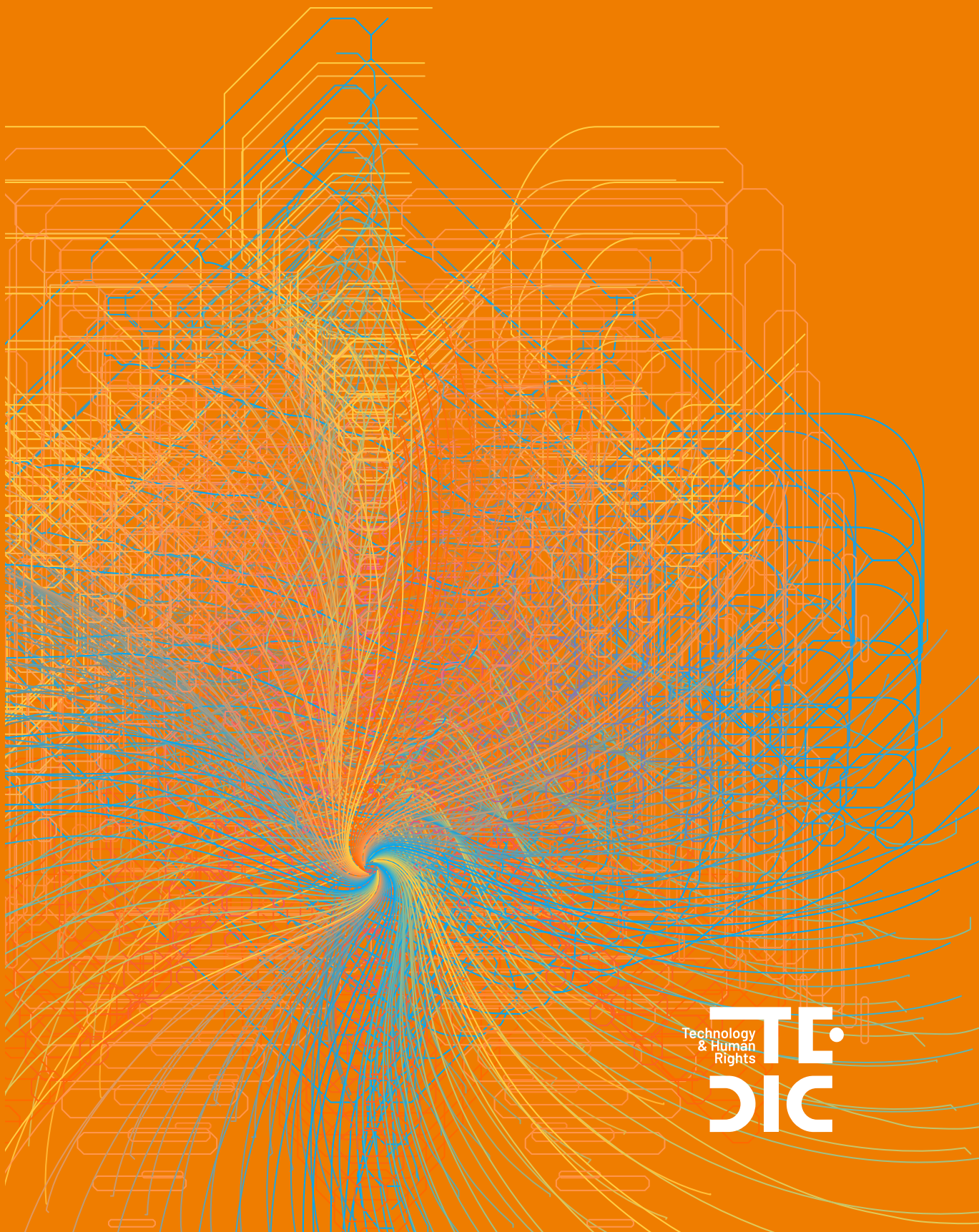
NOT WITH MY FACE

Implementation of facial recognition cameras by the Paraguayan State



Technology & Human Rights

NOT WITH MY FACE

Implementation of facial recognition cameras by the Paraguayan State

Technology & Human Rights

This research was prepared within the framework of the **#MoreCitizenshipLessCorruption** Project, with the support of the Cird Foundation and INDELA - AVINA..

This document is part of TEDIC's campaign **#MyDataMyRights**, which includes the **#NotWithMyFace** initiative.

TEDIC is a non-governmental organization founded in 2012, whose mission is the defense and promotion of human rights in the digital environment. Among its main issues of interest are freedom of speech, privacy, access to knowledge and gender on the Internet.

NOT WITH MY FACE

Implementation of facial recognition cameras by the Paraguayan State

DECEMBER 2024

RESEARCH
Graciela Galeano
Gerardo Paciello
Leonardo Gómez Berniga

COLLABORATION
Maricarmen Sequera
Giuliana Galli

EDITING
Maricarmen Sequera

COMMUNICATION AND PROOFREADING
Araceli Ramírez

DESIGN AND LAYOUT
Horacio Oteiza

TRANSLATION
Alejandra González

TABLE OF CONTENT

EXECUTIVE SUMMARY 6

GLOSSARY 7

INTRODUCTION 8

RESEARCH METHODOLOGY 9

Methodological considerations 9

Documentary review 9

Information search strategies 9

Public Information Request 11

BIOMETRICS AND HUMAN RIGHTS 13

Personal Data Processing in Video Surveillance 13

Privacy and mass surveillance through biometric data 15

International regulations limiting biometric processing 17

Global rollback of facial recognition use 20

Buenos Aires, Argentina 20

São Paulo, Brasil 21

Strasbourg, France 21

European Union 22

Cambridge, United Kingdom 22

United States 23

Human rights and surveillance through facial recognition cameras 26

Mass surveillance as a threat to democratic order 29

Evolution of camera implementation in Paraguay 32

Donations and acquisitions of facial recognition cameras 36

Analysis of official reports 51

Strategic litigation on facial recognition 53

First Litigation: Year 2018 53

Second litigation: Ministry of the Interior (2023) 54

Third litigation: National Police (2023) 55

CONCLUSION 56

RECOMMENDATIONS 58

BIBLIOGRAPHY 59

APPENDIX 63

Nationwide Summary of Cameras – April 2024 63

EXECUTIVE SUMMARY

This study analyzes the implementation of facial recognition cameras in Paraguay, highlighting key concerns related to transparency, human rights and corruption. Since 2018[1], TEDIC has warned about the risks and potential ineffectiveness of these technologies. However, their expansion has continued without adequate regulation, exacerbating issues such as the lack of documentation of stolen or lost cameras and the purchase of inefficient equipment.

The report indicates that, since 2018, Paraguay's National Police has significantly increased the use of facial recognition cameras. However, the results have been ambiguous, raising concerns about privacy and the security of personal data. In addition, concerning patterns of questionable acquisitions were identified, along with an alarming lack of transparency in tender processes, creating conditions conducive to corruption

The study also questions the legality of using the Universal Service Fund (FSU) of the National Telecommunications Commission (CONATEL) to finance these purchases, arguing that they do not align with the fund's objectives. In addition, it highlights the urgent need for comprehensive personal data protection legislation and criticizes the lack of transparency in institutional responses to public information requests.

In its conclusions, the report emphasizes that the acquisition and use of facial recognition cameras was conducted without an adequate legal framework, violating human rights principles and exposing the population to mass surveillance and discrimination. Therefore, the research calls for close monitoring of ongoing public sector projects and urges that these issues be addressed from a global and human rights perspective, given the growing trend of implementing invasive technologies without adequate protection of civil liberties.

KEY WORDS: *Facial recognition, biometrics, privacy, personal data.*

1 TEDIC. 2018. Biometrics and surveillance: the ongoing alienation of our rights. Available at: https://www.tedic.org/wp-content/uploads/2018/12/La-enajenaci%C3%B3n-continua-de-nuestros-derechos_TEDIC_2018-2.pdf

GLOSSARY

ANNP	National Administration of Navigation and Ports
CJI	Inter-American Juridical Committee
CONATEL	National Telecommunications Commission
CSE	Security and Emergency Center
DINAC	National Directorate of Civil Aeronautics
DNCP	National Directorate of Public Procurement
EPH	Permanent Household Survey
FSU	Universal Service Funds
FR	Facial Recognition
ICCPR	International Covenant on Civil and Political Rights
IP	Internet Protocol
MEC	Ministry of Education and Science
MITIC	Ministry of Information and Communication Technologies
PTZ	Pan, Tilt, Zoom
SADLE	Emergency Call Handling and Dispatch System

INTRODUCTION

In 2018, the National Police, the Ministry of the Interior and the National Telecommunications Commission (CONATEL) announced the implementation of a new surveillance system with biometric technology[2]. At the time, TEDIC was already expressing[3] its concern about the possible ineffectiveness of this measure to address insecurity. More importantly, it warned about the risks associated with the introduction of facial recognition technologies.

These concerns focused on the implications for privacy and individual rights, as well as the risk that such practices could perpetuate a legacy of authoritarianism. In addition, there was a troubling lack of transparency and accountability in the acquisition and management of these technologies.

In the previously cited research, TEDIC had already called attention to the risks associated with the management of data obtained through facial recognition software. These risks relate not only to the privacy and security of personal data, but also to the potential consequences for democracy in a country still marked by the shadows of its dictatorial past. The study stressed the importance of greater oversight and regulation in the use of surveillance technologies to protect civil liberties and prevent abuse of power.

Six years after the publication of that report entitled "The ongoing alienation of our rights", this new study seeks to evaluate the actions undertaken by various government institutions to adopt facial recognition technologies in Paraguay.

The main justification for the acquisitions analyzed in this research was the expansion of devices and systems designed to store sensitive information with the aim of exerting greater control. However, these initiatives have overlooked critical aspects related to the security of personal data, its proper use and its exposure to vulnerabilities, largely due to the lack of necessary safeguards.

This analysis aims to provide insight into how the State has handled these technologies, their implications for citizens' privacy and security and the real effectiveness of these tools in supposedly improving public security. Furthermore, it highlights the ongoing lack of an adequate legal framework and data protection measures to safeguard citizens' rights in Paraguay.

Through this investigation, we aim to provide a comprehensive overview of the process and evolution of the acquisition and use of these technologies by the State between 2018 and 2023. Additionally, we critically analyze the results, questioning whether effective measures were implemented during this period to ensure citizen security. The focus on accumulating sensitive data without the necessary safeguards for security and privacy exposes significant deficiencies in the management and protection of personal information.

2 Biometric video surveillance involves the use of security cameras integrated with systems that identify and authenticate individuals. While facial recognition is the most commonly used method, other biometric technologies, such as iris scanning, body movement analysis and fingerprint recognition, can also be employed.

3 TEDIC. 2018. Biometrics and surveillance: the ongoing alienation of our rights. Available at: https://www.tedic.org/wp-content/uploads/2018/12/La-enajenaci%C3%B3n-continua-de-nuestros-derechos_TEDIC_2018-2.pdf

RESEARCH METHODOLOGY

METHODOLOGICAL CONSIDERATIONS

The methodological review was conducted using various procedures to obtain information on the acquisition of facial recognition technologies by the State, and more specifically, by the National Police. Different methods were employed:

- Documentary review of national and international laws and materials related to human rights and the proper management of personal data.
- Information searches on the official websites of the National Directorate of Public Procurement (DNCP) and the National Telecommunications Commission (CONATEL), as well as in press sources.
- Access to information requests submitted to state institutions regarding the purchase of cameras or facial recognition software.

DOCUMENTARY REVIEW

To begin this investigation, the documentary review was guided by three specific questions:

- What laws or international agreements support the protection of human rights in relation to privacy and data protection?
- Is there accurate, accessible and concrete information that ensures transparency in the acquisition and use of facial recognition technology?
- What legislative initiatives are being considered that could either strengthen protections or increase risks related to surveillance and the handling of personal data?

INFORMATION SEARCH STRATEGIES

The research was based on four main types of information sources. First, websites that record most national tenders and public procurement by government institutions were analyzed, along with official government websites related to security. Second, media outlets were reviewed to identify relevant coverage. Third, reports and articles produced by human rights advocacy organizations were included. Finally, platforms containing detailed information on draft legislation, enacted regulations and international standards were consulted, as outlined in Table 1.

TABLE 1. List of secondary information sources

State database	Media	Research and articles from organizations	International sites
National Directorate of Public Procurement (DNCP)	ABC Color	TEDIC	United Nations
National Police	Última Hora	AlSur	Global Investigative Journalism Network
National Telecommunications Commission (CONATEL)	La Nación	Red en Defensa de los Derechos Digitales	
Paraguay Legislative Information System (SILPY)		Human Rights Coordinator of Paraguay (CODEHUPY)	

To filter the data specifically on the DNCP website, the research team searched under Category 25, which refers to "Military and Security Equipment; Security and Surveillance Services".

A combination of keywords such as "closed-circuit", "cameras", "facial recognition", "911 System" and "National Police" was also used. These same keywords were applied in searches across other state sources and media outlets, as shown in Table 2.

At this point, press articles were selected based on their publication date between 2019 and 2023, considering that the National Police officially announced the implementation of facial recognition technology in 2018.

TABLE 2. List of main and alternative keyword

Main keywords	Alternative keywords
Cameras	911 System
Closed-Circuit	National Police
Facial Recognition	CONATEL
Security	Software

PUBLIC INFORMATION REQUEST

The research team submitted over 40 public information requests to a total of 35 State institutions between August and September 2023. These institutions include directorates, secretariats and ministries of the Executive Branch, as well as entities of the Judicial and Legislative Branches, in addition to municipal and departmental governments, as detailed in Table 3.

One of the main inquiries focused on whether these institutions had acquired biometric technology systems, cameras or facial recognition software, and whether they had integrated them into the National Police's 911 system. The research also examined the implementation of closed-circuit cameras and other surveillance systems, as well as the existence of specific protocols for handling and storing personal data. Specifically, the National Police and the Ministry of the Interior were asked to provide concrete information on the number of facial recognition cameras acquired to date and their current locations.

TABLE 3. List of State institutions that received a public information request

National Police of Paraguay
Ministry of Education and Sciences (MEC)
Departmental Government of Misiones
Departmental Government of Paraguarí
National Administration of Navigation and Ports (ANNP)
National Directorate of Migration
Departmental Government of Itapúa
Departmental Government of Central
National Secretariat for the Administration of Seized and Confiscated Assets (SENABICO)
Honourable Chamber of Senators
Departmental Government of Guairá
Ministry of Public Works and Communications (MOPC)
National Directorate of Civil Aeronautics (DINAC)
Departmental Government of Presidente Hayes
Departmental Government of Boquerón
Ministry of Finance (MH)
Ministry of Justice (MJ)
National Anti-drug Secretariat (SENAD)
National Telecommunications Commission (CONATEL)
Yacyretá Binational Entity (EBY)
Government of Caaguazú Department
Municipality of Pedro Juan Caballero
Municipalidad de Pedro Juan Caballero

Municipality of Caacupé
Departmental Government of Cordillera
Honourable Chamber of Deputies
Ministry of Information and Communication Technologies (MITIC)
Municipality of Caaguazú
Municipality of Caazapá
National Customs Directorate (ADUANAS)
Departmental Government of Alto Paraná
Departmental Government of Concepción
Departmental Government of San Pedro
Ministry of the Interior (MDI)

BIOMETRICS AND HUMAN RIGHTS

Biometric data, such as facial features, iris patterns, voice tone and gait, are unique characteristics that allow for the identification of an individual[4]. Facial recognition systems collect and process highly sensitive data that, unlike other personal information, cannot be easily altered, such as when an ID or credit card is reissued after being lost or stolen. This makes them especially vulnerable to leaks or theft, which jeopardizes the privacy and control over individuals' identities. In addition, the use of this technology enables mass surveillance and detailed profiling, thus making it an intrusive and disproportionate tool that could be replaced by less invasive methods that respect human rights. (Privacy Internacional, 2013)

Mass surveillance systems capable of remotely collecting this data can do so in public spaces, such as bus stations and streets[5]. The use of facial recognition cameras has become widespread in some areas. To function, these devices require biometric databases to compare their recordings (photos or videos) with lists, usually of fugitives or individuals with criminal records.

These systems are prone to identification errors, especially for individuals with darker skin tones, women and older adults[6]. When someone is detained due to a system error that misidentifies them as a person with a criminal history, it results in a false positive that can jeopardize their integrity and lead to unjust situations and violations of their rights.

PERSONAL DATA PROCESSING IN VIDEO SURVEILLANCE

Personal data processing involves the capture of images of identified or identifiable individuals using cameras, video cameras or other technological devices, typically for security purposes. This process not only includes the recording of these images, but also their storage and subsequent use for various purposes. As these activities involve the handling of personal information, they must be regulated under specific data protection regulations.

The installation and use of these video surveillance systems must comply with strict legal and operational requirements, based on principles of personal data protection and privacy. This regulatory framework aims to ensure that their implementation does not exceed legal limits nor violates fundamental rights recognized both nationally and internationally.

4 EFF. 2018. Biometrics: facial recognition. Available at: https://www.eff.org/document/facial-recognition-one-pager

5 TEDIC. 2023 "Not with my face": Mass surveillance through facial recognition in Paraguay. Available at: https://www.tedic.org/wp-content/uploads/2022/08/Fanzine-Biometria-web.pdf

6 Many applications of facial and biometric classification techniques, which attempt to predict aspects such as gender or emotions, are based on scientifically unsound theories like phrenology and physiognomy. This results in invalid inferences that perpetuate discrimination and increase the harm caused by mischaracterization and surveillance. Coalition for Critical Technology. 2020. Abolish the @TechToPrisonPipeline. Available at: https://medium.com/@CoalitionForCriticalTechnology/abolish-the-techtoprisonpipeline-9b5b14366b16

In countries such as Argentina, Spain and Peru, these regulations include additional measures, such as the obligation to install visible signs in areas where cameras are located. Such signs must provide clear information about the entity responsible for data processing, as well as accessible contact information, thereby promoting transparency and citizen oversight regarding the use of these technologies.

In this context, biometrics are recognized as a category of sensitive personal data due to their connection to unique characteristics that can be used to identify individuals. According to the research "The ongoing alienation of our rights" (Alonzo et al., 2018)[7] and TEDIC's fanzine "Not with my face"[8] (2023), biometric data includes both physical traits and specific behaviors, classified into two main groups:

1. **Physical and physiological data:** These include unique bodily characteristics such as fingerprints, facial features, hand geometry, DNA patterns, retinal and iris structures, the shape of body parts like the hand or ear and even vein mapping.
2. **Behavioral data:** These include behavioral patterns such as voice, signature, gait and the way an individual interacts with devices, such as typing on a keyboard.

Facial recognition, one of the most widely used biometric technologies, presents significant implications for human rights and privacy. According to Al Sur[9] (2021) "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 feature allows it to be deployed in public spaces for large-scale surveillance, often without people being aware they are being monitored. This type of surveillance, known as mass surveillance, involves monitoring large groups of people without any specific suspicion directed at them. According to Maynier[10] (2023), mass surveillance can be carried out through technologies such as facial recognition in urban surveillance cameras or through wiretapping.

Mass surveillance based on biometric data, such as facial recognition, exposes individuals to serious privacy risks. The European Commission[11] (2023) states that biometric data are highly sensitive and subject to strict processing conditions, particularly when they reveal racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic information, or data related to health, sexual life or sexual orientation.

---

7 Alonzo, Carrillo and Sequera, 2018. The ongoing alienation of our rights. identity systems: biometrics and unregulated surveillance cameras in paraguay. Tedic. Available at: https://www.tedic.org/la-enajenacion-continua-de-nuestros-derechos-sistemas-de-identidad-biometria-y-camaras-de-vigilancia-no-reguladas-en-paraguay/

8 TEDIC. 2023 "Not with my face": Mass surveillance through facial recognition in Paraguay. Available at: https://www.tedic.org/wp-content/uploads/2022/08/Fanzine-Biometria-web.pdf

9 GIJN. 2023. Investigating the Digital Threat Landscape. Available at: https://gijn.org/resource/investigating-the-digital-threat-landscape/

10 European Commission. What personal data is considered sensitive? Available at: https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en

11 Romero Cerdán, T. (2019).Authentication and verification of identity through biometric information as a paradigm of personal data processing in Mexico. Revista Del Posgrado

The misuse of these technologies can result in significant violations of fundamental rights. According to Romero Cerdán[12] (2019), facial recognition allows access to sensitive information such as people's racial origin or gender, and its misuse can lead to discrimination and exclusion.

Moreover, recent studies highlight the high likelihood of errors in facial recognition technologies. According to the Red en Defensa de los Derechos Digitales[13] (2023), these technologies have repeatedly failed to accurately identify individuals, leading to numerous cases of unjust detentions of innocent people mistakenly linked to crimes.

This set of problems demonstrates the urgent need to regulate the use of these technologies under strict data protection and human rights standards, to prevent them from becoming tools of control and discrimination instead of effective security solutions.

PRIVACY AND MASS SURVEILLANCE THROUGH BIOMETRIC DATA

Privacy allows individuals to decide how much they share with others about their thoughts, feelings and personal lives. This right creates space to safeguard what defines us as human beings: our family, bonds of love and friendship, professional relationships, preferences, beliefs and everything that shapes our personality.

As Martin Scheinin, former UN Special Rapporteur, highlights[14]: "In addition to constituting a right in itself, privacy serves as a basis for other rights and without which the other rights would not be effectively enjoyed".

State surveillance is a power that allows governments to monitor and supervise the activities of citizens in order to maintain public order and security. However, this power is subject to strict legal requirements and must be justified by specific and exceptional circumstances. Surveillance may be justified in situations such as the prevention of serious crimes, the protection of national security or the fight against terrorism. For such surveillance to be legitimate, it must comply with the principles of necessity, proportionality and legality[15].

In this context, the limitation of the right to privacy must be carefully regulated to prevent abuses. Privacy is a fundamental right and its restriction may only be applied when strictly necessary and proportionate to the legitimate objective pursued. Any form of state surveillance must be supported by a clear legal basis, be subject to judicial oversight and maintain transparency to guarantee that individual rights are not disproportionately infringed upon.

---

12 R3D (2023). Mass surveillance technologies are authoritarian and do not solve public security issues. Available at: https://r3d.mx/2023/07/11/las-tecnologias-de-vigilancia-masiva-son-autoritarias-y-no-resuelven-los-problemas-de-seguridad-publica/

13 UN. 2009. Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 2009, p.13. Available at: http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf

14 Electronic Frontier Foundation. Necessary and proportionate on the application of human rights to communications surveillance. Available at: https://necessaryandproportionate.org/

15 Any legislation or initiative that restricts freedom of expression "must be made accessible to the public" and "must be formulated with sufficient precision to enable an individual to regulate his or her conduct

accordingly". Such legislation "may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution". Furthermore, any restriction on freedom of expression "must conform to the strict tests of necessity and proportionality" (General comment No. 34). Finally, restrictive measures " must be the least intrusive instrument amongst those which might achieve their protective function; and they must be proportionate to the interest to be protected". UN – CCPR. 1999. General comment 27. Available at: https://docs.un.org/en/CCPR/C/21/Rev.1/Add.9

International human rights treaties establish the conditions under which these rights can be limited. The Universal Declaration of Human Rights, in its Article 29.2, and the American Convention on Human Rights, in its Article 30, state that restrictions must be imposed by law and solely to protect the rights of others, public morals, public order and the general welfare. In addition, General Comment No. 27[16] of the Human Rights Committee (1999) provides guidance on the parameters that must be considered when imposing limitations on the rights enshrined in the International Covenant on Civil and Political Rights, guiding public policy analysis concerning these fundamental rights.

When referring to technologies that enable mass identification of individuals, it is essential to consider the impact of surveillance on the exercise and enjoyment of human rights, a phenomenon known as chilling effects[17]. People who believe that the government monitors their messages tend to censor themselves, avoiding writing or discussing certain topics, including political and social issues that could enrich public discourse. Moreover, this surveillance limits the use of digital platforms as spaces to explore new identities, perspectives and arguments, thereby limiting freedom of expression and open debate.

In relation to privacy and the use of biometric technologies, it is essential to have a legislative framework that protects personal data prior to their implementation. The lack of such regulations, which is very common, has a significant impact on individual liberties from a social and ethical perspective.(Privacy International, 2013).

Mass and indiscriminate monitoring through biometric technologies and facial recognition cameras undermines the presumption of innocence, turning all individuals into potential suspects under constant surveillance. In contrast to the offline world, where covert monitoring for criminal purposes requires a judicial process and is regulated by criminal intelligence operations, the use of these technologies enables continuous surveillance without distinction or specific justification. Instead of visible and targeted patrols by security forces, facial recognition surveillance operates covertly, without clear identification, which amplifies the sense of control and threatens the exercise of individual liberties. (Access Now, 2021).

Moreover, States must assess necessity and proportionality by considering whether there are alternatives that could achieve the same objectives while having a smaller impact on individuals' rights. The installation of biometric cameras to prevent all types of unlawful acts in public spaces reflects a disproportionate approach to the intended goal, disregarding the principle of minimal intervention by the State's punitive apparatus, a cornerstone of what is known as "minimal criminal law"[18].

16 PEN. 2022. Chilling Effects. NSA Surveillance drives US writers to self-censor. Available at: https://pen.org/wp-content/uploads/2022/08/2014-08-01_Full-Report_Chilling-Effects-w-Color-cover-UPDATED.pdf

17 Rolon and Sequera. 2015. Surveillance of Communications in Paraguay. TEDIC. Available at: https://www.tedic.org/wp-content/uploads/2018/12/Vigilancia-estatal-de-las-comunicaciones-y-derechos-fundamentales-en-Paraguay.pdf In this research, the section on minimal criminal law is developed with this definition "The reduction of criminal instances to the minimum and their general codification through the decriminalization of all conduct that does not harm fundamental legal interests, but rather overload judicial work with a useless and harmless squandering of that scarce and costly resource that is punishment, having the triple effect of generally weakening guarantees, increasing inefficiency within the judicial machiner, and devaluing legal interests deserving of criminal protection" Ferrajoli, Luigi. Crisis of the political system and jurisdiction: the nature of the Italian crisis and the role of the judiciary. Revista Pena y Estado año 1 número 1–Argentina 1995: Editores del Puerto s.r.l. p. 113

18 American Convention on Human Rights, articles 11, 13 and 15.

International regulations limiting biometric processing

The impact of mass surveillance on privacy not only affects individuals but also conflicts with the standards established by international human rights norms. Instruments such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the American Convention on Human Rights recognize privacy as a fundamental right that protects individuals against arbitrary and abusive interference in their private lives.

These regulations emphasize the importance of limiting state surveillance and other forms of mass data collection, ensuring that these practices do not undermine the full enjoyment of essential rights such as freedom of expression, association and the right to private life. The Universal Declaration of Human Rights (UN, 1948), in its articles 7 on equality before the law, 11 on the presumption of innocence, 12 on the right to honor and dignity, 13 on freedom of movement, 20 on freedom of assembly and 30 on the indivisibility of rights, guarantees fundamental rights inherent to all individuals, which may be jeopardized by the implementation of video surveillance technologies. Similarly, the International Covenant on Civil and Political Rights[19] (ICCPR, 1966) protects the right to privacy and freedom of expression in its articles 17 and 19, respectively, highlighting the need to safeguard these rights against the advancement of invasive technologies. Regional human rights instruments, such as the American Convention on Human Rights of the OAS, also recognize the rights to freedom of opinion and expression, freedom of assembly, and honor and dignity[20], as well as establish standards related to privacy and freedom of expression (OAS, 1969).

In addition to the existing and binding regulations applicable to Paraguay, UN and OAS special rapporteurs have recommended imposing moratoriums, or even outright bans, on the use of facial recognition. These recommendations stem from the lack of effective safeguards to ensure respect for the rights of data subjects, protecting their privacy and other fundamental rights from being violated.

In relation to the implementation of biometrics, international human rights organizations have expressed concern about the indiscriminate use of biometric technologies. The United Nations High Commissioner for Human Rights has called attention[21] to the implementation of biometric data projects without the necessary legal safeguards, urging States to demonstrate the necessity and proportionality of these systems for legitimate purposes before putting them into use.

Experts such as Frank La Rue[22] and Navi Pillay[23], in their roles as UN Special Rapporteur and UN High Commissioner for Human Rights respectively, have expressed concern about the potential violations of the right to privacy due to the improper use of biometric technologies. These concerns underscore the need for stricter regulation and a more robust protection of personal data.

---

19 General Assembly (UN). 2018. The right to privacy in the digital age. Report of the United Nations High Commissioner for Human Rights. A/HRC/39/29. 2018. Available at: https://docs.un.org/en/A/HRC/39/29

20 UN. 2013. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue* A/HRC/23/40. UN. April, 2013.

21 UN News Centre, 2013. UN rights chief urges protection for individuals revealing human rights violations. Available at: https://news.un.org/en/story/2013/07/444512

22 UN. 2009. Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 2009, p.10-11. Available at: http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf

23 UN. 2019. UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools. Available at: https://www.ohchr.org/en/press-releases/2019/06/un-expert-calls-immediate-moratorium-sale-transfer-and-use-surveillance?LangID=E&NewsID=24736

Martin Scheinin, former UN Special Rapporteur[24], has warned about the specific risks associated with the centralized storage of biometric data. According to his analysis, this practice not only increases the vulnerability of individuals and compromises information security, but could also lead to a significant increase in error rates as more biometric information accumulates in these centralized databases.

> "Cases where biometrics are not stored in an identity document, but in a central database, thereby increasing the information security risks and leaving individuals vulnerable. As the collection of biometric information increases, error rates may rise significantly".

> "The increase in error rates may result in the wrongful criminalization of individuals or social exclusion. Meanwhile, the Rapporteur highlights an aspect we mentioned earlier: biometrics cannot be revoked".

> "(...) once copied and/or fraudulently used by a malicious party, it is not possible to issue an individual [identity] with a new biometric signature".

In June 2019, David Kaye, former UN Special Rapporteur[25], presented to the Human Rights Council the urgent need for States to impose immediate moratoriums on the use of surveillance technologies, including facial recognition, until regulations are in place that respect human rights and incorporate robust safeguards.

The Office of the Special Rapporteur for Freedom of Expression, in its 2022 annual report, references the case of the São Paulo city metro, where the State Court of Justice rejected the implementation of a system for capturing and processing users' biometric data for facial recognition purposes, given its "potential to affect the fundamental rights of citizens"[26].

The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, in their report on Surveillance and Human Rights, emphasized that States should adopt measures to prevent the commercialization of surveillance technologies, with particular focus on their research, development, trade, export and use, considering their potential to facilitate the systematic violation of human rights[27].

For its part, the Inter-American Juridical Committee (CJI) of the Organization of American States (OAS) drafted the Updated Principles on Privacy and Personal Data Protection[28],which should govern the comprehensive use of these devices.

---

24 OAS, 2022. Annual Report of the Office of the Special Rapporteur for Freedom of Expression. Annual Report of the Inter-American Commission on Human Rights 2022. Available at: https://www.oas.org/en/iachr/expression/reports/IA2022ENG.pdf

25 UN, 2019. Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression Available at: https://docs.un.org/en/A/HRC/41/35

26 OAS. 2021. Updated principles on privacy and personal data protection. Available at: https://www.oas.org/en/sla/iajc/docs/Publication_Updated_Principles_on_Privacy_and_Protection_of_Personal_Data_2021.pdf

27 R3D: Red en Defensa de los Derechos Digitales. 2023. Buenos Aires Government requested biometric data from over 200 judges and prosecutors without justification. Available at: https://r3d.mx/2023/05/22/gobierno-de-buenos-aires-solicito-datos-biometricos-de-mas-de-200-jueces-y-fiscales-sin-justificacion/

28 CELS. 2022. Illegal Use of the Facial Recognition System in CABA: At the request of the City government, the Superior Court of Justice (TSJ) removed the judge from the case. Available at: https://www.cels.org.ar/web/2022/07/uso-ilegal-del-sistema-de-reconocimiento-facial-en-caba-a-pedido-del-gobierno-de-la-ciudad-el-tsj-saco-al-juez-de-la-causa/

Among the most important principles regarding personal data protection, the following stand out:

- **Lawful purposes and loyalty:** the images captured by video surveillance equipment must be collected solely for purposes duly established by law and through legal and legitimate means that ensure minimal intervention, proportionality and do not exceed the limits of strict necessity.
- **Relevance and necessity:** the images collected should be limited to those that are relevant and adequate for the specific purposes of their collection and ulterior processing, and should not exceed the minimum necessary for such purposes.
- **Limited processing and retention:** the images collected should be processed and retained in accordance with their specific purpose and for the period necessary to fulfill these purposes.
- **Data Security:** the collected data must be protected according to the principles of confidentiality, integrity and availability. This protection should be implemented through reasonable and appropriate security safeguards at the technical, administrative and institutional levels to prevent unauthorized or illegitimate processing—including access, loss, destruction, damage or disclosure, even if accidental. Such measures must be fully auditable at all levels and permanently updated.

  Likewise, the collected data must not be disclosed, made available to third parties or used for purposes other than those for which it was collected, unless the affected individual has given their consent.

- **Availability:** those responsible for data processing must provide reasonable, agile, simple and effective mechanisms for data subjects to request access to their collected data, as well as its rectification or cancellation.

  There is a growing effort to establish legal frameworks that regulate the processing of biometric data, especially concerning the implementation of facial recognition in public and private spaces. However, experts in the field warn that regulations focused solely on the protection of personal data are insufficient to address the specific challenges posed by biometrics. In the area of privacy, robust theoretical and legislative frameworks are still lacking to fully address risks such as vulnerability to abuse, lack of informed consent and the potential for mass surveillance and discrimination. The lack of an adequate and specialized regulatory approach leaves a critical gap that exposes individuals to significant risks, underscoring the urgent need to develop more detailed regulations with effective safeguards to protect fundamental rights. (Díaz, 2018)

GLOBAL ROLLBACK OF FACIAL RECOGNITION USE

The implementation of facial recognition in public spaces is a global trend. Below, we present examples from Western countries, along with the arguments and discussions taking place around the world to roll back its use.

Buenos Aires, Argentina

In 2023, a facial recognition system initially designed to track and capture fugitives in the Autonomous City of Buenos Aires became the center of major controversy after it was revealed that it had been used to monitor thousands of individuals not listed as fugitives—including judges, public figures and human rights leaders—leading to accusations of espionage and abuse of power[29]. After numerous legal actions by civil society, its implementation was declared unconstitutional and judicial investigations were opened[30].

In addition, the inaccuracy of the system led to irregular and potentially wrongful detentions by the City Police. False positives and the lack of adequate oversight of the system's use raised serious concerns about the protection of civil rights and legal certainty in Argentina. To this day, these issues serve as a reminder of the threats such systems can pose to democracy.

The use of biometric data in surveillance cameras, particularly due to advancements in facial recognition, is under scrutiny amid growing concern from citizens, governments and specialized agencies.

Other cases are being documented globally, as seen in the report "In Focus", published by organizations belonging to the International Network of Civil Liberties Organizations (INCLO), who analyzed how, in various ways, the use of Facial Recognition Systems (FRS) affected the lives of people in 13 countries across the Americas, Africa, Europe, Asia and Australia. (International Network of Civil Liberties Organizations, 2021).

Evidence regarding the severity of implementing surveillance technologies without human rights impact assessments, or through the exploitation of legal loopholes, fuels an inhumane and opaque industry with questionable applications. This industry perpetuates discrimination, biases and even anti-democratic and corrupt practices on a massive scale.

The chain of corruption tied to the expansion of this industry involves multiple elements: manipulated or targeted public procurement, the erosion of criminal due process guarantees, the technologization of tools for ideological and political persecution and the abusive use of personal data, including sensitive information.

Even its potential regulation is now under global scrutiny due to the challenges it poses. As Carmen-Nicole Cox, Director of Government Affairs at ACLU California Action, aptly described: 'Regulating facial surveillance is like trying to block a cannonball with cardboard'—a statement made in the broader context of efforts to push for regulation in California, United States (Holden, 2023)

29 Agencia Brasil. 2023. Court of Justice suspends purchase of cameras with facial recognition in SP https://agenciabrasil.ebc.com.br/saude/noticia/2023-05/tj-suspende-compra-de-cameras-com-reconhecimento-facial-em-sp

30 Court of Justice of the State of São Paulo. 2023 Decition – Mandado. Available at: https://www.migalhas.com.br/arquivos/2023/5/02F4930DEF8E75_decisao-smart-sampa.pdf

The discussion is gaining increasing attention. Below is a summary of key events from around the world between 2022 and 2023:

São Paulo, Brasil

On May 18, 2023, the Court of Justice of São Paulo suspended a tender process for 20,000 facial recognition cameras, following a civil action initiated by Councilor Silvia Ferraro of the Feminist Caucus of PSOL, member of the Municipal Chamber[31].

In his ruling, Judge Luis Manuel Fonseca Pires expressed serious concerns about widespread violations of fundamental rights, particularly highlighting the risk of reproducing social discrimination and structural racism in the absence of mechanisms to review such practices[32]. In the ruling he cited the Network of Security Observatories, which indicates that "90 percent of the arrests made in Brazil using this technology (data collected in 2019) were of Black individuals, and among them, there were identification errors that led to the detention of innocent people".

Even so, the ruling was appealed by the State Prefecture, resulting in a reversal and the scheduling of the bid process[33].

This case adds to many other recent developments, such as the suspension of a call by the City Council and the judicial prohibition of the facial recognition system in the São Paulo metro, following a legal action brought by the Public Defender's Office of the State of São Paulo, the Federal Public Defender's Office, the Brazilian Institute of Consumer Protection (Idec), Intervozes – Coletivo Brasil de Comunicação and Article 19 Brazil[34].

Strasbourg, France

In July 2023, the European Court of Human Rights (ECHR) ruled that Russia violated the rights to privacy, family life and freedom of expression of protester Nikolay Glukhin[35] by using facial recognition technology to identify him after a peaceful solo protest in Moscow[36].

According to Glukhin, the police used videos and photos of his protest on social media, along with images from the Moscow metro's surveillance system, to identify and arrest him. He was fined for protesting without prior notification to the authorities.

Although Russia claimed that Glukhin violated laws on protests, the ECHR found that the use of facial recognition was disproportionate and incompatible with a democratic society, given that the

31 Agencia Brasil. 2023. São Paulo will have facial recognition cameras. Available at: https://agenciabrasil.ebc.com.br/es/justica/noticia/2023-05/justicia-lanza-edicto-de-camaras-con-reconocimiento-facial-en-sp

32 DPL News. 2022. São Paulo Metro banned from using facial recognition system. Available at: https://dplnews.com/metro-de-sao-paulo-tiene-prohibido-utilizar-sistema-de-reconocimiento-facial/

33 HUDOC- European Court of Human Rights. 2023. Use of facial-recongnition technology breached rights of Moscow underground protestor. Available at: https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=003-7694109-10618091&filename=Judgment%20Glukhin%20v.%20Russia%20-%20use%20of%20facial-recognition%20technology%20against%20-Moscow%20underground%20protestor.pdf

34 R3D. 2023. European Court of Human Rights rules against use of facial recognition to identify Russian protester. Available at: https://r3d.mx/2023/07/05/tribunal-europeo-de-derechos-humanos-falla-contra-el-uso-de-reconocimiento-facial-para-identificar-manifestante-ruso/

35 Europarl. 2024. Artificial Intelligence Act: MEPs adopt landmark law. Available at: https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law

36 European Commission. 2024. AI Act enters into force. Available at: https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en

protest was peaceful and did not pose a danger. The Court noted that there was no other way the police could have identified him so quickly.

Organizations welcomed the ruling, emphasizing that facial recognition technologies pose a threat to rights such as freedom of expression and peaceful assembly.

European Union

The European Union approved the European Artificial Intelligence Act[37], which came into force on August 1, 2024. This regulation aims to establish a comprehensive framework for the use of AI technologies, while acknowledging their potential risks[38]. It allows governments and private companies to use facial recognition systems on a large scale, both in real-time (immediate capture and identification of faces) and retrospectively (identification of faces in previous recordings).

In 2023, Amnesty International warned that the European Union underestimates the risks of retrospective facial recognition by arguing that its deferred use allows for the mitigation of potential problems. According to the organization, this stance overlooks critical aspects such as de-anonymization and the suppression of fundamental rights. Additionally, the mere knowledge that these technologies can be applied at any time creates a chilling effect[39] on individuals, limiting their freedom of expression and movement.

In response to the abuses and inequalities associated with the use of these technologies, Amnesty International has called for a complete ban on mass biometric surveillance. The AI Act represents a key opportunity to ensure the protection of human rights and prevent these tools from becoming mechanisms of control and oppression.

Cambridge, United Kingdom

A new report from the Minderoo Centre for Technology and Democracy at the University of Cambridge calls the police use of live facial recognition in the UK "unethical" and possibly illegal[40]. This technology compares faces seen in CCTV cameras in real time with watchlists of wanted criminals. When a match is found, the police are notified.

The report established minimum ethical standards that this technology should meet. No police use case in the United Kingdom passed the test. They did not demonstrate that it is effective or safe and they do not comply with requirements for privacy, human rights and oversight.

Researchers called for a halt to the police use of this technology until benefits are demonstrated and risks are minimized. The Metropolitan Police defended the legality of its use, but experts warn that current laws are insufficient to regulate and limit these invasive systems.

37 Amnesty International. 2023. Surveillance through retrospective facial recognition conceals human rights abuses.Available at: https://www.es.amnesty.org/en-que-estamos/blog/historia/articulo/la-vigilancia-mediante-reconocimiento-facial-retrospectivo-oculta-abusos-contra-los-derechos-humanos/

38 Tech Monitor30. 2022. Police use of live facial recognition "unethical" and possibly illegal.Available at: https://techmonitor.ai/technology/ai-and-automation/police-facial-recognition-live-unethical

39 R3D. 2023. Massachusetts debates law to restrict police use of facial recognition. Available at: https://r3d.mx/2023/08/04/massachusetts-discute-ley-para-restringir-el-uso-policial-del-reconocimiento-facial/

40 Washington Post. 2024. San Francisco becomes first city in the U.S. to ban facial recognition software. Available at: https://www.washingtonpost.com/technology/2019/05/14/san-francisco-becomes-first-city-us-ban-facial-recognition-software/

United States

Existing pressure in the United States has led places like Massachusetts[41], Austin and San Francisco[42], to ban the use of facial recognition[43] by police forces and government entities. On the other hand, New York and Portland, Oregon, are some of the cities in the country that have established restrictions on the use of facial recognition technology in the private sector[44]. However, discussions have deepened with promising advances in ensuring civil liberties, as we will see next.

In 2023, several U.S. senators and representatives, including prominent figures such as Edward J. Markey, Bernie Sanders and Elizabeth Warren, reintroduced the "Facial Recognition and Biometric Technology Moratorium Act"[45]. This legislation seeks to prohibit the government from using facial recognition technologies and other biometric solutions, arguing that these tools present serious privacy issues, civil liberties concerns and disproportionately affect marginalized communities. These concerns have intensified following reports that facial recognition has led to wrongful arrests, particularly of Black men, and that nearly half of the adult faces in the U.S. are in databases of this kind[46].

The legislators' statements emphasize the danger these technologies pose to democracy and the privacy of citizens. Senator Markey highlighted that "the collection of biometric data poses serious risks of invasion of privacy and discrimination". For her part, Representative Jayapal noted that facial recognition technology is not only invasive and error-prone, but has also been used against communities of color. The legislative proposal establishes, among other provisions, a ban on the use of facial recognition and other biometric technologies by federal entities, along with conditions for the allocation of federal funds to state and local entities. Additionally, it seeks to prohibit the use of information collected through biometric technologies in judicial proceedings and grants private rights of action to affected individuals[47].

The "Facial Recognition and Biometric Technology Moratorium Act" has received support from various organizations, including the ACLU, EPIC and the Electronic Frontier Foundation[48]. These groups have emphasized the importance of protecting civil rights and safeguarding citizens' privacy amid the growing adoption of surveillance technologies.

---

41 Washington Post. 2024. These cities bar facial recognition tech. Police still found ways to access it. Available at: https://www.washingtonpost.com/business/2024/05/18/facial-recognition-law-enforcement-austin-san-francisco/

42 Washington, Oregon, California, Colorado and Alabama all have limited government actor or police use. Up to date information about state regulation of facial recognition technology can be found at. Available at : www.banfacialrecognition.com/map/.

43 Congress. GOV. 2023. H.R.1404 - Facial Recognition and Biometric Technology Moratorium Act of 2023. Available at: https://www.congress.gov/bill/118th-congress/house-bill/1404

44 NextGov. Fcw. 2023. Lawmakers Intro Bill to Ban Government Use of Facial Recognition. Available at: https://www.nextgov.com/digital-government/2023/03/lawmakers-intro-bill-ban-government-use-facial-recognition/383691/

45 ED Marley. 2022. Senators Markey and Merkley, and Reps. Jayapal, Pressley to Introduce Legislation to Ban Government Use of Facial Recognition, Other Biometric Technology Available at: https://www.markey.senate.gov/news/press-releases/senators-markey-and-merkley-and-reps-jayapal-pressley-to-introduce-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology

46 EFF. 2020. Facial Recognition and Biometric Technology Moratorium Act of 2020. Available at: https://www.eff.org/my/document/facial-recognition-and-biometric-technology-moratorium-act-2020

47 The Guardian. 2023. Facial recognition bias frustrates Black asylum applicants to US, advocates say. Available at: https://www.theguardian.com/us-news/2023/feb/08/us-immigration-cbp-one-app-facial-recognition-bias

48 BiometricUpdate. 2024. Bills to ban facial recognition spark lively debate in New York council. Available at: https://www.biometricupdate.com/202406/bills-to-ban-facial-recognition-spark-lively-debate-in-new-york-council

On the other hand, migrant rights organizations have expressed concern about the shortcomings of the new mobile application launched by the U.S. government to process asylum applications at the border with Mexico. This tool, called CBP One, uses facial recognition technology that has proven to have biases, especially when attempting to identify individuals with darker skin. The impact has been particularly notable among migrants from Haiti and African countries, who face constant errors when trying to input their data and photographs into the application.

In addition to the clear racial bias in facial recognition technology, many asylum seekers face other obstacles, such as a lack of compatible mobile devices and limited internet access. In response to these challenges, some nonprofit organizations have implemented creative solutions, such as using bright lights when taking photos for the application, to improve the capture of facial features. However, these solutions are not universal and have proven particularly ineffective for children under the age of six. Despite ongoing inquiries and concerns, Customs and Border Protection (CBP) has remained silent, offering neither solutions nor comment on the matter[49].

Two bills have been proposed by members of the New York City Council to restrict the use of facial recognition technology by businesses and residential buildings, preventing its use to identify customers or tenants without their consent[50].

The first bill, sponsored by Council Members Shahana K. Hanif and Jennifer Gutiérrez, seeks to prohibit private businesses, including stadiums and public auditoriums, from using biometric information to identify or verify a customer. If they choose to collect such information, they must notify the customer and obtain written consent, and they would be prohibited from sharing or storing that information.

On the other hand, a second bill focuses on residential buildings, aiming to prohibit landlords from using biometric recognition technologies to identify tenants or their guests. These measures arise in a context where it was revealed that Madison Square Garden, under owner James Dolan, was using this technology, sparking controversy and potential legal sanctions.

In a recent city council discussion, Councilman Kristerfer Burnett, known for his commitment to civil rights and privacy, introduced two bills related to facial recognition technology[51]. His proposal comes in response to growing pressure, both nationally and locally, from civil society organizations concerned about privacy and civil liberties.

Burnett's first bill aims to establish a community advisory commission on surveillance. This commission would require city council approval before the Baltimore Police Department can purchase surveillance equipment. The second bill focuses on setting clear regulations for the use of facial recognition technology, as well as the retrieval, retention and destruction of data.

49 The Baltimore Banner. 2023. Proposals to regulate facial recognition could be 'test case' for Baltimore's authority over its police. Available at: https://www.thebaltimorebanner.com/politics-power/local-government/proposals-to-curb-facial-recognition-could-test-baltimore-authority-over-police-WMHCJLZFNBC55J7BFY2G2GGWFI/

50 WYPR. 2021. Burnett Seeks Regulation Of Facial Recognition Technology In Baltimore. Available at: https://www.wypr.org/wypr-news/2021-02-25/burnett-seeks-regulation-of-facial-recognition-technology-in-baltimore

51 Within the framework of the analysis of the companies found on the list of purchases made by state institutions in Paraguay, a series of names can be identified, as indicated in Table 4.

Burnett expresses special concern for civil liberties and privacy, particularly regarding marginalized communities, which have historically faced discriminatory policing and surveillance practices. The Councilman emphasizes the need to balance public safety with privacy protection.[52]

In this context of global concern, it is worth examining surveillance companies, equipment brands and their relationship to human rights, particularly whether there are concerns about the products they offer or the methods they employ. Below is a list of companies that provide this type of technology to various countries.

TABLE 4. List of companies providing facial recognition cameras worldwide[53, 54]

Hikvision
Senken
QNAP
Avigilon
Sony
Intelligent Security Systems (ISS)
Cellebrite
ZTE
NEC
Dahua
Huawei
Verint

In this regard, it is worth noting that some companies, such as Hikvision, have come under scrutiny, as highlighted in an article[55] by security systems specialist Felipe Arguello. The name of this company appears repeatedly in U.S. government purchases related to closed-circuit cameras.

Hikvision was added to the U.S. government's blacklist on the grounds of committing human rights violations in China's Xinjiang province, specifically targeting Muslim minorities, according to specialist Felipe Arguello and international outlet El Tiempo[56].

52 The items on this list are identified in the following investigations:
1. Access. 2021. Surveillance Tech in Latin America Available at: https://www.accessnow.org/wp-content/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf
2. AL SUR. 2021. Facial Recognition in Latin America. Available at: https://www.alsur.lat/sites/default/files/2021-10/ALSUR_Reconocimiento%20facial%20en%20Latam_EN_Final.pdf

53 Infotecnico. 2018 Available at: https://www.infoteknico.com/mas-sanciones-contra-dahua-y-hikvision/

54 El tiempo. 2019. US blacklists Hikvision for rights violation. Available at: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/administracion-trump-pone-a-hikvision-en-la-lista-negra-de-estados-unidos-420674

55 APP Sindicato. 2023. Dystopia: UFPR and PUC researchers expose "emotion monitoring" in state schools. Available at: https://appsindicato.org.br/distopia-pesquisadoresas-da-ufpr-e-da-puc-denunciam-monitoramento-de-emocoes-nas-escolas-estaduais/

56 The ISS is a software system used by the Paraguayan National Police, which we document below.

A similar case occurred with the brand Intelligent Security Systems (ISS) in Brazil, which presents racial biases, according to researchers[57] from the Federal University of Paraná and the Pontifical Catholic University (PUC-PR) who conducted a study on the use of facial recognition in schools in Paraná[58].

The report underscores weaknesses in surveillance practices and non-compliance with the Data Protection Law, and raises concerns regarding the effectiveness of artificial intelligence in monitoring student behavior. Celepar, a public information technology company in Brazil, in collaboration with PUC-PR, conducted tests of facial biometrics and external monitoring using ISS software and concluded that there are ethnic biases in facial recognition systems, thus highlighting the risk of reproducing social discrimination.

HUMAN RIGHTS AND SURVEILLANCE THROUGH FACIAL RECOGNITION CAMERAS

As highlighted in the section on international human rights, Paraguay is committed to the protection of these rights, and international instruments are binding within its territory. Although there are no specific regulations governing the use of biometric data at the local level, these international obligations should be taken into account when implementing or debating biometric technologies. It is essential that any discussion or implementation of such technologies aligns with the human rights protection standards established in these legal frameworks, to ensure that the fundamental rights of individuals are respected.

State surveillance is a limited power that must be justified for specific reasons, such as the prevention of serious crime or the protection of national security. To be legitimate, it must comply with principles of necessity, proportionality and legality, and the limitation of the right to privacy must be strict and proportional to the objective pursued. This surveillance requires a clear legal basis, judicial oversight and transparency to prevent abuses and protect individual rights. (EFF, n.d.)

The following outlines the rules that apply to limiting the surveillance of communications, which are further supported by international regulations. First, the National Constitution, in its Article No. 33, recognizes the Right to Privacy, which states:

> "Personal and family privacy, as well as respect for private life, are inviolable. Individual behavior that does not affect public order as established by law or the rights of third parties is exempted from the authority of public officials. The protection of the privacy, dignity and private image of each individual is hereby guaranteed".

57 Acuña, Alonzo and Sequera. (2017). Personal data protection in public databases in Paraguay. TEDIC. Available at: https://www.tedic.org/la-proteccion-de-datos-personales-en-bases-de-datos-publicas-en-paraguay/

58 National Congress. (2021). Comprehensive Personal Data Protection Bill. Available at: https://silpy.congreso.gov.py/web/expediente/115707

Likewise, the same legal framework recognizes in its Article No. 25 the Right to the Expression of Personality, and establishes:

> "Every individual has the right to freely express his personality, to be creative and to forge his own identity. Ideological pluralism is guaranteed".

In matters of data protection, the National Constitution provides for Habeas Data as the appropriate legal mechanism for accessing information[59] and data concerning oneself or one's assets held in official or private records of public interest, understanding how they are used and the purposes for which they are processed. It also establishes the appropriate legal mechanism to request the updating, correction or deletion of such data in the event that they are inaccurate or unlawfully infringe upon an individual's rights[60].

In Paraguay, although there are no specific regulations establishing minimum standards for the protection of personal data, including its collection, processing, anonymization or destruction, the existing legal framework does contain general protection provisions.

For its part, Law No. 4868/2013 on Electronic Commerce states in Article 6:

> "In no case may the commercial activity of providers violate: (...) e) the protection of personal data and the rights to personal and family privacy of the parties or third parties involved; and f) the confidentiality of bank records and accounts".

However, it is important to mention the Comprehensive Personal Data Protection Bill presented by several national deputies[61], with the support of the Personal Data Coalition of Paraguay[62]. This proposal aims to establish precise, detailed and modern provisions that ensure respect for the rights and guarantees recognized by the National Constitution. These provisions are aligned with international standards on the subject and seek to provide legal certainty to both citizens and those responsible for data processing.

This bill seeks to establish a state agency for data protection, which would be responsible for overseeing and enforcing the legal provisions outlined in the proposed legislation. The agency would also offer technical assistance to data controllers and the general public regarding its implementation.

The existing regulatory gap within the local legal framework stems from the lack of clear parameters for reasonableness and proportionality in the collection, processing and storage of images captured by facial recognition technology.

---

59 Personal Data Coalition. (2024). Latest version of the personal data bill in Paraguay: A collective and participatory effort. Available at: https://www.datospersonales.org.py/ultima-version-del-proyecto-de-ley-de-datos-personales-en-paraguay-un-trabajo-colectivo-y-participativo/

This version is the third and final version submitted by the members of the Coalition. SILPY Link: https://silpy.congreso.gov.py/web/descarga/dictamencomision-440780?preview

60 Amnesty International Spain. 2023. Surveillance through retrospective facial recognition conceals human rights abuses. Available at: https://www.es.amnesty.org/en-que-estamos/blog/historia/articulo/la-vigilancia-mediante-reconocimiento-facial-retrospectivo-oculta-abusos-contra-los-derechos-humanos/

61 National Police of Paraguay. (2021). Third Semiannual Accountability Report to Citizens 2020. National Police of Paraguay. Available at: https://www.policianacional.gov.py/wp-content/uploads/2021/01/NOTA-07-2021-DIRECCION-CENTRO-DE-SEGURIDAD-Y-EMERGENCIAS.pdf

62 Ultima hora. 2021. National Police: only 60% of 911 cameras are working. Available at: https://www.ultimahora.com/policia-nacional-solo-el-60-las-camaras-del-911-funcionan-n2960069

On the other hand, Law 6534/20 on the protection of personal credit data, a regulation that only addresses data used for credit purposes, defines in its Article 3 (sections a and b) what is considered personal data and sensitive personal data:

- **Personal data:** Any kind of information pertaining to identified or identifiable legal entities or natural persons. A natural person shall be considered identifiable when they can be identified through an identifier or by one or more elements that characterize their physical, physiological, genetic, psychological, economic, cultural or social identity. The rights and guarantees of personal data protection shall extend to legal entities to the extent that they are applicable.
- **Sensitive personal data:** This refers to data related to the intimate sphere of the data subject, or whose improper use could lead to discrimination or pose a serious risk to them. Sensitive personal data is considered any information that may reveal aspects such as racial or ethnic origin; religious, philosophical or moral beliefs; trade union membership; political opinions; data related to health, life, sexual preference or orientation, genetic characteristics, or biometric data used to uniquely identify a natural person.

  However, this law does not provide guarantees or guidelines for the processing of such data; it only defines it and then focuses exclusively on credit-related processing. This is expected to be addressed by the upcoming law currently under discussion in the National Congress on the comprehensive protection of personal data.

As we can see, current regulatory provisions lack clarity on the allocation of responsibility regarding the use of facial recognition technology. This responsibility encompasses the functioning of the equipment, its operation, maintenance, repair in case of malfunction or damage, the processing of the collected data, data security and the accountability of both the officials involved and the institution in cases of misuse of the equipment and collected personal data.

This aspect is crucial, as the equipment is purchased using funds from municipalities, departmental governments and other state institutions outside the National Police. This raises key questions about the ownership of this equipment and the legality of using these funds for the aforementioned purposes.

Global experience shows that even with clear legal and judicial provisions, abuses are frequently committed. This suggests that the regulatory gap would not only facilitate abuses but could even lead to their normalization under the argument of “national security”.

Mass surveillance as a threat to democratic order

During the demonstrations that took place in March 2021, when thousands of protesters took to the streets, driven by desperation due the health crisis caused by the COVID-19 pandemic, the National Police acknowledged that they were profiling individuals using public video surveillance cameras, with discretion and, presumably, without a court order.

- The Head of Public Relations of the Police, María Elena Andrada, reported that a review of the 911 System camera recordings was conducted for each day of the protests and it was possible to identify "the same group of people who participated in all the days with incidents".
- Article in IP Paraguay (IP 2021). "Police have identified individuals who committed disturbances using the 911 System". March 9, 2021.
- This situation became even more evident when the Minister of the Interior at that time, Arnaldo Giuzzio, requested around the same dates to implement more mass surveillance cameras in public spaces using FSU funds (CONATEL, 2021).

Paraguay is not a country where the National Police is known for respecting human rights; rather, its operations remain deeply influenced by practices inherited from the Stroessner dictatorship. (CODEHUPY, 2022). Numerous citizen complaints have been filed against the National Police regarding the excesses they committed against protesters. These incidents were reported by local media and involved both regular officers and members of the so-called Lince Group.

Considering these instances of abuse and their potential extension into the realm of biometric data and facial recognition technology, it would not be surprising if such tools were employed for espionage and/or the surveillance of citizens belonging to opposition political parties and organizations, social activists, or simply ordinary citizens who openly express their discontent with the Government or a specific government official.

This situation, in addition to violating the aforementioned rights, could lead to the criminalization of social movements and the right to protest. It could result in mass, clandestine surveillance of citizens, where individuals' behavior is judged solely at the discretion of an operator, without even the most basic legal safeguards to ensure the effective exercise of their rights.

However, the legal void and the lack of sufficient legal, conceptual and regulatory frameworks in the existing regulations are not limited to operational or technological aspects, but also extend to the very nature of the 911 System itself.

However, the legal void and the lack of sufficient legal, conceptual and regulatory frameworks affecting the aforementioned norms are not limited to operational or technological aspects, but also extend to the very nature of the 911 System itself..

On the other hand, regarding the handling of personal and private data, the National Police have repeatedly stated that they cannot provide the information requested under the Public Access to Information Law regarding facial recognition cameras, arguing that the information is sensitive (TEDIC, 2019).

However, contradictorily to these claims from the state security forces, the lack of a personal data protection law and better management of citizens' personal information became evident precisely after such information was leaked, which was also documented by TEDIC through the article "The leak of police data in Paraguay and the urgent need for answers" (TEDIC, 2023).

The article detailed that this data leak consisted not only of identity document numbers but also of biometric data, with more than four million facial image clips captured by cameras.

This incident raises questions about how this type of technology might be used. In this context, according to Amnesty International Spain[63]:

> "Remote 'deferred' biometric identification is possibly the most dangerous surveillance measure we have ever heard of".

The possibility of incidents similar to the aforementioned data leak occurring again underscores the need for clear regulations and greater transparency from the Paraguayan State in this area. The leaked files, documented by TEDIC, contained information related to children, adolescents, gender non-conforming individuals and sensitive personal data that should have received special protection.

The implementation of this technology, without assessments of necessity and proportionality, currently exposes the population's biometric and sensitive data to the risk of being cross-referenced with other information contained in the same database. This includes data related to organized crime, internal investigations of security forces, proceedings and processes conducted by public forces and other entities that have collaborated with the police

The exponential harm is significant; therefore, it warrants a thorough audit and the immediate suspension of ongoing practices that violate human rights, such as the implementation of facial recognition technologies in public surveillance cameras.

63 La Nación. 2022. Police's 1,447 installed cameras were reduced to 640. Available at: https://www.lanacion.com.py/investigacion/2022/10/18/de-1447-camaras-instaladas-que-tenia-la-policia-se-redujeron-a-640/

911 SYSTEM: PRIMARY INSTITUTION THAT MANAGES FACIAL RECOGNITION CAMERAS

The system was created by Law 4739/12 during the government of former President Federico Franco, and is managed by the Directorate of the Security and Emergency Center (CSE), under the General Directorate of Order and Security of the National Police.

The operational powers of the CSE include the development and operation of the 911 System, the reception and processing of assistance requests, as well as the follow-up of these requests until their resolution, among other purely organizational functions (National Congress, 2012). This directorate is headed by a Commissioner General for Order and Security, as established by the same law.

On May 5, 2014, the Command of the National Police issued Resolution 452, which details the functions and operational aspects of the 911 System. This resolution created and regulated the Camera and Monitoring Division, responsible for the continuous monitoring of security cameras installed in various areas under the jurisdiction of the 911 System (Policía Nacional, 2014). The Division is tasked with ongoing surveillance, identifying suspicious situations involving individuals and vehicles, and controlling license plates in high-traffic areas.

Some of these activities have a high potential to violate the previously mentioned international human rights standards. In addition, both the law establishing the 911 System and the internal regulations of the National Police fail to define clear legal criteria for what constitutes a "suspicious situation". It is not specified who determines these activities, nor the procedure to confirm or dismiss them. There is also no appropriate mechanism for the anonymization, destruction or storage of captured images. (TEDIC, 2015)

The 911 System law defines its main objective as the comprehensive management of emergencies, from the reception of the call to the final report, positioning the 911 system as an emergency response channel offered to citizens by the National Police and other participating institutions (National Congress, 2012). However, the acquisition of equipment with facial recognition technology, financed with the Universal Services Funds (FSU) of the National Telecommunications Commission (CONATEL), raises serious doubts about its legality and alignment with the original purpose of the System.

EVOLUTION OF CAMERA IMPLEMENTATION IN PARAGUAY

The National Police, in 2018, announced the incorporation of 154 closed-circuit cameras, of which 44 had facial recognition technology, according to reports by the newspaper ABC Color (ABC. 2022).

That same year, the report conducted by TEDIC concluded that the mass collection of biometric data "is unnecessary and disproportionate" (TEDIC, 2018). The report made reference to the invasive nature of collecting personal data from individuals moving through public spaces, regardless of whether they were involved in suspicious activities and without apparent guarantees of protection. It also underscored the need for transparency regarding the biometric data software, its use and its scope.

However, despite various media reports from outlets such as Última Hora, La Nación and ABC Color, which we will detail below, and information requests submitted by TEDIC through public access to information channels between August and September 2023 (the responses to which were repeatedly denied by several institutions), it remains virtually impossible to determine the exact number of facial recognition cameras acquired from the time of the initial announcement to the date of this research.

There appears to be no unified criterion for providing information regarding the number of installed closed-circuit cameras. In other words, there is no single source that helps to make these figures transparent. This situation is evidenced by reports from various media outlets.

In January 2021, there were 1,444 cameras nationwide, according to a report published in July 2021[64] by the Directorate of the Security and Emergency Center, a department within the National Police's 911 System. In September 2021, the newspaper Última Hora (UH) reported that the 911 System had a total of 1,458 units[65], which represents 14 additional cameras eight months after the previous publication.

On that occasion, the source of the information was Officer Germán Rodríguez, from the 911 Emergency System of the National Police, and not a report, as was the case with the first instance. Subsequently, in October 2022, La Nación published that the National Police's 911 System had 1,447 cameras[66]. This publication was based on a new report from the Directorate of the Security and Emergency Center of the 911 System. This report indicated only three more cameras than were available in January 2021; however, when compared to what was stated by Officer Rodríguez in September 2021, there are 11 fewer cameras.

Also, according to the newspaper ABC Color, by November 2022, the 911 system already had a total of 1,500 closed-circuit cameras, although it clarified that only 800 were operational at the time due to a lack of maintenance[67]. This information was based on an interview conducted with Commissioner Rafael González, head of the National Police's 911 System.

64 ABC Color. 2022. Out of 1,500 911 cameras in Paraguay, around 800 are not working. Available at: https://www.abc.com.py/policiales/2022/11/11/de-1500-camaras-del-911-en-paraguay-unas-700-no-funcionan/

65 TEDIC. 2023. Judicial amparo actions regarding facial recognition in Paraguay Filed by TEDIC members. Available at: https://www.tedic.org/en/not-with-my-face-mass-surveillance-through-facial-recognition-in-paraguay/

66 La Nación. 2022. Police's 1,447 installed cameras were reduced to 640. Available at: https://www.lanacion.com.py/investigacion/2022/10/18/de-1447-camaras-instaladas-que-tenia-la-policia-se-redujeron-a-640/

67 Última Hora (2022). Smart bus stops will add 8,000 security cameras. https://www.ultimahora.com/paradas-inteligentes-sumaran-8000-camaras-seguridad-n3013537

Official reports from the 911 System reveal discrepancies in the number of cameras reported. Furthermore, the National Police did not respond to the information requests submitted by TEDIC in 2023[68]. These facts point to a lack of transparent documentation regarding stolen or missing cameras, including the absence of follow-up reports, theft records, internal investigations and corresponding resolutions. This lack of traceability fosters an environment conducive to internal corruption.

The severity of the problem in the management and maintenance of this technology is evident in its deficient operation. Concrete cases illustrate this situation[69]:

- In Remansito, district of Villa Hayes, the six cameras intended for vehicle license plate detection are not operating at full capacity.
- In Yby Yaú, department of Concepción, the Pan, Tilt and Zoom (PTZ) cameras are completely inoperative.

These examples demonstrate that the surveillance infrastructure, once installed, does not maintain 100% functionality, which significantly compromises its effectiveness and the purpose for which it was implemented.

Based on these publications by the National Police and media outlets, we have compiled a descriptive table outlining the number of cameras acquired, their type and brand, and whether they are currently in use.

68 See footnote 69.

69 National Congress – Law 7269/2024 https://silpy.congreso.gov.py/web/expediente/128240

TABLE 5. Evolution of camera implementation by the National Police during 2021

DEPARTMENT	CITY	QUANTITY										STATE	
		January 2021					December 2021					Online	Offline
		RF	PTZ	Fixed	LPR	Total	RF	PTZ	Fixed	LPR	Total		
Capital	Asunción	12	390	239	26	667	10	397	231	24	662	**234**	**428**
Central	San Lorenzo	3	155	4	26	188	6	178	4	26	188	**89**	**125**
	Luque												
	Capiatá												
	Ñemby												
Cordillera	Caacupé	0	10	0	4	34	0	10	0	4	34	**22**	**12**
	San Bernardino	2	18	0			2	18	0				
Alto Paraná	Ciudad del Este	10	110	0	12	132	10	104	0	12	126	**58**	**68**
Itapúa	Encarnación	10	88	56	10	164	10	87	56	10	163	**117**	**46**
Caaguazú	Coronel Oviedo	0	35	0	35	35	0	33	0	0	33	**24**	**9**
Amambay	Pedro Juan Caballero	8	76	0	12	96	8	76	0	12	96	**48**	**48**
Misiones	San Ignacio	0	30	0	6	66	0	30	0	6	61	**17**	**8**
	San Juan Bautista	0	30	0	0		0	25	0	0		**32**	**4**
Concepción	Concepción	0	38	0	0	48	0	38	0	0	48	**20**	**15**
	Yby Yau	0	10	0	0		0	10	0	0		**0**	**10**

The data obtained in the framework of this research confirms a clear increase in the acquisition of facial recognition cameras and software by the National Police. Moreover, projections suggest that this number will continue to grow, given current legislative proposals.

An example in this context is the announcement made by the Vice-Ministry of Transport of Paraguay in July 2022[70] regarding plans to implement the National Bus Arrival System, an initiative to modernize public transport in the metropolitan area, with an investment of USD 12 million.

70 CODEHUPY. 2023. Human Rights Report in Paraguay - 2023. Digital Rights Section. Challenges and outstanding issues for the full enjoyment of human rights in the digital environment. Law on the single register of spectators. Page 5. Available at:https://www.tedic.org/wp-content/uploads/2023/12/LIBERTAD-Digitales___Pdf-1.pdf

This project envisions the construction of 130 bus stops, each equipped with security cameras, emergency buttons linked to the National Police and technology for facial and license plate recognition. The project specifications call for the installation of 8,000 cameras[71] at bus stops and on buses, including 130 facial recognition cameras at bus stops and 130 license plate recognition cameras.

Additionally, in June 2024, the National Congress approved Law 7269, "On the Prevention, Control and Eradication of Violence in Sports"[72], proposed by Deputies Basilio Núñez, Juan Carlos Galaverna, Fernando Ortellado, David Rivas and Rocío Abed. The aim of this legislation is to establish mechanisms for controlling and preventing violence at sporting events.

This initiative includes the creation of the National Registry of Spectators (RENAES) to gather information on violent incidents. The law also establishes penalties for both spectators and organizers in cases of non-compliance, and places particular emphasis on the installation of closed-circuit television systems and recording technology in areas surrounding sports venues.

Despite the change in government, there are no signs that the policy shift will incorporate perspectives on human rights, public access to information and greater transparency in this matter[73].

Paraguay still lacks a comprehensive personal data protection law. This absence, combined with a deficient understanding of criminal procedural safeguards and human rights regulations, poses serious threats. There is a risk that controls will be relaxed and that the implementation of technologies that degrade democratic quality will advance and, contrary to popular belief, negatively impact the security of the population in the exercise of their civil liberties. This situation underscores the urgent need to establish a robust legal framework that protects individual rights and adequately regulates the use of surveillance technologies.

71 https://www.conatel.gov.py/conatel/regimen-tarifario-y-fondo-de-servicios-universales/

72 "Article 60. – The telecommunications services reserved to the State, either through direct management or by its public entities, are the following:
- radiocommunication services for meteorological assistance;
- radiocommunication services for air navigation assistance;
- radiocommunication services for river and maritime navigation assistance;
- radiocommunication services for aerospace navigation;
- radiocommunication services for aerospace navigation;
- rescue and safety services for the protection of human life on the country's rivers and on the high seas;
- telecommunications, information and assistance services on roads; and,
- those services that affect the safety of human life, or that are designated as such by the Executive Branch for reasons of public interest.
The State may grant temporary concessions for the provision of these services to private entities, under the conditions established in the relevant legal, regulatory and contractual provisions".

73 CONATEL. LFSU Public Tender. 02.2021. Available at: https://www.conatel.gov.py/conatel/wp-content/uploads/2023/03/4.-pbc-lp-fsu-n-02-2021.pdf

Donations and acquisitions of facial recognition cameras

In Paraguay, the acquisition of facial recognition cameras is primarily carried out through two mechanisms: donations from the Universal Service Funds (FSU) and public tenders through the National Directorate of Public Procurement (DNCP). This section describes each of these processes, as well as their legal basis.

UNIVERSAL SERVICE FUNDS (FSU)

The Universal Service Funds are mechanisms designed to address connectivity gaps arising from the social, economic, geographic and demographic characteristics of the country. The concept of universal service in telecommunications gained international prominence during the World Telecommunication Development Conference (WTDC), organized by the International Telecommunication Union (ITU). These funds emerged in Latin America and the Caribbean in response to the wave of privatizations in the 1980s and 1990s, with the aim of improving access to information and communication technologies (ICT) in underserved areas. Despite their crucial role in regional development, connectivity remains a major challenge. A significant gap persists between urban and rural areas, and broadband internet access is still limited compared to other regions. FSUs aim to bridge these gaps by providing resources for infrastructure investments and subsidies for projects in rural and underserved areas, thereby promoting equitable access to essential services such as education, healthcare and employment. (Alliance for affordable Internet, 2021).

As noted, the primary purpose of the FSU is to subsidize public telecommunications service providers in areas where such support is justified, according to the study "Closing the Digital Connectivity Gap: Public Policies for Universal Service in Latin America and the Caribbean" by the Inter-American Development Bank (IDB). (García Zaballos et al, 2021)

In Latin America, Universal Service Funds (FSUs) are typically financed through mandatory contributions from telecommunications service providers. Each operator contributes 1% of their total revenue generated from service provision, after deducting applicable taxes and fees. (Alliance for affordable Internet, 2021).

The FSU was established in Paraguay in 1995. Law 642/1995, Chapter II, Article 97, provided for the creation of the Universal Service Fund. The law states:

> "The Universal Service Fund is hereby created, to be administered by the National Telecommunications Commission, with the purpose of subsidizing public telecommunications service providers in areas where such support is warranted. The regulation of this Law will define the entities and conditions for contributions to the Fund, as well as the areas eligible for subsidies".

The law thus establishes the purpose of this Fund, while also making the specific conditions of its operation, including the contributing entities and the terms of contribution, subject to regulation by Decree.

Accordingly, Decree No. 14135/96, which regulates Law 642, delegates this regulatory authority to CONATEL itself under Article 129. It establishes that the Commission will approve, through a specific Regulation, the rules governing the operation of the Universal Service Fund, setting the contributing entities, contribution conditions and areas of application, in line with the policies established by the Government. The same article of Decree No. 14135/96 also stipulates a specific restriction on the scope of application of the Universal Service Fund, establishing that CONATEL may not use these resources for its own expenses or financing.

In compliance with this delegated regulatory authority, CONATEL drafted and approved the Regulation of the Universal Service Fund, the initial version of which is not publicly available. Subsequently, through Resolution No. 312[74] of 1999, CONATEL's Board of Directors resolved to amend the Regulation for the first time.

Since CONATEL issued that first specific Regulation in 1999, several versions[75] have followed, modifying both the objectives of the Universal Service Fund (FSU) and the composition of its resources. The following summary briefly outlines the evolution of these changes over time.

Resolution No. 312/99 – The FSU's resources are composed of a minimum of 20% of the exploitation rights fee, which is equivalent to 1% of the provider's gross revenue collected by CONATEL.

Resolution No. 495/2000 – Maintains the composition of the FSU resources. It incorporates Article 47 into the FSU Regulations, modifying the Fund's objectives and expanding its scope. The incorporated article reads as follows:

> "Article 47.- The Universal Service Fund may subsidize, in addition to Universal Service, social programs for the promotion of Education, Culture, Health and Emergency Services, through public telecommunications service providers".

Resolution No. 34/2002 – Maintains the composition of the FSU resources at 20% of the payment for exploitation rights. A significant modification is introduced regarding the objectives of the Fund, which not only broadens its scope but also alters the nature of the contributions it may make.

The FSU is, as established since the first version of its Regulation and continuing to the present, "a fund created to subsidize public telecommunications service operators in areas where such support is justified, either due to the absence of efficient public telecommunications services or for reasons of public or social interest" (Article 2 of the Regulation).

Resolution No. 34/2002, prompted by the signing of a Cooperation Agreement between the Ministry of the Interior and CONATEL, expanded the scope of this Fund to include "telecommunications services reserved for the State, either through direct management or by its public entities", as outlined in Article 60 of Law 642/95".

74 Tender 01/2024 was canceled according to CONATEL's public data. Available at https://www.conatel.gov.py/conatel/licitacion-publica-fsu-n-01-2024/

75 TEDIC. 2019. Who Watches the Watchmen? Facial Recognition in Asunción. Available at: https://www.tedic.org/en/who-watches-the-watchman-facial-recognition-in-asuncion/

However, in addition to extending the scope to specifically include these services reserved for the State, this resolution introduces a change in the nature of the financing mechanism to be implemented through the Fund, which, according to its purpose, is intended to subsidize public telecommunications service operators. To this end, Article 9 of the Regulations stipulates that "financing drawn from FSU resources may be reimbursable or non-reimbursable, and may cover up to 100% of the initial investment. In both cases, the specific terms will be determined by CONATEL for each project, taking into consideration its own economic evaluation of the project". This provision makes it clear that the financing mechanism consists of granting subsidies for projects previously agreed upon with CONATEL.

However, to facilitate the commitment agreed upon with the Ministry of the Interior, it was decided to allow the modification of this financing mechanism in relation to the services listed in Article 60 of Law 642[76], based on the following arguments:

> "WHEREAS: A Cooperation Agreement has been signed between the Ministry of the Interior and the National Telecommunications Commission CONATEL, the purpose of which is "To provide the National Police with an emergency call handling and dispatch system, through the limited and one-time provision of necessary goods and services such as engineering, equipment, software, training a guarantee of operation under normal conditions for a period of two (2) years, for which CONATEL will use the Universal Service Funds. In order for CONATEL to provide subsidies for goods and services, it is necessary to amend the Regulations of the Universal Service Fund and: […]"

Consequently, Resolution No. 34/2002 amends the Regulations of the FSU by including the following provision authorizing the use of its resources:

> "Article 11. CONATEL may provide subsidies for the services covered by Article 60 of Law 642/95, through the provision of goods and services to be specified by it in each project. The aforementioned goods and services must be provided through a public bidding process"

In this way, the FSU is authorized to provide financing as a form of subsidy for the services established therein, directly through the provision of goods and services by CONATEL, introducing a significant modification to the nature of the financing mechanism that may be implemented through the Fund.

Resolution No. 795/2004 – Modifies the composition of the FSU resources, increasing the percentage set at 20% of the contributions paid by operating companies under the Commercial Exploitation Fee to 40%.

76 The document is available for consultation on the website of the Supreme Court of Justice: https://www.csj.gov.py/jurisprudencia/home/DocumentoJurisprudencia?codigo=106501

It is interesting to note the arguments put forth to justify this increase. According to what is stated in the Resolution, these can be summarized as "the noticeable decrease in the revenues expected under the Commercial Exploitation Fee, currently the only source of financing for the aforementioned fund". It is also noted that "the adoption of the suggested measure would not affect the normal functioning of CONATEL". Furthermore, it is argued that "currently and in the future, it will generally be very difficult to rely on other sources of funding for the Universal Service Fund, such as allocations, donations, legacies, transfers or other contributions established in subsection b of Article 6 of the aforementioned Regulation".

The arguments presented highlight the high degree of discretion that CONATEL exercises in making decisions about how the composition of the Fund's resources should be structured, as well as the weak factual basis supporting these decisions. In this case, there is no evidence that the decision is backed by concrete technical studies that clearly demonstrate the need for the changes advocated by the Commission.

Resolution No. 1499/2006 - The composition of the FSU resources is modified again, this time reducing the percentage set at 40% of the contributions paid by operating companies under the Commercial Exploitation Fee to 20%.

In line with what was mentioned earlier, the decision is once again justified with weak arguments, despite being a highly significant measure: a 50% reduction in the resources allocated to the Fund, just two years after an increase of the same proportion had been approved. The argument put forth in the Resolution refers to the amounts budgeted for the FSU in fiscal year 2007, compared to those for 2006 and the available balance of the Fund at the time. This balance is described as "a very high amount compared to the budget forecasts for both fiscal year 2006 and fiscal year 2007", which leads the Administrative and Financial Management to conclude that "the reduction in the contribution percentage to the Universal Service Fund is fully justified".

Resolution No. 196/2014 - Maintains the composition of the FSU resources at 20% of the contributions paid by operating companies under the Commercial Exploitation Fee.

Resolution No. 2474/2018 – Modifies the composition of the FSU resources, increasing the percentage set at 20% of the contributions paid by operating companies under the Commercial Exploitation Fee to 30%. The modification also provides for the incorporation of a new resource to be integrated into the FSU, consisting of "50% of all revenues received as fines for penalties applied to telecommunications service providers".

For this decision, the Administrative and Financial Management argues that the increase would result in an amount no longer available for CONATEL's current expenses, but "considering CONATEL's total revenues, it would not have a significant impact on the fulfillment of the commitments made". Furthermore, it is stated that "the revenues received as FINES can be considered a source of financing that will help strengthen the financial resources of the Universal Service Fund. In this regard, the possibility of allocating 50% of all revenues received from FINES to the Universal Service Fund could be considered, a decision that will not affect the fulfillment of CONATEL's obligations". And, finally, the Planning and Development Management indicates "that in order to achieve the objectives of the National Telecommunications Plan - PNT, the intervention of the regulator is necessary, particularly with regard to areas that are not very profitable for service providers, using the resources of the FSU, for which it would be necessary to modify the Regulations of the FSU with a proposal to increase the percentage of the Commercial Exploitation Fee allocated to constitute the resources of the FSU".

Currently, the sources of resources for the Universal Service Fund, according to Article 6 of the Regulations, are set as follows: 30% (thirty percent) of the payment for exploitation rights, which is equivalent to 1% (one percent) of the provider's gross revenue collected by the National Telecommunications Commission; 50% of all income received as FINES for penalties applied to telecommunications service providers; and allocations, donations, legacies, transfers or other contributions of any kind from natural or legal persons.

Article 3 of the Regulations of the Universal Service Fund details the main objectives of the fund, which are: (a) to finance the expansion of public telecommunications services in rural areas and places of public and social interest; (b) to facilitate efficient and affordable access to telecommunications services for a greater number of Paraguayans, adjusting rates to the income levels of the beneficiaries; and (c) to maximize the economic benefit of telecommunications services, reducing costs in key sectors such as health and education (CONATEL, 2000). In addition, the Regulations include a glossary that defines universal services as access to public telephones or booths with the capacity to transmit voice and data in areas, whether rural or urban, that lack telecommunications services and that are considered of national interest. This definition is provisional and may be modified by CONATEL, although no changes have been made to date (CONATEL, 2000).

The situations highlighted in the evolution of the normative and regulatory framework of the Universal Service Fund point to the following aspects that require special attention:

- Law 642/95, in its Article 97, stipulated that the regulations (which, in accordance with Article 238 of the Constitution, fall under the authority of the President of the Republic) would serve as the normative instrument through which the entities and conditions for contributing to the Universal Service Fund would be established. However, Decree No. 14135/96 omits addressing these definitions in its normative body and delegates to CONATEL the authority to approve them through a specific Regulation.

  The discretionary nature that has characterized CONATEL's regulatory acts concerning the Universal Service Fund underscores the need to promote a new normative framework for defining the Fund's composition—one that respects the normative hierarchy established by law from the outset. The regulatory Decree delegated this power to CONATEL, to be exercised through its Regulations approved by Board Resolution. These constitute administrative acts that, due to their normative status, have less legal stability and less oversight, while also excluding the participation of the Executive Branch in decision-making.

- Update of definitions, objectives and other conditions related to the FSU "according to the policies indicated by the Government": The regulatory Decree of Law 642/95 stipulated that the definitions made regarding the FSU must be "according to the policies indicated by the Government". Currently, under Law 6207/18, which established MITIC, this institution holds ownership of 50% of the Universal Service Fund administered by CONATEL, as provided in Article 18, subsection 3.

  However, despite this significant modification impacting government policy, it has not been reflected in the Fund's regulations. Furthermore, as a result of the current regulatory framework, MITIC's participation in decisions affecting the composition of the Fund is also excluded.

  In addition, there are numerous aspects of the current landscape of telecommunications services and their convergence with ICT services, along with other evolving factors that have emerged over nearly 25 years since the Fund's creation, that warrant a thorough review and update of its regulations and the conditions established therein.

CONNECTIVITY AND THE ACTUAL USE OF FSU

According to CONATEL's reports on subsidies granted from the FSU, over the past six years[77], multi-million-dollar purchases have been made to donate facial recognition cameras and other security equipment for the 911 system. As shown in the reports, very little was allocated to the expansion of public telecommunications services in rural areas and places of public and social interest, such as educational centers. For example, in July of this year, a news article highlighted that directors of educational institutions reported low connectivity in schools (Última Hora, 2023).

The news article also noted that, out of 8,900 educational institutions, only 2,055 had internet connectivity provided by the Ministry of Education and Sciences (MEC) or the Ministry of Information and Communication Technologies (MITIC).

On the other hand, regarding internet access in households, data from the National Institute of Statistics (2023) shows that connectivity gaps are more pronounced when comparing urban areas (83.2%) to rural areas (63.7%) across different types of connections.

While this survey indicates a high percentage of internet access (98.8%), it is important to note that mobile phone connections and access to messaging or social media services do not necessarily guarantee a reliable connection for work or study purposes, as was demonstrated during the pandemic, when issues arose due to poor connection quality.

According to the Permanent Household Survey (EPH: 2023), the Paraguayan population that uses the internet is 76.3%, which represents approximately 4,556,000 people. The percentage growth from 2015 to 2022 has been 26.6% (from 49.7% to 76.3%). On the other hand, internet access varies by area of residence, showing a significant predominance in urban areas compared to rural areas, as 83.2% of people living in urban areas use the internet, compared to 63.7% in rural areas. It is important to note that 9 out of 10 households in the country have access to at least one information and communication technology (telephone, television, radio, computer, cable TV, tablet, among others).

Regarding usage characteristics, according to age, the 20 to 34-year-old group is the most frequent internet user, with usage in this range identified as over 90%. The 35 and older group reaches 69.3%, the 15 to 19-year-old group reaches 87%, and the 10 to 14-year-old group shows 51.6%. Internet usage by sex indicates that 77.6% corresponds to women and 74.9% to men.

An interesting aspect to highlight is the correlation between higher internet usage and a greater number of years of study. In this regard, people with more than 13 years of education use the internet at a rate exceeding 90%.

Therefore, the discretionary and non-transparent use of public resources from the FSU is not only a fact that can lead to public corruption but also contributes to deepening historical structural inequalities, perpetuating an exclusionary model of economic and social development.

77 Unified Portal for Access to Public Information. (n.d.). Requests for public information. Retrieved from https://informacionpublica.paraguay.gov.py/portal/

The high costs of investing in inefficient security technologies and criticism concerning human rights issues contrast with feasible projects, such as strengthening connectivity in remote areas, to address security beyond a repressive perspective.

Based on the information presented regarding the 911 System and the FSU, it is clear that the emergency management channel administered by the National Police does not fully align with the objectives of the FSU nor does it comply with the official definition of universal service established by CONATEL. Nevertheless, the FSU continues to be used, along with departmental governments and other government entities, for the acquisition of equipment with facial recognition technology, raising questions about its alignment with the original purpose of the fund.

FSU DONATIONS TO THE 911 SYSTEM AND MUNICIPALITIES

The FSU, created to close the digital connectivity gap and connect vulnerable groups, has been used to finance purchases for the National Police, specifically facial recognition technology. This issue was criticized internationally by the Alliance for Affordable Internet, in collaboration with the Internet Society. In their analysis of various cases of FSU implementation in Latin America, the Alliance for Affordable Internet identified an exceptional use of these funds for the acquisition of video surveillance cameras by Paraguay. According to their report, "some uses, such as the purchase of ICT equipment, for example surveillance cameras, may not necessarily contribute to the goal of universality for which the FSUs were created" (Alliance for Affordable Internet, 2021, p. 29). This criticism draws on TEDIC's 2018[78] research, which had already raised similar concerns about the alignment of the funds with their original objectives.

CONATEL awarded a total of 27 tenders through the FSU from 2011 to 2022[79]. It is worth noting that, between 2011 and 2016, CONATEL acquired equipment to improve internet access and expand connectivity.

Starting in 2017, CONATEL began making purchases intended for the National Police and for facial recognition technology. Among these tenders, a total of seven involved the acquisition of circuit cameras and facial recognition software. Of these, six were awarded to the company TSV del Paraguay.

An important point to note is that none of these tenders appear on the National Directorate of Public Procurement website, but rather on CONATEL's website, in the section on contracts awarded through the FSU. The tenders awarded to TSV totaled G. 57,550,880,000 (approximately USD 7,831,117 at the current exchange rate) over the five-year period, from 2018 to 2022[80].

78 Supreme Court of Justice (2024). Decision and Ruling No. 5 of the Court of Appeals in Civil and Commercial Matters of the Capital, Fifth Chamber, in the case Leonardo Gómez Berniga v. Ministry of the Interior regarding Amparo, Year 2023 No. 469. Available at: https://www.pj.gov.py/descargas/transparencia/ID217F2-65e85a3cd4366-a-y-s-n-05-de-fecha-21-de-febrero-de-2024.pdf

79 Supreme Court of Justice (2024). Decision and Ruling No. 2 of the Recess Court of Appeals in the case Leonardo Gómez Berniga v. National Police regarding Amparo, Year 2023 No. 395. Available at: https://www.pj.gov.py/descargas/transparencia/ID214F2-65e8627302a1d-a-y-s-n-02-de-fecha-15-de-enero-de-2024.pdf

80 TEDIC. 2018. Biometrics and surveillance: the ongoing alienation of our rights. Available at: https://www.tedic.org/wp-content/uploads/2018/12/La-enajenaci%C3'B3n-continua-de-nuestros-derechos_TEDIC_2018-2.pdf

Below, we present a concise analysis of the key issues observed in the tenders carried out by CONATEL and allocated to the 911 System, managed by the Ministry of the Interior and the National Police of Paraguay:

- **FSU No. 2/2018**

  In 2018, CONATEL continued its procurement for the 911 Emergency System operated by National Police under the Ministry of the Interior. On this occasion, the purchase aimed to expand the SADLE 911 system in the cities of Coronel Oviedo, Caaguazú, San Ignacio, Ciudad del Este and Encarnación (CONATEL, 2018).

  The awarded company was once again TSV del Paraguay, for G. 18,700,000,000 (approximately USD 2,544,000). Among the various items procured, CONATEL acquired video surveillance sites (PTZ IP cameras) with all necessary accessories: 15 for Coronel Oviedo, eight for Caaguazú, 30 for San Ignacio, 60 for Ciudad del Este and 60 for Encarnación. Additionally, for Encarnación, 10 license plate recognition cameras and 10 facial recognition cameras were acquired.

- **FSU No. 2/2019**

  This FSU tender aimed to subsidize the expansion of the National Police's SADLE "through a complementary system for the communication of critical data from all calls received by dialing 911 at the Security and Emergency Centers (CSE) located in the cities of Asunción, Ciudad del Este, Encarnación, Concepción, Coronel Oviedo and San Juan Bautista" (CONATEL, 2019).

  The document specifies that the platform to be provided must include a range of features and functionalities, some of which are particularly noteworthy.

  The system must support the integration of third-party systems, such as CCTV, facial recognition, alarm and license plate recognition systems, among others. This integration will allow the incident management module to send mass notifications to users and/or response teams when an incident is detected by any of these systems. The awarded company was once again TSV del Paraguay for a total amount of G. 7,970,000,000 (approximately USD 1,084,501).

- **FSU No. 01/2020**

  This call for tenders served to subsidize the expansion of the SADLE of the National Police's 911 System, which was carried out and implemented in the Central Department and Asunción (CONATEL, 2020).

  Among a range of items, the acquisition of 50 IP PTZ cameras stands out. The contract specifies that this call requires the provision, installation and commissioning of IP PTZ cameras, with their distribution detailed by city and police stations:

  - Asunción (20 cameras): Police Station No. 3, Police Station No. 12, Police Station No. 13
  - Metropolitan Area (30 cameras): Police Station No. 8 (Capiatá), Police Station No. 53 (Fernando de la Mora), Police Station No. 7 (Ñemby) and Police Station No. 15 (San Lorenzo).

  On the other hand, it also mentions the provision of three facial recognition cameras to be distributed in the Central area: Police Station No. 8, Police Station No. 53 and Police Station No. 7. This is the only tender in this series that was awarded to the company Proseco S.A., for the amount of G. 7,899,900,000 (approximately USD 1,074,962).

The implementation of cameras under this tender raises particular concerns, due to a presumed intent to monitor public spaces used for social protest. This is evidenced in the camera installation report signed in April 2021, just days after large demonstrations took place in downtown Asunción following the health and economic crisis caused by COVID-19 (CONATEL, 2021).

The document, signed by Juan Carlos Duarte, president of CONATEL[81], states that at the request of former Minister Arnaldo Giuzzio, through official notes dated March 16 and 30, the installation of cameras was ordered at locations such as in front of the headquarters of the ruling party, the National Republican Association (ANR), following the demonstrations that took place in Asunción in March 2021 in response to the health crisis (CONATEL, 2021).

The document demonstrates a good practice of public transparency. These are the exact locations where the cameras were installed:

POLICE STATION No. 3 ASUNCIÓN		
No.	**Address/Location**	**Type**
1	Independencia Nacional Ave. at the intersection of Presidente Franco St.	PTZ
2	Independencia Nacional Ave. at the intersection of Paraguayo Independiente St.	PTZ
3	Paraguayo Independiente St. and Nuestra Señora de la Asunción St.	PTZ
4	Nuestra Señora de la Asunción St. and Presidente Franco St.	PTZ
5	Presidente Franco St. and Alberdi St.	PTZ
6	25 de Mayo St. and Tacuarí St.	PTZ
7	Chile St. and Manduvirá St.	PTZ
6	Lorenza Martínez St. and Cmte. Pedro Caballero St.	PTZ
7	Cañadón Chaqueño St. and Sto. 1ro. Eladio Galeano St.	PTZ
POLICE STATION No. 13 ASUNCIÓN		
1	Choferes del Chaco St. and Cap. Aparicio Figari St.	PTZ
2	Eucalipto St. and Carmen del Paraná St.	PTZ
3	Eucalipto St. and Mons. Hermenegildo Roa St.	PTZ
4	Carmen del Paraná St. and Defensa Nacional St.	PTZ
5	Boquerón St. and Cap. Aparicio Figari St.	PTZ
6	Guaraní St. and Chivato St.	PTZ
POLICE STATION No. 7 CENTRAL - ÑEMBY		
1	Fulgencio Yegros Square	PTZ
2	Acceso Sur Ave. at the intersection of Bernardino Caballero St.	PTZ
3	Acceso Sur Ave. and Independencia Nacional Ave.	PTZ
4	Acceso Sur Ave. and Sargento Simeón Gómez St.	PTZ

81 CONATEL n.d. Contracts granted through the FSU. Available at: https://www.conatel.gov.py/conatel/contratos-fsu/

5	Acceso Sur Ave. and Emiliano Vasconcellos Ave.	PTZ
6	Emiliano R. Fernández Ave. and Pratt Gill Ave.	PTZ
7	Pratt Gill Ave. and Santa Librada Ave.	PTZ
8	Santa Rosa St. and Presidente Franco St.	PTZ
POLICE STATION No. 15 CENTRAL - BARCEQUILLO NEIGHBORHOOD		
1	Andrés Barbero Libertad St. and Zavalas Cué St.	PTZ
POLICE STATION No. 53 CENTRAL - B° SAN MIGUEL NEIGHBORHOOD		
1	Mcal. López Ave. and Libertad St.	PTZ
2	Mcal. López Ave. and Cnel. Ayala St.	PTZ
3	Libertad St. at the intersection of Antonio Ruiz Montoya St.	PTZ
4	Cnel. Machuca St. and Laguna Grande St.	PTZ
5	Laguna Grande Ave. and Manuel Britez Borges St.	PTZ
6	Mcal. López Ave. and Libertad St.	RF

- **FSU No. 01/2021**

In 2021, still during the pandemic, CONATEL called for a tender for the "awarding of a subsidy through the Universal Service Fund for the creation of the National Police's 911 System Security and Emergency Center – CSE 911 to be implemented at the Villarrica headquarters, for the Guairá and Caazapá departments (Contract 03/21, 2021).

The terms and conditions required a video surveillance system with 20 IP PTZ cameras distributed throughout the city of Villarrica, connected to the CSE 911 via fiber optic as the access network. Among other items, the amount awarded under this tender was G. 7,990,000,000 (approximately USD 1,087,222), and it was once again awarded to the company TSV del Paraguay.

- **FSU No. 02/2021**

In 2021, CONATEL issued a call for tenders for the awarding of a subsidy through the Universal Service Fund for "the expansion of the Emergency Call Handling and Dispatch System (SADLE 911) of the National Police, to be implemented in the city of Horqueta, Concepción department"[82].

On this occasion, the institution acquired 15 IP PTZ cameras and a software. The terms and conditions indicate that:

> "In addition to a VMS software, the provision, installation and configuration of the software to be provided must be considered; it must include the necessary licenses for the management and recording of fifteen (15) video channels, and additionally one (1) license for facial recognition analytics".

82 Central Bank of Paraguay. Exchange Rates. Rate used at the time of this research: 7,349 PYG per US dollar. https://www.bcp.gov.py/webapps/'eb/cotizacion/monedas

This software was intended for Police Station No. 3, located on Mcal. López Avenue, between Brasil and Ypané streets. Once again, the company TSV del Paraguay S.R.L. was the awarded contractor; however, the awarded amount cannot be determined, as the document is either not available on the website or cannot be downloaded.

This software also includes requirements such as the ability to record and store in the database: facial image, date, time and camera; as well as displaying on the graphical interface the recognition rate (%) and the name of each recognized person.

It also states that the system must be capable of storing an unlimited number of facial recognition watchlists and the profiles of individuals included in them. Additionally, it must include fields for first name, middle name and last name. It even requires that each person's profile can be added to a "blacklist".

- **FSU No. 02/2022**

  With this tender, CONATEL subsidized the implementation of a CSE for the 911 System at the regional headquarters of the Central Department (CONATEL, 2022a). This acquisition was also awarded to the company TSV del Paraguay for G. 13,000,000,000 (approximately USD 1,768,948), for a total of 82 items, among which the following requests stand out:

  - Facial recognition software with a forensic module
  - Guaranteed support and maintenance for the proper functioning of the facial recognition software with forensic module for 730 days
  - A server for the forensic facial analysis module
  - An implementation service for the server for the forensic facial analysis module

- **FSU No. 03/2022**

  This tender is titled "Awarding of a Subsidy Through the Universal Service Fund for the Expansion of the Emergency Call Handling and Dispatch System – SADLE 911 – of the National Police, to be implemented in the city of San Lorenzo, Central Department" (CONATEL, 2022b).

  Among the 18 awarded items was the purchase of a facial recognition analytics server and facial recognition software via a 24-month subscription (per video channel), for a total amount of G. 1,990,980,000 (approximately USD 2,700,918), awarded to the company TSV del Paraguay S.R.L.

  Indeed, the purchases made by the National Telecommunications Commission (CONATEL) through the Universal Service Fund reveal a significant deviation from the fund's original purpose: to close connectivity gaps in the country, which remain considerable.

  This research also reveals a growing trend in the purchase of cameras with facial recognition technology, financed through a series of multimillion-dollar investments. This rise in acquisitions contrasts with the limited effectiveness of such technology in preventing crimes or identifying those responsible, as previously highlighted in this report.

These processes also reveal a concerning lack of diversification in the selection of suppliers, with the company TSV Del Paraguay S.R.L. having been awarded multiple contracts. Additionally, the specifications of certain facial recognition software purchases are noteworthy, not only for their recognition capabilities but also for their ability to generate databases and potentially include individuals on a "blacklist". These concerns are further compounded by the use of mass surveillance, particularly in spaces of social protest, which poses serious risks to democracy and the right to demonstrate. This is exemplified by the 2021 request from then Minister of the Interior, Arnaldo Giuzzio, to install cameras at key protest sites.

- **FSU No. 02/2024**

The public tender FSU 02/2024[83] "For the awarding of a subsidy through the Universal Service Fund for the implementation of a Security and Emergency Center – CSE 911 – of the National Police in the city of Pilar, Ñeembucú Department, and the provision of mobile terminal equipment", was launched in September 2024. At the close of this investigation, according to the terms and conditions of FSU 02/2024[84], the process remains in its final phase, with no bidder awarded and no maximum budget yet defined for the project.

The objective of this tender is to procure computer equipment, surveillance software and video surveillance cameras. Specifically, the terms include the acquisition of 20 PTZ video surveillance cameras and 10 bullet-type cameras.

83 CONATEL. FSU Public Tender. 02.2024. Available at: https://www.conatel.gov.py/conatel/wp-content/uploads/2024/09/anexo-rd-2580-2024-pbc-lp-fsu-n-02-2024_2.pdf

84 Unified Public Information Access Portal. (n.d.). Public Information Requests. Retrieved from: https://informacionpublica.pa'aguay.gov.py/portal/

PROCUREMENT OF FACIAL RECOGNITION CAMERAS THROUGH DNCP TENDERS

Investigating the tenders issued by various public institutions to acquire facial recognition cameras and software proved to be a complex task. Access to this data was difficult because, when publishing information about these purchases, the institutions failed to include relevant keywords in the titles or to classify them under the appropriate categories of the National Directorate of Public Procurement (DNCP).

When investigating the acquisition of facial recognition technology on the DNCP website, only one tender published by CONATEL in December 2022 was identified. The process was titled "National Public Tender for the Acquisition of Security Equipment and Closed-Circuit CCTV Systems", for an amount of ₲ 3,459,800,000 (approximately USD 470,785) (National Directorate of Public Procurement, 2022c)

In this tender, two companies submitted bids: Blue Ocean Company S.A. and TSV del Paraguay S.R.L., with the contract awarded to TSV. The purchase included 58 cameras and facial recognition software from the Israeli brand CORSIGHT, across a total of five items.

No protests were recorded during this process. However, several inquiries and verifications from the National Directorate of Public Procurement were identified. Notably, this acquisition was classified under Category 24, which includes equipment, accessories and software for computing, office use, education, printing, communication and signaling purposes.

As can be observed, the number of cameras the National Police reportedly has for the 911 system differs from the number of purchases reflected in the available data.

Therefore, to find this information, the research team had to set aside the original keywords and replace them with others. It was also necessary to change the specific search category on the DNCP website, considering that the site includes different filters for searching information about tenders.

That was the case for tender No. 419935 from October 2022, titled "Upgrade and Acquisition of Equipment for the Security and Emergency Center of the National Police's 911 System" (National Directorate of Public Procurement, 2022a).

The National Police, through the Ministry of the Interior, was the contracting institution for this purchase, which proved difficult to locate for two main reasons. First, the tender title does not include keywords such as "camera", "monitoring" or "facial recognition". Second, the tender is not categorized under Category 25, which corresponds to "military security equipment and security and surveillance services". Instead, although the tender title refers to a "Security Center", it is classified under Category 24, which covers "equipment, accessories and software for computing, office use, education, printing, communication and signaling purposes". This finding points to a lack of consistent institutional or state-level criteria for the acquisition of facial recognition cameras and software. In other words, this purchase was made for the security center, but it did not fall under the security category. It also included the purchase of facial recognition technology, information that does not appear in the title.

In a multimillion-dollar purchase by the National Police, totaling G. 22,463,000,000 (approximately USD 3,056,606), two lots were acquired: one consisting of 72 items and another of 10 items, which included facial recognition software from the Israeli brand CORSIGHT. Although the tender was challenged, it was not suspended. It is worth noting that not all cameras used by the National Police were purchased directly by the Ministry of the Interior. According to public information access requests made by TEDIC between August and September 2023[85], other public entities, such as municipalities, departmental governments and various directorates, also confirmed having acquired cameras connected to the 911 system.

The institutions that confirmed the use of facial recognition technology in their responses are listed in Table 6.

TABLE 6. Institutions that reported having facial recognition technology

National Administration of Navigation and Ports (ANNP)
National Directorate of Migration
Government of Itapúa Department
Municipality of Paraguarí
Chamber of Senators
National Directorate of Civil Aeronautics (DINAC)

Furthermore, several departmental administrations, along with binational entities, affirmed that they had acquired cameras connected to the 911 system. These institutions include the governments of Presidente Hayes, Boquerón and Caaguazú, as well as the Yacyretá Binational Entity, the Ministry of Finance, the National Anti-Drug Secretariat (SENAD) and the Ministry of Justice, bringing the total to 13.

The procurement of closed-circuit or surveillance cameras, with or without facial recognition capabilities, was carried out not only through the Universal Service Fund (FSU) but also directly by the institutions themselves, with these purchases published on the National Directorate of Public Procurement Website.

To analyze in greater detail how these acquisitions evolved, the following section provides a breakdown of each procurement process and highlights the related observations or concerns.

In April 2012, the National Police conducted a direct contracting process under call No. 240169, which resulted in the awarding of the contract to the company Visual Soluciones Informáticas SRL. However, the list of bidders is not available on the website of the National Directorate of Public Procurement (National Directorate of Public Procurement, 2012a).

The awarded amount totaled G. 110,000,000 (approximately USD 14,968) for the acquisition of 32 closed-circuit cameras of three different types. This purchase was classified under Category 24, which includes equipment, accessories and software for computing, office use, education, printing, communication and signaling purposes.

85 Ruling 70 -2019 – Constitutional Amparo action filed by Maricarmen Sequera Buzarquis, represented by attorneys Federico Legal Aguilar and Ezequiel F. Santagada, against the Ministry of the Interior 2019-609. Available at: https://www.tedic.org/wp-content/uploads/2019/09/Sentencia-de'la-camara_rechazo-a-amparo-MDI_-2019-09-02-09.01.10.pdf

In November 2014, CONATEL conducted a bidding contest for the modernization of its closed-circuit system through tender No. 271004. Six companies participated: Bullers Sociedad Anónima, Cellular S.A., Central Inalámbrica de Monitoreo de Alarmas Sociedad Anónima, Data Lab S.A., Diego Joaquín Rodríguez Barrios and Progress Fábrica de Software S.R.L. (National Directorate of Public Procurement, 2014). The contract was awarded to TSV del Paraguay S.R.L. CONATEL acquired 44 closed-circuit cameras, corresponding to three items, for a total of G. 164,020,083 (approximately USD 22,318).

In November 2015, the National Police made a direct purchase for a Closed-Circuit Television (CCTV) Surveillance System under tender No. 287860. Two firms submitted bids: Hugo Félix Benítez Peralta and Jorge Eduardo Colnago Barrios, with the contract awarded to the latter. The purchase included 16 cameras, totaling G. 117,990,000 (approximately USD 16,055) (National Directorate of Public Procurement, 2015).

In December 2015, the National Police procured closed-circuit cameras for its Identification Department, which is responsible for issuing national identity documents, via tender No. 231138 (National Directorate of Public Procurement, 2012b). This direct purchase, awarded to Comtel Sociedad Anónima for G. 129,340,000 (approximately USD 17,599), did not include a list of bidders.

In April 2021, the National Police conducted a direct contracting process for the purchase of a closed-circuit system under tender No. 392828. Sixteen cameras were procured for a total of G. 18,882,000 (approximately USD 2,569). Four firms submitted bids: José Antonio Duarte Santa Cruz, Online Paraguay S.A., Security Systems Paraguay S.A. and Tes Ingeniería S.A., with the contract ultimately awarded to the last of these (National Directorate of Public Procurement, 2021). Notably, this purchase was classified under Category 22 – Machinery, Equipment and Major Tools – Transportation Equipment.

This investigation highlights the curious fact that this purchase was classified under Category 22 – Machinery, Equipment and Major Tools – Transportation Equipment. Up to that point, camera purchases through the DNCP did not explicitly indicate the inclusion of specialized facial recognition technology. However, this does not necessarily mean that these cameras could not be integrated into a monitoring system with facial recognition capabilities, although their lower resolution could present challenges for accurate detection.

Since November 2022, state institutions have begun procuring facial recognition technology through the DNCP. The Ministry of the Interior initiated tender No. 419935, and in December 2022, CONATEL issued National Public Tender No. 419105. (National Directorate of Public Procurement, 2022b, 2022c)

Both tenders were aimed at acquiring technology with facial recognition capabilities, as detailed in the following section on strategic litigation. This highlights a significant challenge in accessing information regarding the calls for tenders and the purchases made by the various institutions involved. This difficulty stems from the fact that public institutions do not consistently categorize or title tenders related to the acquisition of facial recognition cameras, making it complex to search for this information within the public database of the National Directorate of Public Procurement (DNCP). In essence, the information exists, but it is difficult to access. This lack of easy access raises concerns regarding the transparency of the information provided throughout these processes.

Moreover, inconsistencies in the classification of tenders are evident, as the procurement of security equipment and cameras is not consistently categorized under the appropriate classifications. For instance, tenders involving security technology are often placed in categories related to office equipment or software programs.

The incorrect classification of tenders not only hinders access to data but also suggests a lack of unified criteria in the use of security technology, which could lead to disorganized and opaque management of resources.

Another key finding is the interconnection of cameras across various institutions, showing that the Ministry of the Interior is not the only entity procuring security equipment for the 911 system. It has been confirmed that other institutions, such as municipalities, departmental governments and public entities, have also acquired cameras connected to the 911 network. This not only broadens the use of facial recognition technology across the country but also intentionally makes it more difficult to track the procurement and installation of such systems.

Analysis of official reports

Beyond monitoring the aforementioned purchases and donations, this research also seeks to evaluate the effectiveness of facial recognition technology in enhancing citizen security. In this context, TEDIC submitted a request to the National Police through the Unified Public Information Access Portal, seeking details on the outcomes of the multi-million dollar investment in this technology. The request specifically focused on obtaining data regarding arrests made through its use. While the information provided does not directly specify the number of arrests, it does include annual figures for the alerts generated since the implementation of the cameras and facial recognition software, which are presented below:

TABLE 7. Alerts Generated by Facial Recognition Cameras

Month	2019	2020	2021	2022	2023
January	0	20	1	0	0
February	0	11	0	1	1
March	0	13	1	0	0
April	0	0	0	1	0
May	0	0	1	0	0
June	0	0	2	0	0
July	0	1	0	1	0
August	0	0	1	0	0
September	0	1	4	1	-
October	0	0	1	1	-
November	26	1	5	0	-
December	40	1	1	0	-
Total	**66**	**48**	**17**	**5**	**1**

Source: National Police of Paraguay, 2023.

In this context, it is important to recall that between 2018 and 2022, CONATEL awarded contracts totaling G. 28,590,880,000 for the acquisition of infrastructure, cameras and facial recognition software to support the 911 system.

However, it is crucial to highlight that despite this substantial investment in technology, the results obtained in terms of alerts leading to the detention of suspects or criminals have been modest up to August 2023. According to figures provided by the Prevention and Security Directorate of the Security and Emergency Center, only 137 alerts were generated through the use of facial recognition cameras over a five-year period (National Police of Paraguay, 2023).

This fact leads us to a significant calculation: the average cost to the state for each alert generated by this technology amounts to G. 208,692,554. It is undeniable that this cost per alert is considerably high and raises questions about the effectiveness of such investments in terms of public security and whether they truly achieve the expressed objective. Additionally, it is worth mentioning that during the same period, a total of 7,590 requests were made for access to security camera recordings. (National Police of Paraguay, 2023).

It is important to note that as early as 2019, an article published by the newspaper ABC Color highlighted that the company TSV SRL had become the "eternal supplier" of facial recognition cameras for the National Police through CONATEL (ABC Color, 2019). Moreover, the publication questioned the functionality of these devices and emphasized their lack of effectiveness in apprehending individuals up to that point.

> "There are doubts about the optimal functioning of the cameras, as, given the high rate of robberies and assaults, not many suspects have been identified. Furthermore, not a single arrest was made last year due to the influence of this new technology. On several occasions, ABC requested permission to visit the monitoring center to observe its operation, but these requests were denied, citing 'public security risk' as the reason".

Between November 2019 and March 2020, facial recognition systems issued 110 alerts. However, from April 2020 to August 2023, only 27 alerts were recorded, with just one in 2023.

Although facial recognition technology may be useful in specific situations, such as identifying dangerous criminals wanted by national and international authorities, the statistics from the National Police reveal that, at the local level, the results have been minimal and nearly insignificant. In addition, these figures do not account for the issues of discrimination and bias inherent in this technology, these figures do not account for the issues of discrimination and bias inherent in this technology, which were discussed in sections pertaining to other countries, further highlighting the limitations and risks of its implementation in citizen security contexts.

These results question the need for the continued use of facial recognition technologies in the realm of public security, given that the benefits obtained are limited and do not justify the risk of compromising Paraguay's compliance with international conventions, as previously mentioned.

STRATEGIC LITIGATION ON FACIAL RECOGNITION

TEDIC is actively involved in strategic litigation[86] concerning technology and human rights, often appearing before the Paraguayan Judiciary and the Inter-American System of Human Rights (IAHRS). The organization is currently pursuing national-level litigation on facial recognition, aiming to challenge the disproportionate and invasive use of this technology in Paraguay. This legal action seeks to protect the rights to privacy, non-discrimination and freedom of expression, while also advocating for regulatory frameworks that are fairer and more respectful of human rights.

TEDIC has persued three strategic litigations on the subject matter, one in 2018 and two others in 2023, both aimed at gaining access to public information through amparo (a legal action for the protection of constitutional rights). In all three cases instances, public institutions refused to provide the requested information regarding the implementation and use of these systems, prompting legal action to demand transparency and accountability.

First Litigation: Year 2018

In July 2018, the Ministry of the Interior and the National Police initiated a modernization process for the 911 System in Asunción and the Metropolitan Area, as detailed in the sections on donations and acquisitions related to the implementation of facial recognition cameras. In 2019, Maricarmen Sequera, a lawyer and representative of TEDIC, submitted an information request to the Ministry of the Interior regarding this project through the Unified Public Information Access Portal. The Ministry's response, issued on April 26, 2019, was partial, withholding key information under the justification of confidentiality[87].

Faced with this refusal, Ms. Sequera filed an amparo invoking Law 5282/2014 and Supreme Court Procedural Rule 1005/2015, seeking to compel the release of the requested data. The case was brought before the Ninth Criminal Court of Guarantees of the Capital, where the initial request was dismissed. This decision was later upheld by the Criminal Court of Appeals.

The judicial ruling[88] reflects a concerning reality: state bodies selectively apply legal norms, adhering to some while disregarding others for their own convenience, thereby severely impacting human rights. Most alarming is that judges, who are meant to ensure respect for the law, ultimately legitimize these practices. A case in point is Sentence No. 70, dated August 25, 2019, which acknowledges that no specific law was cited to declare Resolution 238 confidential. Nevertheless, the refusal to provide information was justified on the grounds that the National Police, as an internal security body of the State, may classify its information as reserved under Article 175 of the National Constitution.

This reasoning allows any action by the National Police to be classified as a matter of national security, without a clear legal basis, replicating practices from the period of dictatorship that the National Constitution aimed to eradicate. In doing so, it opens a dangerous window that threatens the rule of law and revives authoritarian logics that Paraguayan society has committed to overcoming.

86 AL SUR. 2021. Facial recognition in Latin America: trends in the implementation of a perverse technology. Available at: https://www.alsur.lat/en/report/facial-recognition-latin-america-trends-implementation-perverse-technology

87 International Covena't on Civil and Political Rights, articles 17 and 19.

88 Paciello and Guerrero. 2022. Habeas data and fraudulent affiliations due to misuse of data. TEDIC. Available at: https://www.tedic.org/wp-content/uploads/2022/10/Habeas-data-y-afiliaciones-fraudulentas-WEB.pdf

Following the second appeal, Ms. Sequera and her legal team decided to take the case to the highest court. In 2019, they appealed to the Supreme Court of Justice, seeking a review of the lower court's ruling and reaffirming the right of access to public information. They argued that the unjustified refusal by state institutions violated fundamental rights and set a dangerous precedent. It was not until 2024, after five years, that the Constitutional Chamber of the Supreme Court of Justice (CSJ) unanimously ruled, through Agreement and Judgment No. 843 dated August 7, 2024, to declare the unconstitutionality of Agreement and Judgment No. 70/2019, issued by the Fourth Chamber of the Criminal Court of Appeals of the Capital[89].

In this ruling, the CSJ upheld the constitutionality of its own Procedural Rule No. 1005, which governs the amparo procedure in cases involving the denial of access to public information. The Court also determined that the decision of the Court of Appeals was arbitrary and affirmed that amparo is indeed the appropriate procedural mechanism for initiating legal actions in such cases.

The CSJ's resolution sets a significant precedent regarding Procedural Rule No. 1005 and creates a renewed opportunity for the justice system to advance the fundamental right of access to information, particularly concerning the sensitive issue of how the State handles our personal information for national security purposes.

Second litigation: Ministry of the Interior (2023)

Once again, in 2023, Leonardo Gómez, a member of TEDIC, submitted formal requests to several state institutions seeking information about cameras equipped with facial recognition technology. Among them was the Ministry of the Interior, which once again responded negatively, citing the only provision in the relevant law that refers to classified information.

In 2023, TEDIC submitted 41 requests for access to information to various public institutions, including ministries, secretariats, departmentals governments and municipalities (see Table 3). Of these, 30 institutions responded. Among the respondents, 20 confirmed the presence of security cameras on their premises. However, only five acknowledged the use of facial recognition systems in those cameras[90].

In an effort to obtain the requested information, TEDIC submitted a request for reconsideration to the Ministry of the Interior following its initial refusal to provide the data. The Ministry once again issued a negative response, justifying its decision by claiming that the information could be classified as reserved public data and that its disclosure could compromise the service and the protection of citizens' personal data.

It is crucial to emphasize that the information request did not seek personal data; rather, it aimed to obtain public information about cameras that store citizens' personal data and operate in public spaces.

Additionally, it is worth noting that while there is no precise figure regarding the number of facial recognition cameras deployed across the national territory, state authorities have consistently announced the incorporation of additional cameras with this capability. This trend raises significant concerns about the expansion of surveillance and highlights the need for a thorough review of the policies and practices related to privacy and transparency in this context.

89 https://www.conatel.gov.py/conatel/wp-con'ent/uploads/2019/10/go-000626-120bis-rd312-1999.pdf

90 CONATEL. Subsidies Granted by Year. Available at: https://www.conatel.gov.py/conatel/subsidios-otorgados/

Faced with the renewed negative response following the request for reconsideration, TEDIC filed a judicial amparo for access to public information against the Ministry of the Interior. The case was randomly assigned to the Third Civil and Commercial Court of First Instance, Secretariat 5.

In its initial ruling, the court rejected the amparo filed by TEDIC. In response, TEDIC appealed the decision, but the appellate court ultimately upheld the original ruling.[91].

Given the continued denial of the right to access public information, the case was brought before the Supreme Court of Justice and is currently under review by the Constitutional Chamber, following the filing of an unconstitutionality claim against the unfavorable rulings issued by both the lower and appellate courts.

Third litigation: National Police (2023)

Similarly, TEDIC filed an amparo against the National Police in December 2023 to obtain statistics on the use of facial recognition technologies, which had already been partially published in 2021, with findings presented earlier in this research. The Police refused to provide the information, citing "national security" as the reason. TEDIC described this refusal as an overreach of the Police's functions, particularly as the same information had been disclosed without issue in the past, underscoring the relevance of its publication for journalistic endeavors and the exercise of citizen oversight.

This amparo was filed with the Nineteenth Civil and Commercial Court of First Instance. TEDIC encountered technical issues while trying to submit an appeal but eventually managed to do so on January 1, 2024. On January 15, 2024, the Court of Appeals ruled in favor of TEDIC, declaring that the National Police's refusal to provide the information was unjustified and affirming that the right of access to public information must be upheld, even in cases involving surveillance technologies[92].

The ruling emphasized that "national security" cannot be used as a blanket justification to withhold information that should be public. This marks an important victory and sets an important precedent that can be referenced in similar cases going forward.

Following this decision, TEDIC urged the court where the case originated to enforce the ruling. As a result, on April 15, 2024, the 911 System Department provided a report with the requested information, revealing the existence of 1,641 cameras installed nationwide under the control of the National Police (see figures reported in Annex I).

91 He was president of CONATEL during the 2019–2023 term and has recently been reappointed to the position. According to a report by ABC, during Duarte's administration, there were cases of misappropriation of institutional funds amounting to over USD 4 million. https://www.abc.com.py/politica/2023/08/18/pena-coloca-en-conatel-al-que-la-cgr-lo-descubrio-con-manejo-discrecional-de-recaudacion/

92 Strategic litigation constitutes a legal tool aimed at driving broader social and legal change through specific cases brought before the courts. It is not merely about winning a case, but rather about challenging laws, policies or practices that violate fundamental rights, seeking to influence legislation and public perception.

CONCLUSION

The methodological review conducted through various procedures has provided a comprehensive understanding of the acquisition and use of facial recognition technology by the Paraguayan state. It involved the analysis of national and international laws and documents, searches on the official websites of the National Directorate of Public Procurement (DNCP) and the National Telecommunications Commission (CONATEL), as well as information requests to gather relevant and up-to-date data.

The findings of this research reveal that the current legal framework does not clearly define who is responsible for the operation of facial recognition equipment. This includes its use, maintenance, data processing, data security and the accountability of both officials and institutions in cases of misuse of the equipment or personal data.

This aspect is crucial, as the equipment is acquired using funds from municipalities, departmental governments and other state institutions outside the National Police, raising questions about the ownership of the devices and their maintenance responsibilities.

The absence of a comprehensive personal data protection law in Paraguay, combined with a limited understanding of due process guarantees in criminal law and human rights standards, poses serious threats to data protection

The implementation of facial recognition technologies poses risks to democratic quality and public security, with negative implications for the exercise of civil liberties. At the same time, purchases made by CONATEL through the Universal Service Fund (FSU) reflect a significant deviation from its original objective, to reduce connectivity gaps, which still remain a pressing issue. What was initially justified as an exception has now become a recurring practice, without the issuance of specific resolutions to authorize such acquisitions.

Furthermore, the research reveals a rise in the acquisition of facial recognition cameras, funded by significant investments. However, this stands in contrast to the technology's limited effectiveness in preventing crimes or identifying those responsible, as highlighted in the report.

These processes also reveal a concerning lack of diversification in the selection of suppliers, as the company TSV Del Paraguay S.R.L. has been awarded contracts on multiple occasions. The specifications of certain facial recognition software purchases include not only facial identification capabilities, but also features for maintaining a database and adding names to a "blacklist". This, along with the installation of cameras in spaces used for social protest, poses a risk to democracy and to the freedom to exercise the right to demonstrate.

On the other hand, the incorrect classification of tenders hinders access to information and suggests a lack of unified criteria in the use of security technology, potentially leading to disorganized and opaque resource management. Additionally, the interconnection of cameras across various institutions, such as municipalities, departmental governments and other public entities, has contributed to the expansion of facial recognition technology nationwide, making it increasingly difficult to trace its procurement and installation.

Although facial recognition technology may be useful in specific situations, such as identifying dangerous criminals wanted by national and international authorities, statistics from the National Police reveal that, at the local level, the results have been minimal and almost insignificant. In addition, these figures do not account for the issues of discrimination and bias inherent in this technology, these figures do not account for the issues of discrimination and bias inherent in this technology, which were discussed in sections pertaining to other countries, further highlighting the limitations and risks of its implementation in citizen security contexts.

These results call into question the necessity of continued use of facial recognition technologies in public security, given that the benefits are limited and do not justify the risk of compromising Paraguay's compliance with international conventions, as noted above.

This research also revealed the limited cooperation of some institutions, notably the National Police, in providing information about the purchase and installation of cameras. The justification offered was that this data could be classified as confidential public information and that its disclosure might compromise service delivery and the protection of citizens' personal data. However, it is crucial to emphasize that the request did not seek personal data, but rather public information on cameras that store citizens' personal data and operate in public spaces.

Furthermore, while no precise data exist on the number of facial recognition cameras deployed nationwide, state authorities have repeatedly announced plans to add more of these devices. This trend raises critical questions about the expansion of surveillance and underscores the urgent need to review privacy and transparency policies and practices in this area.

RECOMMENDATIONS

1. **Develop a comprehensive legal framework for the protection of personal data:**

   Paraguay must establish a comprehensive personal data protection law that regulates the use of surveillance technologies, including facial recognition. This law should guarantee the privacy and security of stored data, as well as establish clear responsibilities for the institutions that handle it.

2. **Improve transparency and accessibility of information:**

   Public institutions must correctly classify and label tenders related to the acquisition of facial recognition cameras. Doing so will facilitate public access to information and strengthen transparency in the procurement and deployment of these technologies

3. **Diversify supplier selection:**

   It is advisable to diversify the selection of suppliers to avoid the concentration of contracts in a single company. This will promote fair competition, reduce the risk of corruption and improve the quality of procured equipment.

4. **Conduct independent audits:**

   The State must commission independent and regular audits of facial recognition systems to assess their effectiveness and identify potential biases or discrimination. The findings of these audits should be made public and used to strengthen surveillance policies and practices.

5. **Limit the use of video surveillance technologies to specific and legitimate purposes:**

   The State must establish appropriate mechanisms to ensure that the use of video surveillance technologies, including facial recognition, is restricted to specific, legitimate and clearly defined purposes. Such use should be proportionate and subject to strict oversight.

6. **Establish mechanisms for oversight and accountability:**

   An administrative authority must be designated to oversee the use of video surveillance and facial recognition technologies. This authority should have the power to establish technical and documentary accountability mechanisms for operators, conduct audits of system operations and sanction those who deviate from the regulatory framework.

7. **Design mechanisms to prevent discriminatory use:**

   The State must implement mechanisms and safeguards to ensure limitations on the use of video surveillance and facial recognition technology. These should include periodic reviews and traceability measures to prevent their use for purposes other than those originally intended.

BIBLIOGRAPHY

1. Alliance for Affordable Internet. (2021). Universal service and access funds in Latin America & the Caribbean https://a4ai.org/wp-content/uploads/2022/01/USAF-Report-English.pdf

2. Alonzo,L , Carrillo, E y Sequera, M . (2018). TEDIC. La enajenación continua de nuestros derechos. Sistemas de identidad: Biometría y cámaras de vigilancia no reguladas en Paraguay. TEDIC. https://www.tedic.org/la-enajenacion-continua-de-nuestros-derechos-sistemas-de-identidad-biometria-y-camaras-de-vigilancia-no-reguladas-en-paraguay/

3. Access Now. (2021). Made abroad, deployed at home https://www.accessnow.org/wp-content/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf

4. Al Sur. (2021).Facial Recognition in Latin America. https://www.alsur.lat/sites/default/files/2021-10/ALSUR_Reconocimiento%20facial%20en%20Latam_EN_Final.pdf

5. EFF. (n.d). Necessary and proportionate on the application of human rights to communications surveillance. Available at: https://necessaryandproportionate.org/

6. García Zaballos, A., Huici, H., Puig Gabarró, P., & Iglesias Rodriguez, E. (2021). Cerrando la brecha de conectividad digital: Políticas públicas para el servicio universal en América Latina y el Caribe. Inter-American Development Bank. https://doi.org/10.18235/0003066

7. Holden, L. (2023). Divisions Grow Over Use of Facial Recognition in California. GovTech. https://www.govtech.com/policy/divisions-grow-over-use-of-facial-recognition-in-california

8. International Network of Civil Liberties Organizations. (2021). Te están mirando. Resistencias frente a las vulneraciones de derechos por sistemas de reconocimiento facial en el mundo. https://files.inclo.net/content/pdf/4/Spanish%20Report.pdf

9. Marianne Díaz. (2018). El cuerpo como dato. Derechos Digitales. https://www.derechosdigitales.org/wp-content/uploads/cuerpo_DATO.pdf

10. Privacy International. 2013. Biometrics: friend or foe of privacy. Available at: https://www.privacyinternational.org/news-analysis/1409/biometrics-friend-or-foe-privacy

11. Rolon, J y Sequera, M. (2015). TEDIC. Vigilancia estatal de las comunicaciones y derechos fundamentales en Paraguay.

12. TEDIC. (2023). La filtración de datos policiales en Paraguay y una imperante urgencia de respuestas [Institutional Webpage]. https://www.tedic.org/la-filtracion-de-datos-policiales-en-paraguay-y-una-imperante-urgencia-de-respuestas/

13. Media outlets consulted

14. ABC Color. (2019). TSV SRL es la eterna proveedora tecnológica del 911 de la Policía. https://www.abc.com.py/edicion-impresa/economia/2019/11/11/tsv-srl-es-la-eterna-proveedora-tecnologica-del-911-de-la-policia/

15. IP Paraguay. (2021, march 9). Policía tiene identificadas a personas que cometieron desmanes mediante Sistema 911. .::.::Agencia IP::. https://www.ip.gov.py/ip/policia-tiene-identificadas-a-personas-que-cometieron-desmanes-mediante-sistema-911/

16. La Nación. (2022). De 1.447 cámaras instaladas que tenía la Policía se redujeron a 640. https://www.lanacion.com.py/investigacion/2022/10/18/de-1447-camaras-instaladas-que-tenia-la-policia-se-redujeron-a-640/

17. Última Hora. (2023, julio 13). De 8.900 escuelas, apenas 2.055 tienen conexión a internet este año [Medio de Comunicación]. Última hora. https://www.ultimahora.com/de-8-900-escuelas-apenas-2-055-tienen-conexion-a-internet-este-ano

18. International standards and instruments

19. General Assembly (UN). 2018. The right to privacy in the digital age. Report of the United Nations High Commissioner for Human Rights. A/HRC/39/29. 2018. https://docs.un.org/en/A/HRC/39/29

20. American convention on human rights - Pact of San Jose (1969). https://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights.pdf

21. Universal Declaration of Human Rights, (1948). https://www.ohchr.org/en/human-rights/universal-declaration/translations/english

22. International Covenant on Civil and Political Rights, (1966). https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

23. OAS. Department of International Law, Secretariat for Legal Affairs. (2023). Updated Principles on Privacy and Personal Data Protection. Organization of American States.

24. UN – CCPR. 1999. General Comment No. 27. https://docs.un.org/en/CCPR/C/21/Rev.1/Add.9

25. UN. 2013. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue* A/HRC/23/40. ONU. Abril, 2013.

26. UN. 2009. Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 2009, p.10-11. Available at: http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf

27. OAS, 2022. Annual Report of the Office of the Special Rapporteur for Freedom of Expression. Annual Report of the Inter-American Commission on Human Rights 2022. Available at: https://www.oas.org/en/iachr/expression/reports/IA2022ENG.pdf

28. UN, 2019. Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression Available at: https://docs.un.org/en/A/HRC/41/35

29. Laws, Regulations, Resolutions and Official Documents

30. CONATEL. (2000). Resolution No 495.

31. CONATEL. (2018). Contract No 27/2018. https://contrataciones.gov.py/licitaciones/convocatoria/328038-adquisicion-sistemas-camaras-vigilancia-lpn-07-sbe-2017-1.html

32. CONATEL. (2019). Contract No 50/2019. https://www.conatel.gov.py/conatel/wp-content/uploads/2020/03/contrato-n-0050-2019-para-el-otorgamiento-de-subsidio-a-traves-del-fsu-para-la-implementacion-del-servicio-de-atencion-y-despacho-de-llamadas.pdf

33. CONATEL. (2020). Contract No 7/2020. https://www.conatel.gov.py/conatel/wp-content/uploads/2021/11/contrato-n-07-2020-proseco.pdf

34. CONATEL. (2021). Note PR 315/2021. https://www.conatel.gov.py/conatel/wp-content/uploads/2021/09/pr-315-2021-ministerio-del-interior.pdf

35. CONATEL. Contract No. 03/21. (2021). [Página oficial]. //www.conatel.gov.py/conatel/wp-content/uploads/2021/11/contrato_n3_2021_tsv_cse_villarrica.pdf

36. CONATEL. (2022a). Contract No 13/2022. https://www.conatel.gov.py/conatel/wp-content/uploads/2022/08/contrato_13-2022_consorcio_voxingenieria_chaco2022_1.pdf

37. CONATEL. (2022b). Contract No 37/2022. https://www.conatel.gov.py/conatel/wp-content/uploads/2023/01/contrato-n-37-2022-sanlo.pdf

38. National Congress (1995) Law 642 /1995 De Telecomunicaciones

39. https://www.bacn.gov.py/leyes-paraguayas/2452/ley-n-642-telecomunicaciones

40. National Congress. (2012). Law 4739/12—Que crea El Sistema 911 de Atención, Despacho y Seguimiento de Comunicaciones de Emergencias. http://digesto.senado.gov.py/detalles&id=7947

41. National Congress (2020) Law 6534/21 De protección de datos personales crediticios. https://www.bacn.gov.py/leyes-paraguayas/9417/ley-n-6534-de-proteccion-de-datos-personales-crediticios

42. National Directorate of Public Procurement. (2012a, July). Contract for Tender 240169—Adquisición de Circuito Cerrado. https://contrataciones.gov.py/licitaciones/adjudicacion/contrato/240169-visual-soluciones-informaticas-s-r-l-1.html

43. National Directorate of Public Procurement. (2012b, December 7). Tender Award 231138—ADQUISICIÓN DE EQUIPO DE CIRCUITO CERRADO PARA EL DEPARTAMENTO DE IDENTIFICACIONES. https://www.contrataciones.gov.py/licitaciones/adjudicacion/231138-adquisicion-equipo-circuito-cerrado-departamento-identifiaciones/resumen-adjudicacion.html

44. National Directorate of Public Procurement. (2014, November 22). Tender Award 271004—MODERNIZACIÓN DEL CIRCUITO CERRADO. https://www.contrataciones.gov.py/licitaciones/adjudicacion/271004-modernizacion-circuito-cerrado/resumen-adjudicacion.html

45. National Directorate of Public Procurement. (2015, December 23). Tender Award 287860—Sistema de circuito cerrado de video vigilancia. https://www.contrataciones.gov.py/licitaciones/adjudicacion/287860-sistema-circuito-cerrado-video-vigilancia-1/resumen-adjudicacion.html

46. National Directorate of Public Procurement. (2021, June 16). Tender Award 392828—ADQUISICIÓN DE CIRCUITO CERRADO. https://www.contrataciones.gov.py/licitaciones/adjudicacion/392828-adquisicion-circuito-cerrado-1/resumen-adjudicacion.html

47. National Directorate of Public Procurement. (2022a, October 4). Tender Planning 419935—Actualización y Adquisición de Equipos para el Centro de Seguridad y Emergencias del Sistema 911 de la Policía Nacional para Asunción y Regionales Ad Referendum Plurianual. https://www.contrataciones.gov.py/licitaciones/planificacion/419935-actualizacion-adquisicion-equipos-centro-seguridad-emergencias-sistema-911-policia-1.html

48. National Directorate of Public Procurement. (2022b, November 28). Tender Award 419935—Actualización y Adquisición de Equipos para el Centro de Seguridad y Emergencias del Sistema 911 de la Policía Nacional para Asunción y Regionales Ad Referendum Plurianual. https://www.contrataciones.gov.py/licitaciones/adjudicacion/419935-actualizacion-adquisicion-equipos-centro-seguridad-emergencias-sistema-911-policia-1/resumen-adjudicacion.html

49. National Directorate of Public Procurement. (2022c, December 12). Tender Award 419105—ADQUISICIÓN DE EQUIPOS DE SEGURIDAD Y SISTEMAS DE CIRCUITO CERRADO CCTV. https://www.contrataciones.gov.py/licitaciones/adjudicacion/419105-adquisicion-equipos-seguridad-sistemas-circuito-cerrado-cctv-1/resumen-adjudicacion.html

50. National Statistics Institute. (2023). Tecnología de la Información y Comunicación en el Paraguay (TIC). EPH 2015-2022. National Statistics Institute. https://www.ine.gov.py/Publicaciones/Biblioteca/documento/226/Tecnolog%C3%ADa%20de%20la%20Informaci%C3%B3n%20y%20Comunicaci%C3%B3n%20EPH%202015_2022.pdf

51. National Statistics Institute. (2023) Resultados preliminares del Censo de Población y Vivienda 2022. Disponible en https://www.ine.gov.py/censo2022/documentos/Revista_Censo_2022.pdf

52. National Police of Paraguay. (2014). Resolution CPN No 452. https://www.policianacional.gov.py/wp-content/uploads/2018/03/RESOLUCI%C3%93N-N%C2%B0-452-POR-LA-QUE-SE-APRUEBA-EL-NUEVO-REGLAMENTO-ORGANICO-FUNCIONAL-SISTEMA-911.pdf

53. National Police of Paraguay. (2023, October 16). Memorandum O.E.G No 10/2023. Respuesta de pedido de acceso a la información pública. https://informacionpublica.paraguay.gov.py/portal/#!/ciudadano/solicitud/74291

APPENDIX

NATIONWIDE SUMMARY OF CAMERAS – APRIL 2024

Capital

City	PTZ	Fixed	LPR	FR	Total
Asunción	448	261	28	12	749

Central Department

City	PTZ	Fixed	LPR	FR	Total
San Lorenzo	86	0	6	1	93
Fernando de la Mora	20	2	0	0	22
Luque	32	1	4	3	40
Lambaré	20	2	4	0	26
Ñemby	14	0	0	1	15
Capiatá	12	0	0	1	13
Mariano Roque Alonso	11	0	4	0	15
Itá	16	0	0	0	16
Villa Elisa	17	0	0	0	17
Total	228	5	18	6	257

Departament of Cordillera

City	PTZ	Fixed	LPR	FR	Total
Caacupé	13	0	0	0	13
San Bernardino	18	0	4	2	24
Total	31	0	4	2	37

Departament of Alto Paraná

City	PTZ	Fixed	LPR	FR	Total
Ciudad del Este	110	0	12	10	132

Departament of Itapúa

City	PTZ	Fixed	LPR	FR	Total
Encarnación	88	56	10	10	164

Departament of Caaguazú

City	PTZ	Fixed	LPR	FR	Total
Coronel Oviedo	35	0	0	0	35
Caaguazú	8	0	0	0	8
Total	43	0	0	0	43

Departament of Misiones

City	PTZ	Fixed	LPR	FR	Total
San Juan Bautista	30	0	0	0	30
San Ignacio	30	0	6	0	36
Total	60	0	0	0	66

Departament of Concepción

City	PTZ	Fixed	LPR	FR	Total
Concepción	38	0	0	0	38
Horqueta	15	0	0	0	15
Yby Yaú	10	0	0	0	10
Total	53	0	0	0	63

Departament of Guairá

City	PTZ	Fixed	LPR	FR	Total
Villarrica	20	0	0	0	20

Departament of Amambay

City	PTZ	Fixed	LPR	FR	Total
Pedro Juan Caballero	76	0	12	8	96

Departament of Presidente Hayes

City	PTZ	Fixed	LPR	FR	Total
Villa Hayes - Peaje Remanso	0	0	6	0	6
Peaje Nueva Asunción - Chacoí	0	0	8	0	8
Total	0	0	14	0	14


Technology
& Human
Rights