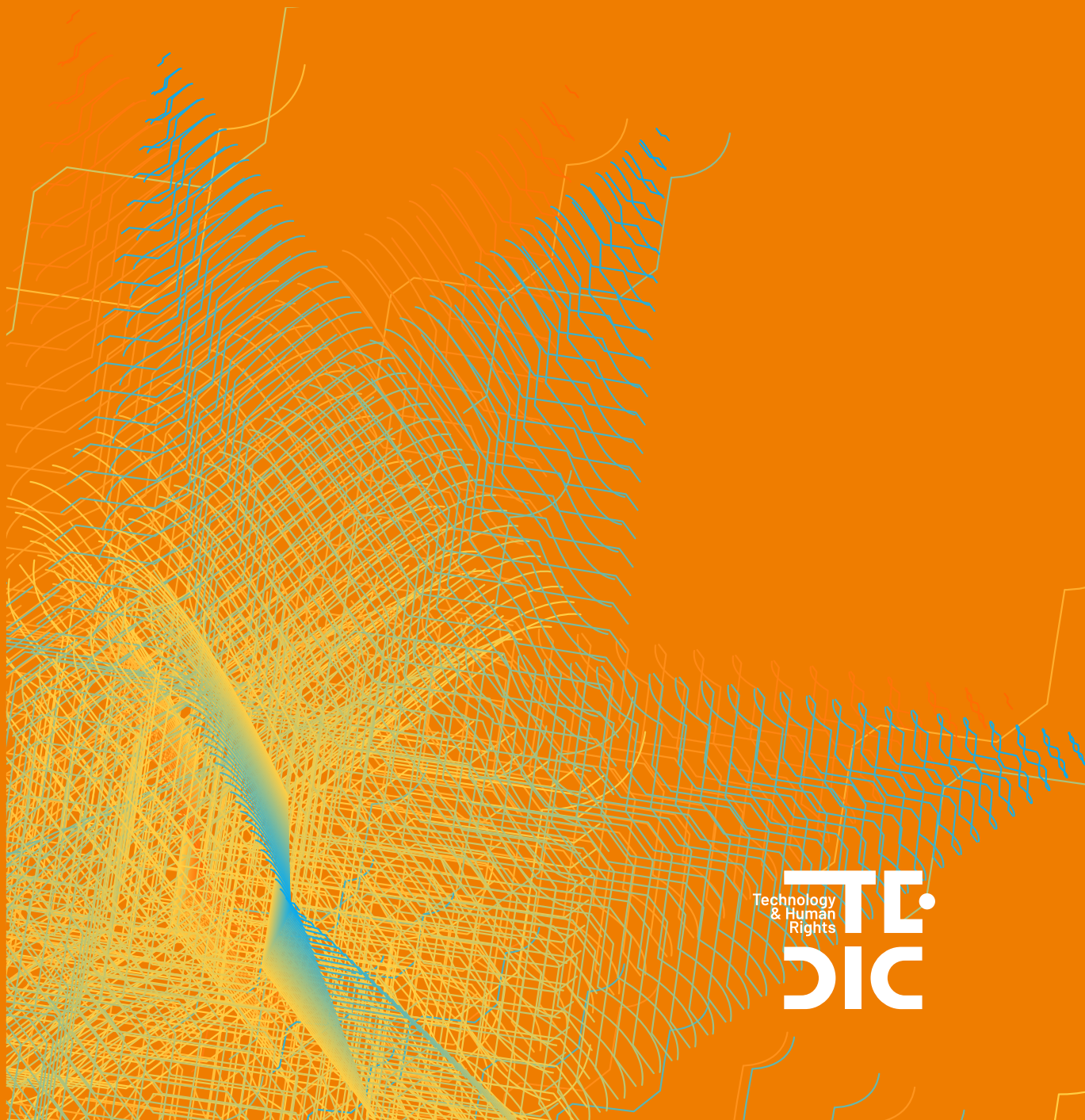
BIOMETRIC SURVEILLANCE: FACIAL RECOGNITION AND HUMAN RIGHTS AT SPORTING EVENTS IN PARAGUAY



Technology & Human Rights
TEDIC

BIOMETRIC SURVEILLANCE: FACIAL RECOGNITION AND HUMAN RIGHTS AT SPORTING EVENTS IN PARAGUAY

Technology & Human Rights
TEDIC

This research was conducted as part of the **Initiative for Digital Public Interest** with support from Rockefeller Philanthropy Advisors.

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.

BIOMETRIC SURVEILLANCE: FACIAL RECOGNITION AND HUMAN RIGHTS AT SPORTING EVENTS IN PARAGUAY

MARCH 2026

AUTHOR
Antonia Bogado Rodas

COORDINATION, EDITING, AND REVIEW
Maricarmen Sequera

REVIEW SUPPORT
Maricel Achucarro

COMMUNICATIONS
Romina Aquino González

DESIGN AND LAYOUT
Horacio Oteiza

How to cite this research in APA format:
Bogado Rodas, A. (2026). *Biometric surveillance: Facial recognition and human rights at sporting events in Paraguay.* TEDIC.

Tecnología & Derechos Humanos

TABLE OF CONTENTS

INTRODUCTION

The expansion of facial recognition technologies (FRT)[1] in Latin America has largely advanced under narratives of efficiency, modernization and public safety, without a substantive democratic debate on their implications for fundamental rights. In Paraguay, the enactment of Law No. 7269/2024 "for the prevention, control and eradication of violence in sports" formally authorized the deployment of video surveillance systems with biometric capabilities in sports stadiums, positioning the country within a regional trend of technological adoption characterized by the absence of prior impact assessments, specific regulatory frameworks and effective mechanisms for independent oversight.

This research builds on and further develops the preliminary evidence produced by TEDIC in the context of the "Con Mi Cara No"[2] ["Not With My Face"] campaign, which documented the installation of biometric surveillance infrastructure without sufficient public information about its operation, contracted providers, databases consulted or protocols for the processing of personal data. It is carried out within the framework of TEDIC's Digital Public Infrastructure project and responds to the need to generate critical, technically informed and situated knowledge on the tensions between surveillance technologies and human rights in the Paraguayan context.

TThe analysis is based on the premise that biometric technologies are not neutral tools, and that their assessment does not depend exclusively on the conditions of use. On the contrary, they incorporate design decisions, data selection and operational logic that structurally shape their impacts on fundamental rights (Criado-Perez, 2020; O'Neil, 2017; Zuboff, 2020). In the case of FRT deployed in public spaces, particularly in publicly accessible settings such as sporting events, their ability to operate in an automated, large-scale and opaque manner poses specific risks to privacy, freedom of expression, equality and the presumption of innocence that go beyond traditional personal data protection frameworks (Access Now, 2021; Díaz, 2018; Pietrasanta et al., 2025).

The Paraguayan context exacerbates these risks. At the time of the implementation of Law No. 7269/2024, the country did not have a general personal data protection law. Law No. 7593/2025 was only enacted in November 2025 and, at the time of this report's preparation, still lacks implementing regulations and a fully operational oversight authority. This situation creates a regulatory paradox, as it allows the mass processing of sensitive biometric data without clear and enforceable standards regarding lawfulness, purpose, data minimization, retention, security or the effective exercise of data subjects' rights. Added to this is institutional opacity regarding procurement processes, provider selection criteria, and the technical characteristics of the deployed systems, which severely hinders democratic oversight and accountability.

1 In this research, the terms "facial recognition technologies," "facial recognition systems," as well as the acronyms "FRT" and "FRS" are used interchangeably to refer to AI-based biometric tools that enable the identification or verification of individuals through the automated analysis of facial features. These technologies encompass various functionalities, such as face detection, facial identification and, in some cases, expression analysis, whose capabilities are specified where necessary.

2 "Con Mi Cara No" ["Not With My Face"] is a project led by TEDIC aimed at critically examining the use of facial recognition technologies in Paraguay. See: https://www.tedic.org/con-mi-cara-no-py/ y https://conmicarano.tedic.org

From this perspective, this study examines the use of FRT in Paraguayan sports stadiums in light of national and international human rights standards. The analysis is structured around four main dimensions.

First, the report develops a theoretical framework that positions facial recognition as a biometric technology based on artificial intelligence (AI), addressing its technical foundations, its primary modes of operation and the features that qualitatively distinguish it from traditional video surveillance (CCTV). This approach is essential for understanding why facial recognition is not merely an extension of CCTV, but rather a technology with greater intrusive potential.

Second, the applicable regulatory framework in Paraguay is analyzed by reconstructing the legal architecture that regulates—or should regulate—the use of FRT at sporting events. This section includes an examination of Law No. 7269/2024 and its implementing decree, the personal data protection framework, as well as constitutional provisions and international treaties ratified by the country that form part of the constitutional framework governing privacy, data protection and fundamental rights in the context of surveillance practices.

Third, the tensions between the biometric surveillance model enabled by law and four fundamental rights that are particularly affected are examined: I) privacy and the protection of personal data, examining the reasonable expectation of privacy in public spaces and the compatibility of the large-scale processing of biometric data with the principles of data minimization and proportionality; II) freedom of expression and peaceful assembly, analyzing the chilling effect that surveillance can have on public participation; III) equality and non-discrimination, evaluating documented algorithmic biases and their differential impact on historically marginalized groups; and IV) the presumption of innocence, questioning the compatibility of mass biometric surveillance, without individualized suspicion, with fundamental procedural guarantees.

Finally, the study applies a proportionality test as a legal analytical tool, examining whether the use of FRT in Paraguayan sports stadiums meets the requirements of legality, necessity and proportionality in the strict sense. This analysis makes it possible to determine whether there is a sufficient legal basis, whether less intrusive alternatives have been explored and whether the alleged benefits justify the extent of the interference with the fundamental rights involved.

A mixed methodology is adopted for this research, combining documentary analysis of primary sources (laws, decrees, resolutions, public contracts, parliamentary debates), systematic review of specialized literature on biometric technologies and human rights, and the use of comparative legal analysis techniques, with reference to regional (Argentina, Brazil, Colombia, Uruguay) and international regulatory developments (the European AI Act, jurisprudence of the Inter-American Court of Human Rights, reports by UN Special Rapporteurs).

The conclusions and recommendations aim to contribute to the democratic debate on technological adoption in Paraguay by providing technical and legal inputs for decision-makers, judicial authorities, security agencies and civil society organizations. The analysis argues that the implementation of mass biometric surveillance without rigorous impact assessments, without an independent oversight authority and without specific safeguards constitutes a structural threat to fundamental rights that the Paraguayan State is obliged to protect, and that the current model of technological adoption reproduces utilitarian approaches to surveillance that are incompatible with democratic standards of governance.

KEYWORDS: *facial recognition, biometric data, biometric surveillance, human rights, personal data protection, proportionality, sports stadiums.*

METHODOLOGY

This study adopts an exploratory and analytical design with a qualitative legal-normative approach, aimed at critically evaluating the implementation of FRT in sports stadiums in Paraguay in light of constitutional, international and comparative human rights standards. The study does not merely describe the current legal framework, but critically examines its adequacy, identifies structural tensions with fundamental rights and formulates regulatory and public policy recommendations grounded in technical analysis.

The analysis is structured around three complementary methodological components. First, a systematic review of specialized literature was conducted on the technical foundations of biometric technologies, regulatory frameworks and human rights standards, as well as empirical evidence on impacts on fundamental rights. The literature search prioritized specialized academic databases, repositories of human rights organizations (CELS, Derechos Digitales, Coding Rights, Karisma, TEDIC) and official documentation from international organizations, focusing on sources published between 2018 and 2026, without excluding earlier foundational works when deemed conceptually relevant.

Second, the empirical component was based on a systematic analysis of primary regulatory and administrative sources, including the full text of Law No. 7269/2024 and its implementing decree, records of parliamentary debates, public information access requests submitted under Law No. 5282/2014 to the National Sports Secretariat and the Ministry of the Interior, and public policy documents on the implementation of biometric surveillance systems. The responses obtained and refusals to disclose information were systematized as evidence of accountability gaps. Additionally, qualitative content analysis techniques were applied to parliamentary debates, institutional narratives and official justifications, identifying techno-solutionist narratives, mechanisms for distributing responsibilities and considerations regarding fundamental rights impact assessments.

Throughout the analysis, the proportionality test was applied as a legal interpretation tool to evaluate the constitutional legitimacy of restrictions on fundamental rights. This test, well-established in comparative constitutional law and adopted by Inter-American jurisprudence, structures the analysis into three criteria: legality (assessment of whether there is a sufficiently clear and precise legal basis), necessity (examination of whether FRT constitutes the least restrictive means available) and proportionality in the strict sense (balancing the intensity of the impact on rights against the relevance of the objective pursued). This tool serves both as a criterion for retrospective evaluation and as a regulatory parameter to guide the future design of technological surveillance policies in accordance with democratic standards.

The study incorporates elements of comparative law through an analysis of documented cases of FRT implementation in Argentina, Brazil, Colombia and Uruguay, which allows for identifying regional patterns of technological adoption without effective safeguards, documenting institutional responses to detected abuses and assessing the relevance of GDPR standards and the EU AI Act as a regulatory framework adaptable to Latin American contexts. This comparison takes into account the region's institutional, social, and technological particularities, avoiding uncritical transpositions of regulatory models developed in different contexts.

The research is based exclusively on public documentary sources and does not involve the collection of primary data through interviews or surveys. This methodological decision stems from ethical considerations regarding the protection of individuals potentially affected by misidentification, project time constraints and the adequacy of documentary sources for the analytical objectives of the study.

The identified methodological limitations are thoroughly documented in the corresponding section, reframing them as structural findings on transparency and accountability gaps within the context of technological surveillance in Paraguay.

The findings are organized around the technical foundations of FRT, the reconstruction of the Paraguayan regulatory framework, the evaluation of tensions with specific fundamental rights, the application of the proportionality test and the formulation of conclusions and recommendations. This structure enables a transition from descriptive approaches to critical, policy-oriented analyses aimed at public policy advocacy.

BIOMETRIC TECHNOLOGY: TECHNICAL FOUNDATIONS AND SCOPE OF FACIAL RECOGNITION

To understand the ethical, legal and political challenges posed by the technology examined in this study, it is essential to begin with an examination of its technical foundations and scope. Far from being neutral or merely instrumental systems (O'Neil, 2017; Zuboff, 2020), biometric technologies incorporate design decisions, data selection and contexts of use that significantly shape their functioning and impacts.

The various applications of this technology are adapted to specific uses. Therefore, understanding its components, modes of operation and limits is essential for evaluating both its functional scope and the risks and harms it may generate, especially when deployed in publicly accessible spaces.

WHAT ARE BIOMETRICS AND FACIAL RECOGNITION?

Biometrics can be defined as a set of automated techniques used to identify or verify a person's identity based on human characteristics (Pietrasanta et al., 2025, p. 15; Smith & Miller, 2022), such as the face, fingerprints, the iris, the voice or certain behavioral patterns (Bourcha et al., 2017, p. 39)[3]. Unlike other identification mechanisms, these systems rely on traits closely linked to the body and the identity of individuals (Díaz, 2018, p. 6), which explains their growing relevance and, at the same time, their particular sensitivity from a human rights perspective (Galeano et al., 2024).

3 In the framework of this research, the analysis focuses primarily on biometric technologies that employ facial recognition, that is, those that process data relating to individuals' faces. While other forms of biometric identification exist that may also pose challenges from a human rights perspective, their examination falls outside the specific scope of this study.

Within this broader field, facial recognition is a particular biometric technology that analyzes facial features from images or video sequences with the aim of identifying or verifying a person through automated processes (Smith & Miller, 2021). These technologies involve the extraction, digitization and comparison of the geometric characteristics of the face, transforming images into data that can be processed by algorithmic systems (Lyon, 2018).

The use of facial recognition technologies has gained increasing prominence in recent years across multiple areas of daily life, from seemingly innocuous applications, such as unlocking mobile devices or accessing digital services, to critical areas such as security, justice and state control (Pérez Trench, 2021; Silva & Varon, 2021). However, the deployment of these technologies in surveillance contexts raises important questions that go beyond their technical definition and require a more detailed examination of how they operate.

HOW DO FACIAL RECOGNITION SYSTEMS WORK?

From a technical standpoint, facial recognition systems operate through a series of successive stages. First, the system detects the presence of a face within an image or video sequence, allowing it to isolate the face from the surrounding visual environment and define the area for subsequent analysis (Pietrasanta et al., 2025; Zalnieriute, 2021).

Once a face has been detected, the system extracts facial features, such as the distance between the eyes, the shape of the nose, the jawline structure and other reference points. These features are quantified and converted into a digital template (Ricanek & Boehnen, 2012), that is, a mathematical representation of the face that enables comparison with other templates stored in databases (Pietrasanta et al., 2025; Ricanek & Boehnen, 2012; Smith et al., 2018, p. 55).

Subsequently, the system compares the generated template with one or more pre-existing templates, calculating a similarity score that indicates the likelihood of a match between the analyzed faces (Ricanek & Boehnen, 2012). This process does not produce absolute binary results, but rather probabilistic estimates, whose level of accuracy depends on multiple technical and contextual factors (Smith, 2018; Lyon, 2018).

This technical mechanism forms the basis for practical applications of facial recognition. However, its effective operation depends on additional variables, such as image quality, lighting, capture angle and environmental conditions (Fundación Via Libre, 2024; Smith et al., 2018), aspects that become particularly relevant in dynamic, high-traffic settings, such as sporting events.

VERIFICATION AND IDENTIFICATION

Based on these technical capabilities, it is possible to distinguish between two main uses of facial recognition: verification and identification. This distinction is important for understanding the different levels of risk associated with their implementation (Brey, 2004).

Verification consists of a one-to-one comparison process through which the system assesses whether the captured face matches a previously declared or registered identity. This use is typically applied in relatively controlled contexts, such as access to devices or closed systems, where individuals voluntarily present themselves to confirm their identity (Brey, 2004; Ricanek & Boehnen, 2012).

A common example of this type of use is unlocking mobile devices using facial recognition. In these cases, the user sets up the system by registering their face, which is then stored as a reference template. Each time access is attempted, the system captures a new image of the face and compares it with the previously stored template. If both match within a certain margin, access is granted.

Identification, on the other hand, involves a one-to-many comparison process in which the captured face is checked against multiple records stored in a database to determine whether there is a match (Brey, 2004; Ricanek & Boehnen, 2012). This use is substantially more intrusive, as it allows individuals to be identified without having declared their identity or necessarily being aware of the process (Pietrasanta et al., 2025). This type of application is precisely the focus of this research.

Identification can, in turn, be either targeted or generalized. In targeted identification, the system is used to search for specific individuals who have been previously identified, whereas in generalized identification it is deployed broadly and often imperceptibly, as in mass surveillance systems designed to track and identify unknown individuals in public spaces. This modality poses the greatest challenges from a legal and human rights perspective (Ibarreche et al., 2025; Richards, 2013; Zalnieriute, 2021).

FACIAL RECOGNITION AS SURVEILLANCE TECHNOLOGY

Beyond its technical foundations, facial recognition technologies become problematic when integrated into surveillance systems (Ibarreche et al., 2025). In these cases, the technology is no longer an isolated tool but part of a broader network of devices, databases and institutional practices aimed at monitoring and controlling individuals in public spaces (Caeiro, 2022; Lyon, 2018; Zalnieriute, 2021).

REAL-TIME, REMOTE AND RETROSPECTIVE SURVEILLANCE

First, it is important to distinguish between the different surveillance modalities under which facial recognition systems can operate, as not all of them present the same level of intrusion or pose the same risks from a human rights perspective. In some cases, these technologies are used in real time, allowing for the immediate identification of individuals as they enter or move through a given space. In others, they are applied retrospectively, through the subsequent analysis of existing recordings, for example, for investigative purposes following a specific incident. Furthermore, facial recognition systems can operate remotely through interoperability with other databases or information systems, which significantly expands their overall functional scope (Brey, 2004; European Union Agency for Fundamental Rights, 2015).

While it is recognized that certain applications of facial recognition may be presented as tools for legitimate security purposes, it is crucial to note that forms of remote and real-time biometric identification pose greater challenges. Such uses not only expand surveillance capabilities through the immediate monitoring of individuals in public spaces, but also enable retrospective analysis and the sharing of biometric data across different institutions, often without the knowledge or participation of affected individuals (Privacy International, 2025).

In this regard, it should be noted that the European Union's Artificial Intelligence Regulation (AI Act)[4] introduces a relevant regulatory distinction between different types of remote biometric identification. In Article 3, it defines these systems as those that identify individuals at a distance, without their active involvement, through the comparison of a person's biometric features with a reference database (Art. 3.41). It also distinguishes between systems that operate in real time, in which capture, comparison and identification occur without significant delay (Art. 3.42), and those that operate retrospectively, based on the analysis of previously recorded images or footage (Art. 3.43).

Therefore, this distinction is key to understanding the differentiated framework of prohibitions and restrictions established for different types of biometric identification systems, which tend to be particularly stringent in the case of systems operating in real time, given their particularly intrusive nature.

4 Regulation (EU) 2024/1689 is cited for comparative and reference purposes, as it constitutes one of the first comprehensive regulatory frameworks to adopt a risk-based approach to regulating artificial intelligence systems. Its inclusion does not imply uncritical acceptance or its automatic application to other contexts; rather, it reflects its relevance as an international benchmark in contemporary regulatory debates.

TRADITIONAL CCTV VS. CCTV WITH BIOMETRIC TECHNOLOGY

Before proceeding with a critical analysis of the practical implementation of facial recognition technologies, it is also important to distinguish between traditional video surveillance systems (CCTV) and those that incorporate biometric identification capabilities, whether remotely or retrospectively. While traditional CCTV is limited to capturing and recording images for observation or subsequent review, video surveillance systems with biometric technology, particularly facial recognition, automate the identification of individuals, transforming images into biometric data for analysis and comparison (European Union Agency for Fundamental Rights, 2015).

This difference is not merely technical, given that the shift from passive observation to automated identification entails a substantial transformation in the nature and scope of the control exercised over individuals. Indeed, Article 22 of the recently enacted Personal Data Protection Law of the Republic of Paraguay (Law No. 7593/2025) regulates data processing through video surveillance, but its scope of application is limited to the capture of images for security purposes, that is, to traditional CCTV systems. However, when biometric processing such as facial recognition is incorporated, data processing goes beyond the framework of Article 22 and falls under the legal regime governing sensitive data—a concept to be discussed later—which imposes considerably stricter legal requirements. This regulatory distinction, which will be examined in greater depth in subsequent sections, reflects the qualitative leap between mere visual surveillance and the automated biometric identification of individuals.

TARGETED SURVEILLANCE VS. MASS SURVEILLANCE

Finally, within this section, it is necessary to distinguish between targeted surveillance and mass surveillance. Targeted surveillance is characterized by the targeted collection of information about specific individuals, based on objective criteria and individualized suspicion; in the criminal justice system, it is generally subject to prior judicial oversight as a guarantee of due process. In contrast, mass surveillance involves the indiscriminate and widespread collection of data from large groups of people, without individualized suspicion or clearly defined purposes, proportionality or time limits for the processing of such data (Brey, 2004; European Union Agency for Fundamental Rights, 2015; International Network of Civil Liberties Organizations, 2016).

Considering this distinction, facial recognition technologies deployed in publicly accessible spaces, such as football stadiums, typically function as systems of mass surveillance, capturing and biometrically analyzing the facial data of all attendees, regardless of their conduct or any connection to illicit acts. This type of practice is concerning, as it challenges fundamental principles of constitutional law and international human rights law, such as the right to privacy, the prohibition of arbitrary or disproportionate surveillance and the prohibition of collective suspicion. By subjecting all attendees to indiscriminate biometric scrutiny, the rights-based logic that requires individualized and well-founded suspicion as a precondition for any state interference in the personal sphere is reversed, dangerously approaching a presumption of suspicion incompatible with the rule of law (Rolón Luna & Sequera, 2016).

Furthermore, the constant development of these technologies should be taken into account. Cotino Hueso (2022) warns that facial recognition technologies powered by artificial intelligence represent "a qualitative leap" compared with traditional public or private video surveillance. Unlike conventional systems, these tools allow captured faces to be compared with lists of wanted persons in milliseconds and automatically generate large volumes of processed data that can be used for multiple purposes. In this context, the author emphasizes that existing regulatory frameworks governing video surveillance, which are "generally insufficient," do not provide adequate legal coverage for these new technological phenomena, highlighting a significant regulatory gap.

The distinctions outlined in this section, between real-time and retrospective surveillance, traditional and biometric CCTV, and targeted and mass surveillance, are not merely theoretical classifications, but reflect substantial differences in the degree of intrusion into fundamental rights. These categories will be decisive for subsequent regulatory analysis, particularly when evaluating how the personal data protection framework must respond differently to each implementation modality, taking into account their specific risks and the safeguards required to ensure their legitimacy.

FACIAL RECOGNITION: LIMITS ANS RISKS

Beyond the technical distinctions outlined in the previous section, it is necessary to examine more closely the implications of deploying facial recognition systems in public and publicly accessible spaces. Although these technologies are often presented as neutral tools aimed at legitimate public safety objectives, their practical implementation reveals problematic dimensions that go beyond mere technical functionality and compromise fundamental rights (Lyon, 2018; Zuboff, 2020).

Facial recognition, unlike other biometric methods, does not require physical contact or the active participation of "targeted" individuals to operate (Venturini & Garay, 2021). This characteristic allows for its silent and widespread deployment in public spaces, subjecting individuals who are not under individualized suspicion of unlawful acts to biometric surveillance, many of whom are unaware that they are being subjected to this type of processing. Indeed, this characteristic is what makes facial recognition a particularly intrusive technology from a human rights perspective.

The association between facial recognition and mass surveillance is not arbitrary. As discussed in the previous section, when these systems are implemented in high-attendance settings, such as football stadiums, public squares or transport terminals, they operate under a logic of indiscriminate data collection. In simpler terms, they biometrically process all individuals present, regardless of their conduct or any connection to acts that would justify such intrusion. This form of surveillance significantly amplifies the state's capacity for control and, frequently, that of private companies that exploit these technologies through security service contracts.

While the justification often invoked for the adoption of these technologies, such as the prevention of crime and violence (Dela Peña et al., 2024), may be understandable in the abstract, their implementation can entail a disproportionate cost. This is the case both in terms of the impact on fundamental rights and in terms of infrastructure, in exchange for a promise of security that cannot be fully guaranteed. In this context, the aphorism frequently invoked in defense of mass surveillance, namely that "if you have nothing to hide, you have nothing to fear," is inadequate when used as a justification against a fundamental right such as privacy, and against a particularly sensitive practice such as the digitization and mass processing of biometric data derived from the human face (Zuboff, 2019).

Additionally, it is important to note that facial recognition faces significant technical limitations that affect its reliability. Image quality has a decisive impact on the algorithm's ability to correctly process and evaluate it (Leslie, 2020). Factors such as low resolution, poor lighting conditions, sudden movements or partial obstruction of the face significantly reduce the likelihood that the system will detect a face or correctly associate it with a specific identity (Smith et al., 2018).

In the context of football stadiums, these limitations may be further exacerbated due to the constant movement of people, variable lighting and common fan practices, such as painting their faces in their team's colors.These situations increase the risk of errors in identification processes, with potentially serious consequences in terms of false positives[5] or false negatives[6]. Both types of error are indicators of the model's accuracy: while false positives violate the fundamental rights of individuals who should not be subject to restriction, false negatives compromise the preventive effectiveness invoked as the main justification for deploying these technologies.

From a critical perspective, as developed in both academic literature and the work of civil society organizations, the normalization of biometric technologies in mass surveillance schemes contributes to the consolidation of models of continuous control over the population, with chilling effects[7] on the exercise of rights and participation in public spaces (Flóres Ruiz & Díaz Benito, 2021; Richards, 2013). The mere awareness of being subjected to biometric surveillance can lead to self-censorship and alter individuals' behavior, affecting their freedom of expression, their right to privacy and their ability to participate freely in cultural and recreational activities, including access to sporting events.

Accordingly, facial recognition systems deployed in public spaces must be evaluated under a heightened standard of justification that does not rely solely on formal legality, as will be discussed below, but instead strictly incorporates a human rights-based approach (Venturini & Garay, 2021). This entails assessing not only whether a legal basis exists to authorize their use, but also whether such use is strictly necessary, proportionate, and compatible with the fundamental guarantees recognized both in the domestic legal framework and international human rights instruments (Electronic Frontier Foundation, 2014).

5 A false positive occurs when the system incorrectly identifies a person as a match with an individual in the database, even though they are not included in it, potentially affecting innocent individuals (Dionis Baeza, 2024). (False positive). IDP UCM. https://www.idpucm.com/falso-positivo-false-positive/)

6 A false negative occurs when the facial recognition system fails to identify a match that actually exists in the reference database. In the context of stadium security, this means that an individual with a documented entry ban is not identified by the system and is able to enter the event (Dionis Baeza, 2024). (False negative). IDP UCM. https://www.idpucm.com/falso-negativo-false-negative/)

7 The chilling effect refers to the phenomenon in which the mere awareness of being under surveillance generates self-censorship and alters individual behavior, even when individuals have not engaged in any illicit conduct (Penney, 2016a). In the context of facial recognition, individuals may refrain from participating in protests, public events or legitimate activities for fear of being identified, tracked or potentially subject to adverse actions, thus affecting the exercise of fundamental rights such as freedom of expression, association and political participation.

INTERNATIONAL EXPERIENCES WITH FACIAL RECOGNITION AT SPORTING EVENTS

The use of facial recognition at sporting events began to gain prominence in the early 21st century. An early and significant example took place during Super Bowl XXXV in Tampa, Florida, in 2001, where authorities used this technology to identify individuals with criminal records among the attendees (Hutchins & Andrejevic, 2020). This pioneering implementation, met with skepticism regarding its effectiveness, laid the groundwork for its expansion to other major sporting events in the years that followed.

Over the years, FRT has become a widely used tool in the security of major sporting events, especially in football. During the Sochi 2014 Olympic Games, the Fan ID was implemented, a mandatory identification system that used facial recognition technologies for all attendees, including minors. This technology was subsequently adopted during the 2018 FIFA World Cup in Russia, where it was used extensively in stadiums, facilitating the identification of fans and the detection of individuals wanted by law enforcement (González et al., 2024).

While these systems are presented as tools aimed at legitimate purposes, such as identifying and restricting access to individuals with a history of violence, streamlining public entry and detecting potential threats, international experience has revealed a significant gap between security promises and actual outcomes. Justifications based on violence prevention must be critically evaluated, considering not only their demonstrated effectiveness but also the costs they impose on fundamental rights when deployed on a massive and indiscriminate scale on all attendees at sporting events (Belli et al., 2024).

To properly contextualize this issue, the following sections examine international experiences with the implementation of facial recognition at sporting events, both in Europe and in Latin America. This comparative analysis will allow for the identification of common patterns and recurring challenges that will subsequently serve as a framework for evaluating initiatives that, although still in their early stages, are already taking shape in the Paraguayan context.

Europe

The implementation of facial recognition in European stadiums has set important legal and regulatory precedents. In 2017, British police used a real-time facial recognition system during the UEFA Champions League final in Cardiff, which resulted in an alarming number of false positives: of 2,470 potential matches detected by the system, 2,297 were incorrect, representing an error rate of over 90% (The Guardian, 2018). These failures not only call into question the technical reliability of the technology but also highlight its serious implications for human rights, by exposing innocent individuals to erroneous identifications and potentially unjustified restrictions on access.

Beyond technical failures, cases of misuse have emerged, highlighting risks of individual misuse. In Sussex, United Kingdom, a police officer used facial recognition technology to harass a woman, leading to legal proceedings that exposed the vulnerabilities of these systems when robust oversight and accountability mechanisms are lacking (Maisner, 2026).

In Spain, the Spanish Data Protection Agency (AEPD) has taken a particularly critical stance. In fact, in 2022, the AEPD deemed that facial recognition systems and the collection of biometric data in football stadiums are highly intrusive with regard to individuals' rights, warning that their implementation is illegal under current Spanish regulations and that less intrusive alternatives must be assessed (Spanish Data Protection Agency, 2022). This position has led to the implementation of such systems being optional rather than mandatory for spectators. The AEPD has issued warnings to the Spanish Football League in response to announcements of large-scale deployments and, more recently, sanctioned Burgos CF for implementing biometric registration of its members without proper consent (Spanish Data Protection Agency, 2023). These precedents reinforce the requirement that any processing of biometric data must be subject to stricter scrutiny as to its purposes and outcomes.

Latin America

In Latin America, the adoption of facial recognition technologies in stadiums has progressed in a context marked by deep social and economic inequalities, where asymmetries can vary significantly between countries (Inter-American Development Bank, 2024). These inequalities are particularly exacerbated when other aspects of intersectionality, such as gender or race, further act as factors of exclusion (Economic Commission for Latin America and the Caribbean, 2024). Despite the documented risks, enthusiasm and investment in facial recognition have not ceased, even in sectors as sensitive as policing or the administration of justice (Mello, 2023).

Brazil was a regional pioneer in implementing facial recognition technologies during the 2019 Copa América. However, this early implementation revealed serious problems, as cases of misidentification were recorded, resulting in the inclusion of innocent people on a "blacklist" in the vicinity of the Maracanã Stadium in Rio de Janeiro (Sceiza et al., 2022). Although Brazil has had a general data protection framework[8] in force since 2020, as well as regulations such as Ordinance No. 793/2019 of the Ministry of Justice and Public Security, which explicitly authorizes the use of facial recognition within the framework of the National Public Security Policy and provides funding for its adoption through the National Public Security Fund, the country still lacks specific regulations governing the use of these technologies according to their purpose and context of application.

This regulatory vacuum has led to a dynamic of accelerated technological adoption without prior impact assessments or robust oversight mechanisms. An illustrative case involves the football club Palmeiras, which used the facial recognition system installed in its stadium in São Paulo to identify the perpetrator of racist abuse during a Copa Libertadores match against Cerro Porteño (El Mundo, 2025). While this use could be justified under anti-discrimination purposes, the absence of clear protocols on proportionality, data retention and the rights of those affected highlights the risks of normalizing mass surveillance under case-by-case justifications, without a regulatory framework to ensure that each implementation complies with standards of necessity, adequacy and proportionality[9].

8 General Personal Data Protection Law (LGPD) or Law No. 13.709/2018, in force since 2020.

9 The principles of necessity, adequacy and proportionality are widely used standards in the analysis of surveillance measures, both in constitutional doctrine and in the work of civil society organizations specializing in digital rights. (Electronic Frontier Foundation, 2014)

In June 2025, Brazil took a decisive step toward mandating these technologies. The General Sports Law No. 14,597, published on June 14, 2023, with a two-year implementation period, established in Article 148 that all stadiums with a capacity exceeding 20,000 people must adopt biometric control systems—such as facial recognition or fingerprint recognition—as a requirement for access (Agência Câmara de Notícias, 2026; Maleson, 2025). This measure made Brazil the first country in Latin America to legally mandate mass biometric surveillance in football stadiums, without prior public evaluation of the system's effectiveness or empirical evidence supporting its proportionality.

The mandatory implementation also occurs in a context where critical regulatory gaps persist, such as a lack of clarity regarding third-party access to the generated databases, the absence of opt-out mechanisms for attendees who do not wish to provide their facial data and the lack of an independent supervisory authority with effective sanctioning powers. This model of technological adoption, characterized by legal mandates without specific safeguards, challenges the principles of data minimization, purpose limitation and informed consent[10] set out in the LGPD, creating a structural tension between the general data protection framework and sector-specific regulations that promote mass biometric surveillance in the sports sector.

Chile has also recently adopted facial recognition in football stadiums. In January 2026, Colo-Colo announced the mandatory implementation of a facial recognition-based fan registry system to access Estadio Monumental (Bertolini, 2025; El Cronista, 2026). The system requires an online biometric enrollment process prior to purchasing tickets, with the stated goal of improving security and streamlining access, without offering alternatives for those who prefer not to provide their facial data (Rodríguez, 2026). However, as this is a very recent implementation, there are no evaluations of its effectiveness, nor is there available data on the processing and storage of the collected biometric data.

Mexico mandated the implementation of FRT in all football stadiums starting with the 2022–2023 season, following the violent incidents that occurred at Estadio Corregidora (González et al., 2024). The Fan ID system, which has been widely adopted, requires the biometric registration of all attendees. However, despite the considerable investment and the mandatory nature of the system, violence in stadiums has not decreased significantly, leading to criticism regarding the actual effectiveness of this technology and the handling of personal data by the Mexican Football Federation (FMF) and its commercial partners.

According to the Mexican organization Red en Defensa de los Derechos Digitales (R3D), the Fan ID system jeopardizes multiple fundamental rights such as privacy, personal data protection, freedom of expression and non-discrimination (2023b). The absence of human rights impact assessments prior to its implementation, coupled with a lack of transparency regarding the final destination of the collected data and the absence of opt-out mechanisms, highlights a model of technological adoption that prioritizes operational efficiency over the protection of fundamental rights.

10 Informed consent in data protection is defined as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they agree to the processing of their personal data. To be valid, it requires that the individual has received clear and understandable information regarding the identity of the data controller, the specific purposes of the processing, the period for which the data will be stored and their rights, including the right to withdraw consent at any time.

Despite these concerns, Mexico, as a co-host of the 2026 World Cup, represents a critical case of escalating use of facial recognition, building on previous instances in the same contex (Bertolini, 2025). Authorities have announced that access to World Cup matches will be "100% digitized" via biometric readers at turnstiles (El Cronista, 2026). This mass implementation is taking place in a context where Mexico faces documented challenges in cybersecurity and data protection, raising questions about the ability to safeguard the biometric information of millions of attendees against risks of data theft, unauthorized access, or unauthorized use. In light of these factors, the absence of independent evaluations of the system prior to implementation and the lack of transparency regarding data processing make the 2026 World Cup an unprecedented experiment in mass biometric surveillance in the region.

Uruguay has implemented FRT in stadiums since 2017 and offers lessons on the long-term limitations of these technologies. Although authorities reported an initial decline in violence attributed to the deterrent effect (Vázquez, 2018), the limited scope of the system has also been noted whenever there is a lack of sustained investment, proper maintenance and trained personnel. As noted above, cameras require specific conditions to function and are frequently circumvented by human error or technical failures. Moreover, the persistence of violent incidents led to the creation in 2023 of a General Directorate for Sports Security, which suggests that violence has not been eradicated despite several years of prior biometric surveillance (Gonçalves Feliz & Piza, 2024, pp. 211–212). Additionally, no official databases are publicly available containing statistics on the system's performance, such as the number of identities analyzed, accuracy rates or false positives, highlighting a lack of transparency that makes it difficult to assess the actual effectiveness of the implemented technology.

While the examples of the use of facial recognition in stadiums across the region could be further expanded, the cases documented in this section illustrate the diversity of regulatory, operational and social contexts in which these technologies have been deployed in Latin America. The experiences of Brazil, Chile, Mexico and Uruguay show distinct trajectories in terms of the mandatory nature, scope and degree of institutionalization of facial recognition at sporting events, as well as heterogeneous regulatory responses to its implementation (Venturini & Garay, 2021).

RECURRING PATTERNS: BETWEEN PROMISES OF SECURITY AND RISKS TO FUNDAMENTAL RIGHTS

A comparative analysis of the international experiences outlined above reveals a series of recurring patterns in the implementation of facial recognition in football stadiums. Beyond contextual differences between countries, the cases examined show that the adoption of these technologies is often accompanied by broad promises of improved security, the empirical effectiveness of which is, in many cases, limited or insufficiently demonstrated. At the same time, significant risks to fundamental rights persist, including the generation of false positives affecting innocent people, identification errors with serious consequences, practices of algorithmic discrimination and the secondary use of biometric data without informed consent (Caeiro, 2022). These risks are not isolated incidents, but rather systematic manifestations of technical limitations and regulatory gaps that characterize the deployment of these technologies in publicly accessible spaces.

Beyond technical failures, the implementation of mass surveillance schemes using facial recognition raises fundamental questions about their compatibility with the principles governing all state interference with fundamental rights. The indiscriminate biometric capture and processing of all individuals attending a sporting event, without individualized suspicion or precise definition of purposes, is in tension with the principle that security measures must be strictly necessary and proportionate to the specific risk they seek to prevent.

These concerns are exacerbated by the frequent lack of transparency in data processing, the absence of independent audits and the weakness of accountability mechanisms. As Neil Richards warns, mass surveillance is not a practice exclusive to authoritarian regimes; rather, it has also been adopted and expanded by democratic states in the name of security (2013, p. 1938). In this context, the use of biometric technologies in spaces with large crowds requires heightened scrutiny that goes beyond formal legality and addresses their actual effects on the exercise of rights.

Comparative experiences are particularly relevant for evaluating similar developments in other contexts, such as Paraguay, where the adoption of facial recognition technologies in stadiums is still in its early stages but shows clear signs of expansion. Likewise, these precedents invite reflection on the suitability of these technologies for specific regional realities and on the effective capacity of Latin American states to audit, regulate and adapt systems whose design, operation and biases remain, to a large extent, opaque and beyond their direct control.

BIOMETRIC DATA AS A SPECIALLY PROTECTED CATEGORY: LEGAL FOUNDATIONS AND REGULATORY CHALLENGES

From a legal and human rights perspective, biometric data differs in nature from other personal data. Defined as data derived from the recording or encoding of unique physical or behavioral characteristics of the human body—such as the face, fingerprints, iris or voice patterns—it has the ability to uniquely identify an individual (Díaz, 2018). This uniqueness is not merely technical; its direct link to the body and personal identity makes such data particularly intrusive when collected, stored or processed without adequate safeguards (Bygrave, 2014; Doneda, 2022).

For this reason, regulatory frameworks consistently classify them as sensitive personal data, a category that recognizes their potential to affect individuals' privacy, dignity and integrity and whose misuse can entail serious risks for data subjects (United Nations High Commissioner for Human Rights, 2021). This classification stems from the recognition that certain data—including those related to health, sexual orientation, religious or political beliefs and biometric characteristics—require a strengthened protection regime with additional legal safeguards for their collection, storage, processing and retention (Smith & Miller, 2021).

At the international level, standards applicable to the processing of biometric data have been developed. The right to privacy, enshrined in the Universal Declaration of Human Rights (UN, 1948) and the International Covenant on Civil and Political Rights (UN, 1966), prohibits arbitrary or abusive interference in the private sphere, which includes the large-scale processing of biometric data without a clear legal basis, lawful purpose and adequate safeguards. At the regional level, the Updated Principles on Privacy and Personal Data Protection (OAS, 2021) expressly recognize biometric data as sensitive data and establish that their processing must be strictly limited to exceptional cases, defined by law and subject to effective controls.

At the national level in Paraguay, this categorization is reflected in multiple regulatory instruments. First, the Constitution of the Republic of Paraguay (1992)—hereinafter, the Constitution—recognizes the protection of the right to private life and the "protection of privacy, dignity and the private image of individuals" (Article 33), as well as habeas data (Article 135) as a mechanism for safeguarding informational self-determination[11]. At the legal level, Law No. 6534/2020 on credit data protection—the current sector-specific regulation—expressly classifies biometric data as sensitive personal data (Art. 3.b), emphasizing that their misuse may lead to discrimination or place data subjects at serious risk. This definition is repealed by Law No. 7593/2025 on the Protection of Personal Data in the Republic of Paraguay (Art. 59), which is scheduled to take full effect in 2027 pursuant to Article 57.

11 Informational self-determination refers to the right of individuals to make autonomous decisions about the collection, use, processing, and disclosure of their personal information, as well as to exercise control over their data.

The new data protection law represents a significant advance in this area (TEDIC, 2025). It includes biometric data within the category of sensitive personal data (Art. 2.7) and expressly defines them in Article 2.4 as:

> "Personal data obtained through specific technical processing, relating to the physical and/or physiological characteristics of a person, that enable or confirm the unique identification of that person, such as facial images, iris recognition or fingerprint data".

This definition is particularly relevant for the analysis of facial recognition technologies, as it clearly delineates the scope of enhanced protection and establishes that "facial images" used for unique identification constitute biometric data subject to the legal regime governing sensitive data.

DISTINCTIVE FEATURES OF BIOMETRIC DATA AND THEIR IMPLICATIONS

Two characteristics of biometric data explain why their processing poses regulatory challenges that exceed general personal data protection frameworks.

First, its irreversible nature. Unlike other identifiers, such as passwords, cards or identification numbers, which can be modified or revoked, biometric data cannot be changed without affecting the individual's very identity. As Díaz (2018) warns, this permanence and high identification capacity imply that, in cases of leaks, unauthorized access or misuse, the harm could be permanent and irreparable. Once compromised, biometric data remains exposed indefinitely, with no possibility of "replacement" as with a breached password (Lyon, 2018; Pietrasanta et al., 2025; Sceiza et al., 2022). In fact, this irreversibility significantly increases the risks associated with the centralized storage of biometric databases and confirms the need to strictly apply principles such as data minimizations[12].

Second, the processing of biometric data frequently occurs within contexts of structural power asymmetries. These asymmetries arise when the State or major private actors impose conditions for access to services, spaces or rights—such as admission to sporting events, public transportation or social services—contingent upon the provision of biometric data (Privacy International, 2025; Silva & Varon, 2021; Venturini & Garay, 2021). In such scenarios, consent, when invoked, can hardly meet the standards of being freely given, informed and voluntary, as individuals face a merely formal alternative: to accept the processing of their personal data or be excluded from engaging in a legitimate activity, such as attending a sporting event (Bygrave, 2014; Doneda, 2022). Regardless of the legal basis invoked for the processing[13], this dynamic reveals a structural power imbalance that undermines the effective protection of data protection guarantees and fundamental rights. This issue has been repeatedly highlighted by international human rights bodies (United Nations High Commissioner for Human Rights, 2021) and specialized organizations (Privacy International, 2024), which warn of the risks of nor malizing the processing of personal data—particularly sensitive data—in contexts characterized by the absence of real alternatives and the imposition of conditions for access.

12 The principle of data minimization requires that only personal data strictly necessary to fulfill a legitimate and specific purpose be collected and processed, avoiding the excessive or indiscriminate collection of information that is not relevant to that purpose.

13 Consent is not the only legal basis for the processing of personal data. Data protection frameworks typically recognize other legal grounds, such as compliance with a legal obligation, reasons of public interest, the exercise of official authority or legitimate interest, among others. Nonetheless, each legal basis is subject to specific conditions, substantive limits and enhanced safeguards, especially in the case of sensitive or biometric personal data, the processing of which demands stricter scrutiny.

LEGAL REGIME: WHY IS ENHANCED PROTECTION RECOGNIZED?

As noted above, the processing of biometric data is subject, under contemporary personal data protection frameworks, to a regime of enhanced safeguards, given its particularly sensitive nature and the risks that its misuse poses to fundamental rights. Generally, such data may only be processed under strict conditions, including a clear definition of purpose, the adoption of technical and organizational security measures and, in many cases, the explicit consent of the data subject (Jasserand, 2024).

Furthermore, in accordance with international human rights standards, sensitive data, including biometric data, should not be processed as a general rule, except in exceptional cases clearly defined by law, such as compliance with legal obligations, court orders or strictly necessary reasons of public interest, public safety or the protection of third-party rights (OAS, 2021). In other words, the legal basis must be precise, foreseeable and accompanied by enhanced safeguards.

However, in practice, these requirements are often eroded by the breadth and vagueness of legal exceptions, particularly those invoked in the name of public safety or crime prevention, as has been extensively discussed in various contexts (ADC por los Derechos Civiles, 2019; Arthur Dela Peña et al., 2024; Wickins, 2007). This has facilitated the deployment of highly intrusive technologies, such as FRT, without prior impact assessments, effective oversight mechanisms or consideration of less harmful alternatives (Pérez Trench, 2021; Privacy International, 2025). This dynamic creates a gap between the formal recognition of the sensitive nature of biometric data and its effective protection in practice.

Comparative experience in Latin America illustrates this tension (Caeiro, 2022; Pietrasanta et al., 2025). Countries such as Argentina, Brazil, Colombia and Uruguay have relatively well-established general data protection frameworks; however, the implementation of facial recognition systems has, in many cases, occurred without fundamental rights impact assessments[14] or opt-out mechanisms for affected individuals (Access Now, 2021).

In Paraguay, although biometric data has been recognized as sensitive, both in sector-specific regulations and in the recent Law No. 7593/2025, the absence of a fully operational independent supervisory authority limits the capacity for oversight, enforcement and effective protection against potential abuses. This situation demonstrates that mere regulatory recognition of the sensitivity of biometric data is insufficient to mitigate the risks associated with its mass and automated use (Díaz, 2018). The lack of specific criteria for high-risk technologies, opacity regarding how systems operate and institutional weaknesses in oversight allow for the expansion of biometric surveillance practices without substantive controls (United Nations High Commissioner for Human Rights, 2021). In addition, there is a structural dependence on technologies developed by actors outside the region, trained on data and cultural assumptions that are foreign to local contexts (Fundación Via Libre, 2024; O'Neil, 2017; Venturini & Garay, 2021).

14 Fundamental Rights Impact Assessments, in the context of personal data protection, are preventive tools designed to identify, analyze and mitigate the risks that data processing may pose to individuals' rights and freedoms prior to the implementation of such processing.

Thus, although the Paraguayan regulatory framework formally recognizes the need for enhanced protection of biometric data, a significant gap persists between declarative regulation and effective protection. . This gap highlights the need to focus the implementation of facial recognition technologies in sports stadiums not only on formal compliance with the law but also on a substantive assessment of necessity, proportionality and compatibility with constitutional and human rights standards.

Summary of the legal regime applicable to biometric data under Law No. 7593/2025 (Paraguay)		
Aspect	**Articles**	**Key provisions**
Definition of sensitive personal data	3.7	Personal data whose improper processing may significantly affect an individual's fundamental rights. They include information relating to physical, physiological or biological characteristics that enable the unique identification of a person.
Definition of biometric data	3, paragraphs 5 and 7	Personal data resulting from specific technical processing related to physical, physiological or behavioural characteristics that allow for or confirm the unique identification of a person, such as facial images or fingerprints.
Express consent required	5.1, 6, 7 & 20	The processing of biometric data requires the data subject's express, free, informed and unambiguous consent for a specific purpose. The burden of proof rests with the data controller.
Protection regime	20	Enhanced.
Legal exceptions	8, 20, paragraphs 2–11	Compliance with legal obligations or court orders; protection of vital interests; grounds of public security, national defense or public order; and the exercise of powers of public authorities, provided these are prescribed by law.
Data retention period	4, sub-paragraphs c, d & e	Data may not be retained for longer than is strictly necessary to fulfil the purpose for which it was collected. Once this purpose is fulfilled, the data must be erased, anonymized or pseudonymized, unless otherwise required by law.
Data subject rights	27,28,29,30,31 & 33	Rights of access, rectification, objection, erasure (right to be forgotten), portability and the right not to be subject to decisions based solely on automated processing that produce legal or similarly significant effects.

Table 1. Prepared by the author

ANALYSIS OF THE PARAGUAYAN CONTEXT: LAW NO. 7269/2024 AND ITS IMPLEMENTATION

In 2024, Paraguay enacted Law No. 7269/2024 "On the prevention, control and eradication of violence in Sports" (Legislative Branch of the Republic of Paraguay, 2024), subsequently regulated by Decree 3337/2025 (Presidency of the Republic of Paraguay, 2025). This law establishes the obligation to implement video surveillance in stadiums, including facial recognition technology to identify individuals attending sporting events classified as high risk. Although the law is presented as a response to episodes of violence in sporting contexts (Dávalos Acuña, 2025; La Nación, 2025), its regulatory scope may conflict with the constitutional and legal framework for personal data protection in force in Paraguay.

As discussed in previous sections, the implementation of facial recognition systems in stadiums involves the mass processing of biometric data, a category recognized as particularly sensitive under current data protection regulations. In contrast, Law No. 7269/2024 establishes a mandatory biometric registration model that raises critical questions regarding its compatibility with key principles such as free consent, data minimization and proportionality.

THE NATIONAL REGISTRY OF SPORTING EVENTS (RENAED)

Article 4 of Law No. 7269/2024 establishes the National Registry of Sporting Events (RENAED), which will operate "automatically" and "will be connected to the National Police database", including "biometric data of individuals wishing to attend a sporting event" along with their identity document, full name, address, mobile phone number and email. In turn, Article 11 of Implementing Decree No. 3337/2025 specifies that RENAED will require "biometric data for its use, both for purchasing a ticket, whether paid or complimentary, and to facilitate effective access" to the sporting venue.

This regulatory framework raises questions about the nature of consent in a context where biometric registration becomes an indispensable condition for exercising the right to leisure and recreation. If access to sporting events[15] is contingent on providing biometric data, can consent be considered freely given as required by the current regulatory framework? Data protection literature has consistently emphasized that consent is not valid when its refusal results in exclusion from a service or activity, constituting what is termed "forced consent" or "consent by necessity" (Fundación Via Libre, 2024; J Zuiderveen Borgesius et al., 2017, p. 360).

15 The right to engage in sports is constitutionally recognized under Article 84 of the Constitution (Convención Nacional Constituyente, 1992).

PERSONAL DATA PROTECTION AND THE RENAED MODEL: CONVERGENCE WITH OTHER SECTOR-SPECIFIC REGULATIONS

Law No. 7593/2025 on Personal Data Protection establishes principles that may conflict with the RENAED model. Article 8 of this law regulates "legitimate interest" as a legal basis for data processing, but imposes strict conditions: processing must be "necessary" to pursue such an interest; the data subject's fundamental rights and freedoms must not override that interest; it must take place "within the framework of a relevant and appropriate relationship"; only "strictly necessary data" may be processed; transparency must be ensured; and it must be recognized that "the data subject shall have the right to object at any time" to the processing by challenging the controller's legitimate interest.

The purposes of RENAED may raise clear tensions with basic principles of personal data protection. If biometric registration is mandatory for access to stadiums, how can the right to object be exercised without being excluded from the event? If biometric data is processed "automatically" and kept "interconnected" to police databases, is the principle of data minimization, which requires processing only strictly necessary data, being upheld? Furthermore, the absence of non-biometric alternatives for accessing sporting events suggests that the system fails to comply with the principle of proportionality (Electronic Frontier Foundation, 2014), which requires exhausting less intrusive measures before resorting to the mass processing of sensitive data.

Additionally, Implementing Decree No. 3337/2025 devotes only four articles (19–22) to the "Use, Processing and Protection of Information", with fairly generic provisions. Article 19 limits the use of RENAED information to "monitoring compliance with the purposes established therein", but does not define audit mechanisms, retention periods or data deletion protocols. Article 20 permits use for "statistical or criminal policy purposes", opening the door to secondary uses without defining specific safeguards. Article 21 establishes that institutions "shall have protocols" for processing and protection, but delegates their definition without establishing mandatory minimum requirements or deadlines for their implementation. This regulatory laxity contrasts sharply with international standards on biometric surveillance.

An additional regulatory tension arises with other provisions governing the processing of personal data in sector-specific contexts such as digital commerce. Law No. 4868/2013 on Electronic Commerce stipulates in Article 6 that commercial activity "under no circumstances" may violate "the protection of personal data and the rights to personal and family privacy". Meanwhile, Law No. 6822/2021 on trust services for electronic transactions provides in Article 9 that service providers "may only collect personal data directly from the individual", who must give "express and informed consent", and that the data "may not be processed for any purpose other than the agreed purpose without the express consent of the data subject".

Given that RENAED links biometric registration to ticket purchases, which constitute a commercial transaction managed by private providers, a critical question arises: how does the "automatic" and mandatory nature of registration align with the requirement for "express and informed consent" established in these sector-specific laws? Can a trust service provider process biometric data when consent is conditioned on access to the service? These regulatory tensions have not been resolved either by the law or by its implementing regulation.

PUBLIC-PRIVATE CONFIGURATION

A critical element in the analysis of facial recognition implementation in Paraguay is the institutional framework that preceded and shaped the regulatory framework. In October 2023, five months after the bill was introduced and before its legislative approval, the National Sports Secretariat (SND) signed a sponsorship agreement with the company ITTI S.A.E.C.A., valued at USD 1,733,000 over four years (Unified Public Information Access Portal, 2024). This prior contractual arrangement inverts the logical regulatory sequence; that is, the technological infrastructure preceded the regulatory framework meant to govern it.

The agreement establishes obligations that involve the development of biometric data infrastructure and user profiling: (a) provision of cameras with identity verification technology for fans (clause 2.3); (b) development of user databases with business intelligence capabilities (clause 4.1); (c) profiling of spectators for access management (clause 4.2); (d) real-time behavioural reporting (clause 4.3); (e) provision of security cameras (clause 4.5). Critically, clause 5 states that the transactions "do not require additional consent," expressly waiving the requirement to obtain informed consent from data subjects. Clause 8 on confidentiality states that the information processed constitutes "valuable property belonging to the SPONSOR" (ITTI), raising questions about the ownership of biometric data and creating opacity around information of clear public interest (Unified Public Information Access Portal, 2024).

ITTI is part of Grupo Vázquez[16], a conglomerate that vertically controls Red UTS (ticketing provider for APF events), UENO Bank[17] (official sponsor of the Paraguayan national team and APF competitions), and the facial recognition systems installed in stadiums. In June 2024, ITTI was recognized as a qualified trust service provider by the Ministry of Industry and Commerce (General Directorate of Electronic Commerce, n.d.). This vertical integration, which concentrates ticketing, payment processing, access control and biometric surveillance within a single corporate group, was consolidated without public bidding, any fundamental rights impact assessment or independent oversight mechanisms.

In response to a request for information sent to ITTI regarding the system's technical and operational aspects, an electronic acknowledgment of receipt (ticket No. 93945/2026) was received, indicating that the request was "being reviewed by support staff". As of the closing date of this investigation, no formal response containing the requested information had been received. This lack of response from the private provider of the technological infrastructure reinforces concerns about accountability and access to information in a system that will process biometric data from thousands of individuals.

16 Official website of ITTI:: https://www.itti.digital

17 Official website of Ueno Bank: https://www.ueno.com.py

CURRENT IMPLEMENTATION STATUS: OPERATIONAL UNCERTAINTY AND ASSOCIATED RISKS

As part of the methodology for this study's data collection, information regarding the topic was requested from the Ministry of the Interior. A response was received on January 15, 2026, via Note No. 04/2026, in which the Department of Security for Sporting and Special Events of the National Police reported that "to date, the National Police has not implemented facial recognition technology in sports stadiums", noting that RENAED "is currently being regulated by the Council for Security in Sporting Events, under the Ministry of the Interior" (Unified Public Information Access Portal, 2026b). Similarly, the National Sports Secretariat, through Memorandum No. 4 dated January 29, 2026, indicated that the SND "has not implemented the Facial Recognition System for entry into its facilities and that there is currently no regulation requiring its implementation in sports stadiums" (Unified Public Information Access Portal, 2026a).

This situation constitutes a regulatory paradox. There is an enacted law, an implementing decree in force, agreements signed with private providers and technological infrastructure installed in stadiums, yet there is no formal operational implementation of biometric registration. This lack of clarity raises several risks: under what legal framework are facial recognition systems potentially installed in stadiums currently operating? If RENAED is not operational, how is the biometric data potentially captured being handled? Are there protocols for the retention, access and deletion of data collected during this preoperational or experimental phase?

This uncertainty regarding the system's operational status reinforces the perception that technological adoption has preceded the definition of adequate legal and technical safeguards.

Another significant risk in the context of the case examined is the phenomenon of "function creep," which refers to the progressive expansion of data use beyond the original purpose for which it was collected (Koops, 2021). This use does not always occur explicitly or transparently. Biometric data may be repurposed, for example, to train artificial intelligence systems or agents, without the data subject's knowledge or control. The "interconnection" of RENAED to National Police databases, coupled with the authorization for use for "criminal policy" purposes (Art. 20 of Decree 3337/2025), creates conditions conducive to biometric data collected nominally for sports security being used for purposes other than those declared.

The lack of clear limits regarding who may access this data, for which specific purposes, and under what prior judicial oversight also creates the possibility of uses incompatible with the stated purpose. This concern is heightened in the context of mass biometric registration systems without prior impact assessments, at least none that are publicly accessible, and lacking a fully operational independent oversight authority[18] and effective accountability mechanisms.

18 Under the current legal regime in Paraguay, oversight of personal data protection has historically been fragmented and sector-specific. Although Law No. 7593/2025 provides for the creation of a supervisory authority, it is not yet fully operational. This limits the existence of an independent, specialized and cross-cutting mechanism for the oversight and enforcement of biometric data processing.

Far from remaining at the level of policy or rhetoric, the incidents that took place during the superclásico between Club Olimpia and Cerro Porteño on April 19, 2026 — which led to the suspension of the match and violent clashes inside and outside Estadio Defensores del Chaco — accelerated the State's move toward implementation. That same Monday, the Ministry of the Interior announced a package of five measures for "immediate application," backed by the Office of the Attorney General. These included individual ticket validation through the Identification Department of the National Police, the gradual introduction of facial recognition and the AFIS system as biometric controls at high-risk matches, and the completion of the National Registry of Sporting Events (RENAED). This shift confirms that the risks examined in this study are no longer merely hypothetical or prospective. Instead, they are now part of a concrete process of administrative implementation, reinforcing the need to assess these measures in light of the principles of legality, necessity, and proportionality discussed in the following sections (ABC Color, 2026; Infobae, 2026; OneFootball, 2026). Importantly, as this exploratory study discusses, these measures had already been proposed in the past without ever being fully implemented. This raises further questions about the institutional capacity to ensure effective safeguards in a context of reactive policymaking, driven more by the urgency of the incident than by prior technical and legal planning.

ASSESSMENT: A SURVEILLANCE AND PREVENTION MODEL WITH MORE QUESTIONS THAN GUARANTEES

The preceding analysis shows that Paraguay's regulatory framework presents features that diverge from regional and international standards governing biometric surveillance in public spaces. A literal interpretation of the law, alongside the current national context, raises more questions than guarantees regarding the effective protection of the fundamental rights of individuals wishing to attend sporting events. This gap between the stated regulatory protection and the safeguards actually implemented calls for a critical analysis from the perspective of the principles of necessity and proportionality, which will be addressed in the following sections.

APPLICABLE LEGAL FRAMEWORK AND INTERNATIONAL CRIMINAL LAW

INTERNATIONAL PROTECTION OF PRIVACY AND REGULATION OF BIOMETRIC SURVEILLANCE

The right to privacy constitutes a fundamental human right recognized in numerous international and regional instruments. Article 12 of the Universal Declaration of Human Rights (UN, 1948) establishes that "no one shall be subjected to arbitrary interference with his privacy," which is complemented by Article 17 of the International Covenant on Civil and Political Rights (UN, 1966), which prohibits arbitrary or unlawful interference with privacy and guarantees legal protection against such interference. These instruments, ratified by Paraguay and having a higher legal status than national laws under Article 137 of the Constitution, establish clear limits on the state's powers of surveillance and collection of personal data.

In fact, the Universal Declaration of Human Rights (UN, 1948) constitutes the cornerstone of the international protection of fundamental rights, enshrining principles directly applicable to the analysis of biometric surveillance technologies: the principle of equality before the law (Art. 7), the presumption of innocence (Art. 11), the protection of honour and reputation (Art. 12), the freedom of peaceful assembly and association (Art. 20) and the indivisibility of human rights (Art. 30). The principle of indivisibility requires States to take a comprehensive approach to the individual and the protection of their rights, recognizing that interference with privacy through mass surveillance necessarily impacts the exercise of other rights such as freedom of expression, association and participation in cultural life.

Furthermore, the International Covenant on Civil and Political Rights (UN, 1966) complements this framework by expressly prohibiting arbitrary interference with privacy (Art. 17) and protecting freedom of expression (Art. 19) and the right to peaceful assembly (Art. 21). These rights are particularly relevant in the context of sporting events, spaces of cultural expression and assembly, where biometric surveillance can have a chilling effect on public participation.

Other international instruments ratified by Paraguay reinforce these protections in specific contexts such as the present case. The Convention on the Rights of the Child (United Nations, 1989) establishes the duty to preserve the identity of children and adolescents (Art. 8), protect their freedom of expression (Art. 13) and freedom of assembly (Art. 15), and guarantee protection against abusive interference with their privacy (Art. 16). Given that sporting events are often attended by minors, the implementation of facial recognition systems requiring mandatory biometric registration challenges these provisions, particularly given that children lack full legal capacity to provide informed consent.

The International Convention on the Elimination of All Forms of Racial Discrimination (United Nations, 1979a) obliges States to adopt measures to prevent and mitigate discrimination in all its forms, guaranteeing the exercise of the rights to freedom of opinion, expression, peaceful assembly and movement. This instrument is particularly relevant in light of documented evidence that facial recognition systems exhibit differential error rates across gender, racial and ethnic groups, resulting in a higher number of false positives in these groups (Buolamwini & Gebru, 2018). The Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) (United Nations, 1979b) is also relevant, as it prohibits any form of gender-based discrimination (arts. 1, 2, 3, 15), including the misuse of technologies that may disproportionately affect women.

Within the Inter-American system, the American Convention on Human Rights (Pact of San José, Costa Rica) (OAS, 1978) constitutes an indispensable legal framework for the protection of rights in the region. This instrument expressly protects the right to privacy (Art. 11), the freedom of thought and expression (Art. 13), and guarantees effective judicial protection (Art. 25). The Inter-American Court of Human Rights, in key rulings, has interpreted Article 11 to mean that state interference with privacy must be provided for by law, pursue a legitimate aim, and be necessary and proportionate in a democratic society (Case of Escher et al. v. Brazil, 2009; Case of Tristán Donoso v. Panama, 2009), a standard directly applicable to the evaluation of mass biometric surveillance systems.

The Organization of American States also establishes specific standards directly applicable to the processing of biometric data (OAS, 2021). Among the most relevant principles are "lawful purposes and loyalty", which requires that data processing pursue specific, explicit and lawful purposes; "transparency and consent", which calls for clear information and the data subject's free and informed consent; "relevance and necessity", which requires limiting data collection to what is adequate, relevant and strictly necessary; and "sensitive personal data", which establishes a reinforced protection regime for biometric data, requiring additional safeguards for their processing.

In comparative terms, the AI Act (Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Regulation), 2024) represents the most advanced regulatory standard for biometric identification systems. This instrument classifies remote biometric identification systems in public spaces as "high-risk" and prohibits their use except in strictly defined circumstances subject to prior judicial authorization.

Additionally, it imposes obligations related to rights impact assessments, effective human oversight, comprehensive technical documentation, operational traceability and independent audit mechanisms. The gap between this standard and the Paraguayan framework is significant, highlighting the inadequacy of the safeguards currently provided for in Law No. 7269/2024 and its implementing decree.

PRINCIPLES OF CRIMINAL LAW VS. INDISCRIMINATE MASS SURVEILLANCE

The implementation of facial recognition systems linked to police databases raises additional questions from the perspective of criminal law and due process guarantees. Article 17 of the Constitution enshrines the principle of presumption of innocence, establishing that "in criminal proceedings, or in any other proceedings from which a penalty or sanction may result, every person has the right to […] be presumed innocent". This fundamental principle implies that no person may be treated as a suspect without objective and individualized grounds to justify such treatment (Fernández Prieto and Tumbeiro v. Argentina, 2020; Inter-American Court of Human Rights, 2009).

Mass biometric surveillance effectively reverses this presumption by subjecting all individuals attending a sporting event to the automated capture, processing and comparison of their facial data against police databases; that is, it treats everyone as potential suspects without individualized grounds. The requirement of individualized suspicion constitutes an essential limit on law enforcement action and a fundamental pillar of the criminal justice system. The possibility that any person may be considered a suspect without specific grounds opens the door to practices incompatible with the rule of law in a democratic society (Rolón Luna & Sequera, 2016).

The principle of minimal criminal intervention or ultima ratio (Ferrajoli, 2009), recognized in constitutional doctrine and jurisprudence, establishes that the State's punitive power must be reserved for the most serious offenses and only when other means of social control prove insufficient. This principle also applies to investigative and preventive surveillance powers. Highly intrusive measures, such as mass biometric surveillance, are justified only under an exceptional standard that requires their strict necessity to prevent serious crimes, the absence of less intrusive alternatives and that they be applied exclusively to individuals for whom there are well-founded and individualized suspicions. (United Nations High Commissioner for Human Rights, 2021). Under this premise, the United Nations Special Rapporteur on the right to privacy maintains that mass and indiscriminate surveillance is per se incompatible with international human rights law. This incompatibility lies in the fact that, even when the State pursues legitimate security objectives, the deployment of such technologies across the population inherently violates the principles of necessity and proportionality by nullifying the presumption of innocence and due process through automated and widespread monitoring.

Article 200 of the Paraguayan Code of Criminal Procedure establishes that the interception of communications must be judicially authorized and based on a specific and justified need. Although this provision refers specifically to the interception of communications, the standard it sets could be considered to understand the level of safeguards required for other highly intrusive surveillance measures, such as mass facial recognition. As Rolón Luna and Sequera (2016, p. 17) note, "all mass surveillance is unnecessary and clearly violates the fundamental guarantees of criminal law when there is no genuine informed consent or judicial authorization based on individualized suspicion".

In summary, the applicable international and constitutional legal framework establishes clear limits on state surveillance powers. Interference with privacy must be provided for by clear and precise law; pursue lawful purposes in a democratic society; be strictly necessary to achieve those purposes; be proportionate to the objective pursued; be based on individualized suspicion when involving data processing for the purposes of crime prevention or investigation; have prior judicial authorization in cases of highly intrusive measures; and guarantee effective mechanisms for oversight, accountability and redress. The evaluation of the facial recognition system provided for in Law No. 7269/2024 must be conducted in light of these standards, an analysis that will be developed in the following section through the application of the proportionality test.

FACIAL RECOGNITION IN STADIUMS AND HUMAN RIGHTS: KEY CHALLENGES

The deployment of facial recognition technologies in mass gathering spaces such as sports stadiums poses significant challenges to the protection of fundamental rights recognized in both international instruments and national constitutional frameworks. As the Office of the United Nations High Commissioner for Human Rights has warned, remote biometric recognition "dramatically increases the ability of State authorities to systematically identify and track individuals in public spaces, undermining the ability of people to go about their lives unobserved and resulting in a direct negative effect on the exercise of the rights to freedom of expression, of peaceful assembly and of association, as well as freedom of movement" (United Nations High Commissioner for Human Rights, 2021, p. 8).

The intrusive nature of these technologies is not limited to the mere capture of images, but involves the automated processing of unique human characteristics, systematic comparison with pre-existing databases, and the potential generation of behavioral and movement profiles of attendees (Pietrasanta et al., 2025). This capacity for identification, tracking and predictive analysis qualitatively transforms the relationship between the State, the private actors operating these systems and the citizens participating in sporting events, generating specific risks to certain rights simultaneously and in an interrelated manner.

Additionally, the documented technical limitations of these systems exacerbate human rights risks. As Feldstein notes (Feldstein, 2019, p. 19), facial recognition systems may perform well under ideal, controlled conditions, but their performance suffers significantly when unexpected variables are introduced, such as those characteristic of dynamic environments like stadiums. This may generate high rates of false positives that can lead to misidentifications, unjustified access restrictions and the stigmatisation of innocent people.

The following subsections will examine the key fundamental rights affected by the implementation of facial recognition in Paraguayan stadiums, in light of both national constitutional protections and international human rights law standards.

PRIVACY AND PERSONAL DATA PROTECTION

In the context of deploying FRT, the issue of privacy goes beyond the mere processing of personal data to encompass more complex dimensions: What data underpins the purported accuracy of these systems? On what legal basis is biometric data, originally obtained for other purposes, collected and repurposed? What standards of security, data minimization and purpose limitation govern their processing? What safeguards exist to prevent secondary uses or unauthorized access? These questions are critical from a human rights perspective.

In practice, there is insufficient public information in Paraguay to ascertain whether these systems are trained using official databases, including those held by the Identification Department—which is responsible for issuing national identity documents—criminal record databases, or other state or private sources.. It is precisely this lack of transparency that prevents an assessment of whether the processing of biometric data associated with facial recognition complies with data protection principles, and undermines any claim regarding its legitimacy from a human rights perspective.

Furthermore, the right to privacy and the protection of personal data[19] do not operate in isolation. Violations of these rights also have ripple effects on other fundamental rights, giving rise to what could be described as a "chain of violations". The Paraguayan constitutional framework, for example, recognizes this interdependence in several articles, such as Article 33—cited above—and Article 38, which recognizes the right to the defense of common interests:

> "Any person has the right, individually or collectively, to demand from public authorities measures to defend the environment, the integrity of the habitat, the public health, the national cultural heritage, the interests of the consumers and others that, because of their legal nature, pertain to the community and are related to the quality of life and to the collective patrimony" (National Constituent Convention, 1992).

This formulation is particularly relevant for challenging the implementation of facial recognition technologies that do not merely affect individual rights in isolation, but also impact collective legal interests. In particular, these systems alter the social fabric and erode the collective expectation of privacy in public spaces. As the Human Rights Committee has emphasized, "The right to privacy applies to everyone. Differences in its protection on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status are inconsistent with the principle of non-discrimination laid down in articles 2 (1) and 3 of the International Covenant on Civil and Political Rights. Discrimination on these grounds also violates the right to equality before the law contained in article 26 of the Covenant" (Human Rights Committee (HRC), 1988, para. 2).

Therefore, from a human rights perspective, it is imperative to identify and challenge technologies, such as facial recognition in its most intrusive form, that jeopardize hard-won rights. Fundamental rights cannot be traded off for supposed greater security, particularly when the State or the entities responsible for their deployment cannot guarantee transparency, accuracy or infallibility.

19 While in some legal systems the right to personal data protection has been recognized as an autonomous fundamental right, most notably in Europe following its enshrinement in Article 8 of the Charter of Fundamental Rights, this work adopts an integrative approach that conceives them as closely intertwined rights. As Purtova (2018) argues, data protection constitutes a specific manifestation or dimension of the broader right to privacy, aimed at ensuring individual control over personal information in the context of automated processing. This perspective is consistent with the Latin American jurisprudential tradition, where data protection has largely developed as derived from the right to privacy and habeas data. In Paraguay, for example, the Constitution does not expressly establish an autonomous right to data protection; however, it does recognize the right to privacy (Art. 33) and the constitutional guarantee of habeas data (Art. 135), articulating both instruments to protect the informational dimension of privacy. Therefore, in this context, it is appropriate to refer to both rights jointly, acknowledging their functional interdependence without prejudice to the technical and regulatory specificities each may present in specific regulatory frameworks.

REASONABLE EXPECTATION OF PRIVACY: IS VOLUNTARY PRESENCE IN PUBLIC SPACE A JUSTIFICATION FOR MASS SURVEILLANCE?

The notion of "reasonable expectation of privacy" is a key element in defining the scope of the right to privacy in the context of facial recognition technologies. This concept, developed primarily in common law jurisprudence but also incorporated into continental legal systems[20], helps assess whether a person can reasonably expect certain aspects of their life to remain protected from observation or intrusion by third parties, even when they are in publicly accessible spaces.

As Vaninetti (2021a, pp. 89–92) notes, the reasonable expectation of privacy is not limited to physically private or enclosed spaces, but extends to settings where, depending on the circumstances and the social context, a person can legitimately expect not to be subject to systematic or continuous surveillance. This expectation is based on objective elements such as prevailing social norms, the design of the space and signage, as well as subjective elements such as the individual's perception of whether they are exposed to constant observation.

In the context of FRT deployed in public spaces, this expectation is radically altered. Traditionally, being in a public space implied a certain degree of visibility but also anonymity. In other words, a person could be seen but not necessarily identified, tracked or profiled in a systematic and continuous manner. There is a substantial difference between mere passive observation, which is inherent to social life, and automated technological surveillance that enables identification, recording, storage and predictive analysis (Vaninetti, 2021a, pp. 156–159).

A frequently cited argument to justify the use of surveillance technologies in public spaces is that voluntary presence in these spaces entails tacit acceptance of the conditions of surveillance. However, this logic has serious flaws from a fundamental rights perspective.

It is worth asking to what extent one can speak of "voluntariness" when access to certain essential spaces or services is made conditional on being subjected to facial recognition systems. As Bohigues Esparza (2021, pp. 8–10) warns, consent must be free, informed and specific to be considered valid; conditions that are difficult to meet where there is a power imbalance, a lack of real alternatives and insufficient clear information about the scope of data processing.

The issue becomes even more questionable when policies explaining the purpose of data processing, data retention periods, who accesses the data or where it is stored are not even easily accessible. This opacity not only violates the principle of transparency, enshrined in virtually all data protection frameworks, but also strips any notion of informed consent of its actual substance.

The Spanish Supreme Court has established key criteria for assessing when technological surveillance exceeds the limits of reasonable expectations of privacy. In its judgment STS 489, the Criminal Chamber noted that, although individuals do not have an absolute expectation of privacy in public spaces, this does not justify any form of technological surveillance, especially when it allows "the exhaustive reconstruction of a person's movements, relationships and habits" (STS 489/2018, 2018).

20 In common law systems, a landmark case is Katz v. United States, 389 U.S. 347 (1967), in which the U.S. Supreme Court established that constitutional protection extends to situations where a "reasonable expectation of privacy" exists, shifting the focus from physical property to the protection of the person. Meanwhile, in civil law systems and under the GDPR framework, the Court of Justice of the European Union has further reinforced this protection in public spaces. For instance, in the Buivids case (C-345/17), the Court determined that video recording, even of public officials performing their duties, constitutes the processing of personal data, which must be subject to strict criteria of proportionality and purpose limitation.

This line of case law may be applicable to the use of FRT in public spaces such as football stadiums and large-scale sporting events. As the UN High Commissioner for Human Rights warns, "remote biometric recognition is linked to deep interference with the right to privacy. A person's biometric information constitutes one of the key attributes of her or his personality as it reveals unique characteristics distinguishing her or him from other persons". (2021, p. 8).

The ability of these systems to operate continuously, imperceptibly and on a large scale radically transforms the nature of surveillance. It is no longer a matter of occasional or one-off observation, but rather systematic tracking capable of generating detailed profiles of behavior, movement and association. This technological persistence challenges the expectation of anonymity that has historically characterized life in public spaces.

However, the Paraguayan Constitution (Art. 33) does not draw a strict distinction between public and private spaces, but rather provides comprehensive protection for privacy, private life and personal image. Given this, constitutional protection of privacy cannot be interpreted restrictively or limited solely to the domestic sphere. It must extend to all situations where there is a legitimate expectation of not being subjected to systematic surveillance (Vaninetti, 2021b, pp. 201–204). In this case, its scope of protection should extend to scenarios such as the one examined here.

As Bohigues Esparza (2021, pp. 15–17) notes, the proliferation of surveillance technologies requires rethinking traditional criteria for assessing the reasonable expectation of privacy. It is not enough to determine whether a space is formally public or private; rather, attention must be paid to the type of activity being carried out, the nature of the data collected, the intensity and persistence of the surveillance and whether viable alternatives exist. Furthermore, from a human rights perspective, the burden of proof must fall on those who promote these technologies. It is up to them to demonstrate that their implementation respects the principles of legality, necessity, proportionality and transparency, and that effective safeguards exist to protect the reasonable expectation of privacy that every person retains, even when moving through public spaces.

FREEDOM OF EXPRESSION, PEACEFUL ASSEMBLY AND THE RIGHT TO PROTEST

The implementation of facial recognition technologies in public spaces also poses significant challenges to fundamental rights such as freedom of expression, the right to peaceful assembly and freedom of association (United Nations High Commissioner for Human Rights, 2021, p. 6).

In Paraguay, the Constitution establishes a framework for protecting freedom of expression. Article 25 recognizes that "All persons have the right to freely express their personality, to creativity, and to forge their own identity", expressly guaranteeing "ideological pluralism". Article 26 further provides that "freedom of expression and freedom of the press, as well as the dissemination of thought and opinion, are guaranteed without any censorship," adding that "every person has the right to generate, process or disseminate information, as well as to use any lawful and appropriate means for such purposes" (National Constituent Convention, 1992).

This constitutional protection is reinforced at the international level, particularly within the inter-American human rights system. The Inter-American Court has emphatically stated that freedom of expression is a cornerstone of the very existence of a democratic society. It is indispensable for the formation of public opinion. It is also an indispensable prerequisite for the full development of political parties, trade unions, scientific and cultural societies and, in general, those who seek to influence society. In short, it is a condition for society to be sufficiently informed when exercising its choices. Consequently, a society that is not well informed is not fully free (Inter-American Court of Human Rights (IACHR), 1985, para. 70).

Along these lines, the Special Rapporteur on Freedom of Expression (2010, p. 5) has stated that freedom of expression also has a dual dimension. In other words, it protects both the individual right to express ideas and the collective right to access a diversity of information and opinions. This dual dimension highlights its relevance not only to individual autonomy but also to the proper functioning of deliberative democracy. In this regard, and in light of these considerations, one of the most serious risks associated with facial recognition systems in public spaces is their capacity to generate a chilling effect on the exercise of fundamental rights.

For organizations such as Privacy International (2024), the knowledge or reasonable suspicion of being subjected to automated facial surveillance can lead individuals to self-censor their participation in demonstrations, protests or public gatherings, for fear of being identified, tracked and subject to subsequent reprisals. This phenomenon, known as the "chilling effect," has been extensively documented in studies on surveillance and democracy. Penney (2016a) empirically demonstrated that, following Edward Snowden's revelations about mass surveillance programs, there was a statistically significant decline in searches for sensitive terms on Wikipedia, demonstrating how the mere perception of surveillance alters people's behavior, even in perfectly legitimate activities. In the context of FRT, this effect is amplified due to their capacity to operate imperceptibly, persistently and retrospectively.

As warned by the United Nations Special Rapporteur on the rights to freedom of peaceful assembly and association, the use of surveillance technologies, including facial recognition, for monitoring protests can have a serious chilling effect, violate the principle of proportionality and undermine the legitimate exercise of fundamental rights (2019, para. 26). Moreover, this chilling effect is particularly concerning in contexts where there is already a history of repressive use of technology.

Furthermore, it is important to note that technology is not neutral and surveillance deployed in contexts of protest or social mobilization does not always operate objectively or uniformly. As noted by Simone Browne (2004; 2015), cited in Araceli Ramírez (2025), surveillance technologies are historically embedded in logics of racialized, class-based and colonial control, reproducing preexisting social hierarchies and deepening structural inequalities. Rather than affecting the entire population equally, these systems tend to have a disproportionate impact on individuals and groups already in vulnerable positions. In the Paraguayan context, this may translate into heightened surveillance practices targeting young people, racialized individuals, people from working-class backgrounds or members of LGBTIQ+ communities, thereby increasing the risks of stigmatization, profiling and exclusion under the pretext of public safety.

Cases documented in the region show that FRT are not implemented neutrally, but rather tend to be deployed in contexts of social protest and political mobilization. During the 2021 National Strike in Colombia, human rights organizations denounced the use of facial recognition to identify protesters, constituting a form of intimidating surveillance incompatible with international standards (Fundación Karisma, 2021). In Argentina, for example, statements by authorities about the use of facial recognition to identify protesters and link their participation to the possible loss of social benefits (Red en Defensa de los Derechos Digitales, 2023a) illustrate how these technologies can become tools of political control that erode democratic space.

This practice creates a significant asymmetry. While the state and corporate actors deploy sophisticated technological capabilities to identify, track and profile citizens legitimately exercising their political rights, those citizens lack equivalent means to oversee and hold them accountable. As Privacy International (2024) argues, this informational power asymmetry threatens the political equality that should characterize any genuine democracy.

The situation is exacerbated when biometric identification operates under ambiguous legal frameworks that enable discretionary interpretations. In Paraguay, Law No. 7269/2024 classifies excessively broad and vague behaviors as infractions, including “offenses against honor and sportsmanship” or “banners with messages inciting violence” (Art. 18, sub-paragraph g), without establishing objective parameters to define these concepts. This regulatory ambiguity, combined with automated identification capabilities, could enable selective surveillance practices where legitimate political demonstrations or critical expressions may be arbitrarily reframed as “violent conduct” and sanctioned with bans of up to 10 years from accessing sporting events (Art. 20).

This risk is not merely hypothetical. Given documented cases of fans protesting government policies in stadiums (ABC Color, 2022), the operational question becomes unavoidable: Who will determine whether these peaceful protests constitute “offenses against sportsmanship”? Under what verifiable criteria? With what procedural safeguards for those affected? The absence of clear regulatory answers transforms facial recognition into a potential tool for the preventive criminalization of dissent, where the mere technical ability to identify protesters could translate into the preemptive inhibition of the legitimate exercise of fundamental freedoms.

In this regard, the IACHR has established that certain types of speech deserve heightened protection, particularly political speech or speech related to matters of public interest, as they are essential for the formation of public opinion and democratic debate (Special Rapporteurship for Freedom of Expression (RELE), 2010, p. 12). This differentiated protection implies that any restriction on such speech must face particularly rigorous scrutiny. The Spanish Supreme Court has also warned that technologies enabling "the exhaustive reconstruction of a person's movements, relationships and habits" disproportionately interfere with the exercise of fundamental rights (STS 489/2018, 2018). However, FRT operates precisely in the opposite manner, as they increase surveillance over spaces where political speech takes place, such as demonstrations, protests and public events, creating conditions for self-censorship and silencing.

It is well established that freedom of expression is not an absolute right. There are legitimate limits, particularly regarding speech that directly incites violence, discrimination or hatred. Inter-American jurisprudence recognizes that States can and must restrict hate speech to protect the dignity and rights of vulnerable individuals and communities (Special Rapporteurship for Freedom of Expression (RELE), 2010, para. 20). However, for such restrictions to be valid, they must meet certain strict standards.

Specifically, the Inter-American human rights system has established that any restriction must: i. be prescribed by law; ii. pursue a legitimate objective; iii. be necessary in a democratic society; and iv. be proportionate to the objective pursued (Inter-American Court of Human Rights (IACHR), 1985, para. 46). This four-part test is particularly relevant when evaluating laws such as Law No. 7269/2024, which prohibits "banners, flags, symbols or other signs bearing messages that incite violence, discrimination or promote offenses against honor and sportsmanship" (Art. 18, Sec. g).The vagueness of these terms creates a risk of arbitrary enforcement, allowing legitimate political criticism to be treated as punishable "offenses".

The concern in the context examined here is that the capacity of advanced facial recognition technologies to automatically identify individuals displaying critical banners, engaging in political chants, or participating in other forms of symbolic protest may become a mechanism for preventive control. In such a scenario, the mere possibility of future identification and sanction may inhibit the exercise of rights in the present. As the Inter-American Court has emphasized, any restriction on freedom of expression must be based on a clearly defined law, pursue a legitimate objective and be strictly necessary and proportionate (Inter-American Court of Human Rights (IACHR), 1985, para. 70).

For this reason, minimum human rights safeguards are required in response to technologies with such significant chilling potential as FRT. This standard must be applied with particular rigor, always favoring the interpretation most conducive to the full exercise of fundamental rights.

RIGHT TO EQUALITY AND NON-DISCRIMINATION

There has been extensive discussion of the impact of new technologies, such as facial recognition with advanced automation techniques, on equality and non-discrimination. The concern centers on the inherent risk that such technologies may perpetuate or even exacerbate discrimination by reflecting historical biases embedded in the datasets used for their training, such as the tendency for the disproportionate application of police measures against certain minorities (Muñoz Gutiérrez, 2021).

In Paraguay, the Constitution establishes an unequivocal mandate for equality. Article 46 provides that "all the inhabitants of the Republic are equal in dignity and rights. No discrimination is admitted. The State will remove the obstacles and prevent the factors that maintain or propitiate them". Article 47 also guarantees equality in access to justice, before the laws, in public access to public functions and in the enjoyment of the benefits of nature, material goods and culture (National Constituent Convention, 1992).

These rights are further protected by the international obligations undertaken by Paraguay through its ratification of international human rights treaties and conventions. In this regard, the American Convention on Human Rights requires States to "undertake to respect the rights and freedoms recognized herein and to ensure to all persons subject to their jurisdiction the free and full exercise of those rights and freedoms, without any discrimination" (Art. 1). The International Covenant on Civil and Political Rights further provides that "all persons are equal before the law and are entitled without any discrimination to the equal protection of the law" (Art. 26).

However, in this specific case, the impact of these technologies on these rights intensifies in proportion to their technical sophistication. The operational effectiveness of facial recognition systems depends on interrelated factors such as the volume and diversity of biometric data used to train algorithmic models, and their ability to classify identities through probabilistic calculations and large-scale facial pattern matching (Gentzel, 2024). It is precisely in this technical architecture, designed to maximize identification rates through statistical processing of large data volumes, that the structural problem of automated discrimination lies.

For example, when datasets representing certain demographic groups are underrepresented in the training data, or when algorithms are optimized using metrics that prioritize aggregate accuracy over distributive fairness, the system could reproduce and amplify preexisting biases in a systematic, opaque and large-scale manner (Barocas & Selbst, 2016). Unlike interpersonal discrimination, algorithmic discrimination[21] operates under the guise of technical objectivity, making it difficult to identify, challenge and correct it through traditional legal mechanisms.

Various studies have documented that facial recognition systems exhibit significantly disproportionate error rates across variables such as gender, skin tone or age. The landmark study by Buolamwini and Gebru (2018) found that these systems show between 12% and 19% higher error rates when identifying darker-skinned faces, and between 8% and 20% higher error rates when identifying women compared to men. This disparity is primarily attributed to the underrepresentation of certain groups in the training data, which tends to overrepresent the faces of white men.

21 The term algorithmic discrimination is used to describe situations in which automated or algorithmic systems produce disadvantageous or unjustified outcomes for specific groups or individuals, as a result of biased data, proxy variables, design choices, or implementation contexts. The concept began to be systematically developed in the law and technology literature following the work of authors such as Barocas and Selbst, who warn that algorithms can replicate and amplify pre-existing structural inequalities, even in the absence of explicit discriminatory intent.

The U.S. National Institute of Standards and Technology (NIST) confirmed these findings and found that algorithms developed in China are particularly inaccurate in identifying non-Asian populations (Grother et al., 2019; Vila Seoane & Álvarez Velasco, 2024). This observation is particularly concerning in Latin America, where Chinese companies such as Dahua and Hikvision supply much of the facial recognition technology deployed, even as these companies have been criticized by human rights organizations for their involvement in discriminatory practices (ADC por los Derechos Civiles, 2019; Pietrasanta et al., 2025; Venturini & Garay, 2021).

Discrimination particularly affects trans and non-binary people. A study by Coding Rights in Brazil found that 90.5% of the trans people surveyed perceived facial recognition technology as transphobic, and 95.2% believed it could expose them to situations of vulnerability and stigma (Silva & Varon, 2021). In fact, Buolamwini and Gebru (2018, p. 3) acknowledge the simplified and binary representation of gender derived from the labels available in benchmark datasets as a methodological limitation. Given this limitation, they advocate moving toward more comprehensive analyses that consider diverse gender identities and allow for the evaluation of accuracy across intersectional subgroups.

Furthermore, it should be noted that many embedded biases are not identified until numerous cases of adverse outcomes have been reported. In the case of facial recognition technology, these biases can lead to profiling based on ethnicity, race, national origin, sex and other protected characteristics, thereby amplifying preexisting dynamics of structural discrimination (United Nations High Commissioner for Human Rights, 2021).

The concept of "bias" in the context of emerging technologies refers to a "systematic error" in the outputs generated by these systems, arising from statistical, social or institutional factors (Bellamy et al., 2019). This phenomenon goes beyond mere "discrimination," understood as an "unfair error," and can arise both consciously and, more often, unintentionally (Barocas & Selbst, 2016).

These biases can infiltrate multiple stages in the development of FRT, beginning with the training data. The use of biased variables, the collection of non-representative data, incorrect labeling and the use of proxies correlated with protected characteristics systematically contribute to reproducing inequalities (Barocas & Selbst, 2016, p. 691). As Criado Pérez (2020) argues, the exclusion of diverse perspectives in data collection not only distorts results but also perpetuates historical inequalities.

Another stage takes place during the labeling process. The "human factor" can introduce additional biases, as those who label the data often unintentionally transfer their own prejudices (Diakopoulos, 2014, p. 401). Algorithmic design is another area where the technical architecture of systems incorporates value-laden decisions that may deliberately or inadvertently encode gender or racial disparities (Bivens, 2017; Lessig, 2006). Finally, another influential factor lies in team composition. The lack of diversity in development teams—composed mostly of young, white men from the Global North, leads these systems to reflect homogeneous values and perspectives that do not represent human diversity (Gorwa, 2019).

In environments such as football stadiums, the limitations of FRT are exacerbated. Constant movement, variable lighting, dynamic expressions and common practices such as painting one's face in team colors significantly increase the risk of misidentification. These adverse technical conditions call into question the reasonableness of their use in high-density and dynamic environments (Access Now, 2021; Belli et al., 2024; Pietrasanta et al., 2025).

While there is a common misconception that removing protected variables from training data eliminates algorithmic bias, the literature has shown that seemingly neutral variables can act as proxies, indirectly perpetuating discrimination (Wachter et al., 2020). Seemingly neutral variables such as financial records or consumption patterns can correlate with gender, race, socioeconomic status or other protected characteristics, thereby indirectly reinforcing discriminatory outcomes (Veale & Binns, 2017).

This highlights the need for rigorous technical scrutiny of the type and quality of the databases that underpin these technologies. In the case of Paraguay, it is essential to know: where the facial recognition systems to be used under Law No. 7269/2024 were developed; who the contracted providers are; what representative data the algorithms were trained on; what their accuracy rate is when disaggregated by demographic group; and whether this accuracy was evaluated under real-world operational conditions, not only in laboratory settings. These questions are not optional technicalities but minimum requirements to assess the direct impact on the right to equality and non-discrimination.

Furthermore, any implementation must be fully transparent. Without this public and verifiable information, it is impossible to determine whether the deployed systems reproduce biases documented in algorithms developed with data that is not representative of the Paraguayan population. As Silva and Varón (2021) argue, technologies based on predictive and automated analysis, developed by humans and trained with real-world data, easily reproduce structural inequalities. Recognizing this should prompt reflection and the establishment of clear limits before their widespread adoption, since without adequate intervention these tools perpetuate dynamics of social exclusion and violence rather than ensuring equitable and respectful access to human rights. In this regard, identity verification through FRT reinforces the need to question their limitations and ensure that their implementation does not perpetuate exclusions or violate the rights of individuals attending sporting events.

RIGHT OF ACCESS TO CULTURE

Another aspect potentially affected—and often overlooked in debates—is the right of access to culture, recreation and participation in sporting activities. The Constitution expressly recognizes that "every person has the right to participate in the cultural life of the community, as well as to access cultural goods and values" (Art. 63), and further establishes that "the State shall promote physical education, sports and recreational activities for all inhabitants" (Art. 84). This protection is reinforced by the International Covenant on Economic, Social and Cultural Rights, which recognizes "the right of everyone to take part in cultural life" (Art. 15.1.a) and obliges States to adopt measures to ensure its full realization.

As Privacy International (Privacy International, 2024) notes in its submission to the UN Special Rapporteur on cultural rights, access to sporting events is not merely optional entertainment but a legitimate form of cultural participation that fosters community bonds, the expression of collective identities and the exercise of citizenship. Making this access conditional on submission to mass biometric surveillance may constitute a barrier that violates both the right to culture and the constitutional right to equal opportunities in the enjoyment of cultural goods (Art. 47).

The implementation of facial recognition systems as a mandatory requirement for accessing sporting events could lead to various forms of exclusion. The first is technical exclusion, which may arise when individuals lack compatible devices, internet access or have limited digital literacy, creating significant barriers to completing prior biometric registration processes (Algorithm Watch, 2024). Second, it leads to exclusion driven by institutional mistrust. Groups historically subjected to excessive surveillance, such as ethnic minorities, migrants and social activists, may choose to self-exclude out of a well-founded fear of being profiled (Privacy International, 2024). Third, it restricts the exercise of conscientious objection. Individuals who, due to ethical or political convictions, refuse to undergo biometric surveillance may find their access to spaces that should be public and inclusive limited. Finally, it generates exclusion due to technical errors. As previously documented, FRT exhibit differential error rates that disproportionately affect dark-skinned women and non-binary individuals, who may face unjustified denial of access or humiliating situations involving manual verification (Buolamwini & Gebru, 2018; Silva & Varon, 2021).

Paraguay's Law No. 7269/2024 could exacerbate this structural tension. Although formally justified as a measure to prevent violence, its implementation radically transforms the nature of stadiums. That is, they shift from being spaces of social gathering and community celebration to zones of intensive surveillance where every attendee is potentially suspect, identifiable and subject to sanction (Galeano et al., 2024). This transformation particularly affects working-class communities for whom football is one of the few accessible forms of recreation and cultural participation. When access to sporting events is conditioned on the provision of biometric data without viable alternatives, it creates a form of "covert privatization" whereby only those who accept surveillance can fully exercise their right to culture, illegitimately reversing the burden of proof. Rather than the State being required to rigorously justify the need for intensive surveillance, it is presumed that everyone must submit to biometric identification, thereby relinquishing reasonable expectations of privacy (Pérez Trench, 2021; Privacy International, 2024, 2025).

The right to participate in cultural life and sporting activities cannot be subordinated to technological imperatives or become a privilege conditional on the acceptance of mass surveillance. In accordance with the national and international legal framework, the State has a positive obligation to ensure that technological advances do not erode the effective exercise of cultural rights, especially when these constitute essential spaces for democratic participation by vulnerable groups.

RIGHT TO THE PRESUMPTION OF INNOCENCE

As noted in a previous section, FRT structurally challenge the principle of presumption of innocence, enshrined both in Article 17 of the Constitution and in international instruments such as the International Covenant on Civil and Political Rights (Art. 14.2) and the American Convention on Human Rights (Art. 8.2). As Pérez Trench (2021, p. 77) warns, facial recognition "carries the risk of violating the presumption of innocence or, even worse, may invert it and transform it into a burden that the accused must prove".

This inversion occurs through a framework of preemptive surveillance that subjects all individuals to constant scrutiny, regardless of the existence of reasonable suspicion or an ongoing judicial process. Such indiscriminate surveillance erodes the fundamental distinction between suspects and innocent individuals, treating anyone in public spaces as a potential offender. Moreover, when these systems generate alerts or positive identifications—even erroneous ones—they shift the burden of proof onto the identified individual, who must demonstrate that the system made a mistake, thereby reversing the procedural logic that should presume their innocence.

As documented by the UN High Commissioner, these systems "can trigger interventions by the State, such as searches, questioning, arrest and prosecution, even though AI assessments by themselves should not be seen as a basis for reasonable suspicion due to the probabilistic nature of the predictions" (United Nations High Commissioner for Human Rights, 2021, p. 7). This warning is particularly critical when surveillance technologies such as FRT are implemented without clear protocols on the evidentiary value of their results, without effective mechanisms for challenge and without independent judicial oversight.

Furthermore, the risk is exacerbated when there are no clear parameters governing the long-term storage of biometric data. Such data may be exposed to future forms of exploitation not foreseen at the time of collection, become inaccurate over time or perpetuate historical identification errors that lead to biased or erroneous outcomes in future processing, as discussed in previous sections. Additionally, documented disparities in error rates—especially for dark-skinned individuals, women and non-binary people (Buolamwini, 2023; Buolamwini & Gebru, 2018; Harwell, 2019; Lohr, 2018)—mean that certain groups face a higher likelihood of being subject to erroneous identifications that trigger unjustified state interventions, constituting a form of structural discrimination in the exercise of the right to the presumption of innocence.

In the context of Law No. 7269/2024, this tension could intensify. By enabling biometric identification systems in stadiums without precisely defining what constitutes "violent behavior" or establishing procedural safeguards to challenge identifications or sanctions, the law creates a regime in which mere presence at a sporting event may lead to serious administrative sanctions or even criminal proceedings, based on automated identifications whose accuracy and legitimacy cannot be effectively challenged by the affected person. As Díaz (2018) warns, regulating biometric data solely through the lens of personal data protection limits our ability to address the predictive and classificatory dimensions of these technologies, which introduce unprecedented forms of selective profiling and algorithmic discrimination.

Addressing these issues could help prevent a utilitarian surveillance regime, in which preemptive control displaces fundamental procedural guarantees such as the presumption of innocence, disproportionately affecting individuals with no connection to acts of violence and eroding fundamental principles of due process.

IMPACT ON THE RIGHTS OF VULNERABLE POPULATIONS: CHILDREN AND PEOPLE WITH DISABILITIES

IMPACT OF FACIAL RECOGNITION TECHNOLOGIES ON CHILDREN

The deployment of FRT affecting children represents one of the most invasive interventions in the development of their personality and autonomy within a democratic society. As established in Recital 38 of the General Data Protection Regulation (GDPR)[22], children require specific protection because they are less aware of the risks and consequences of the processing of their data. However, in the context of Paraguay, the implementation of these systems—particularly in spaces of mass attendance such as stadiums—tends to disregard the rights-protective framework of the Constitution, whose Article 54 enshrines the principle of the best interests of the child, requiring the family, society and the State to guarantee their harmonious development and the full exercise of their rights (National Constituent Convention, 1992).

In this context, a relevant technical-legal issue to consider is the lack of algorithmic precision. As Barrett (2020) warns, facial recognition systems exhibit significantly higher error rates in minors due to the biological immaturity of their facial features, which are in constant transformation. This technical limitation is no minor detail; it translates into a risk of erroneous criminalization. A "false positive" at a stadium could lead to an unjustified police intervention, potentially marking a minor's record and violating their right to the presumption of innocence. In Paraguay, this directly conflicts with Article 29 of Law No. 1689/2001 (Code of Childhood and Adolescence), which strictly prohibits the identification of children in connection with punishable acts. By capturing and processing images of minors at scale without prior individualized suspicion, the State fails to uphold its duty of confidentiality, exposing identities that the law mandates to protect.

Furthermore, the use of children's biometric data erodes "practical obscurity", a concept that allows for anonymous movement in public spaces. If children grow up under a surveillance system that permanently identifies and tracks them, it creates a chilling effect that constrains their freedom of association and expression. Given the sensitivity of the matter, the processing of children's biometric data must be afforded enhanced protection. The basis of "legitimate interest" for the surveillance of stadiums is insufficient, as the risk of a security breach in these databases would create a generational vulnerability. Unlike a password, a child's face is an immutable credential; if compromised, it jeopardizes their cybersecurity and leaves them exposed to risks of fraud and identity theft throughout their adult life.

22 The GDPR is one of the most influential frameworks in personal data protection and has had a significant impact on the development of international standards and comparative legal frameworks.

BIOMETRICS AND PEOPLE WITH DISABILITIES: RISKS OF EXCLUSION

From a disability perspective, the analysis of surveillance technologies such as facial recognition must move away from the traditional medical model and adopt the social model enshrined in the Convention on the Rights of Persons with Disabilities (CRPD), ratified by Paraguay. Under this approach, disability arises when the environment imposes barriers that prevent full participation. Tiffany Lee (2016) argues that biometric systems often fall short of legal compliance because they are designed on the basis of an assumption of anatomical "normality" that excludes functional diversity.

This exclusion is particularly critical for people with certain phenotypic variations, such as midface hypoplasia or the inclination of palpebral fissures[23], because algorithms trained on standard symmetry models often fail to accurately recognize these features or misclassify them. This undoubtedly constitutes a manifestation of algorithmic discrimination. If access to a sporting event or a public service depends on facial scanning, the Paraguayan State would be violating Article 46 of the Constitution (On the Equality of Persons) and Article 58 (On the Rights of Exceptional Persons) by imposing a technological barrier that renders invisible and marginalizes those who do not fit the training parameters of complex automated systems.

The risk of erroneous accusation, as the case documented by Hill (2020), could be heightened for this group. A person with a disability who exhibits tics, involuntary movements or a distinct facial structure may be flagged as "suspicious" by software that confuses difference with behavioral anomaly. Furthermore, the legal bases authorizing the processing of biometric data must be examined with particular caution. In the case of persons with disabilities, it is not legally acceptable to presume the existence of "implied consent," for example derived merely from entering a stadium, in contexts marked by a clear power imbalance, the absence of accessible alternatives and a lack of real options to object to the processing of their personal data.

Likewise, the implementation of facial recognition technologies without prior impact assessments may violate the right to universal accessibility. The State not only has a negative obligation not to discriminate but also a positive duty to adopt "reasonable accommodations" that guarantee equality in access to and exercise of rights. The imposition of surveillance systems that, by their very design, fail to accommodate certain physical, sensory or cognitive disabilities constitutes a regression in human rights, as it prioritizes operational efficiency or control over the dignity, autonomy and inclusion of persons, in violation of Paraguayan law and applicable international standards.[24]

23 Midface hypoplasia refers to underdevelopment of the central part of the face (specifically the cheekbones, upper jaw, and nasal bridge) while the inclination of the palpebral fissures describes the characteristic orientation of the eye openings. These features may be present, among other conditions, in individuals with Down syndrome and in other genetic or developmental variations. Their mention in this work is included solely to illustrate how certain facial recognition systems, trained on limited or standardized datasets, may exhibit higher error rates when processing faces that deviate from the dominant patterns used in algorithmic training.

24 The obligation to ensure universal accessibility and to provide reasonable accommodations is enshrined in the Convention on the Rights of Persons with Disabilities (CRPD), which has been ratified by Paraguay and requires States to adopt appropriate measures to ensure that persons with disabilities can exercise their rights on an equal basis with others. In the context of FRT (Facial Recognition Technology), this obligation entails an ex ante assessment of whether implemented systems exclude, fail to function effectively or impose disproportionate burdens on certain groups, as well as ensuring accessible alternatives that prevent indirect discriminatory effects.

APPLICATION OF THE PROPORTIONALITY TEST: STRUCTURED EVALUATION OF FRT IN PARAGUAY

The application of the proportionality test to FRT deployed in stadiums is not an abstract theoretical exercise but an indispensable operational tool for assessing the legitimacy of measures that interfere with fundamental rights. As established by the American Convention on Human Rights (Art. 11.2) and General Comment No. 34 of the CCPR (Human Rights Committee (CCPR), 2011), any interference with privacy must be provided for by law, pursue a legitimate aim and comply with the requirements of suitability, necessity and proportionality in the strict sense[25].

However, to understand the true scope of this test, one must trace it back to its origins as a limit on the exercise of power. Judith Gardam (2004) emphasizes that proportionality, originally linked to the control of the use of force, is not merely a balancing tool but a guiding principle that prohibits excess in the deployment of such force. This view aligns with that of Sullivan and Frase (2008), who emphasize that proportionality must act as a constraint on abusive government action. Building on these considerations, we assess the implementation of FRT within the framework of Law No. 7269/2024.

The first requirement—legality—requires that the measure be provided for by a clear, precise and accessible law. In Paraguay, although Law No. 7269/2024 formally authorizes "biometric controls", this legal basis falls short of human rights standards. As noted in the Principles on Communications Surveillance (Electronic Frontier Foundation, n.d.), laws must allow individuals to foresee their application.

The aforementioned law, however, delegates critical decisions to the Ministry of the Interior without establishing limits on which databases may be consulted, retention periods or conditions for exceptions to consent. This lack of specificity contradicts the principle of strict legality (IACHR, 2013) and the standard set by the European AI Act, which requires a detailed legal basis to prevent arbitrariness. Here, legal certainty concerns are central, given that the use of biometric technology should not depend on vague administrative delegations but rather on clear and strict rules.

On the other hand, the requirement of necessity requires demonstrating that no less intrusive means with equivalent effectiveness exist. On this point, Gardam (2004) emphasizes that proportionality is meaningless without first assessing necessity: if a less harmful means exists, the use of a more intrusive measure is, by definition, illegitimate.

In this regard, Paraguayan authorities face a burden of justification that they have failed to meet. According to TEDIC (2024), despite the mass installation of cameras, the National Police recorded only five alerts between 2022 and 2023, calling into question their actual effectiveness. In contrast, the FIFPRO report (2024) identifies priority alternatives such as education for fans, the physical separation of supporters and the ban of already identified offenders. These measures comply with the principle of data minimization without requiring mass surveillance, demonstrating that FRT fails the necessity test even before reaching the balancing stage.

25 The proportionality test, as systematically developed in German constitutional doctrine—particularly by Robert Alexy—is an analytical tool used to assess the legitimacy of restrictions on fundamental rights. This test consists of three sub-principles: suitability, which requires that the measure be capable of achieving the intended aim; necessity, which requires that no equally effective, less restrictive alternative exists; and proportionality in the strict sense, which involves weighing whether the benefits of the measure outweigh the harm caused to the rights affected.

So, does the benefit outweigh the harm? This entails assessing whether the intensity of the restriction is justified in relation to the aim pursued. While Robert Alexy's (1993) theory is the dominant standard, critics such as Jürgen Habermas (1999) warn that this method reduces rights to mere compensable "interests," allowing the State to erode them in the face of security narratives.

In the Paraguayan case, the outcome of the balancing is unfavorable. On the one hand, the impact is severe. This involves the mass processing of data on children and adults without individualized suspicion, with a chilling effect on civil liberties and exposure to algorithmic bias. On the other hand, the benefits are minimal, as there is still no relevant statistical data to justify the implementation of this type of technology to pursue the stated goal. Following Gardam (2004), one could argue that there is a structural imbalance, where the magnitude of state force—the monitoring of thousands of faces—bears no relation to the threat. As Sullivan and Frase (2008) suggest, human dignity is immeasurable and cannot be sacrificed in a balancing exercise against unproven police efficiency.

In short, the implementation of facial recognition technologies under Law No. 7269/2024 faces serious difficulties in meeting the proportionality test. The combination of an insufficient legal basis, the absence of a rigorous evaluation of less intrusive alternatives and the severe impact on fundamental rights supports the conclusion that these measures are disproportionate in the strict sense and, therefore, incompatible with applicable constitutional and human rights standards.

CONCLUSIONS

The analysis conducted in this study leads to the conclusion that Paraguay's model of biometric surveillance in stadiums presents structural flaws that could compromise fundamental rights and erode essential principles of the rule of law.

First, Paraguay's regulatory framework presents a critical chronological inversion: the technological infrastructure and contracts with providers preceded the definition of specific legal safeguards. Law No. 7269/2024 formally authorizes biometric control systems without establishing clear limits on what types of identification are permissible, which databases may be consulted, what the maximum retention periods are or under which conditions exceptions to consent apply. Its implementing decree delegates critical decisions on system compliance to the Ministry of the Interior and the National Council for Security at Sporting Events, without establishing verifiable technical criteria or mechanisms for independent oversight. This regulatory vagueness contradicts the principle of strict legality that must govern any interference with human rights.

Second, the absence of an independent authority responsible for data protection oversight at the time of implementation results in a critical institutional vacuum. Although Law No. 7593/2025 was enacted, it still lacks implementing regulations and an operational authority, leaving the processing of sensitive biometric data without effective oversight. This situation is particularly serious given that: (i) biometric data is particularly sensitive personal data and require enhanced protections under international standards; (ii) their automated and mass processing generates specific risks of algorithmic discrimination and systemic errors; (iii) the technical complexity of these systems exceeds the oversight capabilities of traditional authorities.

Third, the human rights impact analysis reveals irreconcilable tensions between the implemented surveillance model and basic constitutional guarantees such as: (i) The mass and indiscriminate processing of biometric data of all attendees—including minors, with no distinction between individuals with a history of violence and the general public—contradicts the principles of data minimization and proportionality. The lack of information regarding the origins of the databases consulted, their updating, security and potential reuse prevents an assessment of the lawfulness of the processing. (ii) Biometric surveillance has a documented chilling effect (Penney, 2016b; Pérez Trench, 2021; Privacy International, 2024) on civic participation. The combination of automated identification with vague provisions regarding "offenses against sportsmanship" or "banners inciting violence" enables the potential criminalization of legitimate political protest in sports venues. (iii) The widely documented algorithmic biases in facial recognition systems—significantly higher error rates for dark-skinned individuals, women, and transgender people (Buolamwini & Gebru, 2018; Lohr, 2018)—create risks of structural discrimination. Without public assessments of accuracy disaggregated by demographic groups or independent audits, these systems reproduce and amplify preexisting inequalities. (iv) Mass surveillance without individualized suspicion reverses the burden of proof, turning every attendee into an object of preventive scrutiny. When erroneous algorithmic identifications trigger severe sanctions—such as bans of up to 10 years—the affected individual must prove the system's error, effectively undermining the presumption of innocence.

Fourth, the application of the proportionality test, commonly used in the context of state surveillance and human rights, demonstrates that the current implementation fails to satisfy any of its three requirements: (i) Legality: Absence of a clear, precise and accessible legal basis defining purposes, operational limits and safeguards for data subjects. (ii) Necessity: Absence of studies demonstrating that FRT is indispensable and that no less intrusive alternatives capable of achieving the intended purpose with equivalent effectiveness exist. The available data—a mere five alerts recorded over two years (TEDIC, 2024)—call seriously into question both its effectiveness and its necessity. (iii) Proportionality in the strict sense: A manifest imbalance between the magnitude of the impact on fundamental rights (mass processing of biometric data of every attendee) and the demonstrated benefits (minimal operational effectiveness, with no evidence of a reduction in violence compared to alternative measures).

Fifth, the current governance model perpetuates structural opacity that hinders democratic oversight. The lack of transparent information regarding the status of the implementation of these technologies, contracted providers, technical specifications of deployed systems, databases consulted and processing protocols creates an information asymmetry incompatible with principles of accountability. As this research documents, basic information on the operation of these systems, costs, error rates and impact assessments remains inaccessible to the public and human rights organizations. The economic implications warrant critical scrutiny.

In light of this diagnosis, it is necessary to question the foundational premise of the current model: the question is not whether the technology is technically effective, but whether the State can legitimately justify its use without eroding the human rights it is constitutionally bound to protect. The available evidence suggests that the answer is no. Facial recognition technologies may be useful for specific and limited purposes, but their large-scale and indiscriminate deployment in spaces of public access, without trained personnel, without the political will to establish effective safeguards and without the enforcement of sanctions for abusive use, transforms security into an arbitrary exercise subject to algorithmic fallibility and opaque discretionary decision-making.

The technological promise of precision in identifying individuals wanted by law enforcement cannot justify the lack of clear information on the origins of the databases used, applicable data protection standards, disaggregated error rates, and independent auditing mechanisms. It is impossible to assess the legality, necessity and proportionality of these technologies. In contexts of high institutional opacity such as Paraguay, this lack of transparency does not constitute a minor technical flaw, but rather a structural risk to the rights to privacy, informational self-determination and equality.

From this situated perspective, it is evident that the large-scale implementation of FRT systems cannot be justified by appealing to the mere "voluntary" nature of attendance at sporting events. When access to spaces essential for cultural participation is conditional on being subjected to biometric surveillance, when there are no clear mechanisms allowing individuals to opt out, and when information on data processing is opaque or inaccessible, there can be no valid consent or legitimate waiver of the right to privacy. The right to recreation and culture cannot be subordinated to the compulsory provision of sensitive biometric data.

Furthermore, the analysis of the Paraguayan case highlights a deeper tension between models of technology adoption. On the one hand, a reactive, utilitarian model centered on private providers, where public policy decisions are subordinated to technological availability without critical scrutiny of relevance, necessity or compatibility with fundamental rights. On the other hand, a deliberative, rights-based model centered on democratic safeguards, where technology adoption is subject to rigorous impact assessments, informed public debate and the prior establishment of limits, safeguards and accountability mechanisms.

Paraguay currently has an enabling legal framework, technological infrastructure already in place and existing contracts with private providers, but lacks public implementation protocols, operational oversight mechanisms and concrete safeguards for affected data subjects. This situation creates legal uncertainty that affects both individuals, who are generally unaware of the extent of the surveillance to which they are subjected, and operators, who lack clear compliance parameters.

Ultimately, it is essential to preserve human rights as a pillar of a democratic state, while recognizing that structural issues related to algorithmic bias, institutional opacity and the lack of critical assessment must be effectively addressed before technologies such as facial recognition are deployed by the State in democratic contexts. The adoption of these tools without first addressing these underlying issues compromises not only the legitimacy of the public policies that incorporate them, but also the substantive protection of fundamental rights.

RECOMMENDATIONS

Considering the empirical findings, the theoretical framework developed, and the applicable national and international human rights standards, the following recommendations are addressed to decision-makers, judicial authorities, law enforcement agencies and sports governing bodies:

1. **Moratorium on the collection of biometric data given the sensitive nature of biometric data:** In the absence of a fully operational independent oversight authority and the absence of prior impact assessments, it is recommended to refrain from proceeding with the mass collection of biometric data in public spaces and at sporting events. The processing of sensitive personal data cannot constitute the general rule, but rather must remain a strictly limited exception subject to enhanced safeguards which, under current conditions, are not guaranteed.

    1.1. **Institutional framework and personal data protection:** It is imperative to adopt implementing regulations and ensure the effective implementation of Law No. 7593/2025 through the establishment of a personal data protection authority with technical, functional and financial autonomy. In contexts such as the one analyzed in this study, this authority plays an essential role as a democratic counterweight, ensuring compliance with the principles of legality, proportionality and accountability in the processing of biometric data.

2. **Assessment of surveillance technologies under human rights standards and international criminal law:** Surveillance technologies, particularly facial recognition, should not be treated as mere administrative tools, but rather as measures that entail a significant interference with fundamental rights. In accordance with the principle of minimum criminal law and the standards established by international human rights law, their use is only legitimate where it can be demonstrated that they constitute the least intrusive means available to achieve the intended purpose. Furthermore, mechanisms must be established to ensure ex post notification—where this does not compromise an investigation—and the effective right of individuals to challenge both the validity of algorithmic identification and the legality of the processing of their data.

3. **Mandatory Human Rights Impact Assessments:** Prior to any deployment of facial recognition technologies, the State must conduct and publish human rights impact assessments that document, at a minimum, the risks to privacy and personal data protection, freedom of expression and assembly, potential biases affecting persons with disabilities and the specific impact on the rights of children and adolescents.

4. **Proactive transparency and accountability:** Entities responsible for the implementation and operation of facial recognition systems must publish periodic reports that include verifiable information on their functioning, error rates, false positives, evaluation criteria and associated costs. Likewise, clear mechanisms for accountability and sanctions must be established to address and sanction discriminatory or abusive uses by public officials or private-sector actors, especially when these technologies are used to restrict rights or stigmatize historically excluded or marginalized groups.

5. **Prioritizing non-invasive alternatives:** Authorities should prioritize less intrusive, prevention-oriented alternatives, such as improvements to stadium infrastructure, non-biometric identification-based entry systems, and public education and culture-of-peace programs aimed at fans and attendees. The security approach should shift from punitive technological control toward community-based prevention strategies and respect for “practical obscurity” in public spaces.

6. **Multi-level governance and dialogue with sports stakeholders:** It is recommended that a permanent platform for dialogue and participatory governance be established, led by the National Sports Secretariat (SND) and the Paraguayan Football Association (APF), and including sports clubs, human rights organizations and fan groups. The objective should be to develop security policies centered on human security and democratic coexistence in stadiums, avoiding the treatment of fans as subjects of mass surveillance and promoting mechanisms of shared responsibility.

7. **Safeguards in the event of implementation (contingency plan):** In the event that, despite the identified risks, the implementation of facial recognition technologies under specific regulatory frameworks is deemed unavoidable, the following safeguards must be guaranteed, at a minimum:

   7.1. **Data transparency and the right to information:** Data subjects must be informed in a clear, accessible and prior manner (through visible signage and information campaigns), about the existence of the technology, the identity of the data controller, the specific purposes, retention periods and the rights available to them.

   7.2. **Alternative access mechanisms (opt-out):** A manual, non-biometric access mechanism must be ensured for all individuals who cannot or do not wish to be subjected to facial recognition systems. Access to sporting events, as an expression of the rights to culture and recreation, cannot be made conditional on the mandatory provision of sensitive biometric data.

   7.3. **Ensuring non-discrimination and accessibility:** The State and sports clubs must establish specific protocols to prevent discriminatory effects, particularly affecting persons with disabilities, racialized individuals and other groups for whom the technology has higher error rates. No person should be delayed, stigmatized or denied access as a result of technical failures, algorithmic biases or a lack of representativeness in the training data.

LIMITATIONS OF THE STUDY

This research is subject to structural limitations that must be considered not as methodological weaknesses, but as findings in their own right regarding the conditions under which knowledge is produced. The following limitations have constrained the analytical scope of the study and at the same time constitute evidence of gaps in transparency and accountability in technological surveillance in Paraguay.

First, it should be noted that there is seemingly contradictory information, along with a lack of transparency regarding the deployment of facial recognition systems. Despite requests for access to public information, the following remain inaccessible: (i) full contracts with technology providers, including clauses on data ownership, reuse, model training and service enhancement; (ii) detailed technical specifications of acquired systems, including accuracy rates disaggregated by demographic group, training conditions of the algorithms and databases used; (iii) operational protocols for implementation, data retention, auditing and deletion; (iv) human rights impact assessments prior to deployment. This opacity hindered direct empirical analysis.

Consequently, it was not possible to identify public data on the number of people identified through FRT, the proportion of true alerts to false positives, average processing time, protocols for responding to positive matches, mechanisms for notifying affected individuals or records of administrative or judicial challenges. The only available data—five alerts between 2022 and 2023 reported by the National Police (TEDIC, 2024)—are insufficient to assess operational effectiveness, proportionality or the differential impact on vulnerable groups.

Additionally, there are limitations in the empirical assessment of algorithmic biases in local systems. While there is abundant international evidence regarding biases in facial recognition systems, it was not possible to conduct empirical testing on specific systems deployed in Paraguay. This limitation is particularly critical given that several commercial providers identified in the region have been questioned internationally for differential accuracy in populations underrepresented in their training data.

It should also be noted that the study was conducted during a critical period of regulatory transition: Law No. 7593/2025 on personal data protection was enacted during the research, but it still lacks implementing regulations and an operational oversight authority. This situation creates legal uncertainty regarding the applicable regulatory regime, thereby hindering a definitive assessment of compliance. Furthermore, the absence of specific domestic case law on FRT limited the analysis to constitutional, international and comparative standards.

With regard to the methodological design, for ethical and safety reasons, no interviews were conducted with individuals affected by erroneous identifications or sanctions arising from the use of facial recognition. This limitation also constrained the documentation of specific impacts on fundamental rights from the perspective of data subjects, restricting the analysis to documentary sources and literature review.

With regard to the geographic and temporal scope, the study focuses on the Paraguayan case, with comparative references at the regional and international levels, without seeking to generalize to other Latin American contexts. The period of analysis spans from case documentation and data collection in 2024 to February 2026, recognizing that subsequent regulatory, jurisprudential or technological developments may significantly alter the landscape under analysis.

Finally, it is important to emphasize that these limitations do not invalidate the research findings, but rather underscore the urgency of establishing effective mechanisms for transparency, independent evaluation and accountability in technological surveillance. The inability to access basic information about systems that process biometric data of thousands of individuals constitutes, in itself, evidence of structural deficits in democratic governance that this research sought to document and critically examine.

DECLARATION ON THE USE OF ARTIFICIAL INTELLIGENCE TOOLS

In compliance with academic transparency standards, we disclose the use of artificial intelligence tools (Claude.AI and Notebook.LM) exclusively for: style review and editing; systematization and organization of bibliographic information; and support in identifying relevant sources during the literature review. All analytical content, normative interpretation and argumentative development remain the product of the authors' direct intellectual work.

BIBLIOGRAPHY

ABC Color. (2022, September 7). Video: Hinchas de Olimpia cantan "¡Para Horacio, la extradición!" https://www.abc.com.py/nacionales/2022/09/07/video-asi-hinchas-de-olimpia-exigen-extradicion-de-horacio-cartes/

Access Now. (2021). Surveillance Tech in Latin America. Access Now. https://www.accessnow.org/wp-content/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf

ADC por los Derechos Civiles. (2019). Your digital self. Discovering narratives on identity and biometrics in Latin America: The case of Argentina, Brazil, Colombia and Mexico. Asociación por los Derechos Civiles. https://adc.org.ar/wp-content/uploads/2021/01/201904-Tu-Yo-Digital-EN.pdf

Agência Câmara de Notícias. (2026). Comissão aprova projeto que obriga câmeras de reconhecimento facial em estádios Fonte: Agência Câmara de Notícias. Câmara Dos Deputados. https://www.camara.leg.br/noticias/1237433-comissao-aprova-projeto-que-obriga-cameras-de-reconhecimento-facial-em-estadios

Agencia Española de Protección de Datos. (2022). Gabinete Jurídico. N/REF: 0098/20222 [Legal Opinion / Report]. AEPD. https://www.aepd.es/documento/2022-0098.pdf

Agencia Española de Protección de Datos. (2023). Expediente No: AI/00394/2023. Asunto: Advertencia (AI/00394/2023) [Administrative decision]. AEPD. https://www.aepd.es/documento/ai-00394-2023-advertencia.pdf

Algorithm Watch. (2024, October 24). Show Your Face and AI Tells Who You Are. Algorithm Watch. https://algorithmwatch.org/en/biometric-surveillance-explained/

Arthur Dela Peña, Mitzi Gutierrez, & Mercy Guinto. (2024). Balancing Security and Privacy: A Study on Biometric Authentication Implementation in Airports and Airlines. International Journal of Advanced Research in Science, Communication and Technology, 410–424. https://doi.org/10.48175/IJARSCT-22659

Barocas, S., & Selbst, A. D. (2016). Big Data's Disparate Impact. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2477899

Barrett, L. (2020). Ban Facial Recognition Technologies for Children–and for everyone else. 26(2). https://www.bu.edu/jostl/files/2020/08/1-Barrett.pdf

Bellamy, R. K. E., Dey, K., Hind, M., Hoffman, S. C., Houde, S., Kannan, K., Lohia, P., Martino, J., Mehta, S., Mojsilović, A., Nagar, S., Ramamurthy, K. N., Richards, J., Saha, D., Sattigeri, P., Singh, M., Varshney, K. R., & Zhang, Y. (2019). AI Fairness 360: An extensible toolkit for detecting and mitigating algorithmic bias. IBM Journal of Research and Development, 63(4/5), 4:1-4:15. https://doi.org/10.1147/JRD.2019.2942287

Belli, L., Britto Gaspar, W., & Zingales, N. (2024). Regulating Facial Recognition in Brazil: Legal and Policy Perspectives. In The Cambridge Handbook of Facial Recognition in the Modern State (pp. 228–240). Cambridge University Press.

Bertolini, P. (2025). Cómo Brasil, Rusia y Qatar redefinieron la transformación digital en cada Mundial de Futbol. https://dplnews.com/como-brasil-rusia-y-qatar-redefinieron-la-transformacion-digital-en-cada-mundial-de-futbol/

Bivens, R. (2017). The gender binary will not be deprogrammed: Ten years of coding gender on Facebook. New Media & Society, 19(6), 880–898. https://doi.org/10.1177/1461444815621527

Bohigues Esparza, M. D. (2021). La ilicitud de la prueba con vulneración de derechos fundamentales. A propósito de la sentencia del Tribunal Constitucional núm. 61/2021 de 15 de marzo. IUSLabor. Revista d'anàlisi de Dret Del Treball, (2), 263–287. https://doi.org/10.31009/IUSLabor.2021.i02.9

Bourcha, C., Louiza Deftou, M., & No, A. (2017). Data mining of biometric data: Revisiting the concept of private life? IUS ET SCIENTIA, 3(2), 37–62. https://doi.org/10.12795/IETSCIENTIA.2017.i02.04

Brey, P. (2004). Ethical aspects of facial recognition systems in public places. Journal of Information, Communication and Ethics in Society, 2(2), 97–109. https://doi.org/10.1108/14779960480000246

Buolamwini, J. (2023). Unmasking AI: My Mission to Protect What Is Human in a World of Machines (1st ed). Random House Publishing Group.

Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research, 81, 1–15. http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

Bygrave, L. A. (2014). Data privacy law: An international perspective. Oxford university press.

Caeiro, C. (2022). Regulating facial recognition in Latin America. Policy lessons from police surveillance in Buenos Aires and São Paulo. US and the Americas Porgramme. https://doi.org/10.55317/9781784135409.

Case of Escher et al. v. Brazil, Series C No. 200 ___ (Inter-American Court of Human Rights (CIDH) 2009). https://www.corteidh.or.cr/docs/casos/articulos/seriec_200_ing.pdf

Case of Fernández Prieto and Tumbeiro v. Argentina (Inter-American Court of Human Rights (CIDH) September 2020). https://www.corteidh.or.cr/docs/casos/articulos/seriec_411_ing.pdf

Case of Tristán Donoso v. Panamá ((Inter-American Court of Human Rights (CIDH) January 2009). https://corteidh.or.cr/docs/casos/articulos/seriec_193_ing.pdf

Club Social y Deportivo Colo-Colo. (2026). Registro facial Colo-Colo 2026: Todo lo que necesitás saber para ingresar al Estadio Monumental. Colo-Colo. https://colocolo.cl/noticia/registro-facial-colo-colo-2026-todo-lo-que-necesitas-saber-para-ingresar-al-estadio-monumental

Cotino Hueso, L. (2022). Sistemas de inteligencia artificial con reconocimiento facial y datos biométricos. Mejor regular bien que prohibir mal. El Cronista Del Estado Social y Democrático de Derecho, (100), 68–79.

Criado-Perez, C. (2020). Invisible women: Exposing data bias in a world designed for men. Vintage.

Dávalos Acuña, J. R. (2025, October 20). Unos seis hinchas detenidos por violentos en operativo seguridad durante el superclásico. https://www.radionacional.gov.py/2025/10/20/unos-seis-hinchas-detenidos-por-violentos-en-operativo-seguridad-durante-el-superclasico/

Diakopoulos, N. (2014). Algorithmic Accountability Reporting: On the Investigation of Black Boxes. https://doi.org/10.7916/D8ZK5TW2

Díaz, M. (2018). El cuerpo como dato. https://www.derechosdigitales.org/wp-content/uploads/cuerpo_DATO.pdf (Original work published Derechos Digitales)

Doneda, D. (2022). Guidelines for judicial actors on privacy and data protection. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000381298

Economic Commission for Latin America and the Caribbean. (2024). Social Panorama of Latin America and the Caribbean 2023: labour inclusion as a key axis of inclusive social development. United Nations.

El Cronista. (2026). Tiembla el crimen en México: Edomex activará reconocimiento facial con IA para identificar y capturar delincuentes. https://www.cronista.com/mexico/actualidad-mx/tiembla-el-crimen-en-mexico-edomex-activara-reconocimiento-facial-con-ia-para-identificar-y-capturar-delincuentes/

El Mundo. (2025). El Palmeiras investiga a un hincha por gestos racistas a los seguidores del Cerro Porteño. https://diario.elmundo.sv/deportes/el-palmeiras-investiga-a-un-hincha-por-gestos-racistas-a-los-seguidores-del-cerro-porteno

Electronic Frontier Foundation. (n.d.). Necessary&Proportionate on the application of Human Rights to communications surveillance.

Electronic Frontier Foundation. (2014). International Principles on the Application of Human Rights to Communications Surveillance [International Human Rights Principles]. Necessary& Proportionate Coalition. https://necessaryandproportionate.org/principles/

European Union Agency for Fundamental Rights. (2015). Surveillance by intelligence services: Fundamental rights safeguards. European Union Agency for Fundamental Rights (FRA). https://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services-summary-0_en.pdf

Feldstein, S. (2019). The Global Expansion of AI Surveillance [Working Paper]. Carnegie Endowment for International Peace. https://assets.production.carnegie.fusionary.io/static/files/files__WP-Feldstein-AISurveillance_final1.pdf

Ferrajoli, L. (2009). Derecho y razon: Teoria del garantismo penal (9. ed). Ed. Trotta.

FIFPRO. (2024). 2023 Men's Football Workplace Safety Report. The Impact of Violence Towards Footballers In Their Workplace. https://media.fifpro.org/media/3hznnaib/fifpro_workplace-safety-report-2023_final_light.pdf

Flóres Ruiz, J. F., & Díaz Benito, C. O. (2021). Videovigilancia con reconocimiento facial, inteligencia artificial y derechos humanos: Ni apocalipsis ni utopía. CETyS & LATAM DIGITAL. https://proyectoguia.lat/wp-content/uploads/2022/08/reconocimiento-facial-V5.pdf

Fundación Karisma. (2021, June 2). Tecnología, manifestación social y control de la protesta en Colombia. Fundación Karisma. https://web.karisma.org.co/tecnologia-manifestacion-social-y-control-de-la-protesta-en-colombia/

Fundación Via Libre. (2024). Reconocimiento facial: Presentamos lineamientos técnicos mínimos para una auditoria [Letter]. https://www.vialibre.org.ar/reconocimiento-facial-presentamos-lineamientos-tecnicos-minimos-para-una-auditoria/

Galeano, G., Paciello, G., & Gómez Berniga, L. (2024). Not with my face: Implementation of facial recognition cameras by the Paraguayan State. TEDIC. https://www.tedic.org/wp-content/uploads/2025/04/Not-with-my-face-web.pdf

Gardam, J. (2004). Necessity, Proportionality and the Use of Force by States (1st edn). Cambridge University Press. https://doi.org/10.1017/CBO9780511494178

General Directorate of Electronic Commerce. (n.d.). Listado de prestadores de servicios de confianza. Ministry of Industry and Commerce. Retrieved from: https://www.acraiz.gov.py/html/Certif_1PrestaServ.html

Gentzel, M. J. (2024). Facial profiling technology and discrimination: A new threat to civil rights in liberal democracies. Philosophical Studies, 181(6–7), 1369–1392. https://doi.org/10.1007/s11098-024-02156-0

Gonçalves Feliz, A. B., & Piza, E. (2024). Dilemas do uso da Tecnologia de Reconhecimento Facial: O caso do Uruguai e o uso do reconhecimento facial na segurança pública desportiva como vitrine tecnológica. 4(2), 181–226.

González, M., Velazco, A., & Zamora, A. (2024). El reconocimiento facial avanza en los estadios de fútbol de América Latina. https://www.lapoliticaonline.com/politica/controlados-y-fuera-de-juego-el-reconocimiento-facial-copa-los-estadios-de-futbol-en-la-region/

Gorwa, R. (2019). What is platform governance? Information, Communication & Society, 22(6), 854–871. https://doi.org/10.1080/1369118X.2019.1573914

Grother, P., Ngan, M., & Hanaoka, K. (2019). Face recognition vendor test part 3: Demographic effects (NIST IR 8280; p. NIST IR 8280). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8280

Habermas, J. (1999). Between facts and norms: Contributions to a discourse theory of law and democracy (1. MIT Press paperback ed., 3. print). MIT Press.

Harwell, D. (2019). Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use. https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/

Hill, K. (2020, June 25). Wrongfully accused by an algorithm. https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

Human Rights Committee. (1988). General Comment No. 16: Article 17 (Right to Privacy) (CCPR/C/GC/16). United Nations. https://www.refworld.org/legal/general/hrc/1988/27539

Human Rights Committee. (2011). General comment No. 34. Article 19: Freedoms of opinion and expression. United Nations. https://www.refworld.org/legal/general/hrc/2011/83764

Hutchins, B., & Andrejevic, M. (2020). Olympian Surveillance: Sports Stadiums and the Normalization of Biometric Monitoring. 15.

Ibarreche, X., Elebi, C. M., & Lorenzo, C. D. (2025). Facial recognition and surveillance technologies in Latin America: cases, providers and commercial dynamics. (p. 68). AlSur. https://www.alsur.lat/sites/default/files/2025-08/Facial%20recognition%20and%20surveillance.pdf

Inter-American Court of Human Rights. (1985). Compulsory Membership in an Association Prescribed by Law for the Practice of Journalism (Arts. 13 and 29 American Convention on Human Rights) (Advisory Opinion OC-5/85; Series A No. 5) https://hrlibrary.umn.edu/iachr/b_11_4e.htm

Inter-American Commission on Human Rights (CIDH). (2009). Report on Citizen Security and Human Rights (No. 57; OEA/Ser.L/V/II.). Organization of American States. https://www.oas.org/en/iachr/docs/pdf/citizensec.pdf

Inter-American Development Bank. (2024, March 6). The Complexities of Inequality in Latin America and the Caribbean. IDB. https://www.iadb.org/en/news/complexities-inequality-latin-america-and-caribbean

International Network of Civil Liberties Organizations. (2016). Surveillance and Democracy: Chilling Tales from 10 Countries. INCLO. https://inclo.net/wp-content/uploads/2024/02/surveillance-and-democracy.pdf

J Zuiderveen Borgesius, F., Kruikemeier, S., C Boerman, S., & Helberger, N. (2017). Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation. European Data Protection Law Review, 3(3), 353–368. https://doi.org/10.21552/edpl/2017/3/9

Jasserand, C. (2024). Processing of special categories of personal data. In E. Kosta & F. Boehm (Eds), The EU Law Enforcement Directive (LED) (pp. 217–230). Oxford University Press. https://doi.org/10.1093/law/9780192855220.003.0010

Koops, B.-J. (2021). The concept of function creep. Law, Innovation and Technology, 13(1), 29–56. https://doi.org/10.1080/17579961.2021.1898299

La Nación. (2025, February 9). Peña reglamentó la ley que castiga la violencia en el deporte. https://www.lanacion.com.py/politica/2025/02/09/pena-reglamento-la-ley-que-castiga-la-violencia-en-el-deporte/

Lee, T. (2016). Biometrics and Disability Rights: Legal Compliance in Biometric Identification Programs.

Legislative Branch of the Republic of Paraguay. (2024). Ley N.o 7269/2024 'De prevención, control y erradicación de la violencia en el deporte' (Law No. 7269). Legislative Branch of the Republic of Paraguay..

Leslie, D. (2020). Understanding bias in facial recognition technologies. Zenodo. https://doi.org/10.5281/ZENODO.4050457

Lessig, L. (2006). Code: Version 2.0 (2nd ed.). Basic books.

Lohr, S. (2018, February 9). Facial Recognition Is Accurate, if You're a White Guy. https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html

Lyon, D. (2018). The culture of surveillance: Watching as a way of life. Polity.

Maisner, S. (2026, January 16). Police officer appears in court over stalking case. https://www.bbc.com/news/articles/c5yxl5zllz0o

Maleson, R. (2025, June 15). Reconhecimento facial passa a ser obrigatório em estádios com mais de 20 mil lugares; entenda. https://ge.globo.com/gato-mestre/noticia/2025/06/15/reconhecimento-facial-passa-a-ser-obrigatorio-em-estadios-com-mais-de-20-mil-lugares-entenda.ghtml

Mello, D. (2023, May 23). Justiça libera edital de câmeras com reconhecimento facial em SP. Agência Brasil. https://agenciabrasil.ebc.com.br/justica/noticia/2023-05/justica-libera-edital-de-cameras-com-reconhecimento-facial-em-sp

Muñoz Gutiérrez, C. (2021). La discriminación en una sociedad automatizada: Contribuciones desde América Latina. Revista Chilena de Derecho y Tecnología, 10(1), 271. https://doi.org/10.5354/0719-2584.2021.58793

National Constituent Convention. (1992). Constitution of the Republic of Paraguay, unofficial English translation [Constitution]. Organization of American States. https://www.oas.org/ext/Portals/33/Files/Member-States/Parag_intro_textfun_eng_1.pdf

OAS. (1978). American Convention on Human Rights "Pact of San jose, Costa Rica. Organization of American States. https://www.oas.org/dil/treaties_b-32_american_convention_on_human_rights.pdf

OAS. (2021). Updated Principles on Privacy and Personal Data Protection. Organization of American States. Department of International Law. Secretariat for Legal Affairs https://www.oas.org/ext/DesktopModules/MVC/OASDnnModules/Views/Item/Download.aspx?type=1&id=1185&lang=1

Office of the Special Rapporteur for Freedom of Expression (RELE). (2010). The Inter-American Legal Framework regarding the Right to Freedom of Expression. Inter-American Commission on Human Rights. https://www.oas.org/en/iachr/expression/docs/publications/INTER-AMERICAN%20LEGAL%20FRAMEWORK%20OF%20THE%20RIGHT%20TO%20FREEDOM%20OF%20EXPRESSION%20FINAL%20PORTADA.pdf

O'Neil, C. (2017). Weapons of math destruction: How big data increases inequality and threatens democracy (First paperback edition). B/D/W/Y Broadway Books.

Penney, J. W. (2016a). Chilling Effects: Online Surveillance and Wikipedia Use. https://doi.org/10.15779/Z38SS13

Penney, J. W. (2016b). Chilling Effects: Online Surveillance and Wikipedia Use. https://doi.org/10.15779/Z38SS13

Pérez Trench, S. N. (2021). Los sistemas de reconocimiento facial: Una mirada a la luz del examen de proporcionalidad. Revista Internacional de Derecho Humanos, 12(01), 55–88. https://doi.org/10.26422/RIDH.2022.1201.per

Pietrasanta, F., Macías, G., & Narvéez, S. (2025). No Nos Vean la Cara: Vigilancia en el espacio público con Tecnologias de Reconocimiento Facial en Mexico.

Presidency of the Republic of Paraguay. (2025). Decreto N.o 3337/2025 (Decreto No. 3337/2025). Executive Branch of the Republic of Paraguay. https://silpy.congreso.gov.py/web/descarga/decreto-100839?preview

Privacy International. (2024, May). Privacy International's response to the call for submissions on the right to participate in sporting life [Response to the call for submissions]. https://privacyinternational.org/sites/default/files/2024-05/PI%20submission%20-%20Special%20rapporteur%20cultural%20rights%20-%20May%202024.pdf

Privacy International. (2025, October 1). Toward Regulation: Addressing the Legal Void in Facial Recognition Technology. https://privacyinternational.org/long-read/5682/toward-regulation-addressing-legal-void-facial-recognition-technology

Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. Law, Innovation and Technology, 10(1), 40–81. https://doi.org/10.1080/17579961.2018.1452176

Ramírez, A. (2025, May 13). IMSI catchers in Paraguay: the invisible surveillance threatening your right to protest. https://www.tedic.org/en/imsi-catchers-in-paraguay-the-invisible-surveillance-threatening-your-right-to-protest/

Red en Defensa de los Derechos Digitales. (2023a). Ministra de Seguridad de Argentina asegura que utilizarán reconocimiento facial para identificar protestantes. R3D. https://r3d.mx/2023/12/23/ministra-de-seguridad-de-argentina-asegura-que-utilizaran-reconocimiento-facial-para-identificar-protestantes/

Red en Defensa de los Derechos Digitales. (2023b, May 2). El FAN ID no es una solución para erradicar la violencia en los estadios. R3D. https://r3d.mx/?s=Fan+ID

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), Pub. L. No. Regulation (EU) 2024/1689 (2024). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32024R1689

Special Rapporteur on the rights to freedom of peaceful assembly and of association. (2019). Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association (A/HRC/41/41). Human Rights Council of the United Nations. https://docs.un.org/en/A/HRC/41/41

Ricanek, K., & Boehnen, C. (2012). Facial Analytics: From Big Data to Law Enforcement. Computer, 45(9), 95–97. https://doi.org/10.1109/MC.2012.308

Richards, N. M. (2013). The Dangers of Surveillance. 126(7). https://harvardlawreview.org/print/vol-126/the-dangers-of-surveillance/

Rodríguez, J. (2026). 'Tu cara será tu entrada': Colo Colo implementa Registro Facial de Hinchas para entrar al Monumental. https://www.meganoticias.cl/deportes/512679-colo-colo-registro-facial-de-hinchas-entradas-estadio-monumental-entrada-sera-la-cara-20-01-2026.html

Rolón Luna, J., & Sequera Buzarquis, M. (2016). State Communications Surveillance and the Protection of Fundamental Rights in Paraguay. TEDIC y EFF. https://www.tedic.org/wp-content/uploads/2016/10/paraguay_en_march2016.pdf

Sceiza, B., Rodríguez, N., Aguilar, L., & López, M. (2022). Vigilados en la cancha. Bootcamp TEDIC. https://bootcamp.tedic.org/vigilados-en-la-cancha/

Silva, M. R., & Varon, J. (2021). Reconhecimento Facial No Setor Público E Identidades Trans. Coding Rights. https://codingrights.org/docs/rec-facial-id-trans.pdf

Smith, M., Mann, M., & Urbas, G. (2018). Biometrics, crime and security. Routledge. https://doi.org/10.4324/9781315182056

Smith, M., & Miller, S. (2021). Facial Recognition and Privacy Rights. In M. Smith & S. Miller, Biometric Identification, Law and Ethics (pp. 21–38). Springer International Publishing. https://doi.org/10.1007/978-3-030-90256-8_2

Smith, M., & Miller, S. (2022). The ethical application of biometric facial recognition technology. AI & SOCIETY, 37(1), 167–175. https://doi.org/10.1007/s00146-021-01199-9

STS 489/2018, No. 489/2018 (Tribunal Supremo. Sala de lo Penal 23 October 2018). https://vlex.es/vid/746243401

Sullivan, E. T., & Frase, R. S. (2008). Proportionality Principles in American Law. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780195324938.001.0001

TEDIC. (2024, September 25). Surveillance, censorship and punishment: warning about a new sports law in Paraguay. Personal Data. https://www.tedic.org/en/notwithmyface-2/

TEDIC. (2025, November 28). The law on the protection of personal data in Paraguay: a collective achievement based on evidence and plural participation. Personal Data. https://www.tedic.org/en/the-law-on-the-protection-of-personal-data-in-paraguay-a-collective-achievement-based-on-evidence-and-plural-participation/

Unified Public Information Portal. (2024). Solicitud #83985. Acuerdo de patrocinio entre la SND y ITTI. (No. 83985). https://informacionpublica.paraguay.gov.py/public/2024/1721253014_1_AcuerdodepatrocinioSNDITTISAECA1.PDF

Unified Public Information Portal. (2026a). Solicitud # 99418. Reconocimiento facial en estadios deportivos en Paraguay (No. 99418). https://informacionpublica.paraguay.gov.py/#!/ciudadano/solicitud/99418

Unified Public Information Portal. (2026b). Solicitud # 99419. Reconocimiento facial en estadios deportivos en Paraguay (No. 99419). https://informacionpublica.paraguay.gov.py/#!/ciudadano/solicitud/99419

United Nations. (1948). Universal Declaration of Human Rights [International Declaration]. United Nations. https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/eng.pdf

United Nations. (1966). International Covenant on Civil and Political Rights [International Treaty]. United Nations. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

United Nations. (1979a). Convention on the Elimination of All Forms of Discrimination against Women. https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-elimination-all-forms-discrimination-against-women

United Nations. (1979b). Convention on the Elimination of All Forms of Discrimination against Women. https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-elimination-all-forms-discrimination-against-women

United Nations. (1989). Convention on the Rights of the Child. UNICEF. https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

The Guardian. (2018, May). Welsh police wrongly identify thousands as potential criminals. https://www.theguardian.com/uk-news/2018/may/05/welsh-police-wrongly-identify-thousands-as-potential-criminals

United Nations High Commissioner for Human Rights. (2021). The right to privacy in the digital age (A/HRC/48/31). United Nations General Assembly / Human Rights Council. https://docs.un.org/en/a/hrc/48/31

Vaninetti, H. A. (2021a). Derecho a la Intimidad en la Era Digital (1a, Vol. 2). Editorial Hammburabi S.R.L.

Vaninetti, H. A. (2021b). Derecho a la Intimidad en la Era Digital (1a, Vol. 3). Editorial Hammurabi S.R.L.

Vázquez, J. (2018). Cámaras de reconocimiento facial erradicaron episodios violentos en el fútbol. Presidencia Uruguay. https://www.gub.uy/presidencia/comunicacion/noticias/camaras-reconocimiento-facial-erradicaron-episodios-violentos-futbol

Veale, M., & Binns, R. (2017). Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data. Big Data & Society, 4(2), 205395171774353. https://doi.org/10.1177/2053951717743530

Venturini, J., & Garay, V. (2021). Facial recognition in Latin America. Trends in the implementation of a perverse technology. AlSur. https://www.alsur.lat/sites/default/files/2021-10/ALSUR_Reconocimiento%20facial%20en%20Latam_EN_Final.pdf

Vila Seoane, M. F., & Álvarez Velasco, C. M. (2024). The Chinese surveillance state in Latin America? Evidence from Argentina and Ecuador. The Information Society, 40(2), 154–167. https://doi.org/10.1080/01972243.2024.2317057

Wachter, S., Mittelstadt, B., & Russell, C. (2020). Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3547922

Wickins, J. (2007). The ethics of biometrics: The risk of social exclusion from the widespread use of electronic identification. Science and Engineering Ethics, 13(1), 45–54. https://doi.org/10.1007/s11948-007-9003-z

Zalnieriute, M. (2021). Burning Bridges: The Automated Facial Recognition Technology and Public Space Surveillance in the Modern State. Science and Technology Law Review, 22(2), 284–307. https://doi.org/10.52214/stlr.v22i2.8666

Zuboff, S. (2020). The age of surveillance capitalism: The fight for a human future at the new frontier of power (First trade paperback edition). PublicAffairs.


Technology
& Human
Rights