



DOSSIER

The State of the Data: From Registry to Surveillance

"The State of the Data: From Registry to Surveillance"

Authored by: Margarita Trovato

Project Direction: Beatriz Busaniche

With the support of the Heinrich Böll Foundation

Buenos Aires, June 2026

This document is distributed under the terms of the Creative Commons Attribution-ShareAlike International License

<https://creativecommons.org/licenses/by-sa/4.0/>

© Fundación Vía Libre (2026)



Index

Index.....	2
1. Introduction.....	4
2. The State as a Data Accumulator: From Civil Registries to Surveillance	
Infrastructure.....	4
The Biometric Expansion.....	5
Data in the Hands of the State Today.....	5
3. Inferred Data, Profiling, and Automated Decisions.....	6
What is Inferred Data?.....	6
How They Are Regulated in Other Jurisdictions.....	7
4. Argentina: The Current Regulatory Framework and Its Limits.....	8
Law 25.326: Insufficient Protection.....	8
Weak Controls.....	9
The Need for Regulatory Reform.....	10
5. Regulations Enabling Surveillance: Reforms to Intelligence System Agencies and Security Forces (2024–2025).....	10
6. The Social Digital Twin: A Hypothetical Case Illustrating Concrete Risks.....	11
What the Program Would Imply.....	11
Core Problems Concentrated in the Program.....	11
7. Conclusion.....	12

1. Introduction

In this report, we analyze what the Argentine State can do today with citizens' personal data and what protections exist against that power, within a context mediated by the use of technologies.

We begin with a description of the data ecosystem that the Argentine State accumulates today, and then address the issue of inferred data. What are they? How are they protected? We walk through the regulatory frameworks for data protection and their weaknesses, followed by a review of some recent reforms that enable increased surveillance. The objective is to characterize and understand the scenario in which data processing technologies are deployed today, alongside the associated risks regarding citizens' human rights.

The document draws on two previous reports by Fundación Vía Libre that form its analytical foundation, to which we refer for a deeper dive into their respective topics: *Legal Protection of Inferred Personal Data*¹, which analyzes the category of inferred data and its implications for current regulatory frameworks; and *Personal Data in the Hands of the State*², which describes the legal regime and practices of the Argentine State in this area. At the same time, for a more detailed read on the reforms to the intelligence system and their impact on rights—which we address in summary form in this document—we recommend reading the report prepared by the Initiative for Citizen Control of the Intelligence System (of which we are a part), *State of the Regulatory Framework for Intelligence in Argentina (2025)*³.

2. The State as a Data Accumulator: From Civil Registries to Surveillance Infrastructure

The Argentine State has been accumulating personal data long before that process had a proper name. Its registry function—understood as the need to know and count the population in order to govern it—lies at the very origin of its constitution as a modern state: first managed by the Catholic Church, then by the provinces, and finally centralized in the National State starting with the Civil Registry laws of the 1880s and, later, with the creation of the National Registry of Persons (RENAPER) in 1948. From its inception, this function involved collecting data on births, deaths, marriages, and progressively also on parentage, identity, fingerprints, and photographs. Within this mandate, over the years it decisively changed its scale, available technology, and consequently, **the potential for intrusion into citizens' private lives and the magnitude of the effects of its decisions on rights.**⁴

¹ Trovato, M., [“Legal Protection of Inferred Personal Data”](#), Vía Libre Foundation, 2023.

² Trovato, M., [“Personal Data Management by the State”](#), Vía Libre Foundation, 2024.

³ Iniciativa para el Control Ciudadano del Sistema de Inteligencia (ICCSI), [“State of the Intelligence Regulatory Framework in Argentina”](#), 2025.

⁴ To explore the evolution of this process in greater depth—which we outline in this section—we recommend reading Chapter 1 of the report “Management of Personal Data by the State.”

The most visible turning point is the National Identity Document (DNI): since its earliest origins in 1968⁵, it created a unique identification number that would become the "primary key" with which the State articulates dozens of databases today: the voter registry, the tax system (CUIT), the social security system (CUIL), the SUBE transport card, the digital medical record, among others. The DNI is, in practice, the gateway to almost any interaction with the State and, increasingly, with the private sector. What began as an identification instrument gradually became the backbone of a data infrastructure that none of the citizens carrying it authorized in those terms.

The Biometric Expansion

The advancement of technology deepened (and continues to deepen) the data structure in the hands of the State. Starting in 2009, the DNI incorporated biometric data through Decree 1766/2011 and its amendatory Decree 243/2017. In 2011, the Federal Biometric Identification System (SIBIOS) was created—a database of this type for all Argentines—with the stated objective of facilitating identification via cameras on public roads, albeit without sufficient controls. As we noted at the time⁶, biometric identification systems increase the State's capacity for intrusive surveillance, partly due to the ease of interoperating with database technologies. The risk was not merely theoretical: RENAPER data began to be transferred to other agencies for purposes that vastly exceeded the original purposes for which they had been collected.

One case illustrates this precisely. The facial recognition system implemented by the Autonomous City of Buenos Aires draws on RENAPER's biometric database through an inter-jurisdictional agreement. In 2022, it came to light that the City had requested nearly 10 million biometric records from RENAPER, while the number of fugitives the system sought to identify was approximately 40,000. The stated purpose of the system and the actual use of the data bore no reasonable proportion. It was the predictable consequence of, among other things, a design lacking controls over the destination of data once transferred⁷.

Data in the Hands of the State Today

Today, with technological advancement and under regulatory frameworks that we will analyze in the following sections, the national State concentrates immense volumes of citizens' personal data. The purposes for which it hoards them are no longer solely related to its original registry function, but rather to the administration of a broad spectrum of public policies.

Through its various agencies, it possesses information regarding the identity and biometrics of every inhabitant (RENAPER), their financial and tax status (ARCA), their

⁵ Decree-Law 17,671 of 1968, on "Identification, Registration, and Classification of the National Human Potential", currently in force.

⁶ [State of Generalized Surveillance in Argentina](#) | Vía Libre Foundation, May 2012.

⁷ See ["Why the City of Buenos Aires Facial Recognition System Was Suspended" - Chequeado](#), April 2022. Cited in the report "Management of Personal Data by the State", p. 11.

employment and pension status (ANSES), their migration movements (DNM), their public transit activity (SUBE), their health data (healthcare providers and public hospitals), their educational background, and their judicial and police records, among others. Added to this, as detailed below, is the ability to access information on social media activity, communication metadata, and, through inferences, construct profiles that extend far beyond what any individual directly provided, with very few limitations. The question is what the State can do with all of this, under what rules, and with what oversight.

Added to this, as we will see below, is the possibility of accessing information on social media activity, communications metadata, and—through inferences—building profiles that go far beyond what each person directly provided, with very few limitations. The question is what the State can do with all of that, under what rules, and with what controls.

3. Inferred Data, Profiling, and Automated Decisions

So far, we have described what the State collects directly: what citizens provide with consent within the framework of their interactions with various agencies. But there is a second layer of information, invisible to data subjects, that radically transforms the landscape. This has to do with the data that can be inferred about all of us without even knowing it, and the decisions made on the basis of them.

What is Inferred Data?

Inferred data is information relating to an identified or identifiable natural person that is not provided directly by the data subject, but rather created through the analysis (generally automated) of existing data. It has also been defined as that generated through "an intellectual operation that includes comparison or deduction" or as "the derivation of information, data, presumptions, or conclusions from facts, evidence, or another source of information or data."⁸

What these definitions share is an emphasis on three characteristics:

1. The data is not provided by the data subject.
2. It is created by whoever processes the original data.
3. It is constructed from the analysis of large volumes of information.

In other words, someone takes data about a person (or many people) and produces new information from it that that person never handed over and generally does not know about. Furthermore, this information has a persistent character: it can be stored

⁸ The definitions correspond, respectively, to: Wachter, S. and Mittelstadt, B., "A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI", *Columbia Business Law Review*, 2019; European Court of Justice, judgment of August 1, 2022, Case C-184/20; California Consumer Privacy Act (CCPA), Sec. 1798.140(r). All addressed in Chapter 1 of the report "[Legal Protection of Inferred Personal Data](#)".

indefinitely and serve as the basis for future analyses, possibly of the same statistical type.

Inferences function primarily as the basis for two types of processes:

- Profiling: The use of personal data to evaluate certain personal aspects of a natural person, in particular to analyze or predict aspects concerning professional performance, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.
- Scoring: The translation of that analysis into a number that summarizes a person for the purposes of whoever constructed it.

Both processes are usually invisible to the person experiencing them.

An example that clearly illustrates the risks in the Argentine context was the 2018 announcement in the province of Salta of the implementation of a system that would allow predicting adolescent pregnancies among individual women.⁹ The Applied Artificial Intelligence Laboratory of UBA-CONICET analyzed the methodology and found serious technical and conceptual errors, biased and inadequate baseline data, and pointed out the risk of incorrect public policy decisions. But beyond the technical errors, the case raised a fundamental question: what impact does it have on a girl's life for the State to categorize her as "predestined" to become pregnant, without her being able to know that categorization and, consequently, discuss or challenge it? Obviously, this implies a direct infringement on privacy, but the impact on rights is broader: from informational self-determination to, eventually, violations of the right to education, equality and non-discrimination, autonomy, and health, among others.

We see that the risk increases in as much as these inferences are currently the foundation of decisions with a direct impact on rights: who accesses a social welfare program, who is identified as a security risk, which electoral candidates are considered "threats." Moreover, decisions are often made within the framework of the very processes that infer this data—that is, in an automated manner. One must question the level of human review over the prescriptions of the software used, which is often insignificant or insufficient.

How They Are Regulated in Other Jurisdictions

Although there is still no model legislation comprehensively regulating inferred data in all its dimensions, several legal systems have taken significant steps in that direction:¹⁰

United States (California): The California Consumer Privacy Act (CCPA, 2018) explicitly incorporated inferred data into its definition of personal information and considers it personal data when it forms a profile about a consumer. In 2022, the Attorney General

⁹ For more information on the case and its implications, see Sternik, I., [“The intelligence that doesn't think”](#), Página/12, April 2018, and the report “Legal Protection of Inferred Personal Data”, p. 25.

¹⁰ For more information on the different jurisdictions and a more in-depth analysis of those mentioned here, see Chapter 4 of the report “Legal Protection of Inferred Personal Data.”

of California specified that inferences generated by a company about a consumer are personal information under the CCPA and must be disclosed upon consumer request.

European Union: The GDPR recognizes inferred data under the umbrella of personal data, albeit with significant gaps. The Court of Justice of the European Union held that inferences based on specially protected categories must receive the same protection as those sensitive data.

United Kingdom: The UK does not restrict its definition of personal information to factual data: it includes opinions and inferences to the extent they relate to an individual and lead to their identification.

Thus, the most advanced international regulations recognize that what must be protected is not only the information a person hands over, but also the information others construct about them. Argentinian Law 25.326 does not explicitly recognize them, which becomes especially problematic when the data controller is the State itself.

4. Argentina: The Current Regulatory Framework and Its Limits

So far, we have described two processes running in parallel: the Argentine State accumulates increasing amounts of personal data, and technology expands the capacity to build inferences on that data and automate decisions based on them. We will now address the regulatory framework—fundamentally Law 25.326 (2000)—in which these activities unfold.

Law 25.326: Insufficient Protection

In the scenario we have been describing, the Personal Data Protection Law 25.326 of the year 2000, created as a mirror of an already repealed European directive, has two main problems:

It does not explicitly contemplate inferred data or automated decisions. As we saw, inferred data exhibits characteristics that distinguish it from "personal data" in the strict sense (understood as primary data actively or passively provided by the data subject) and, therefore, under a restrictive interpretation, it may fall outside the scope of this norm.

It allows data transfers between different State agencies in an almost absolute manner. In the context of the proliferation of AI systems and the mass generation of inferences for profiling and automated decision-making, this authorization is alarming.

The law does establish, following international standards, a set of principles that must govern any data processing: respect for purpose, proportionality and minimization, informed consent, and access rights. It also recognizes sensitive data (racial/ethnic

origin, political opinions, religious convictions, health, and sex life) that merit enhanced protection.¹¹

However, it is extremely broad in its exceptions. Articles 5.2.b, 11.3.b, and 11.3.c of Law 25.326 allow the State to transfer citizens' data between its departments for purposes different from those for which they were collected, without informing or requesting new consent, insofar as it is necessary for "the exercise of inherent functions of the State" or by virtue of a "legal obligation." This exception is a blank check for any state use of personal data.

Regarding these exceptions, the Supreme Court of Justice of the Nation (CSJN) recently ruled in the "Torres Abad"¹² case, declaring them unconstitutional for being contrary to privacy protections under the Constitution and international human rights treaties. The Court emphasized that consent and knowledge are necessary to guarantee informational self-determination, and that exceptions must be reasonable, proportionate, and necessary for a legitimate purpose.

As the Court noted (cons. 14):

(...) due to the breadth with which Law 25.326 designed the exceptions under review, state entities would be exempt, virtually in all cases, from complying with the consent requirement... It is simply impossible to imagine in what cases they would not do so (...). It is not perceived what legitimate interest would justify allowing the State to organize a system of storage and traffic of personal data without the knowledge of its subjects...

Thus, the Court concluded that the problem is not the interpretation of the norm but its formulation: the exceptions are unreasonable and disproportionate, and virtually render privacy ineffective. While this applies to the specific case, it serves as a strong basis to demand state compliance and insist on legal reform.

Weak Controls

The effects of regulatory deficiencies become more concerning insofar as control bodies are not robust.

The enforcement authority is currently the National Directorate for Personal Data Protection, housed within the Public Access to Information Agency (AAIP). This presents two main problems:

¹¹ Law 25,326, Arts. 4, 5, 7, and 11. For more information, see Chapter 2 of the report "Management of Personal Data by the State."

¹² Supreme Court of Argentina (CSJN), "Torres Abad, Carmen v. EN-JGM re: Habeas Data", Case No. 49,482/2016/CA1, judgment of April 30, 2026.

Structural Design: Combining access to information and data protection under one roof places two conflicting logics together. In practice, data protection was subordinated to the access-to-information agenda.

Lack of Independence: The AAIP operates under the Chief of Cabinet of Ministers, and its head is appointed/removed exclusively by the Executive Branch without Senate confirmation or specific expertise requirements.

Added to this are implementation issues. Low political priority has resulted in meager budgets and insufficient technical capabilities. To date, no state database has ever been inspected by the DNPDP, as the State avoids the sanctioning power of a weak control body over hierarchical equals or superiors.¹³

When public data leaks or privacy-infringing corporate practices occurred, the AAIP's response was minimal—limited to expressions of concern or unverified announcements of investigations.¹⁴ This landscape worsened in 2024 when Decree 780/24 restricted the universe of information considered public, weakening citizen oversight.¹⁵¹⁶

The Need for Regulatory Reform

Law 25.326 is old enough, inspired by a 1995 European directive. It ignores AI, inferences, and automated decisions. Past reform proposals even excluded the portability of inferred data while including vague "public security" exceptions.

A proper reform of Law 25.326 should:

- Explicitly recognize inferred data as personal data
- Establish rights and guarantees against automated decisions
- Update state exceptions so they are itemized and precise (in line with *Torres Abad*)
- Grant the enforcement authority independence from the Executive Branch

¹³ Association for Civil Rights (ADC), [“The Collector State: A Study on Argentina and Citizens' Personal Data”](#) (2014), p. 8; cited in Chapter 4 of the report “Management of Personal Data by the State”.

¹⁴ Such cases are frequent. For example, in October 2021, it was revealed that RENAPER's database had suffered a security breach in which information from national identity documents, such as photos and processing numbers, was extracted (see [Renaper Data Leak: Sensitive Data of 60,000 Argentines Released. Nearly \\$17,000 Demanded for All DNIs](#)). For more information, see Chapter 3 of the report “Management of Personal Data by the State.”

¹⁵ We are referring to cases such as Worldcoin, the company that offers iris scans in exchange for financial compensation, or the recent leaks of state databases at the hands of the company SudamericaData. In the former, the AAIP launched an investigation in 2023, and its last public report—noting that the process was still ongoing—was in 2024 (see [AAIP's Investigation into Worldcoin and the Use of Personal Data Advances](#) | [Argentina.gob.ar](#)). Regarding the latter, it reported initiating ex officio investigations in December 2025, with no subsequent updates (see [AAIP Initiates Ex Officio Investigation into Alleged Massive Personal Data Leak](#) | [Argentina.gob.ar](#)).

Regarding this case, from FVL we submitted public information requests regarding the progress of those proceedings, which were answered negatively, citing the confidentiality of the investigations.

¹⁶ For more information, see [“A Decree Cannot Limit Access to Public Information”](#) | Via Libre Foundation, September 2024.

- Align with Convention 108 and Protocol 108+ regarding the right to explanation in data processing

5. Regulations Enabling Surveillance: Reforms to Intelligence System Agencies and Security Forces (2024–2025)

While the protection framework was already insufficient, regulatory reforms in 2024 and 2025 regarding intelligence and surveillance expanded the State's informational power in the opposite direction. Protections are weakened, while surveillance authorizations expand: more data concentrated in fewer hands, fewer judicial controls, more secrecy, and threat categories broad enough to target journalists, activists, social organizations, and political dissent.¹⁷

First, the National Intelligence System was modified by decrees (DNU 614/24, 615/24, and 941/25), introducing structural changes in the SIDE. DNU 941/25 forces public agencies and jurisdictions to share their databases with the SIDE, bypassing consent, purpose limitation, and minimization principles. It centralizes information and authorizes sharing sensitive data with foreign intelligence agencies without judicial control.¹⁸

Furthermore, secrecy is the general rule: DNU 941/25 declares all intelligence activities "covert" by definition, rendering basic rights of access, rectification, and cancellation under Law 25.326 inoperable.

This ties directly into the political orientation of the 2025 National Intelligence Policy, which defines "threats" so broadly that it enables political and social surveillance. RENAPER, ARCA, ANSES, migration, judicial, and police data—plus inferences—serve as raw material for intelligence profiles.

Simultaneously, the surveillance powers of federal security forces were also increasing. Through ministerial resolutions, cyber-patrolling (the surveillance of public digital spaces) was formalized in 2024, and the Unit for AI Applied to Security (UIAAS)¹⁹ was created. This unit grants the security forces a broad set of powers—in many cases of dubious legality—which now includes the possibility of being exercised through AI, without further clarification as to what this entails, what controls or limitations apply, what software is used, etc. Along the same lines, through a series of decrees in 2025, the Executive reformed the organizational structures of the federal forces with the objective of "modernizing" them in the face of technological

¹⁷ To expand on the information in this section, we recommend reading the ICCSI report ["State of the Intelligence Regulatory Framework in Argentina,"](#) from December 2025 (prepared prior to the publication of Emergency Decree [DNU] 941 of 12/31/25).

¹⁸ Arts. 14–17 of Emergency Decree (DNU) 941/25, inserting the new Arts. 10 quater, quinquies, sexies, and septies into Law 25,520.

¹⁹ Resolutions 428 and 710/24 of the Ministry of Security of the Nation, respectively. For more information, see ["Neither Artificial nor Intelligence, Illegal Surveillance"](#) | Vía Libre Foundation, July 2024.

advancement. The result is a broad set of powers to access public databases and request access to private databases for criminal intelligence purposes, as well as to conduct cyber-patrolling without a prior judicial warrant and without further specifics or requirements—leaving tools, search parameters, and retention periods for the collected information undefined.

6. The Social Digital Twin: A Hypothetical Case Illustrating Concrete Risks

In the preceding sections, we described a set of authorizations granted to the Argentine State: from consolidating data from various agencies within the SIDE to drawing inferences from those databases and monitoring citizens' digital activity without a judicial warrant—all under a veil of secrecy.

Within this framework, the National Government announced a program called "Social Digital Twin" (*Gemelo Digital Social*) on the social network "X" in May of this year.²⁰ At the time of writing this report, there is still no public administrative act formally establishing or implementing it; consequently, we do not know its scope, nor do we have any further information about it beyond the public announcement. However, with this caveat in mind, analyzing the program helps illustrate the types of processes that can be carried out under the authorizations we have outlined, whether through this specific program or another down the line.

What the Program Would Imply

According to available information, the program would consist of processing large volumes of data by cross-referencing and integrating various databases: police, biometric, financial, social media, etc. In other words, it involves setting up a decision-making infrastructure through inferences, in the terms we described above. According to the official announcement²¹, the software would allow officials to "sort, describe, predict, and prescribe," thereby facilitating public policy decision-making. Just as questions remain regarding its implementation due to the lack of available information, the announcement also leaves many questions about its concrete operation: Will decision-making be automated? What is the mechanism for human review? Will the decision-maker understand the information production process—that is, the algorithmic logic by which the software reaches its output? What will be the discussion process for those decisions? Where will the generated data be hosted, and who will guarantee its security?

It is important to clarify that, because these are inferences, the information generated by these models will likely not be treated as personal data in the strict sense and, consequently, data subjects will neither be notified nor able to contest it. How can

²⁰ [Tweet dated 05/22/2026 from the official account of the President of the Nation](#), Javier Milei.

²¹ [Tweet dated 05/27/2026 from the official account of the Minister of Human Capital](#), Sandra Pettovello.

someone contest being placed in a category when they are unaware of it? How can "profiling" be corrected without knowing it exists? In fact, it was officially reported that personal data would not be used for the operation of the program. But what if it involves inferences?

In any case, the indiscriminate circulation of data within the State directly violates the principles of consent and purpose specification. RENAPER data was collected to identify individuals for state registry functions; ANSES data, to manage their pension contributions; Migrations data, to record their movements. None was collected to construct a predictive profile for social policy.

Use in the terms proposed collides with the Personal Data Protection Law, privacy, and informational self-determination, while also posing a massive risk to the enjoyment of other rights. We must ask what happens if, furthermore, it were to be used for other purposes: consider, for instance, criminal policy based on profiling built from this vast volume of data. What happens to the right to defense?

This connects directly to another pending concern: how it would be controlled and what the audit mechanisms would be. In turn, this raises questions regarding vendors and reliance on them (known as "vendor lock-in") when the purchaser itself (in this case, the State and its data infrastructure) becomes tied to the proprietary systems of a single private vendor, operating under foreign regulations and covered by commercial secrecy that prevents independent access.

Furthermore, this is occurring in the context of Big Tech expansion and its arrival in our region. Consider, for example, the case of Palantir Technologies—a US company that develops large-scale data analysis platforms for applications in the civil, military, and intelligence sectors—whose founder recently moved to Argentina and met with the President. Its international track record on human rights is the subject of documented criticism²², meaning that its arrival represents, at a minimum, a potential threat to citizens' rights within the framework we have been describing.

Core Problems Concentrated in the Program

As we can see, a program of the "Digital Twin" type illustrates the convergence of problems across multiple dimensions.

In terms of personal data, we observe cross-referencing without consent or compatible purpose, sensitive data processed on a massive scale, and the absence of a prior impact assessment. Regarding automated decisions, inferences serve as the basis for policies that affect rights without human review or mechanisms for appeal. With respect to controls (or the lack thereof), commercial secrecy, algorithmic opacity, and weakened oversight bodies prevail. Finally, and as a corollary, regarding state and private surveillance: the very same infrastructure that processes data for social policy can—if the vendor offers intelligence products and the State holds the described

²² For more information on Palantir, its deployment in other countries, and local risks, we recommend reading the report ["The Palantir Case in Argentina"](#) by Amnesty International Argentina.

authorizations—be directed toward political surveillance. This has a direct impact on freedom of expression and its derivative rights (press, assembly, protest), which can result in self-censorship (the “chilling effect”).

It is important to be clear that technology itself is not the main problem. The cross-referencing of state databases can be a legitimate tool if carried out under a clear legal framework, with a published prior impact assessment, an independent audit of the algorithm, human review of decisions that affect individual rights, guarantees regarding the sovereignty of state data and decision-making, and with a vendor whose track record on human rights is reasonably compatible with those objectives. None of these elements appear to be present in this scenario.

7. Conclusion

The overview presented in this document allows us to map out a state of affairs. The Argentine State consolidates immense volumes of personal data, holds legal authorizations to draw inferences from them and make automated decisions, and relies on a protective regulatory framework that is insufficient, outdated, and further eroded by recent reforms. Oversight mechanisms are weak or weakened—a scenario that becomes even more critical in the face of the secrecy (whether state or commercial) surrounding these activities. The result is a severe power asymmetry between the State and the citizens: the State's informational power over individuals is expanded, while the mechanisms that would allow for its restraint and the challenging of its effects are diminished.

The rights affected are varied and can overlap. Privacy and informational self-determination are compromised when individuals cannot know or challenge the profiles the State constructs about them. Mass surveillance exerts a chilling effect on freedom of expression, of the press, and of association, even before any concrete action is taken against the targeted individual. Profiling systems reverse the presumption of innocence by categorizing individuals based on what they might do. Furthermore, automated decisions concerning fundamental rights—such as access to social benefits, identification as a security risk, or submission to intensified surveillance—remain opaque and lack accessible avenues for challenge.

What safeguards govern the execution of these programs? What oversight mechanisms are in place? How much power and sovereignty does the State retain over its data and decision-making processes? Technology is neither neutral nor an inherent problem in itself. The core issue lies in how it is trained, to what ends it is used, and how it is audited.