipality with a monitoring system. In exchange, the municipality pledged to facilitate the installation of telecommunications networks in the district.

By way of conclusion: facial recognition does not protect us, it makes us vulnerable

Various governments around the world have begun to impose bans and moratoriums on the implementation and use of facial recognition, and some software developers have committed to restricting sales of this type of system in certain situations. This is the case of Amazon,[45] Microsoft[46] and IBM,[47] who have made express statements in this regard in the wake of the episodes of racial justice protests in the United States in 2020. These protests are occurring at the same time that racial bias is being discovered in this technology.[48]

International experts have also expressed their support for the imposition of this type of measure,[49] considering that facial recognition systems imply a series of impacts on the exercise of human rights.[50]

Why not? Impact on human rights and risks associated with the use of facial recognition

We should remember that facial recognition technology allows the individualized identification of any person and, with that, the monitoring of their personal trips and habits in real time. The transformation of such information into metadata that can, in turn, be stored and analyzed in aggregate form implies the additional possibility of inferring a series of behaviors and even attempting to predict future actions.

Especially when implemented in public spaces - as is the case with most of the initiatives identified from this mapping - facial recognition systems consist of a covert mass surveillance technology that affects all people circulating in a given space, without their knowledge or the possibility of consenting to the collection of sensitive personal information, such as their biometric data. This includes, for example, children and adolescents (NNA), whose privacy enjoys special protection due to the enormous impact that abusive use or leaks of this extremely sensitive information can have on the free development of their personality. Civil society organizations have identified the improper inclusion of minors' data in the databases of the Facial Recognition System for Fugitives (SRFP) implemented in some subway stations of the Autonomous City of Buenos Aires.[51]

[45] El País. Amazon suspende indefinidamente la venta de su tecnología de reconocimiento facial a la policía. See: https://elpais.com/tecnologia/2021-05-21/amazon-suspende-indefinidamente-la-venta-de-su-tecnologia-de-reconocimiento-facial-a-la-policia.html

[46] The Washington Post. Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM. See: https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/.

[47] El País, IBM abandona la tecnología de reconocimiento facial por las dudas éticas sobre su uso. See: https://elpais.com/tecnologia/2020-06-09/ibm-abandona-la-tecnologia-de-reconocimiento-facial-por-las-dudas-eticas-sobre-su-utilizacion.html.

[48] See Buolamwini J.; Gebru T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research 81:1–15, 2018. Retrieved: http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

[49] See https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736

[50] Moratorium call on surveillance technology to end "free-for-all" abuses: UN expert. En: UN News [Internet]. June 25, 2019 [quoted February 18 2020]. Retrieved: https://news.un.org/en/story/2019/06/1041231

[51] See https://www.hrw.org/es/news/2020/10/09/carta-al-lic-horacio-rodriguez-larreta-sobre-el-sistema-de-reconocimiento-facial-de

The installation of facial recognition systems for the surveillance of public spaces, therefore, necessarily implies restrictions to the right to freedom of movement, since those who do not want the system to collect their biometric data would have to look for alternative ways or means of transportation. On the other hand, the degree of intrusion inherent to this type of technology implies a violation of the right to privacy and, associated with it, the right to the protection of personal data.[52]

Also, the monitoring and behavior prediction capabilities compromise the exercise of the right to free association, expression and peaceful assembly, since they allow the profiling of participants of movements that oppose established political or economic interests, violating their anonymity and facilitating the criminalization or persecution of legitimate expressions of a different nature.[53] More than an imaginative exercise, this is a concrete risk in countries marked by a history of authoritarianism and countless recent examples of abuses, for example, in the surveillance of political opponents, as is the case in most of the countries analyzed. The possibility of being under constant surveillance, moreover, encourages silencing and self-censorship, and represents a very serious risk for democratic societies.

The implications of real-time individualized surveillance of people do not only affect those involved in the defense of human rights or different forms of activism. In a region particularly marked by structural racism, machismo and homophobia, this type of system facilitates sexual violence by those who have access to the operation of the system. While operators are expected to be subject to strict rules and controls, episodes of abuse and discrimination by police officers are not uncommon in the region.

The right to non-discrimination, recognized in Articles 1 and 24 of the American Convention on Human Rights, is also directly threatened by the high rates of false positives that facial recognition systems produce, a problem that increases exponentially when the people under surveillance belong to historically vulnerable groups such as women, dark-skinned people or transgender people.[54] The systems implemented in the region have already registered errors that resulted in serious consequences for the people affected.

In the Facial Recognition System for Fugitives (SRFP) implemented in the Autonomous City of Buenos Aires, Argentina, there are records of at least two cases of false positives, one of which involved the detention of an innocent person for six days.[55] Similar situations were also identified

[52] See, for example: Asamblea General de las Naciones Unidas. 20 de noviembre de 2013. El derecho a la privacidad en la era digital. A/RES/68/167. Retrieved: https://undocs.org/pdf?symbol=es/A/RES/68/167 y Naciones Unidas, resolución del Consejo de Derechos Humanos, 'El derecho a la privacidad en la era digital', A/HRC/34/L.7/Rev.1, Naciones Unidas, Nueva York, 2017.

[53] See: United Nations High Commissioner for Human Rights, Report "Impacto de las nuevas tecnologías en la promoción y protección de los derechos humanos en el contexto de las reuniones, incluidas las protestas pacíficas", A/HRC/44/24, June 24, 2020, paragraph 31, available at: https://undocs.org/es/A/HRC/44/24. See also: Relator Especial sobre los derechos a la libertad de reunión pacífica y de asociación, Informe Derechos a la libertad de reunión pacífica y de asociación, May 17, 2019, paragraph 56, available at: https://undocs.org/es/A/HRC/41/41. On the implications of surveillance on the right to freedom of expression see: Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos. Estándares para una Internet Libre, Abierta e Incluyente. OEA/Ser.L/V/II CIDH/RELE/INF.17/17. Organización de Estados Americanos; 2017 mar. Retrieved: http://www.oas.org/es/cidh/expresion/docs/publicaciones/INTERNET_2016_ESP.pdf and Consejo de Derechos Humanos, Asamblea General de Naciones Unidas. El derecho a la privacidad en la era digital. A/HRC/28/L.27. United Nations; March 24, de 2015. Retrieved: https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_28_L27.pdf.

[54] United Nations High Commissioner for Human Rights, Report "Impacto de las nuevas tecnologías en la promoción y protección de los derechos humanos en el contexto de las reuniones, incluidas las protestas pacíficas", A/HRC/44/24, June 24, 2020, paragraph 32, available at: https://undocs.org/es/A/HRC/44/24

[55] See: https://www.pagina12.com.ar/209910-seis-dias-arrestado-por-un-error-del-sistema-de-reconocimien

in Brazil,[56] where organizations have denounced that out of a total of 151 people detained as a result of the use of facial recognition systems, 90% are of African descent.[57]

The implementation of facial recognition systems therefore entails the technical reproduction of social exclusion biases and, when used for surveillance purposes, threatens the right to dignity, due process and the presumption of innocence.

Finally, when implemented as identity authentication mechanisms to condition access to public services, facial recognition (as well as other biometric technologies) can represent a barrier to the exercise of economic and social rights. In addition, it implies that some people, mainly those dependent on social assistance, are subject to inferior guarantees in terms of the protection of their fundamental rights. When applied in this way, the technologies reinforce and deepen the historical structural inequalities that affect the region.[58]

From lack of public transparency to citizen resistance

For all the reasons outlined here, it is crucial that decisions associated with the implementation of facial recognition systems be subject to strict democratic controls - including criteria of legality, necessity and proportionality - and public oversight. However, the present mapping carried out by Al Sur member organizations shows that such criteria are scarcely respected in Latin America.

First, implementations lack public discussions prior to their implementation. In most cases, the initiatives are made public through press releases in specialized media of restricted circulation, through the publication in official media of public procurement processes (especially when they are carried out through public tenders, which is not always the case) or when there are already records of abuses or other types of corruption scandals. More serious is that, even during this investigation process, there have been barriers to access to information about these systems

Secondly, only two of the 38 initiatives identified included a mechanism for public participation prior to the implementation of the technologies. When it comes to conducting previous studies on the impact on privacy or human rights, again only two initiatives implemented them. Finally, only three of the initiatives provided for an external audit to offer minimum guarantees for the proper implementation of the systems.

The regional context is complemented by weak regulations on personal data protection and access to public information, insufficient controls on both public spending and technology implementation, a history of authoritarianism and contempt for human rights, high social insecurity, austerity policies and the eternal promise of development in the form of technology imports. The result is that Latin America has become a fertile field for the adoption of facial recognition for multiple purposes and without any safeguards to prevent its use contrary to the democratic principles that govern each of the countries in the region.

Faced with this situation, civil society organizations have turned to the courts to obtain more information and question the deployment of these systems in their countries or cities, due to the potential risks involved. In Brazil, the judiciary has confirmed the illegality of a system of emotion

[56] See https://gizmodo.uol.com.br/rio-de-janeiro-reconhecimento-facial-erra-mulher-detida/.

[57] See https://reconocimientofacial.info/denuncian-sesgo-racial-en-tecnologias-de-reconocimiento-facial-brasilenas/.

[58] See https://www.derechosdigitales.org/13900/vigilancia-control-social-e-inequidad/.

recognition cameras installed in subway stations.[59] The ruling is the result of a class action led by the Brazilian Consumer Defense Institute (IDEC). In addition to the discontinuation of data collection through the system, determined as early as 2018,[60] compensation of 100 thousand reais for collective moral damages is established.[61] Other actions are currently underway in São Paulo to challenge the installation of facial recognition cameras in public transportation.[62]

In Argentina, there are currently two ongoing legal cases against the Facial Recognition System for Fugitives: a Declaratory Action of Unconstitutionality (ADI) against the Government of the City of Buenos Aires, filed by the Asociación por los Derechos Civiles (ADC)[63] and a collective injunction case brought by the Observatorio de Derecho Informático Argentino (O.D.I.A.) seeking to stop the initiative.[64] Also, an amparo lawsuit was recently admitted against the operation of facial recognition technology systems in Coahuila, Mexico.

In Peru, a group of students have challenged the mandatory use of facial recognition for participation in a public university admission exam.[65] And in Paraguay, the organization TEDIC has filed an action of unconstitutionality, challenging the Paraguayan government's declaration that information related to the implementation of facial recognition systems in the country is national security and, therefore, reserved.

Faced with the attempts of the states of the region to hide, cover up and omit from public debate the increase in surveillance capabilities through facial recognition technologies, their failures, incapacity, negligence and dangers, civil society resists and denounces their illegality and abuses. This is not a technical problem, it is a political discussion about the type of society we want and the role that technologies should have in it: tools for the integral development of people and society as a whole or a way to perpetuate social and historical inequalities, through technically assisted authoritarianism.

This is a particularly important battle in Latin America, where human rights and the notions of dignity and autonomy of individuals are often undermined by the interests of political and economic elites, and where democracy must constantly resist the onslaught of corruption and abuses of power. In the face of the opacity that protects despotism, we demand transparency; in the face of arbitrary impositions, we demand democratic debate and plural participation in decision-making processes regarding the implementation of invasive technologies such as facial recognition. In the face of crude technosolutionism, we demand a broad, robust and sophisticated human rights perspective. In the face of empty promises of modernity, we demand development and dignity for all people.

The depredation of fundamental rights for the sake of political and economic interests that support the implementation of the different facial recognition systems listed here requires a strong response from civil society against governments that do not seem willing to treat the

[59] See https://idec.org.br/noticia/idec-obtem-vitoria-contra-reconhecimento-de-emocoes-no-metro-de-sp.

[60] See https://idec.org.br/noticia/justica-impede-uso-de-camera-que-coleta-dados-faciais-do-metro-em-sp.

[61] See https://teletime.com.br/10/05/2021/justica-condena-viaquatro-por-reconhecimento-facial-de-passageiros-sem-consentimento/.

[62] See https://reconocimientofacial.info/metro-tera-que-explicar-licitacao-de-cameras-de-reconhecimento-facial/.

[63] See https://adc.org.ar/2019/11/06/el-reconocimiento-facial-para-vigilancia-no-pertenece-a-nuestro-espacio-publico/

[64] See https://amicus.odia.legal/

[65] See https://reconocimientofacial.info/peru-uso-de-reconocimiento-facial-en-examen-de-admision-a-universidad-publica-genera-cuestionamientos/.

problem with the necessary seriousness. We hope that this report will serve as an input to the fight already being waged by different people, in different locations in Latin America, as well as an incentive for the preparation of tomorrow's fights.

www.alsur.lat

AlSur